Материалы Второй международной научной конференции по проблемам безопасности и противодействия терроризму

Московский государственный университет
им. М. В. Ломоносова
25–26 октября 2006 года

Московский государственный университет
им. М. В. Ломоносова

Институт проблем информационной
безопасности МГУ

Академия криптографии Российской Федерации

Материалы Второй международной научной конференции по проблемам безопасности и противодействия терроризму

Московский государственный университет
им. М. В. Ломоносова, 25–26 октября 2006 г.

ББК 32.81В6
М34

Организация и проведение Пятой Общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-06) *было поддержано грантом РФФИ* № 06-01-10126-*З*.

РФФИ

М34 **Материалы** Второй международной научной конференции по проблемам безопасности и противодействия терроризму. Московский государственный университет им. М. В. Ломоносова. 25—26 октября 2006 г. — М.: МЦНМО, 2006. — 000 с.

В подготовке и проведении конференции участвовали:
Университет штата Нью-Йорк (США);
Университет им. Генриха Гейне (Дюссельдорф, Германия);
Университет Кембриджа (Великобритания);
Аппарат Совета Безопасности Российской Федерации;
Правительство Москвы;
Группа компаний «Метро»;
ОАО «Газпром»;
Академия информационных систем;
Европейский Центр им. Дж. К. Маршалла;
Фонд гражданских инициатив в политике Интернет;
Программа НАТО «Безопасность через науку».

ISBN 978-5-94057-316-6
9 785940 573166 >

© Коллектив авторов, 2007
© МЦНМО, 2007

Я рад приветствовать участников Второй международной научной конференции по проблемам безопасности и противодействия терроризму. В программу конференции включены доклады по широкому спектру научных направлений — математических, компьютерных, философских, политологических, психологических. И все они посвящены поиску ответа на один вопрос: как сделать жизнь человека в современном мире более безопасной?

XXI век принес человечеству новые глобальные процессы, вызовы и угрозы. Стремительное развитие информационно-телекоммуникационных технологий приводит к массовому освоению информационного пространства, а в этом есть и свои «плюсы», и свои «минусы». Научный анализ этих «плюсов» и «минусов», а также научное обоснование механизмов безопасного поведения в информационном пространстве — одна из главных задач нашей конференции.

Надеюсь, что три дня работы конференции будут плодотворными, дадут новый импульс научным исследованиям, а через год мы вновь встретимся в стенах Московского университета и обсудим полученные результаты.

Академик В. А. Садовничий,
Председатель конференции,
Ректор Московского государственного
университета им. М. В. Ломоносова.

Оглавление

Общая информация о конференции 10

I. Приветственные выступления 13

Ректор Московского государственного университета имени М. В. Ломоносова В. А. Садовничий 15

Заместитель Секретаря Совета Безопасности Российской Федерации В. А. Соболев 18

Первый заместитель Генерального директора Службы безопасности ОАО «Газпром» С. Ф. Хомяков 20

Director of Cambridge Security Program R. Rohozinski. 22

Prof. Dr. J. von Knop (Heinrich Heine University, Düsseldorf, Germany) 29

II. Пленарные доклады 31

Ш. Кросс. США/НАТО, Россия в противодействии идеологической основе терроризма в информационную эпоху: на пути к построению комплексной стратегии. 33

Т. Ирлет. Швейцарская система центров реагирования на компьютерные атаки 61

А. М. Ивашко. Некоторые методологические и организационные проблемы обнаружения и предупреждения компьютерных атак на критически важные объекты информационной инфраструктуры Российской Федерации. 67

А. В. Галатенко. Комплекс активного аудита распределенных многопользовательских систем 74

Lu Shuwang. On the Social Application of Cryptography and its Development 84

В. Б. Бетелин, В. А. Галатенко, К. А. Костюхин, Н. В. Шмырев. Применение конечных автоматов для спецификации подозрительного поведения программ как элемент контролируемого выполнения 90

П. Д. Зегжда, С. С. Корт. Модель хостовой системы обнаружения вторжений. 102

А. М. Шойтов. Вероятностные модели псевдослучайных последовательностей в криптографии 116

И. Б. Бурдонов, А. С. Косачев, В. В. Кулямин. Безопасность, верификация и теория конформности 135

В. А. Васенин, К. А. Шапченко, О. О. Андреев. Математические модели и механизмы логического разграничения доступа в операционной системе Linux: текущее состояние и перспективы развития 159

А. В. Тишков, И. В. Котенко, Е. В. Сидельникова, О. В. Черватюк. Обнаружение и разрешение противоречий в политиках безопасности 172

В. В. Корнеев, В. В. Райх. Интеграция сигнатурного и поведенческого механизмов анализа данных мониторинга в системах обнаружения атак 186

III. Секция «Математические проблемы информационной безопасности» 199

Б. А. Погорелов, М. А. Пудовкина. Метрические свойства некоторых классов функций 201

М. С. Лобанов. Неулучшаемая оценка нелинейности функции через значение алгебраической иммунности 210

В. И. Солодовников. Гомоморфизмы регистров сдвига в линейные автоматы. 218

О. А. Логачёв, Д. С. Назарова. Локальное аффинное обращение. . . 227

В. В. Баев. Рекуррентные соотношения на выходную последовательность фильтрующего генератора и их обобщения. 249

В. В. Баев. Структура пространства аннигиляторов для булевых функций с фиктивными переменными 255

С. В. Агиевич. Свойства кубических бент-функций специального вида 259

А. Н. Алексейчук, Р. В. Проскуровский, Л. В. Скрыпник. Статистическая атака на комбинирующий генератор гаммы с неравномерным движением в режиме реинициализации начального состояния 264

Ю. С. Харин, А. И. Петлицкий. Выявление зависимостей высокого порядка на основе модели (s, r) 270

А. Н. Ярмола, Ю. С. Харин. INAR-последовательности и их применение в задачах защиты информации 276

Е. В. Разинков, Р. Х. Латыпов. Встраивание цифрового водяного знака в изображение с использованием комплексного преобразования Адамара 281

В. Н. Цыпышев. Оценки ранга второй координатной последовательности линейной рекурренты максимального периода над собственным кольцом Галуа нечетной характеристики 286

С. Н. Конюшок. Схемы широковещательного шифрования, основанные на блоковых кодах 290

Л. В. Ковальчук. Обобщенные марковские шифры: построение оценок практической стойкости к дифференциальным атакам 295

А. С. Маслов. О группе тактовых подстановок *SA*-криптосистем . . . 300

Н. В. Кошкина, О. Ю. Никитина. Стеганография: выделение инварианта для процесса печати и сканирования 304

А. В. Зырянов. Особенности форматов MPEG с точки зрения их использования для сокрытия информации в видеопоследовательности 308

IV. Секция «Математическое и программное обеспечение безопасности компьютерных систем» 313

А. А. Климовский, М. В. Большаков, Ф. М. Пучков. Объекты критически важных инфраструктур: анализ защищенности и риски успешной реализации компьютерных атак 315

В. Б. Савкин. Профили защиты элементов критически важных объектов и меры по поддержанию доверия 336

В. А. Пономарев, О. Ю. Богоявленская, Ю. А. Богоявленский. Система мониторинга поведения транспортного протокола на уровне ядра операционной системы 349

А. В. Галатенко. Реализация сервисов безопасности с помощью неинтерактивных встраиваемых модулей 358

Д. П. Зегжда, А. В. Коротич. Контроль доступа к информационным ресурсам в многозвенных информационных системах. 363

В. С. Богданов, И. В. Котенко. Проактивный подход к мониторингу выполнения политики безопасности компьютерных сетей. 373

С. А. Афонин, А. С. Козицын, А. С. Титов. Автоматизированная система обработки информации в интересах обеспечения безопасности критически важных объектов 383

Ф. М. Пучков, К. А. Шапченко, О. О. Андреев. К созданию автоматизированных средств верификации программного кода 401

О. Ю. Богоявленская, Ю. А. Богоявленский. Метод обнаружения несправедливого захвата ресурсов реализациями транспортного протокола Интернет на основе модели производительности. 440

П. Н. Девянин. Моделирование безопасности управления доступом и информационными потоками в компьютерных системах 448

И. В. Котенко, М. В. Степашкин. Оценка защищенности компьютерных сетей на основе анализа графов атак. 466

V. Семинар-круглый стол «Борьба в Сети: научные, политические и юридические аспекты противодействия кибертерроризму» 483

И. В. Котенко, А. В. Уланов. Противостояние в Интернет: моделирование противодействия распределенным кибер-атакам 485

В. А. Васенин, М. В. Большаков, В. Б. Савкин. Концептуальные положения обеспечения информационной безопасности объектов национальной информационно-телекоммуникационной инфраструктуры 495

J. Bird. Terrorist Use of the Internet 508

Ю. П. Зинченко, Р. С. Шилко. Психологические модели и методы в исследованиях ресурсов развития терроризма. 515

Е. Л. Вартанова, Е. Е. Пронина, Н. В. Ткачева. Комплексный анализ взаимоотношений современного терроризма и средств массовой информации. 519

И. Б. Котлобовский. О международной практике и российском сегменте страхования риска «террористический акт» 535

Д. Н. Кавтарадзе. Имитационные модели и игры в противодействии терроризму 544

A. A. Brudny, E. S. Molchanova. Prototypes and Schemata of Terrorism: Semantic Mapping and Problem Solving Processes 558

В. И. Таирян, Е. И. Таирян. О необходимости исследования и моделирования процессов взаимодействия метацивилизаций современности по критерию всеобщей информационно-психологической безопасности 564

В. Кадыров. Роль религии в развитии безопасности и противодействии терроризму. 570

Р. А. Шаряпов. Противоречия глобальной информационной среды как источник роста трансграничной преступности и международного терроризма. 574

А. Н. Курбацкий. К вопросу о разработке операционных сред с открытыми исходными текстами, ориентированных на обеспечение безопасности государственных информационных систем. 581

В. А. Иванов, Е. В. Гречишников, А. А. Двилянский. Обеспечение безопасности инфотелекоммуникационных объектов при воздействии электромагнитного импульса 590

Приложение 1. **Л. И. Левкович-Маслюк.** Между киберземлей и кибернебом: Цензура в Сети рухнет первого декабря (интервью с директором группы перспективных исследований сетевой безопасности Кембриджского университета Р. Рогозинским) 594

Приложение 2. **Л. И. Левкович-Маслюк.** Доктринальное лидерство (интервью с заместителями директора ИПИБ МГУ В. В. Ященко и А. А. Сальниковым) 605

VI. Круглый стол «Комплексная безопасность критически важных объектов топливно-энергетического комплекса» 617

Вступительное слово проректора МГУ им. М. В. Ломоносова В. А. Мамонтова. 619

Б. Н. Епифанцев, К. С. Патронов. Перспективные технологии предотвращения несанкционированного доступа к трубопроводам . . . 621

А. А. Швыряев. Этапы становления оценки риска опасных производственных объектов ОАО «Газпром» 625

В. Н. Пожарский, В. В. Лесных, Е. А. Иванов. Разработка моделей и методов управления безопасностью критически важных объектов топливно-энергетического комплекса 628

И. И. Тюхов. Возобновляемая энергетика для безопасности объектов ТЭК 636

В. А. Мамонтов, Н. И. Бурдаков. Проектирование комплексных систем обеспечения безопасности объектов нефтегазовой отрасли, критически важных для национальной безопасности по критериям риска 643

В. Б. Ляхов. Унифицированные проектные решения (УПР) по комплексам ИТСО и САЗ объектов ОАО «Газпром» 646

И. А. Калайда. Основные направления работ по оценке соответствия ИТСО и САЗ в системе добровольной сертификации ГАЗПРОМСЕРТ 650

А. В. Чекер. Некоторые проблемы защиты подводных участков магистральных газопроводов и объектов газодобывающей и газотранспортной инфраструктуры прибрежного, шельфового и морского базирования. 652

Общая информация о конференции

Пятая Общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-06)

Организаторы — Московский государственный университет им. М. В. Ломоносова, Академия криптографии Российской Федерации.

Семинар-круглый стол «Борьба в Сети: научные, политические и юридические аспекты противодействия кибертерроризму»

Организаторы — Московский государственный университет им. М. В. Ломоносова, Программа по изучению безопасности университета Кембриджа (Великобритания) при поддержке аппарата Совета Безопасности Российской Федерации, программы «Россия — НАТО» и при участии Университета штата Нью-Йорк, Университета им. Г. Гейне (г. Дюссельдорф).

Круглый стол «Комплексная безопасность критически важных объектов топливно-энергетического комплекса»

Организаторы — Московский государственный университет им. М. В. Ломоносова, ОАО «Газпром», при поддержке аппарата Совета Безопасности Российской Федерации.

Семинар-совещание руководителей проектов по приоритетному направлению «Безопасность и противодействие терроризму» ФЦНТП

Организаторы — Московский государственный университет им. М. В. Ломоносова, Рабочая группа Научно-координационного совета ФЦНТП.

Конференция проводится при финансовой поддержке ОАО «Газпром», Российского фонда фундаментальных исследований, группы компаний «Метро», Программы НАТО «Безопасность через науку».

Сопредседатели конференции:

- В. А. Садовничий — ректор МГУ им. М. В. Ломоносова;
- В. П. Шерстюк — помощник Секретаря Совета Безопасности РФ;
- Н. Н. Андреев — президент Академии криптографии РФ;
- С. К. Ушаков — заместитель Председателя Правления ОАО «Газпром».

Руководители семинара-круглого стола «Борьба в Сети: научные, политические и юридические аспекты противодействия кибертерроризму»:

- Р. Рогозинский — содиректор семинара (Университет Кембриджа);
- А. А. Стрельцов — содиректор семинара (аппарат Совета Безопасности РФ);
- В. В. Соколов — содиректор семинара (ИПИБ МГУ);
- А. В. Беляева — координатор семинара (Фонд гражданских инициатив в политике Интернет, Россия);
- Р. Госенде — координатор семинара (Университет штата Нью-Йорк);
- Я. фон Кноп — координатор семинара (Университет им. Г. Гейне, г. Дюссельдорф);
- Дж. Робертс — координатор семинара (Европейский Центр им. Джорджа К. Маршалла).

Руководители круглого стола «Комплексная безопасность критически важных объектов топливно-энергетического комплекса»:

- В. А. Мамонтов (МГУ им. М. В. Ломоносова);
- В. Н. Пожарский — начальник Управления Службы безопасности ОАО «Газпром»;
- А. И. Ефимов — начальник Управления Службы безопасности ОАО «Газпром»;
- Ю. Г. Попов — начальник отдела Управления Службы безопасности ОАО «Газпром».

Оргкомитет конференции:

- В. В. Ященко — председатель Оргкомитета, заместитель директора ИПИБ МГУ;
- В. Н. Сачков — вице-президент Академии криптографии РФ;
- В. В. Данилин — первый заместитель руководителя Департамента международных связей города Москвы;
- С. Ф. Хомяков — первый заместитель Генерального директора Службы безопасности ОАО «Газпром»;
- В. Н. Пожарский — начальник Управления Службы безопасности ОАО «Газпром».
- М. М. Глухов (Академия криптографии РФ);
- А. В. Сурин (факультет государственного управления МГУ);
- О. А. Логачёв (ИПИБ МГУ);
- В. А. Васенин (ИПИБ МГУ).

Секретариат конференции:

- Р. А. Шаряпов — ответственный секретарь Оргкомитета (ИПИБ МГУ);
- В. И. Солодовников (Академия криптографии РФ);
- Ю. В. Малинин (Академия информационных систем);
- Н. В. Табаченко;
- М. И. Анохин;
- Т. А. Браташ;
- М. Е. Семина;
- Н. Н. Костина;
- А. В. Соколова.

Часть I

ПРИВЕТСТВЕННЫЕ ВЫСТУПЛЕНИЯ

Ректор Московского государственного университета имени М. В. Ломоносова В. А. Садовничий

Уважаемые коллеги!

Разрешите открыть Вторую международную конференцию по проблемам безопасности и противодействия терроризму.

В зале я вижу много знакомых лиц, которые уже традиционно собираются в МГУ в конце октября для обсуждения междисциплинарных межведомственных проблем безопасности. Труды прошлогодней конференции и ряд других материалов вы получили и сегодня мы продолжим дискуссии и обсуждение новых идей и результатов.

Мы планировали начать конференцию с обсуждения доклада помощника Секретаря Совета Безопасности России, директора Института проблем информационной безопасности МГУ Владислава Петровича Шерстюка «О стратегии развития информационного общества в России». Но сейчас Владислав Петрович находится в Пекине, где проходят консультации о формировании рабочей группы по международной информационной безопасности. Решение о создании такой группы приняли президенты стран Шанхайской организации сотрудничества на своем саммите в мае этого года и, видимо, сегодня-завтра эта группа будет сформирована и приступит к работе. Несомненно, что многие результаты участников нашей конференции могут быть востребованы в качестве научного фундамента будущих предложений и решений группы.

Вчера Владислав Петрович звонил из Пекина, просил передать привет и поздравления всем участникам конференции с ее открытием и пожелания больших успехов в ее работе. Кроме того, он отметил большой успех, достигнутый на переговорах с китайской стороной о формировании рабочей группы.

В проекте «Стратегии развития информационного общества в России», которую вы получили, учтены многие результаты дискуссий на семинаре, который работает в МГУ уже 5 лет. И один из первых вариантов стратегии мы обсуждали на этом семинаре 2 марта этого года. После этого проект обсуждался на заседании Межведомственной Комиссии по информацион-

ной безопасности, а затем было общественное обсуждение во всех федеральных округах России. Сейчас проект Стратегии готовится к принятию в качестве концептуального документа, определяющего развитие России на ближайшее десятилетие.

Еще одна тема, которая постоянно звучит на наших конференциях, — разработка понятийного аппарата в области научных проблем информационной безопасности. Ясность в толковании базовых терминов и определений — один из важнейших атрибутов научного подхода. А мы как в дискуссиях с представителями различных организаций России, так, тем более, в разговоре с нашими зарубежными коллегами, часто вкладываем разный смысл в понятия «защита информации», «информационная безопасность», «кибертерроризм», «информационное оружие» и так далее, и так далее.

Месяц назад в Московском университете прошел очередной международный семинар в рамках научного совета «Россия—НАТО». Тема семинара — «Принципы разработки многоязычного глоссария по информационной безопасности». В результате дискуссий создана рабочая группа и готовятся предложения в научный совет «Россия—НАТО» о порядке продолжения этой важной работы. И, кто знает, быть может, через год-два мы раздадим на нашей конференции согласованный многоязычный глоссарий. Тем более, что потребность в нем очень большая и это отмечается на самых различных конференциях, форумах и совещаниях. В этой связи хотелось бы с удовлетворением отметить, что сегодня вы получили «Словарь криптографических терминов». Это итог четырехлетней работы коллектива высококвалифицированных ученых Московского университета и Академии криптографии Российской Федерации. Но работа еще не закончена: словарь асимметричный — в нем нет толкования терминов на английском языке. И здесь мы ждем помощи от наших зарубежных коллег и прежде всего, от наших постоянных партнеров по организации этой конференции — университета штата Нью-Йорк, университета Кембриджа, университета Генриха Гейне.

Уважаемые коллеги! При подготовке программы нашей конференции мы остаемся верны базовым принципам — фундаментальность, междисциплинарность, межведомственнсть. В зале, как и прежде, ученые и специалисты из органов государственной власти, силовых структур, высших учебных заведений и научных организаций, промышленности и бизнеса, представители различных научных школ.

Всех нас объединяет желание найти ответ на один вопрос: как сделать жизнь человека в современном мире более безопасной? В Московском университете для придания еще большей целенаправленности таким исследованиям создан Координационный совет по приоритетному научному направлению «Безопасность и противодействие терроризму», в который

вошли руководители 17 подразделений — от физического факультета до философского факультета. Сегодняшняя конференция — это тоже одно из мероприятий Координационного совета. Мы будем свидетелями очень интересных докладов, участниками дискуссий и круглых столов.

Позвольте мне пожелать успешной работы нашей конференции и объявить ее открытой.

Заместитель Секретаря Совета Безопасности Российской Федерации В. А. Соболев

Уважаемые участники и гости конференции!

Разрешите приветствовать Вас от имени Совета Безопасности Российской Федерации.

Сегодня человечество вплотную подошло к рубежу, за которым начинается новый этап его развития, получивший название «информационного общества». Как неоднократно отмечал Президент Российской Федерации В. В. Путин, мы не имеем права проспать разворачивающуюся в мире информационную революцию.

Следует особо отметить, что вместе с большим количеством преимуществ этот этап несет в себе принципиально новые, высокотехнологичные угрозы. События последних лет дают нам большое количество примеров использования высоких технологий в террористических и иных преступных целях. Успешно противостоять таким угрозам, можно только объединив усилия специальных служб государства, фундаментальной науки и гражданского общества.

В Московском университете при поддержке ректора академика Виктора Антоновича Садовничего активно разрабатываются научные проблемы обеспечения безопасности и противодействия терроризму. МГУ находится в числе пионеров разработки гуманитарной составляющей проблем обеспечения информационной безопасности. Решением Научного совета при Совете Безопасности Российской Федерации Московский университет определен головной организацией по научным проблемам обеспечения информационной безопасности, имеющим гуманитарный характер. Дополнительный импульс развитию этого направления научных исследований был дан созданием в рамках МГУ Института проблем информационной безопасности. Деятельность Института направлена на проведение фундаментальных и прикладных научных исследований проблем безопасности информационного общества, имеющих комплексный междисциплинарный характер, координацию исследований по проблемам безопасности и противодействия терроризму, которые ведутся учеными и творческими коллективами университета.

С ноября 2004 года в России реализуется Федеральная целевая научно-техническая программа «Исследования и разработки по приоритетным направлениям развития науки и техники». Значительное место в этой программе отведено теме «Безопасность и противодействие терроризму». Московский университет активно участвует в реализации этой темы, примеры тому — доклады по широкому спектру научных проблем безопасности и противодействия терроризму, включенные в программу нынешней конференции.

Информационное пространство не имеет границ, и поэтому ни одна страна в одиночку не способна решить проблемы обеспечения безопасности глобального информационного общества. Необходимость международного научного сотрудничества в области информационной безопасности отмечается в Доктрине информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации Путиным В. В., в проекте Стратегии развития информационного общества в России, в национальной стратегии США по обеспечению безопасности киберпространства, утвержденной Президентом США Дж. Бушем, а также в аналогичных концептуальных документах ряда других стран. Российские ученые активно участвуют в международных конференциях и проектах, совместно с зарубежными коллегами разрабатывают новые предложения по проблемам безопасности и противодействия терроризму. Эффективно заработали новые механизмы научного сотрудничества, такие как — Программа НАТО «Безопасность через науку», Научный Совет «Россия — НАТО» и ряд других.

Без сомнения, что одним из элементов общемировой системы противодействия новым угрозам является и ставшая уже традиционной Ежегодная международная научная конференция по проблемам безопасности и противодействия терроризму, проводимая МГУ имени М. В. Ломоносова.

Хотелось бы пожелать участникам конференции плодотворной работы. Уверен, что результаты конференции дадут новый импульс развитию концептуальных подходов и практических решений по обеспечению безопасности и противодействию терроризму.

Первый заместитель Генерального директора Службы безопасности ОАО «Газпром» С. Ф. Хомяков

Уважаемые участники конференции!

От имени руководства ОАО «Газпром» и Службы безопасности ОАО «Газпром» разрешите приветствовать вас в связи с началом работы Второй международной научной конференции по проблемам безопасности и противодействия терроризму.

За год, прошедший со времени проведения предыдущей конференции, проявились новые негативные тенденции, расширился спектр угроз объектам топливно-энергетического комплекса (ТЭК), связанных с террористическими проявлениями и иными противоправными действиями. Вместе с тем, повысился уровень консолидации усилий и координации совместных действий государства и бизнес-структур по противодействию террористическим угрозам, благодаря чему стали более эффективно реализовываться меры по усилению антитеррористической защищенности объектов ТЭК.

Необходимость обеспечения безопасного функционирования и устойчивого развития Единой системы газоснабжения обусловливает то большое внимание, которое уделяется в обществе проблеме противодействия терроризму, в первую очередь, такому ее аспекту, как антитеррористическая защита критически важных объектов ОАО «Газпром». Осуществление работ по реализации принятой в обществе стратегии развития в сфере освоения новых месторождений, транспортировки газа и его переработки обусловливает и увеличение числа критически важных объектов, требующих принятия мер безопасности. Из наиболее крупных проектов следует выделить освоение газовых и нефтяных месторождений на морском шельфе, прокладка Северо-Европейского газопровода и газопровода в страны Азиатско-Тихоокеанского региона, увеличение объемов морской транспортировки сжиженных углеводородных газов. Данные проекты исключительно важны, так как обеспечивают рост и надежность поставок энергоносителей для нужд внутреннего рынка, а также для выполнения обязательств по экспорту газа зарубежным потребителям.

Решение указанных задач неразрывно связано с разработкой и внедрением дополнительных и более эффективных мер безопасности. В соответствии с принятыми решениями ОАО «Газпром» осуществляет деятельность по обеспечению безопасности объектов от угроз террористического характера на основе программно-целевого планирования, проведения единой технической политики. В Обществе реализуются меры по переходу на новые принципы политики безопасности, заметно усиливается техническая компонента в системе защиты объектов, внедряются новые технологии и интегрированные системы инженерно-технических средств охраны и средств антитеррористической защиты, ориентированные на модульно наращиваемые комплексы и унификацию проектно-технических решений.

В рамках данной деятельности совершенствуются концептуальные основы обеспечения безопасности важных и потенциально опасных объектов ОАО «Газпром», в частности, активно внедряются современные подходы, основанные на разработке моделей угроз и управлении рисками. Совместно с органами государственного управления предпринимаются усилия по созданию нормативно-правовой базы в сфере противодействия террористическим угрозам в отношении объектов газовой отрасли. ОАО «Газпром» участвует в работе Государственной Думы Федерального Собрания, Совета Безопасности, Аппарата Правительства Российской Федерации, федеральных органов исполнительной власти по подготовке новых и изменению действующих законодательных и правовых актов в сфере усиления мер комплексной безопасности объектов ТЭК, в создании необходимых регулирующих механизмов.

Надеемся, что в ходе работы Конференции и Круглого стола «Комплексная безопасность критически важных объектов ТЭК», соорганизатором которого выступает ОАО «Газпром», будут обсуждены проблемы, возникающие при практической реализации мероприятий по совершенствованию антитеррористической защиты ключевых энергетических инфраструктур, и предложены научно обоснованные меры по их решению.

Еще раз поздравляю вас с открытием конференции и желаю плодотворной работы, осуществления намеченных планов и успехов в профессиональной деятельности.

Director of Cambridge Security Program R. Rohozinski

It brings me great pleasure and honor to welcome you to Second Annual Russia — NATO Advanced Workshop examining legal, political, and security issues common to information global society. The NATO Science Program, to whom we are very much indebt for supporting this event for the second year, provides an ideal form for being able to bridge the best of what scientific cooperation can bring to these important questions. But beyond the NATO umbrella this conference is also a cooperation between two great academic institutions — the University of Cambridge and Moscow State University, both of whom in their countries act as a vital bridge between the scientific community and policy community, both of which are vital for coming with solutions that help to enhance personal, national, and global security challenges that face us in global information society. But advanced research workshops are far more than just presentations of academic findings from participants. There are also opportunities to interrogate, explore, and challenge issues, which are at time difficult. There are here to challenge conventions, challenge the way of thinking, and help us think about problems in different ways. In this way our first workshop last year focused on the question that at that time was not terribly popular in policy circles, which is to say unconventional informational warfare. What we meant by that is that we looked at the question if our policies, our approaches to terrorism in cyberspace really focused on the right question, if the threat is really coming from the terrorist use of the Internet as a way to attack a critical infrastructure or if the threat is really coming from the appropriation of the space of cyberspace by terrorist organizations, full mobilization, propaganda, and other forms of psychological effects. Interestingly our findings certainly pointed at the last matter.

Much in the same way topic of this year Advanced Research Workshop looks at the question of fighting in the net. By fighting in the net we can mean many things. We can talk about fighting cyber crime; we can certainly talk about fighting terrorist entities and countering ideological operations. But I would like in my opening remarks put a focus on one tendency, which I think this year has come to the fore, and which certainly will benefit from out careful consideration. That is a fast developing militarization of cyberspace.

Militarization of cyberspace in 2006 was driven and propelled by two events. One is more known, one is less known. Less known has been a declaration of intention by the United States Department of Defense to elaborate a military strategy for operations in cyberspace, which the first time when the term cyberspace in that domain was identified in such a way. The second the more public was a defeat of a major regional superpower, in this case Israel, Israeli Defense Forces, at the hence of an asymmetrical actor. This is worthy of a few notes.

The summer war between the Israeli and Hezbollah demonstrated a degree to which a well-organized asymmetric actor could leverage both the opportunities afforded by technology and could prevail over a much larger better organized and stronger conventional military actor. Paradoxically, while the Israeli Defense Forces concentrated on maximizing their military effect through the application of advanced network centric warfare concepts to target, attack, and degrade Hezbollah forces in acts of persuasion, Hezbollah instead concentrated on political and informational level of the conflict. It used networks, networks technology, and integrated military political strategy through cyberspace to target its military effects to maximum informational effect, which the IDF could neither match nor defeat.

Some of the ways that Hezbollah followed through on this strategy.

One, and this is possibly the greatest surprise, is that they actually hacked in effectively monitored Israeli communication channels and used the information gleaned from that in order to set a tempo as well as the agenda of information war. For example, the intercepted information pertaining the Israeli casualties and immediately made that information public. They also timed their attacks for maximum informational effect. So at the time that the Chinese made radar guided missile was being successfully launched against Israeli frigate, at the same time Hezbollah was already advertising and communication the success of the attack using its multimedia channel. Hezbollah therefore used the domain of cyberspace far more effectively than IDF, which dominated the tactical military space. As a result Hezbollah was able to effectively turn a military defeat or at least a stalemate into a major political victory.

The IDF, the Israeli Defense Force, experience in South Lebanon echoes in maybe much more dramatic effect, some of the lessons are being learned and the experiences of the U.S. military in a pursuit of its global war on terror and its counter insurgency operations in Iraq. Paradoxically, despite the huge investment in a development of command and control warfare which has created unprecedented situational awareness for commander as well as shortened lethal link between the sensors and shooters, this superior technology is not helping the U.S. Forces in winning and prevailing against these insurgents

in Iraq. As one commander recently put it, "great intelligence and fantastic technical capabilities are no good if they can not tell me who the enemy is".

Secondly, and perhaps more importantly, is that despite huge institutional and organizational human investment towards the development of five core capabilities information operations as a way to dominate the information environment and in the case to win Iraqis hearts and minds, this have revealed a little or no positive effect. As in the case of the Israelis the U.S. Military outmaneuvered, outpaced, and outmatched by insurgent forces who are more adoptable and, paradoxically, better networked for information effect than the most advanced army in the world.

Nowhere has the U.S. faced a greater challenge than in being able to source the insurgency online that is to say in cyberspace. At the local level tactical commanders who struggled to engage local population with targeted psychological operations product often find themselves outmatched by local insurgents who tap in both local and global sources for ideological support, material support, and technical information as well as leveraging their social networks in order to be able to dominate their local environment. They are the ones that tell the stories that are believed, they are the ones who are able to communicate their truth better and faster.

At the global level if aggregate this, the global insurgency has managed to leverage these local resources into real global momentum. If we look at it simply from quantative level, we have seen a rapid rise in both number, quality, and sophistication of global online resources, which be identified as jihads or jihads supported, rising from about 200 authoritative such resources in 2003 to over 4000 in 2006. This is despite, a very concentrative and all-in-compassing campaign in order to try to counter this. Of course this rise, these failures can not be simply laid at the doorstep of the failure of IO or information operations policy alone. In variably some of the policy choices made the U.S. administration had led to a large unpopularity among large segments of population in the world, which can not be addressed by strategic communications themselves. It is difficult to sell an unpopular product. If we look at the results of polls taken by Pew Foundation, we see a dramatic decline of support for the U.S. policies over the last three years — from 70 to 40 percent in Europe; 50 to 20 percent in most Muslim countries; and in some critical Muslim countries from 77 to 21 percent, as for example in Morocco.

However, despite the role of policy in this the inability of the U.S. successfully engage and challenge asymmetric actors in cyberspace may be seen as a major capabilities gap and must be addressed. It may come as a surprise for some of you, the world leading superpower did not have up to now a military strategy for cyberspace. In face one of reasons for this is a simply a problem

of defining what it is a cyberspace encompasses. Is it the infrastructure? Is it the code that makes the infrastructure improbable? Or is it the content that actually forms the substance which is carried by the infrastructure? At the moment there is no consensus around it, and I am aware of at least four definitions of cyberspace, which been talked about within the Department of Defense itself.

In part we can also argue that the absence of military strategy for cyberspace on the part of the U.S. has also been a part of the consequence of the U.S. leadership in dominance at least over the components of which cyberspace is made and also at extend to which developing specific capabilities to affect components of cyberspace through information operations have also been taken. The result has been that between early 2000 and 2006 the U.S. missed a degree to which a domain to define a cyberspace actually globalized and also more importantly the degree globalized cyberspace has become a domain, which is capable of sustaining a robust meaningful and social political and military action.

On the first point — the physical control domain of cyberspace — the U.S. influence over this has declined quite precipitously from the 1990's during the time which were mostly the infrastructure of fiber optic cable linking continence and satellites resided with U.S. companies like TIC, FLAG, Global Crossing, all of which since 2000's have become owned by foreign entities. Indian companies now own two of the major underwater fiber optic networks. And a third, Global Crossing, is owned by wholly owned subsidiary of Chinese government. Similarly in the realm of technology itself U.S. leadership over software production has declined as outsourcing has taken a greater and greater percentage of this outside of direct the U.S. control. Outsourcing grooved from 1,8 billion dollars in 2003 to an estimated 26 billion dollars in 2006–2007. Similarly production of military significant technologies such as for example thermal batteries that are used in smart bombs, 80 percent of which are now produced outside of the U.S. In terms of the provision of these services or the impact it had on the military action just to quote one statistic, during operation Iraqi Freedom more than 80 percent of the long hold telecommunications backboned that were used by the Department of Defense were procured from commercial providers, some of which were not U.S. based at all.

Finally and probably most importantly, in realm of online life where as in 1990's the center hub of this global community of online users really existed and more or less hosted about of the U.S. based cyberspace. Beginning in the early 2000's this is now balkanized and has really become globalized. For example, many jihads sites now exist on networks, which lie outside of both legal and physical jurisdiction of the U.S. Government itself.

Basically all this points to a position of further decline. In this respect the decisions undertake of the national military strategy for operations in cyberspace recognizes the importance of this declining influence and basically points to the need to develop set capabilities to secure access and to be able to fight and win in this domain of cyberspace.

What does this mean? One level as it provides a mechanism for military leadership and military commanders to identify cyberspace as an operational domain, to define operational concepts and perimeters, identify risks, set guidance, and develop capabilities for combat in cyberspace. At the conventional level this probably simply means an expansion and integration of what is meant by the capabilities of the IO focused on cyberspace itself, meaning that ethnographic intelligence will be used to find what is known about the environment of cyberspace in an area of military operations. Consideration of cyberspace will be incorporated both in the way the network centric corporations are undertaken, how the operation security is framed, how military deception is going is used, and in effect how the plans for both computer network attack and defense are also employed in theatre. We can also expect more of an emphasis on network attacks against critical cyberspace nods within immediate theatres of actions.

However, more serious thing since the bulk of the global war on terror really is a global undertaking. We can also see or hypothesis a large increase at the unconventional level both in an expansion and use of computer network exploitation against targeted resources and individuals as well as a rather steep increase in an extension of psychological operations, which specifically target cyberspace resources. Some of the techniques that are currently under discussion include intense monitoring of the information resources through both technical and ethnographic techniques, the use of leads identified through these techniques in order to identify transient ideology, resources, and networking, and then also active measure which include disruption through the injection of negative messages designed to pollute the information flow, so distrust among the member of network, effect the information resource through a variety of means, viruses, trilogies, and devices, and also to include incursion of alternative narratives, so called white propaganda in ruder to change the temper. Most of these techniques may seem unknown, some are well-known among the members of police community because they are very much focus on those. However, unlike the world of policing, in which things happen in fairly defined conventions and norms, military operations in cyberspace proposes to do this only in the national interest. It proposes to apply fairly narrow national interest towards a global infrastructure and one with global reach itself.

There are several serious questions that this raises for international system and for international cooperation. First of all is the line that has plagued the whole area of computer network operation specifically, is exactly how permissible are these under existing international law. Does the targeting of civilian infrastructure by military means standing contravention to Geneva Convention? But more seriously the directed attacks on resources in cyberspace that may exist in different sovereign jurisdiction also poses a much different problem of how do we then define and how then it does define the problem of sovereignty and cyberspace overall.

Secondly, what are these risks? Because even though the national cooperation for military operations in cyberspace is consistent with national security such as strategy of the U.S., which recognizes the right to use force preemptively against emerging threats. In a physical realm the actual application of that strategy is circumscribed by risks that the over use of military force and resources that it requires actually brings. There are far fewer such restrictions and limitations on the application of such actions in cyberspace because the threshold is lower and because the capabilities to certain extent are less costly to develop than conventional weapon systems. It can be expected that such systems will be developed in increasing number of states. Therefore, states will simply not risk becoming subject to a significant strategic disadvantage by not so doing. So there is a real risk here that this step not being taken may precipitate an arm race in cyberspace. All of these put at risk existing international security cooperation that exists in cyberspace as it does around questions of countering terrorism and cyber crime. The moment when the emphasis shifts from using mechanisms of international cooperation to a largely policing and intelligence and towards a military sphere of actually weaponising an approach the basis for cooperation declines as the levels of trust also potentially fall. There is a risk of balkanization of cyberspace as more and more state pursues this capability.

Of course the U.S. is not the only country seeking the superiority in cyberspace and to some extent the emergence of successful acts of actors such as Hezbollah makes the militarization of cyberspace rather inoperable. Neither is the path to this militarization, taking this from actual operating concepts of informational weapon system, free from unintended consequences and blowback, already limited experience with the employment of computer network attack on platforms has shown up significant problems engaging both their effectiveness or preventing unintended consequences such is, for example, what happens when your blocked propaganda actually gets to be discovered as blocked propaganda or when there is a possibility of tracing back the origins of cyberattacks.

For all of these reasons, I think, it is a responsibility of experts like those who are gathered here today, representing countries East and West, representing also different communities — practitioners, social scientists, technologists — to take a very close look at these emerging strategies and really access what kind of alternatives really exist before these concepts become operational reality and de facto and upsetting international norms. In this spirit I wish the participants of these workshop and conference success in addressing these important and developing issues. May our collective wisdom and former leadership to take wiser choices then enhance rather than decrease the security in our emerging global information society.

Prof. Dr. J. von Knop (Heinrich Heine University, Düsseldorf, Germany)

Respected Vice Rector Professor Belokurov, Ladies and gentlemen, Dear colleagues,

I am delighted to have the honour of welcoming the organisers and delegates of the "Second International Conference on Security and Countering Terrorism Issues," which is dedicated to questions of interest not only to scientists and specialists, but also to society as a whole.

I would specially like to emphasize that this conference is taking place right here in Moscow — a city with which Düsseldorf — my home city — has supported a close cooperative alliance for a long time. I am pleased to note that the traditional forms and subjects of the economic collaboration between these two cities has been complemented by a very strong cooperation in science in general and especially on security issues between Lomonosov State University and the University of Düsseldorf for many years. We also received generous financial support from the METRO-Foundation, which I am also representing here in Moscow.

Please allow me to say a few words about the cooperation between our two universities. Vice Rector Belokurov has already spoken very kindly about the scientific cooperation between Lomonsov Moscow State University and Heinrich Heine University Düsseldorf.

One of the highlights of the cooperation with LMSU was the conference "Security and Privacy in the Information Age" which was held in Düsseldorf in October 2005 within the framework of the first Moscow Economic Days in Düsseldorf. We were very happy that this conference was opened by the First Deputy Mayor of Moscow, Petr Nikolaevich Aksenov.

The general conference chair was held by my very honourable colleague, Prof. Dr. Vladislav Sherstyk, Member of the Security Council of the Russian Federation and Director of the Institute for Infomation Security of the LMSU, by Professor Dr. Vladimir Sokolov, Deputy Director of this institute and by myself.

The Programme Committee of the conference, which was chaired by Prof. Dr. Valerij Yashenko, Lomonosow State University Moscow and myself, joined 25 scientists from the LMSU. The Programme Committee was responsible for the high standard of the conference's scientific programme.

At the conference 75 lectures were presented by leading scholars from Germany, Russian Federation, the USA, Israel and other European countries. From the Russian Federation, we had 22 scientific presentations which gave us a profound impression of the very high standard of security research in Russia. The scientists reflected on general security issues, cyber terrorism, international aspects of information security, ethical behavior, new trends in defence of terrorism and counterterrorism research.

At the conference, potential dangers to the so-called information society were deeply analysed; economic, basic political and legal conditions discussed, and systematic methods for risk defence elaborated upon. The conference consisted of four parts:

Phenomenology of Modern Terrorism. This part focused on new changes in modern terrorism such as the suicide attacks phenomenon, the nature of future cyber threats including the possible use of spam and fishing by terrorists, electromagnetic pulse hazard to aircraft.

Counter-Terrorism Challenges in the Information Society. The challenge of conducting efficient counter-terrorism campaigns in democratic societies. Human rights compliance in counter-terrorism campaigns with special focus on interrogation of terrorism suspect. Diplomacy as a tool for counter-terrorism and the special role of the Russian Security Council.

The Challenge of the Information Society — international considerations and self-regulation considerations of information security. Questions of ethical behavior and operational, internal and international aspects of legislation, internet crime, corruption and critical infrastructure threats.

The Perspective of Industry — early warning systems and the challenges that they pose to international operating companies, internet Security and IT governance.

Ladies and Gentlemen, metropolises like Moscow and Düsseldorf and other cities in Germany must constantly watch the general state of security and take preventive action. This calls for a strong cooperation of science and the state or city authorities with companies specialising in security matters.

I wish the Second Scientific Conference on Security and Countering Terrorism at the Lomonosow State University in Moscow a successful series of presentations and further discussions, enabling us to come to an even deeper level of understanding about these current issues.

Часть II

ПЛЕНАРНЫЕ ДОКЛАДЫ

США/НАТО, Россия в противодействии идеологической основе терроризма в информационную эпоху: на пути к построению комплексной стратегии

Ш. Кросс

Аннотация

Д-р Шерил Кросс является профессором по вопросам национальной безопасности в Европейском центре по изучению вопросов безопасности им. Джорджа Маршала в Гармиш-Партенкирхене, Германия. В этой статье автор высказывает свою точку зрения. В статье не отражена официальная концепция или точка зрения Европейского центра по изучению вопросов безопасности им. Джорджа Маршала, Европейского командования ВС США, Министерства обороны США или правительства США. Основные выводы, приведенные в этой статье, были кратко изложены автором на Второй международной научной конференции по проблемам безопасности и борьбе с терроризмом, прошедшей в Московском государственном университете им. М. В. Ломоносова 25–27 октября 2006 года. Автор хотела бы выразить благодарность за поддержку в работе, оказанную директором Центра им. Дж. Маршала, предоставившему ей исследовательский грант. Эта статья будет также частично опубликована в журнале *Connections*, том 4, зима 2006 г. под названием «США/НАТО, Россия в противодействии идеологической поддержке терроризма в информационную эпоху: на пути к построению комплексной стратегии» Шерил Н. Кросс.

Введение

В политике Соединенных Штатов противодействие идеологической основе терроризма (ПИОТ) определяется как первоочередная задача во всеобщей борьбе против мирового терроризма [1]. После трагических взрывов

[1] См. *Стратегия национальной безопасности Соединенных Штатов Америки* (Вашингтон: Белый дом, март 2006 г.), 9–11, доступ: `http://www.whitehouse.gov/nsc/nss/`

в Лондоне и Мадриде, после захвата заложников в школе в Беслане, ученые и политические деятели Европы и Евразии также начинают придавать большее значение «борьбе идей». Это диктуется необходимостью выработки ответных мер на вызовы радикальных религиозных экстремистских движений, действующих на территории этих стран[2]. Для успеха любой операции ПИОТ потребуется беспрецедентное согласие стран, активно участвующих в защите мирового сообщества от терроризма, по вопросам определения основных целей, связи и координации. Это единственный способ уберечь мир от опустошения и потерь, которые способны нанести террористические акты, инспирируемые религиозным экстремизмом.

Противодействие идеологической основе терроризма не является универсальным средством (так сказать, «серебряной пулей») в борьбе с мировым терроризмом. Однако совершенно ясно, что для того чтобы подорвать влияние радикальных террористических движений на долгое время, надо выходить на прямое общение с теми, к кому обращены террористические идеологии, так сказать, воздействовать на их «сердца и умы». Соединенные Штаты и другие государства уделяют все больше внимания и ресурсов на разработку средств для дискредитации идеологии Аль-Каиды, джихадистов-салафистов и других схожих исламистских групп. Тем не менее, пока ни одна страна в мире не может утверждать, что нашла оптимальный метод борьбы с воинствующим религиозным экстремизмом или эффективный способ подрыва идеологических основ терроризма. Бывший министр обороны США Дональд Рамсфельд, оценивая деятельность Америки «в развертывающейся борьбе идей», поставил ей «слабенькую троечку».[3]

Эффективная стратегия разоблачения идей или мифов, использующихся террористическими группами, должна быть основана на глубоком понимании уникальных условий в каждом контексте. В мире не найти и двух регионов, одинаково уязвимых перед идеологией/мифами террористов. Современные исламистские экстремистские группы (включая радикальных суннитов, исламистов-салафистов, радикальных шиитов и других) могут разделять некоторые основные убеждения, определять общих врагов и преследовать одни и те же цели, но между этими группами существуют значительные идеологические, теологические и тактические различия. Так что,

2006/; председатель Комитета Начальников Штабов «*Национальный военный стратегический план по войне с терроризмом*» (Вашингтон: Министерство обороны, 1 февраля 2006 г.), 24–25; брифинги и интервью, взятые автором, Государственный департамент США, ноябрь 2006 г.

[2] См. *Стратегия Европейского Союза по борьбе с радикализмом и вербовкой кадров для терроризма* (Брюссель: Совет Европейского Союза, 25 ноября 2005 г.); см. Оливер Рой. «Ответ Европы на радикальный ислам». *Современная история* (ноябрь 2005 г.)

[3] Рамсфельд. «Мы проигрываем в борьбе идей». *Carlisle Sentinel*, 28 марта 2006 г.

занимаясь такой сложной проблемой, как разработка стратегии по дискредитации в глазах населения радикальных насильственных идеологий, мы должны обращаться за помощью к тем, кто знаком с местными условиями, социальными традициями и ценностями.

В этой статье анализируется возможность построения сотрудничества между Соединенными Штатами/НАТО и Россией в области противодействия идеологической основе терроризма в информационную эпоху. После событий 11-го сентября США/НАТО и Россия сделали большой шаг вперед в развитии сотрудничества в области борьбы с терроризмом, в основном, через Совет Россия—НАТО (СРН) и Российско-американскую рабочую группу по борьбе с терроризмом. Совпадение интересов Соединенных Штатов, государств — членов НАТО, России и других стран мира показывает, что проблема борьбы с идеологическими импульсами, разжигающими терроризм, является общим приоритетом безопасности и что в ближайшие десятилетия ее важность будет только нарастать. Сильный международный антитеррористический альянс поможет определить угрозы, но очевидно, что любая трещина или разногласия могут быть использованы террористами в своих целях. Объединение усилий государств трансатлантического сообщества в попытках привлечь на свою сторону дружественные страны мусульманского мира для противостояния религиозному экстремизму может помочь в создании основы для установления беспрецедентного уровня мирового сотрудничества, необходимого для снижения террористической угрозы открытым, уязвимым мировым обществам.

Активизация сотрудничества между США/НАТО и Россией в противодействии идеологической основе терроризма

Для России основной проблемой, связанной с терроризмом, является угроза, исходящая из Чечни и близлежащих регионов Северного Кавказа. Еще до событий 11 сентября президент России Владимир Путин пытался привлечь внимание международной общественности к тренировочным лагерям террористов в Афганистане и проникновению радикально настроенных исламистских групп в Евразию и на Балканы[4)]. Сразу же после

[4)] Более подробно о реакции Владимира Путина на проблемы терроризма для России см. Шерил Кросс. «Поворот Путина в сторону Запада: Россия, США/НАТО и война с терроризмом после событий 11 сентября», в *Посткоммунистические страны в глобализирующемся мире* (*Post-Communist Countries in the Globalizing World*), под ред. Константина Худолея (Санкт-Петербург, Россия: газета Санкт-Петербургского государственного университета, 2004 г.); а также Шерил Кросс. «Отношения России с Соединенными Штатами/НАТО

событий 11 сентября Путин был первым из мировых лидеров, предложивших поддержку администрации президента Буша. Путин назвал ситуацию в Чечне и атаки 11-го сентября «угрозой всему цивилизованному миру» [5]. И действительно, д-р Айман Аль-Завахири в книге «Рыцари под знаменем пророка» рисует картину, когда чеченские и кавказские маджахеды присоединяются к так называемому «маджахедскому исламскому поясу к югу от России», который вовлекает сочувствующих мусульман из Центральной Азии, Афганистана, Ирана, Турции, и разрастаясь, таким образом, на восток до Пакистана, сливается с движениями маджахедов в Кашмире [6].

Не существует официальной статистики о количестве мусульман в России. Цифры колеблются от 3 миллионов до 30 миллионов. Большинство источников называют цифру от 18 до 20 миллионов человек, которые в основном проживают в крупных городах, Волжско-уральском регионе и регионах Северного Кавказа [7]. Демографическая тенденция показывает снижение рождаемости среди православного населения России и рост рождаемости среди мусульманского населения страны. Это в свою очередь предполагает возможную смену политического и социального влияния в будущем. В то время, как большинство российских мусульман, которые, в основном, являются последователями суннитских, ханафистских и суфистких традиций, мирно исполняют религиозные обряды, приверженцы антисуфистского нового исламского движения, а также радикальные шахиды и салафисты стремятся к общей цели, а именно к «праведному Халифату» или к установлению фундаменталистского исламского государства [8].

Несмотря на то, что в России не было такой масштабной террористической атаки, которая бы унесла сразу тысячи жизней, как это произошло 11-го сентября в Соединенных Штатах, тем не менее за последние несколько лет страна пострадала от целого ряда террористических актов.

в глобальной войне против терроризма под руководством США». *Journal of Slavic Military Studies* (*Журнал военных исследований в славянских странах*), 2006 г. А также см. Рубин Азизян «Российско-американские стратегические отношения после событий 11 сентября», статья была озвучена на 35-й Национальной конвенции Американской ассоциации содействия славянским исследованиям, Торонто (20–23 ноября 2003 г.).

[5] Для дальнейшего анализа мотивов Путина в ответ на события 11 сентября см. Кросс. «Поворот Путина в сторону Запада».

[6] См. Айман Ал-Завахири. «Рыцари под знаменем пророка» (Лондон, Аль-Шарк аль-Авсат, по-арабски), отрывки переведены на английский в *FBIS Translated Text*, документ № GMP200201080000197 (2 декабря 2001 г.).

[7] Для обсуждения и подтверждения данных о численности мусульманского населения в России см. Ширен Т. Хантер. «Ислам в России: политическая идентичность и безопасность» (Нью-Йорк: М. Е. Шарп, 2004), 42–45.

[8] По теме различных исламских и радикально исламистских движений в России см. Хантер. «Ислам в России», 46–93; а также Дмитрий Горенбург. «Россия столкнулась с радикальным исламом». *Современная история* (октябрь 2006 г.).

Например, взрывы жилых домов в Москве и Волгодонске в 1999-м году; вторжение Шамиля Басаева в Дагестан в 1999-м году и объявление исламского джихада России; захват заложников в театре на Дубровке в октябре 2002-го года; взрывы в метро; а также взрывы на борту двух пассажирских авиалайнеров в августе 2004-го года, которые были совершены чеченскими террористками-смертницами. Кульминацией этих событий был трагический захват школы в Беслане в сентябре 2004-го года, который вызвал такой же общественный резонанс в России, как события 11 сентября в США.

Чеченцы обладают четко выраженной идентичностью, которая сложилась за многие века, и историей противостояния русским — наследие, которое проявляется в традиции горцев восхвалять смерть в бою против значительно превосходящего по силе врага. После распада Советского Союза в 1991-м году, чеченцы осознали, что у них есть возможность примкнуть к волне освободительных движений народов Балтии, Центральной Азии и Кавказа, которые добивались признания своей государственной независимости. И хотя первоначально в основе чеченского конфликта лежали внутренние, а не внешние причины, со временем конфликт приобрел международный характер. Две чеченские войны и конфликты на Южном Кавказе и Центральной Азии послужили поводом для проникновения международных экстремистских вахабитских сетей, которые финансировали закупки оружия и военную подготовку, а также поставляли воинов джихада. Имеются документальные подтверждения, что Аль-Каида посылала своих солдат для подготовки в Чечню [9)].

Ситуация с Чечней, скорее всего, останется проблемной для российского руководства. В результате миграции, которая последовала за вторжением вооруженных сил России в 1996 и 1999 гг., чеченское население рассредоточилось по всей России. В основных городах страны были созданы общины, которые могут быть использованы для оказания поддержки террористическим организациям. Помимо желания получить автономию от Москвы, у чеченцев есть также территориальные притязания на часть Ставропольского края и Дагестана.

Концепция национальной безопасности России от января 2000 года определяет терроризм как «серьезную угрозу национальной безопас-

[9)] Об участии Аль-Каиды в событиях на Кавказе см. Игорь Плугатаев «Местные конфликты 2005/Вялая война с Халифатом», *Независимое военное обозрение*, 49 (декабрь 2005 г.); «Аль-Каида среди чеченцев», *Christian Science Monitor* (7 сентября 2004 г.); «Подозреваемый в проведении терактов в Европе прошел подготовку в Аль-Каиде», *CNN.com* (6 февраля 2003 г.), доступ на `http://www.cnn/2003/US/02/06/sprj.irq.alqaeda.links`; а также Ариель Кохен. «После Масхадова: исламский терроризм угрожает Северному Кавказу и России», *Backgrounder Report* No. 1838 (опубликован Heritage Foundation) 1 апреля 2005 г., доступ на `http://www.heritage.org/Research/RussiaandEurasia/upload/76370_1.pdf`.

ности» и утверждает, что «международный терроризм проводит открытую кампанию по дестабилизации Российской Федерации…» [10]. Московские чиновники ввели законодательные меры борьбы с внутренними террористическими угрозами и начали упорядочивать отношения между антитеррористическими организациями в разных регионах страны. [11] Как сказано в Концепции национальной безопасности, международное сотрудничество имеет приоритетное значение для ответной реакции России на террористическую угрозу: «борьба [с терроризмом] требует единства усилий всего международного сообщества… Следует устанавливать эффективное сотрудничество с другими государствами и их правоохранительными органами, а также между международными организациями, призванными бороться с терроризмом… Необходимо широко использовать международный опыт по борьбе с этим явлением, а также создать отлаженный механизм для противостояния международному терроризму» [12]. Министр иностранных дел России Сергей Лавров подтвердил, что «глобальный характер террористической угрозы свидетельствует, что безопасность в сегодняшнем мире неделима… Мы должны нести коллективную ответственность за сохранение этого мира безопасным… Борьба с терроризмом должна объединять государства, а не сталкивать их друг с другом» [13].

После событий 11 сентября были достигнуты определенные успехи в российско-американском двустороннем сотрудничестве в области борьбы с терроризмом, в том числе: согласие России на размещение военных баз в первую фазу глобальной войны с терроризмом; взаимодействие ФБР и ФСБ в области перехвата партий оружия, предназначенного для террористов; а также сотрудничество по перекрытию источников финансирования террористов.

Российско-американская рабочая группа по борьбе с терроризмом является основным механизмом, способствующим установлению двустороннего сотрудничества в области противодействия терроризму. Рабочая группа включает в себя как региональные (Афганистан, Балканы, Центральная Азия, Юго-Восточная Азия и т. д.), так и функциональные подгруппы (разведывательные, правоохранительные, по предотвращению распростра-

[10] Концепция национальной безопасности Российской Федерации. *Российская газета* (18 января 2000 г.).

[11] «Россия: терроризм способствует волне нового законодательства». *Независимое военное обозрение* (8 апреля 2005 г.); а также В. И. Молтенской, Ю. А. Мартесенюк и С. Г. Чекинов. «Об организации анти-террористической деятельности государства». *Военная мысль*, 1 (2005).

[12] Концепция национальной безопасности Российской Федерации. *Российская газета* (18 января 2000 г.).

[13] Сергей Лавров. Заявление на 59-й сессии Генеральной Ассамблеи ООН, 23 сентября 2004 г., опубликовано в *International Affairs* (Москва) 6 (2004).

нения ОМП, по перекрытию финансовых потоков террористам, по борьбе с наркотиками)[14]. Говоря о группе, ее участники как из Вашингтона, так и из Москвы отмечают, что если до событий 11 сентября 2001 года работа группы носила более «общий», «теоретический» характер, то в дальнейшем она превратилась в проблемно-ориентированный орган с четким расписанием и сроками выполнения определенных функциональных задач.[15]. Участники также заметили, что на официальных заседаниях стараются не поднимать спорные вопросы, такие как вторжение в Ирак и права человека в Чечне[16]. Однако, обе стороны говорят о том, что у них была возможность обсудить эти и другие сложные проблемы на менее формальных заседаниях и при личной беседе[17].

И участники из США, и участники из России подчеркивают, что не следует переоценивать потенциал и успехи рабочей группы, но в то же время ее деятельность, безусловно, помогла в достижении согласия по отдельным вопросам, способствовала укреплению доверия и сыграла роль в решении важных конкретных задач по обеспечению безопасности. Обе стороны утверждают, что периодические заседания послужили важным форумом для обмена информацией, расширяющим возможности для противостояния террористическим вызовам на многочисленных фронтах.

Что касается взаимодействия России и НАТО в области противодействия терроризму, то совещания в рамках первого Совместного постоянного совета (СПС) Россия—НАТО потерпели провал во время войны в Косово в 1999-м году, потому что российская сторона сочла, что Совет не обеспечил России соответствующего влияния на принятие НАТО решений. С приходом к власти Путина подход России к внешней политике стал прагматичным: связи с Западом важны для будущей безопасности стра-

[14] Государственный Департамент США/Отдел пресс-службы. Общее заявление для прессы Российско-американской рабочей группы по противодействию терроризму, 1 апреля 2004 г.

[15] Интервью автору дали: Андрей А. Чупин, бывший глава отдела по Северной Америке в Министерстве иностранных дел Российской Федерации, март 2004 г.; Нерисса Дж. Кук, Директор отдела политики и глобальных проблем, Бюро по делам Европы и Евразии Государственного департамента США, апрель 2004 г. и ноябрь 2004 г.; а также Владимир Андреев, заместитель директора отдела новых вызовов и угроз, Министерство иностранных дел Российской Федерации, июнь 2005 г.

[16] Там же.

[17] Например, заместитель секретаря по политическим делам Николас Бёрнс и замминистра иностранных дел Сергей Кисляк отметили на пресс-конференции, которая состоялась после заседания рабочей группы в декабре 2005 года, что пока предложенное спорное законодательство по вопросам регламентации работы Неправительственных организаций в России не является частью формального диалога, имеет смысл рассматривать эти и другие вопросы в форме личного дипломатического обмена параллельно с официальными заседаниями рабочей группы. Комментарии для прессы, сделанные заместителем секретаря по политическим делам Николасом Бёрнсом и замминистра иностранных дел Сергеем Кисляком, *Особняк* (Москва) (2 декабря 2005 г.).

ны и подъема экономического уровня жизни. Несмотря на решительный протест России против расширения НАТО в 90-е гг., Путин стремился к сотрудничеству со странами НАТО в области противодействия терроризму. Основным инструментом взаимодействия стал Совет Россия—НАТО, учрежденный в Риме в мае 2002-го года вместо СПС. Совет Россия—НАТО предоставил России возможность прямого участия в заседаниях по принятию решений государствами членами НАТО, в то время как согласно регламенту СПС, Россия могла высказать свою точку зрения только после того, как эти решения уже были приняты.

НАТО и Россия сделали конкретные шаги по укреплению сотрудничества в области контртерроризма, включая официальное осуждение террористических актов; заявления, подтверждающие готовность коллективно бороться с терроризмом; а также определение отдельных областей взаимодействия [18]. В 2002-м году Совет Россия—НАТО финансировал совместные конференции, посвященные роли вооруженных сил в борьбе с терроризмом. Генерал-полковник Ю. Н. Балуевский в *Военной мысли* положительно отозвался об этих заседаниях и уровне «взаимопонимания» между Россией и НАТО относительно необходимости как «предупреждения» террористических актов, так и средств, необходимых для борьбы с терроризмом [19]. Периодически НАТО и Россия созывали рабочие группы, которые занимались разработкой мер безопасности и противодействия терроризму. В своей работе они использовали опыт, извлеченный из террористических актов на общественном транспорте в Лондоне и Москве. План действий России-НАТО в отношении терроризма призывал к «практическому» и «целенаправленному» обмену разведывательными данными по оружию массового поражения, уничтожению избытков боеприпасов, контролю за перемещениями переносных зенитных ракетных комплексов и т. д., что способствовало углублению сотрудничества [20].

Совсем недавно сотрудничество России и НАТО в области противодействия терроризму перешло на новый уровень в связи с программой «Активные усилия» (Operation Active Endeavor). Эта программа предусматривает обеспечение связи между боевыми кораблями России и НАТО и первый

[18] «Совет Россия—НАТО единодушен в осуждении недавних террористических актов в России», 7 сентября 2004 г.

[19] Ю. Н. Балуевский. «Россия и НАТО: Принципы взаимоотношений, проблемы и перспективы сотрудничества». Военная мысль 6 (2003), 12–17; «Россия присоединяется к партнерству по соглашению о статусе вооруженных сил», 21 апреля 2005 г., доступ на `http://www.nato.int/docu/update/2005/04-april/e0421a.htm`.

[20] «План действий по терроризму России-НАТО», 9 декабря 2004 г., доступ на `http://www.nato.int/docu/basictxt/b041209a-e.htm`; также см. «Совет Россия—НАТО приходит к согласию в отношении Плана по борьбе с терроризмом», 8 декабря 2005 г., доступ на `http://www.nato.into/docu/update/2004/12-december/e1209b.htm`.

в истории случай развертывания инструкторской команды НАТО на борту российского боевого корабля. Программа «Активные усилия» появилась из главы 5, которая служила ответной реакцией на события 11-го сентября. В феврале 2006-го года министры обороны Совета Россия—НАТО встретились в Таормине, Италия, для обмена мнениями по приоритетным целям на оставшийся 2006-й год и далее. Особый акцент был сделан на продолжение сотрудничества в области противодействия терроризму, включая обмен разведывательными данными и совместную оценку угроз.

Российско-американская рабочая группа по противодействию терроризму создала основу для общих и тематических консультаций и сотрудничества. Несмотря на некоторое напряжение в отношениях между двумя странами в целом, общие интересы Соединенных Штатов и России в области противодействия терроризму привели к сотрудничеству в этой области. Недавние инициативы в области противодействия терроризму в рамках Совета Россия—НАТО помогли рассеять сомнения Москвы, основанные на том, что прежний СПС был «слишком расплывчатым» и «неопределенным»[21)]. Что касается НАТО, инициативы в области развития сотрудничества по противодействию терроризму помогают достичь цели в определении четких установок на 21-й век для проверенного и испытанного альянса. Так, после событий 11-го сентября был заложен фундамент для расширения сотрудничества между США/НАТО и Россией в области противодействия терроризму. Попытки затронуть «сердца и умы» уязвимых слоев общества и противодействовать идеологическим мотивировкам, побуждающим современные экстремистские группы к насильственным действиям, могут вывести сотрудничество США/НАТО и России в области противодействия терроризму на новый уровень. Разрабатывая общие подходы, США, НАТО и Россия будут способствовать созданию широкой поддержки во всем мире, направленной на разоблачение источников, идеологически подпитывающих современные террористические сети.

[21)] Среди прочих комментариев можно процитировать слова д-ра Андрея Келина, заместителя директора Департамента европейского сотрудничества Министерства иностранных дел Российской Федерации, который делает вывод, что Совет Россия—НАТО «уже показал свою жизнеспособность и эффективность». Он также замечает, что цели Римского Саммита, прошедшего в 2002-м году, были достигнуты путем установления сотрудничества между Россией и НАТО в области терроризма, распространения оружия массового поражения и торговли наркотиками. См. Андрей Келин. «Россия—НАТО: на пути к новому уровню взаимодействия». *International Affairs* (Москва) 51:1 (2005), 34–42.

Трансатлантическое сообщество и вопрос противодействия идеологической основе терроризма

После событий 11-го сентября Соединенные Штаты решились на глобальный подход к борьбе с терроризмом, в то время как Россия и другие европейские государства направили больше сил и средств на борьбу с внутренними террористическими угрозами. Тем не менее, международное сотрудничество трансатлантического сообщества в области противодействия терроризму продолжает развиваться и выходить на новые уровни, в том числе это касается обмена разведданными, пресечения финансовых потоков террористам, а также внутренней обороны государств. С недавними террористическими атаками в Европе и России пришло понимание, что эффективная стратегия не может разделять внутренние и международные аспекты угрозы и заниматься ими по отдельности[22]. Новые документы и программы НАТО выделяют сотрудничество в области противодействия терроризму как одну из важнейших миссий Альянса.

В 2005-м году Европейский Союз издал *Стратегию ЕС против радикализации и вербовки кадров для терроризма*, в которой специальное внимание уделяется экстремизму:

> Радикализация отдельных приверженцев мусульманской веры в Европе является достаточно новым явлением. Даже те территории Европы, в которых радикализация на сегодняшний день не является серьезной проблемой, или те территории, на которых не существует крупных мусульманских общин, могут стать целью для экстремистов. ЕС будет продолжать развивать коллективное понимание проблем, прислушиваясь к мусульманам и др, сопоставляя внутреннее положение разных стран и утверждая европейское понимание ситуации… Ключом к нашему успеху будет уровень участия неправительственных групп — сообществ, религиозных властей и других организаций — в противодействии экстремистам и осуждении их криминальных действий[23].

[22] Интервью автора с сотрудниками Министерства иностранных дел Российской Федерации, 27 октября 2006 г. См. Джеймс Витер. «Работа в прогрессе: Кампания Объединенного королевства против радикализации», статья была озвучена на конференции под названием «Противодействие идеологической основе терроризма/извлеченные уроки и политика в будущем: междисциплинарные, теологические и международные региональные перспективы», Центр им. Дж. Маршала, Гармиш-Партенкирхен, Германия, 25 сентября 2006 г. (издано в этом томе).

[23] Стратегия Европейского Союза против радикализации и вербовки кадров для терроризма (Брюссель: Совет Европейского Союза, Брюссель, 25 ноября 2005 г.).

«Белая книга» о внутренней безопасности и борьбе с терроризмом (*White Paper on Domestic Security Against Terrorism*) была издана в 2005-м году. В документе излагается доктрина Франции по борьбе с терроризмом, причем целый раздел посвящается так называемой «Битве идей»[24]. Хотя французы отвергают понятие «войны» с терроризмом, под «борьбой» или «битвой» идей они понимают стратегию, сосредоточенную на продвижении демократических ценностей как основы для противодействия религиозному экстремизму[25]. Джеймс Витер замечает, что в стратегии Великобритании внимание концентрируется на неравенстве и отсутствии возможностей, способствующих мусульманской радикализации, на законодательстве по борьбе с радикализмом, а также на привлечении к сотрудничеству мусульманского сообщества[26].

Российские политические деятели уже подчеркивали, что очень важно избежать реального или надуманного «столкновения цивилизаций» с мусульманским миром. С точки зрения Москвы, Россия обладает уникальным культурным опытом, который мог бы помочь построению «моста» между конфликтующими Западными и исламскими государствами. Например, д-р Михаил Титаренко, директор института по Дальнему Востоку Российской Академии наук, сделал следующее заявление:

> ... культура и традиции являются такими же важными, как и экономика, ... для взаимопонимания и сотрудничества... Это также очень важно для определения особой роли России как моста и фактора в Западно-Восточном диалоге. В России очень богатая мусульманская культура, это культура двадцати миллионов россиян, проживающих в России. И этот факт можно использовать для того, чтобы показать уважение к тому вкладу, который внесла мусульманская и арабская культура в мировую культуру... Лидеры мусульманских стран развили комплекс неполноценности, потому что их чувство собственного достоинства уязвлено. Они с готовностью пойдут на контакт с любой державой, с любой культурой, если с ними будут говорить на равных[27].

---

[24] «Победа в битве идей». *«Белая книга» о внутренней безопасности и борьбе с терроризмом* Париж, 2005, 113–123.

[25] Там же.

[26] Противодействие международному терроризму: стратегия Объединенного королевства, См. 6888 (июль 2006 г.); также см. Витер. «Работа в прогрессе», 12.

[27] Михаил Тетаренко. «Исламский мир и российская внешняя политика». *International Affairs* (Москва) 4 (2005).

Российские официальные лица и политологи признают важность привлечения мусульманских сообществ в процесс формирования мировоззрения и противостояние радикальному насильственному исламизму. В. И. Молтенской, Ю. А. Мартсенюк и С. Г. Чекинов в статье в *Военной мысли* за 2005-й год утверждали, что «основные усилия» антитеррористической правительственной деятельности должны включать «идеологическую и религиозную сферу… активное взаимодействие с религиозными и духовными лидерами, поддерживающими государство в войне против терроризма, и распространение с их помощью идеи, что никакая религия в ее чистой форме не одобряет методы борьбы, используемые террористами…» [28]. В 2004-м году администрация президента России проводила конференцию, в которой принимали участие чиновники, занимающиеся внешней политикой, духовные лица ислама и лидеры других вероисповеданий, представители различных культурных организаций, а также послы из нескольких мусульманских стран [29]. Целью этой конференции было наметить пути создания «последовательной стратегии в отношениях между Россией и исламским миром» [30].

Анатолий Сафонов, спецпредставитель президента Российской Федерации (позиция была создана в 2004-м году) по проблемам международного сотрудничества в борьбе против терроризма и международной преступности, также выступил за прекращение злоупотребления религией террористами и за противодействие идеологии терроризма, и назвал эти две проблемы основными для международного сотрудничества [31]. Обращение к идеологическим основаниям терроризма согласуется с основным направлением российской политики противодействия терроризму — борьбой с «корнями» терроризма [32].

И хотя, безусловно, существуют различия между Соединенными Штатами, Европейскими государствами и Россией в расстановке акцентов, терминологии и стратегии борьбы с идеологическими основаниями террористических движений, между ними существует единодушное согласие в по-

[28] Молтенской и другие. «Об организации». 22–27.

[29] ИТАР-ТАСС, агенство новостей. «Москва проводит конференцию «Ислам против терроризма»», 3 июня 2004 г.

[30] Там же.

[31] Интервью автора с д-ром Владимиром Андреевым, замдиректора Департамента по новым угрозам и вызовам Министерства иностранных дел Российской Федерации, а также с д-ром Игорем Неверовым, директором Департамента по Северной Америке Министерства иностранных дел РФ, 27 октября 2006 г.; а также дискуссии с представителями Государственного департамента США, ноябрь 2006 г. Эта точка зрения возникла после трагических событий в Беслане в 2004-м году, а Анатолий Сафонов был первым назначен на этот пост.

[32] Интервью автора с д-ром Игорем Неверовым, директором Департамента по Северной Америке Министерства иностранных дел РФ, 27 октября 2006 г.

нимание того, что решение этой проблемы является крайне важным для глобальных контртеррористических усилий. Только посредством расширения сотрудничества, обсуждения проблем и действенного сотрудничества эти страны в будущем смогут повысить уровень координации и эффективность противодействия насильственному религиозному экстремизму.

Информационная революция: идеологический фактор в «холодной войне» и современная борьба с терроризмом

Рост информационных технологий, особенно сети Интернет, создает еще одну идеологическую угрозу, с которой куда сложнее бороться, чем в период Холодной войны. Исламистские экстремисты проявили себя как талантливые манипуляторы на киберарене. Террористические группы мастерски используют технологию Интернет для вербовки последователей, распространения литературы, незамедлительной трансляции обезглавливания и других жутких актов насилия. Эффективное управление информационным каналом является крайне важным для формирования представлений и суждений зрителей, а также для влияния на последующие действий этих зрителей. Все усилия должны быть направлены на обеспечение надежного, последовательного, заслуживающего доверия, честного и эффективного управления информацией [33)].

Мы должно работать совместно с партнерами по всему миру с тем, чтобы установить правильный баланс между обеспечением гражданских свобод и защитой свободных и открытых сообществ от угрозы терроризма. Когда государства забывают об основах демократического государства, пытаясь бороться с религиозным экстремизмом? [34)] Как далеко могут зайти государства в своих попытках установить контроль на веб-сайтах, например, в случаях, когда террористы используют эти веб-сайты для вербовки и для организации актов насилия? Кибер сфера будет бросать новые вызовы демократическим обществам, стремящимся определить необходимую степень контроля над технологиями, использующимися в целях разрушения и насилия.

[33)] Эту точку зрения высказал подполковник Фред Т. Кравчук в «Стратегическая связь: интегральный компонент при проведении операции по подавлению восстаний», *Connections*, 5:3 (Зима 2006 г.)

[34)] Французский политолог д-р Себастьян Пейруз заяляет, что остатки авторитаризма наблюдаются в некоторых государствах Центральной Азии в вопросе религиозной свободы и толерантности к экстремистским тенденциям ислама. Себастьян Пейруз, лекция «Ислам и политика в Центральной Азии: реакция на глобализацию», Международный центр для ученых им.Вудроу Вильсона, Вашингтон, 21 ноября 2006 г.

Распространение посланий, в которых делается ударение на общечеловеческие ценности (семья, достоинство, справедливость), разделяемые Западными (или немусульманскими), и мусульманскими обществами, может помочь найти точки соприкосновения и улучшить преставления друг о друге. В этих посланиях обязательно должно звучать уважение к достижениям и к вкладу различных обществ и порядков. Телевидение, средства массовой информации и информационные технологии должны максимально использоваться для того, чтобы привлечь внимание общественности к зверствам, которые пережили жертвы терроризма. Сообщения о страданиях жертв могут помочь разработать мировые нормы, которые клеймили бы теракты. Усилия международных дипломатических миссий и организаций, занимающихся вопросами безопасности, по разоблачению взглядов и действий исламистов должны постепенно привести к созданию единого мирового мнения, однако они могут привести и к росту влияния экстремистов.

Мы должны понимать, что противодействие идеологической основе терроризма включает в себя значительно больше, чем ответную реакцию в сфере общественной дипломатии. Умело управляемая общественная дипломатия, получающая достаточную финансовую поддержку, является одним, но не единственным, компонентом общей стратегии. При разработке стратегии ПИОТ мы должны начать с основополагающей предпосылки о важности восприятия и каждого элемента, воздействующего на восприятие. Мы должны постоянно анализировать и оценивать, как интерпретируются наши действия, поведение, послания и политика.

Ни одно государство не сможет самостоятельно противостоять мировой угрозе исламистского экстремизма, тем более уничтожить ее. Стратегия должна разрабатываться и координироваться многочисленными международными партнерами. Сохранение высокого уровня коммуникации будет крайне важным для формирования и совершенствования стратегии, а также для поддержания плодотворного сотрудничесва, необходимого для решения этой сложной проблемы.

Международные объединения, занимающиеся вопросами развития сотрудничества в области противодействия терроризму, такие как Совет Россия—НАТО и двусторонняя Российско-американская рабочая группа по противодействию терроризму, прорабатывают конструктивные пути решения этой проблемы в будущем. Любая стратегия, обращенная к «сердцам и умам», возникающая в результате работы многосторонних или двусторонних международных групп, обязательно должна привлекать к сотрудничеству мусульманские государства и общины. При создании программ ПИОТ и использовании различных информационно-коммуникационных источников и сетей необходимо привлекать к работе партнеров, знакомых с местной культурой и традициями. Нам следует поощрять потенциаль-

ный вклад неправительственных организация, духовных лиц и религиозных лидеров, преподавателей и представителей частного сектора в борьбу с идеологией терроризма. И хотя взаимодействие осуществляется на традиционном государственном уровне и на уровне общин, параллельно должен использоваться и этот путь решения проблемы на базе совместных стратегических целей.

Построение действенного плана мероприятий по противодействию идеологической притягательности религиозного экстремизма

При попытке построить всестороннюю стратегию привлечения «сердец и умов» следует постоянно разъяснять, что мы отрицаем всякое «столкновение культур» или «столкновение цивилизаций» между Западом и мусульманским миром, которое бы могло привести к насильственной конфронтации. Существуют значительные различия между немусульманскими и мусульманскими культурами, ценностями и традициями. Однако, если мы позволим этим различиям перерасти в крупномасштабную войну религий и цивилизаций, как это уже бывало в прошлом, то понесем огромные потери в силу большей доступности средств массового поражения в современной обстановке международной безопасности. Обязательным условием работы является стимулирование достижения консенсуса между немусульманскими и мусульманскими государствами, приверженными защите гражданского населения от зла, которое несут те, кто искажает учение ислама в своих политических целях.

И хотя уже были случаи успешного переубеждения молодых приверженцев террористических движений посредством вмешательства религиозных властей, по большому счету, надежда на изменение или переориентацию фундаментальных целей или убеждений исламистских воинствующих экстремистов крайне мала. Фанатизм сторонников экстремизма связан с их виденьем прославленного прошлого и с яростью, направленной против международного порядка, который они характеризуют как несправедливый, аморальный, отделенный от Бога и всего духовного. Автор нескольких фундаментальных текстов по исламистскому радикализму Саид Абуль Аля Маудуди еще десятки лет назад сказал о необходимости изменения международного порядка: «Целью исламского джихада является уничтожение правления неисламской системы и установление вместо нее исламской системы правления. Ислам не будет ограничиваться проведением этой революции в одном государстве или нескольких странах; цель ислама провести

всеобщую революцию».[35] Поскольку оправдание насилия можно найти как у радикальных духовных лиц, так и в разных толкованиях к Корану, то и светские общины, и правоверные мусульмане сталкиваются с трудностями, определяя суть экстремистских постулатов.[36]

Это вовсе не означает, что во всем мире светские открытые сообщества окружены непримиримыми мусульманами. «Террористы-духовники» на протяжении всей истории возникали с тем, чтобы искажать религиозные традиции многих верований и культурных контекстов. Влиятельные представители мировых мусульманских общин открыто отрицают тактику и взгляды исламистских экстремистов. Король Иордании Абдулла II призвал «безмолвствующее большинство мусульман» «отобрать нашу религию у громогласных, жестоких и невежественных экстремистов…»[37]. Великий шейх мечети Аль-Азхар в Каире, шейх Мухаммед Саид Танвати, постоянно выступает против актов терроризма. Являясь представителем высшей духовной власти мусульман-суннитов, он осудил взрывы террористов-самоубийц, направленные против израильтян, и назвал «экстремизм» «врагом ислама»[38]. Как показывает статистика опросов общественного мнения, проведенных Pew Research Center, значительно уменьшилось число мусульман, поддерживающих взрывы, осуществляемые террорстами-самоубийцами, и другие акты насилия. Интересно, что эти показатели в Иордании снизилась после теракта в Аммане в 2005-м году[39]. Очевидно, что послания воинствующих радикальных групп отвергаются мусульманским сообществом, так как они идут вразрез с фунда-

[35] Саид Абул Ала Мавдуди. «Джихад в исламе», лекция была прочитана в Лахоре в день Икбала (13 апреля 1939 г.), переиздано в *Voices of Terror*, под ред. Лакуера, 398.

[36] Сообщалось, что Осама Бен Ладен получил одобрение от духовного лица из Саудовской Аравии на использование ядерного оружия против Соединенных Штатов. В книге *Исцеляя сердца верующих* (*Healing the Breast of the Believers*) Марк А. Габриель обратил внимание на то, что Ал-Завахари приводит логическое объяснение убийств ни в чем не повинных случайных людей, цитируя следующую строфу из Корана: «Боритесь с ними так, чтобы Аллах наказал их вашими руками, опозорьте их, победите их и исцелите душу верующих, устраните злобу из сердец верующих…», Сура 9: 13–15; перевод Марка А. Габриеля *Путешествие в разум* (*Journey Into the Mind*), 56–57; а также см. Осама Бен Ладен. «Джихад против евреев и крестоносцев». *World Islamic Front Statement* (23 февраля 1998 г.).

[37] «Король Иордании Абдулла II прзывает к сдержанности». *Washington Post* (14 сентября 2005 г.).

[38] См. «Великий шейх осуждает теракты террористов-самоубийц», *новости BBC* (4 декабря 2001 г.); а также см. «Духовное лицо осуждает теракты террористов-самоубийц», *новости BBC* (11 июля 2003 г.).

[39] До теракта в Аммане в 2005-м году 57 процентов населения Иордании считали теракты с использованием террористов-самоубийц «часто» или «иногда» оправданными. Эта цифра упала до 27 процентов после теракта. См. *Мусульмане Европы более сдержаны: великий раздел: как представители Запада и мусульмане видят друг друга* (*Europe's Muslims More Moderate: The Great Divide: How Westerners and Muslims View*

ментальными учениями и ценностями ислама и не соответствуют реалиям современной жизни.

Исламистские экстремисты представляют собой лишь малую долю от 1,4 миллиардов мусульман по всему миру. И у нас не должно быть иллюзий относительно возможности влияния на закоренелых радикально настроенных террористов. Стратегия противодействия идеологической основе терроризма должна состоять в том, чтобы распознавать, а затем дискредитировать и изолировать исламистских экстремистов. Объединение с мусульманским сообществом в совместной борьбе против идеологии, которая наносила и продолжает наносить ущерб открытым сообществам, а также пресечение попыток исламистов завербовать новобранцев — в этом залог долгосрочного успеха. Осама Бен Ладен пытался охарактеризовать этот конфликт как религиозную войну и, говоря о «новом крестовом походе Америки против исламских государств», призывал *умму* «объединиться во имя защиты ислама» [40)]. Нужно четко определить врага: угроза исходит от небольшого экстремистского ядра, а не от ислама или всего мусульманского сообщества. Неспособность точно определить источник угрозы приведет к тому, что экстремистам будет легче манипулировать большим числом представителей мусульманского сообщества, с тем чтобы достичь своих политических целей, представляя этот конфликт как войну против ислама.

В 2006-м году и Совет Россия—НАТО, и Российско-американская рабочая группа по противодействию терроризму определили проблему идеологической основы терроризма как приоритетное направление для развития сотрудничества в области противодействия терроризму [41)]. Существуют несколько областей, в которых Соединенные Штаты, НАТО и Россия, совместно с мусульманскими государствами, могли бы начать создавать комплексный подход для борьбы с воинствующим религиозным экстремизмом. Хотя это, конечно, не полный список возможностей, но некоторые идеи для дальнейшего обсуждения и рекомендаций возникли в ходе

Each Other) (Вашингтон: The Pew Global Attitudes Project, 22 июня 2006 г.); доступ на `http://pewglobal.org/reports/pdf/253.pdf`.

[40)] «Корреспондент встречается с оппозиционным лидером Бен Ладеном», *Channel* 4 (Лондон) (20 февраля 1997 г.); «Пакистан берет интервью у Осамы Бен Ладена», Исламабад, Пакистан (18 марта 1997 г.), процитировано Кристофером М. Бланчердом в «Аль-Каида: утверждения и развитие идеологии», *CRS Report for Congress* (26 января 2006 г.; обновлен 24 января 2007 г.), доступ на `http://fpc.state.gov/documents/organization/80743.pdf`.

[41)] Интервью автора с Игорем А. Нееровым, директором Департамента по Северной Америке Министерства иностранных дел Российской Федерации, октябрь 2006 г.; интервью с Нерисса Дж. Кук, директором Департамента политики и глобальных проблем (Бюро по делам Европы и Евразии, Государственный департамент США), ноябрь 2006 г.; а также периодические дискуссии с Керемом Альпом, Совет Россия—НАТО, НАТО, ноябрь-декабрь 2006 г.

недавних дискуссий, посвященных этому вопросу, в Центре им. Маршала (в дискуссиях участвовали представители многих стран). Выдвинутые предложения касаются практической сферы взаимодействия, и, возможно, помогут в определении основополагающих элементов долгосрочной комплексной стратегии для борьбы с идеологической основой терроризма.

Диалог и координация работы организаций на внутреннем и международном уровне

Ни одно государство не обладает достаточными ресурсами, чтобы финансировать «узкопрофессиональные встречи» с их бесконечными дискуссиями, дающими минимальный результат. С другой стороны, невозможно разработать эффективную стратегию противодействия идеологической основе терроризма без постоянного проведения международных дискуссий и консультаций. Прогресс, достигнутый мировой общественностью в общем определении терроризма, был результатом честных и открытых обсуждений предпосылок и перспектив в ООН и на других международных форумах. Министр иностранных дел России Сергей Лавров недавно подтвердил необходимость «борьбы с терроризмом по единым стандартам…» [42)]. Создание «единых стандартов» или хорошо скоординированной стратегии может быть достигнуто только через постоянный и непрерывный диалог.

В настоящее время установлены механизмы для проведения периодических дискуссий по различным подходам, темам и сообщениям между различными учреждениями правительства США, занимающимися вопросами противодействия идеологической основе терроризма (государственными, оборонными, разведывательными и др.). Совместные семинары и постоянные консультации между Пентагоном, Государственным Департаментом и другими государственными органами правительства США будут способствовать совершенствованию координации и более глубокому пониманию проблем. Осуществление эффективной стратегии по противодействию идеологической основе терроризма потребует не только оптимального уровня координации между внутренними учреждениями, но и приведет к следующему этапу: привлечению международного участия к межведомственным форумам правительства США. Совет Россия—НАТО, Россий-

[42)] «Государства, скрывающие террористов, должны выполнять указы ООН». Новости (10 декабря 2005 г.). Для ознакомления с интересной дискуссией о необходимости введения международного определения терроризма см. Боаз Ганор. *Головоломка противодействия терроризму: руководство для лиц, принимающих решения* (*The Counter-Terrorism Puzzle: A Guide for Decision Makers*). Лондон: Transaction Publishers, 2005, 1–24.

ско-американская рабочая группа по противодействию терроризму и другие группы, занимающиеся объединением государств для противодействия терроризму, создают перспективные механизмы для направления ресурсов на развитие общих подходов к борьбе с вызовами.

Дискредитация намерений исламистских экстремистов

Глобальная стратегия обращения к «сердцам и умам» должна предлагать приемлемые альтернативы тоталитарным представлениям и насилию во имя джихада, которые выдвигаются исламистскими экстремистами. Демократия, справедливость, правовые нормы, экономические возможности — притягательны для всех, даже в случаях, когда общества разделены по этно-религиозным принципам и находятся в неблагоприятных экономических условиях. Те средства, которые в демократических системах позволяют участвовать в политическом процессе или помогают разрешить споры, могут стать необходимыми и эффективными альтернативами насилию и терроризму в достижении политических целей. Тем не менее, построение демократического государства в обществе, где отсутствуют выше названные традиции, потребует терпения и времени, здесь явно недостаточно простого проведения выборов. Импульс к построению демократии должен возникнуть внутри самого общества. Потребуются десятки лет, а не месяцы или годы, для построения демократических институтов и гражданского общества.

Серьезным вызовом становится тот факт, что светсткие сообщества во многих отношениях противоречат исламу. Как сказал профессор Саид Хусейн Назр из Тегеранского университета,

> Если бы мусульмане отделили религию от общественной жизни (которая впоследствии стала бы светской, как это произошло на Западе во времена Ренессанса), то таким образом они бы предали доктрину Единства, которая лежит в основании исламского послания. Их действия были бы направлены против сунн пророка и шли бы вразрез с 14 веками поддержания исламской традиции [43)].

Секуляристские и модернистские силы внутри мусульманского сообщества столкнулись с проблемой баланса приверженности исламским ценностям и традициям, с одной стороны, и концепциями демократического управления, с другой.

[43)] Саид Хусейн Назр. *Ислам, религия, история и цивилизация* (*Islam, Religion, History and Civilization*). Сан Франциско: Harper Collins, 2003, 113.

Вместо того, чтобы изобретать строгую систему измерения демократического развития, основанную на опыте Запада, надо понять, что более реалистичным и плодотворным будет проведение процесса демократизации в зависимости от уникальных условий каждого отдельного общества. А попытки навязать демократические обычаи или стандарты сопротивляющимся сообществам лишь усилят их неприятие. Специалисты из мусульманских сообществ часто говорят об «унижении» или «негодовании», которое испытывают эти сообщества при «столкновении с Западом» [44]. Демократия должна поощряться, но нельзя обострять вышеназванные чувства, пытаясь насадить систему управления тогда, когда общество еще не готово к переменам.

Для того, чтобы развенчать идеологические установки радикального исламизма, необходимо привести взгляды Аль-Каиды и других исламистских боевиков на будущее международного порядка. Мировоззрение исламистского экстремиста включает в себя такое понятие, как выход из кризиса посредством насилия. Однако перспектива установления фанатичного тоталитарного теократического порядка вряд ли покажется привлекательной или реалистичной сегодняшнему международному сообществу или большинству мусульманского населения.

Женщины мусульманских сообществ готовы внести свой вклад в демократизацию и в противодействие терроризму. Число работающих женщин в мусульманских сообществах постоянно увеличивается, и крайне важным является продвижение общественных ценностей посредством влияния женщин внутри семьи. Бен Ладен постоянно повторял, что при режиме талибов Афганистан стал моделью исламского государства [45]. Несмотря на различия в понимании «уважения к женщинам» Запада и мусульман, остается бесспорным тот факт, что при режиме талибов женщины подвергались крайней несправедливости, лишениям и унижениям [46]. Отношение к женщинам при режиме Талибан, к счастью, не является показателем условий жизни женщин во всем мусульманском мире. Очень важным так-

[44] Ладан Бороманд и Роя Бороманд. «Террор, ислам и демократия». *Journal of Democracy*, 13:2 (апрель 2002 г.), 16.

[45] «Программа Аль Жазира Бен Ладена», *Al Jazeera Television* (Доха, Катар), 10 июня 1999 г.); процитировано Бланчардом в «Аль-Каида: утверждения и развитие идеологии», 3

[46] На вопрос «С уважением ли мусульмане относятся к женщинам» 27 процентов немусульман в Великобритании ответили Да, а 59 процентов ответили Нет; в США 19 процентов сказали Да и 69 процентов ответили Нет; во Франции 23 процента ответили Да и 77 процентов дали отрицательный ответ; в Германии цифры составили 17 процентов Да и 80 Нет. На вопрос «относятся ли на Западе к женщинам с уважением» мусульманское население в Иордании ответило 38 процентов Да и 50 процентов Нет; в Пакистане 22 процента Да и 52 Нет; в Индонезии 38 процентов Да и 53 процента Нет; в Турции 42 процента Да и 39 процента Нет. «Мусульмане в Европе более сдержаны/Великий раздел».

же является осознание того, что основные установки и цели исламистских джихадистов неприемлемы для большинства женщин международного сообщества XXI века. Необходимо поощрять участие мусульманских женщин в дискредитации деспотических намерений исламистов, их тактики насилия, и суицидного разрушения.

Государства, участвующие в борьбе с терроризмом, должны продолжать уделять внимание и выделять ресурсы на борьбу с общественными силами, создающими условия для разжигания терроризма. Привлекательность Хамас в Палестине и Хезболлы в Ливане объясняется их способностью удовлетворить социальные потребности обществ, разрушенных войной. Соединенные Штаты, Россия и другие страны оказывают поддержку частному сектору, таким образом помогая борьбе с терроризмом. Социально ответственный частный бизнес может создать экономические возможности, программы подготовки специалистов и рабочие места для тех, кто находится в отчаянии. Мы должны предоставить альтернативу потенциальным новобранцам террористических движений.

Вовлечение мусульманских сообществ: ограничения и обязательства

Представляется очевидным, что лидеры мусульманских сообществ должны сделать основной вклад в дискредитацию террористической идеологии. На назначенных руководителях и на религиозных властях мусульманских общин лежит ответственность за письменное толкование и обучение в образовательных и религиозных учреждениях. Победа в соперничестве идей будет зависеть от проницательности, направленности и ответственности настоящего и будущих поколений мусульманского сообщества.

Ведущие специалисты в области политики и ислама оценивают духовные основания и традиции ислама как лучшее решение для противодействия идеологии исламистского терроризма. Д-р Абдеслам Маграуи, директор Мусульманской мировой инициативы в Институте мира в Соединенных Штатах, говорит о том, что «проблема ‘религиозного экстремизма’ в мусульманском мире — это идеологический вызов, с которым надо бороться при помощи исламской гуманности и прогрессивных традиций» [47)]. Иранские ученые Ладан Бороманд и Роя Бороманд написали в *Journal of*

[47)] Доклад д-ра Абдеслама Маграуи был сделан на конференции «Противодействие идеологической основе терроризма/извлеченные уроки и политика в будущем: междисциплинарные, теологические и международные/региональные перспективы», Центр им. Дж. Маршала, Гармиш-Партенкирхен, Германия, 15 сентября 2006 г.; а также д-р Абдеслам Маграуи «Внешняя политика США и исламское обновление», Институт мира США, Специальный доклад № 164 (июль 2006 г.) (перепечатано из оригинала в этот выпуск).

Democracy, что «до Аль Каиды и Хезболлы история ислама не знала случаев неограниченного насилия». Они утверждают: «Самоубийство путем намеренного лишения жизни женщин, детей, людей всех религий и классов — не будем забывать, что среди сотрудников Мирового торгового центра были и мусульмане — не имеет никакого отношения к исламу…» [48)]. Недавно в Лондоне и других городах прошли общественные дискуссии между мусульманскими духовными наставниками и лидерами исламистских экстремистов. Они показали, что внутри ислама существуют резкие различия в толковании Корана и его учений.

Вновь, во избежание неправильной трактовки или недопонимания, хотелось бы повторить: любые антитеррористические действия трансатлантического инициативы (Совет Россия—НАТО, Российско-американская рабочая группа по противодействию терроризму и другие), направленные на борьбу с идеологической основой терроризма, должны реализовываться во взаимодействии с мусульманским миром. Светские государства с преобладающим числом мусульманского населения могут внести особый вклад в построение отношений с мусульманскими государствами. Естественно, существуют пределы вовлечения мусульманских сообществ. Порой очень сложно разглядеть законный источник власти в исламе. В исламе отсутствует единая религиозная власть, как, например, Папа римский в католической церкви. Расплывчатый характер власти в исламе делает веру уязвимой со стороны экстремистских духовных самозванцев, использующих ее в своих целях. Это, в свою очередь, усложняет работу законных и ответственных религиозных властей по исправлению искажений или неправильных толкований святых учений. Помимо этого многие мусульманские религиозные лидеры опасаются сотрудничать с западными или светскими государствами, потому что близость с этими странами может негативно сказаться на их репутации и даже безопасности. Слишком очевидная американо-трансатлантическая кампания по продвижению сдержанности вместо экстремизма в мусульманском мире будет, скорее всего, непродуктивной. Сложность заключается в том, чтобы оказывать сбалансированную поддержку мусульманским сообществам, противостоящим терроризму, не навязывая при этом своей позиции.

Вынесенные уроки и практические результаты

Одним из наиболее эффективных методов борьбы с идеологическими основами исламистского экстремизма является проведение совместных встреч профессионалов в области противодействия терроризму (из

[48)] Бороманд и Бороманд «Террор, ислам и демократия», 6

военных организаций и структур безопасности), для обмена мнениями по противодействию идеологической поддержке терроризма. Эти дискуссии обычно носят конкретный характер, вырабатывают четкие рекомендации, основанные на реальном опыте борьбы с террористами, мотивированными религиозным экстремизмом, в разных странах. На этих дискуссиях обсуждается широкий спектр вопросов, в том числе контроль над действиями радикальных террористов, распространение литературы, методы пресечения вербовки, совместная работа с имамами в целях консультирования молодых новобранцев. Предпринимаются также попытки обратиться к глубинным причинам, лежащим в основе проблемы, например, выработать инструменты для борьбы с бедностью.

Такой взаимный обмен поможет достичь «практических результатов», обеспечит военных профессионалов и специалистов, занимающихся вопросами безопасности, методами для противодействия идеологической основе терроризма. Кроме того, создание каналов коммуникации между профессионалами, занимающимися вопросами противодействия терроризму, увеличит обмен разведданными, что еще больше поможет в борьбе с радикализмом. Периодический обмен профессионалами для развития инициатив в области противодействия терроризму между странами, входящими в Совет Россия—НАТО и в Российско-американскую рабочую группу по противодействию терроризму, также поможет в достижении практических результатов. Повторюсь: эти военные и занимающиеся вопросами безопасности антитеррористические сети являются основой для повседневной успешной борьбы с терроризмом по всему миру.

Традиционные религии и диалог между религиями

Ориентирующееся на государственные структуры дипломатическое сообщество недооценило потенциальный положительный вклад основных мировых религий в разрешение конфликтов[49]. Сложность и возможные

[49] В основном отредактированном томе под названием *Религия, недостающее измерение управления государством* (*Religion, the Missing Dimension of Statecraft*). участники рассуждают о том, что после окончания «холодной войны» традиционные религии делают очень важный вклад в разрешение конфликтов, связанных с самоидентификацией. Один из редакторов, Дуглас Джонсон, говорит следующее: «Если посмотреть на конец века и далее, то можно увидеть, что проблемы предотвращения и разрешения конфликтов становятся еще острее, чем в прошлом. Как показывают сегодняшние проблемы, связанные с этнической и националистической враждой, независимо, носят они внутренний или межгосударственный характер, их очень сложно разрешить посредством дипломатического компромисса. Раз добиться примирения сложно, то потребуются разнообразные подходы. И, возможно, действенными окажутся те, которые ищут ключ в давно укоренившихся человеческих отношениях, а не в государство-центрических доктринах. Сегодня от внешней политики и от религиозных

последствия неудач в борьбе против террористической угрозы делают поддержку религиозных властей и духовных лиц разных конфессий еще более важной.

Политические деятели по всему миру признают тот факт, что традиционные религии посредством межконфессионного диалога могут сыграть важную роль в противостоянии террористическим вызовам. На саммите Большой восьмерки в Санкт-Петербурге, который состоялся в июле 2006-го года, президент России Владимир Путин призвал к «широкому диалогу религий для отражения атаки экстремистов»[50]. Эту же мысль высказала в январе 2006-го года президент Филлипин Глория Масапагал-Арроя. Отмечая снижение угрозы терроризма и успех переговоров о мире в Миндано, она отметила, что диалог между религиями — «лучшее противоядие терроризму»[51]. Карен Хьюз, заместитель государственного секретаря по делам общественной дипломатии и связям с общественностью, выделила важность диалога религий в своем недавнем интервью в Праге:

> … основные мировые религии имеют много общего. Все основные мировые религии считают, что мы должны попытаться жить в мире и любви друг к другу, что мы должны возлюбить Бога и ближнего своего. Они все учат тому, что жизнь бесценна и что неправильно отнимать жизнь у невинных людей. Очень важно говорить о таких вещах. Разумеется, у нас есть различия. Но у нас столько общего. Я считаю очень важным стимулирование такого диалога[52].

Доверие к террористам может быть подорвано более высокими властями, которые борются с использованием религии в политических целях. Во время недавнего Саммита Большой восьмерки лидеры основный мировых религий (христианство, ислам, иудаизм, буддизм и другие) подписали совместное заявление, в котором говорится следующее о терроризме и экстремизме:

деятелей требуется гораздо более глубокое понимание человеческого фактора в конфликте и его разрешении, чем это было до сих пор». См. Дуглас Джонсон «Вступление: политика за пределами власти» («Introduction: Beyond Power Politics») в *Религия, недостающее измерение управления государством*, под ред. Дугласа Джонсона и Синтии Сэмпсон. Оксфорд: Oxford University Press, 1994, 7.

[50] «Президент России Путин призывает к диалогу религий для противостояния экстремизму», РИА Новости (3 июля 2006 г.). Путин заметил, что «незнание основ истории религии делает человека, особенно молодого человека, уязвимым перед лицом опасного экстремистского движения».

[51] «Президент Филлипин продвигает диалог религий в борьбе против террора», *Manila Times* (28 января 2006 г.).

[52] «Помощник госсекретаря США продвигает диалог религий», *RFE/RL* (11 июня 2006 г.).

> Мы осуждаем любые формы терроризма и экстремизма, а также попытки оправдать их с помощью религии. Мы считаем своим долгом противостоять политической, этнической и религиозной неприязни. Мы скорбим о действиях псевдо религиозных групп, разрушающих свободу и здоровье людей, а также этическую обстановку в сообществах. Основным вызовом сегодня является использование религии для разжигания ненависти или для оправдания преступлений против личности, морали и гуманности. Эту проблему можно разрешить только посредством образования и укрепления моральных основ. Школы, средства информации и наставления религиозных лидеров должны вернуть нашим современникам полное знание их религиозных традиций, которые призывают их к миру и любви [53)].

Папа Иоанн Павел II также признавал потенциальный вклад межрелигиозного диалога в борьбе с терроризмом: «Я уверен, что великие религии человечества должны взаимодействовать друг с другом в целях устранения социальных и культурных причин терроризма. Сделать это можно через утверждение величия и достоинства человека, а также развивая сознание единства человеческой расы» [54)]. Поездка его преемника Папы Бенедикта XVI в Стамбул в ноябре 2006-го года была очень важным шагом для улучшения отношений между христианскими и мусульманскими общинами, а также для создания основы сотрудничества в области противодействия самым серьезным вызовам, с которыми столкнулось международное сообщество в двадцать первом веке.

Идеологические основы современных насильственных религиозных экстремистских групп должны быть подвергнуты теологическому опровержению. Межрелигиозный диалог может привлечь внимание мировых общин к искажениям этими группами священных писаний, а также к несоответствию жестоких террористических актов миролюбивым учениям основных мировых религий. Работая вместе, религиозные власти смогут препятствовать эскалации основного конфликта двадцать первого века, связанного с религиозно-этническими и культурными различиями.

На международном уровне следует привлекать представителей религиозных общин на форумы, где обсуждаются вопросы, как противостоять воздействию терроризма на «сердца и умы». В местных общинах важными являются каналы распространения авторитетных источников информации

[53)] «Заявление саммита в Москве, прочитанное на встрече Большой восьмерки», *Catholic World News* (18 июля 2006 г.).

[54)] «Межрелигиозный диалог может помочь в противодействии терроризму, говорит Папа римский», *Catholic World News* (12 декабря 2003 г.).

и истинных исламских учений. Возможно, ни одна проблема в области безопасности не отвечает принципам правительственного и религиозного взаимодействия так, как противодействие экстремистски настроенному терроризму.

Межкультурные исследования/взаимодействие в области образования

Терроризм не являлся основной областью изучения теории безопасности в США. Во времена конфронтации между США и СССР огромные ресурсы были вложены в развитие научных центров по изучению Советского Союза. Ведущие ученые занимались исследованиями и оказывали содействие в выработке политики и стратегии. Терроризм изучался в ряду других научных дисциплин, и количество программ или центров, занимающихся вопросами терроризма, как в США, так и в других странах было немного (Центр по изучению терроризма и политического насилия университета Сент-Эндрюса в Шотландии был одним из них). Ограниченное выделение ресурсов на изучение вопросов терроризма привело к нехватке экспертов и исследований в этой области.

При формировании идеологической кампании нам потребуется более глубокое понимание мотивов исламистских террористов. Современная научная и политическая литература предлагает разные объяснения тому, почему люди решают присоединиться к террористическим движениям: рациональный фактор; групповая психология; низкая самооценка/компенсация; религиозные побуждения; уровень образования и подготовки[55)]. И хотя существуют многочисленные параметры терроризма, для того, чтобы найти правильные методы борьбы с террористической идеологией, необходимо понять, что лежит в основе мотивации террористов или почему они добровольно соглашаются на теракты-самоубийства.

Дополнительное целевое и скрупулезное исследование различных национальных и культурных контекстов поможет в выработке разнообраз-

[55)] Джераль М. Пост. «Психологические операции и противодействие терроризму». *Joint Force Quarterly* 37 (2003); Марк Сагман. «Понимание террористических сетей». Филадельфия: University of Pennsylvania Press, 2004; Марта Креншоу. «Логика терроризма: поведение террориста — это результат стратегического выбора». *Корни терроризма: психология, идеология, теология, душевное состояние* (*Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*) под ред. Уолтера Райха (Вашингтон: Woodrow Wilson Center Press and Johns Hopkins University Press, 1998); Ролберт А. Пэйп. *Умереть для победы: стратегическая логика террористов-самоубийц* (*Dying to Win: The Strategic Logic of Suicide Terrorism*). Нью-Йорк: Random House, 2005; а также Мия Блум. *Умереть, чтобы убить: притягательность терроризма-самоубийства* (*Dying to Kill: The Allure of Suicide of Terrorism*). Нью-Йорк: Columbia University Press, 2005.

ных мер по противодействию экстремизму. Новые организации, такие как Центр борьбы с терроризмом, учрежденный в 2003-м году в военной академии США Вест-Поинт, должны расширить наше понимание источников террористической мотивации и помочь в формулировании политики [56]. Программа НАТО «Наука за мир и безопасность» является великолепной моделью совместных международных исследований. Совет Россия—НАТО может предпринять финансирование совместных исследовательских проектов с участием как ученых, так и специалистов в области безопасности/политики из СРН и мусульманских государств, вовлеченных в работу по противодействию терроризму и идеологической основе терроризма. Активизация такого научного сотрудничества приведет к углублению знания и межкультурного понимания источников насильственного экстремизма, и, возможно, даст значительные политические результаты.

Важность правильного донесения намерений через послания и политику

Крайне важно, чтобы попытка завоевать сердца и умы потенциальных последователей исламистских экстремистских движений не воспринималась как манипулирование обществом или как поворот к другой идеологии. И хотя для установки коммуникации мы должны использовать новейшие технологии информационной революции, нельзя переоценить важность элемента доверия к посланнику. Для того чтобы усилия общественной дипломатии были эффективными, передаваемые сообщения не должны противоречить существующей политике и поведению. Иначе любые попытки общественной дипломатии или коммуникации будут восприниматься как простая пропаганда или как попытки манипулировать сознанием. Всесторонняя стратегия по противодействию идеологической основе терроризма должна включать в себя постоянную оценку воздействия на политические приоритеты и предпочтения. Стремление к согласованности наших намерений и действий заглушит обвинения в лицемерии и двойных стандартах и поможет оказать благотворное влияние на сердца и умы следующего поколения мусульман.

Обсуждения, посвященные противодействию идеологической основе терроризма, с нашими коллегами с Ближнего Востока будут постоянно приводить к поиску решений Израильско-палестинского кризиса. Воз-

[56] Недавно Центр издал очерк, в котором, например, «выделяются самые влиятельные люди среди мыслящего класса джихадистов, то *как* они думают, а также *где* уязвимые места их идеологии». См. *Атлас по идеологии боевиков* (*Militant Ideology Atlas*) под ред. Джаррета Брахмана. Вест Поинт: Центр по борьбе с терроризмом, ноябрь 2006 г.).

можно, разрешение этой проблемы не остановит терроризм, но улучшение ситуации поможет оздоровить психологический климат в регионе и уничтожит основной источник гнева террористов, способствующий вербовке все новых кадров. Обновленное международное внимание к решению таких важных политических проблем, как урегулирование Израильско-палестинского конфликта, а также интеграция мусульман в Европейские и другие сообщества, продемонстрирует искренность намерений, лежащих в основе борьбы с источниками воинствующего религиозного экстремизма, который угрожает безопасности и свободе всего мирового сообщества.

Швейцарская система центров реагирования на компьютерные атаки

Т. Ирлет

Мое выступление покажется вам отличным от того, к чему вы привыкли. Я бы хотел вам рассказать, какие мы принимаем в Швейцарии меры для установления системы ACERT. Могу вам сказать, что в Швейцарии пока нет системы ACERT — команды быстрого реагирования на нарушения компьютерной безопасности.

Я работаю на Министерство обороны, ARMASUISSE. ARMASUISSE — это организация, которая занимается снабжением. Мы покупаем все необходимые материалы для швейцарской армии. Лично я занимаюсь исследованиями и консультирую по вопросам снабжения.

Мое выступление будет разделено на три большие части. Первая часть сравнительная: как отличается Швейцария от России; в чем состоят эти различия. Во второй части я расскажу о политической обстановке в Швейцарии. А третья часть будет посвящена проблемам, с которыми мы боремся при отсутствии команды реагирования на компьютерные аварии, и нашим действиям в этой области.

Россия — огромная страна по сравнению со Швейцарией. По площади территорий соотношение между двумя странами примерно равняется 440:1, а что касается населения, то соотношение здесь будет примерно 122:1. Швейцария по размеру примерно равняется Московской области, не включая федеральный город Москву. То есть Швейцария — очень маленькая страна, а это имеет свои последствия. Мощь нашей нации во много раз меньше России. Экономики наших стран тоже сильно различаются. В Швейцарии, в основном, преобладает малый и средний бизнес, хотя есть и несколько крупных компаний. Два больших банка UPS и Credit Swiss, фармацевтическая химическая компания, и всемирно известная Nestle Food. Экономика страны базируется на малом и среднем бизнесе, а это имеет свои последствия. Государство не может обеспечить информационную безопасность. Разумеется, в крупных компаниях или в банках работают люди, которые занимаются вопросам информационной безопасности, но у малого и среднего бизнеса таких возможностей нет.

Поэтому часто возникают дискуссии, должно ли государство или правительство заниматься этим вопросом.

Где находится Швейцария? Швейцария находится в самом центре Европы. И мы окружены Европейским союзом, что очень важно для нашей политики, так как она во многом зависит от Европейского союза. Мы координируем наши действия, хотя мы можем действовать и независимо, но мы все-таки находимся в самом центре Европы, поэтому предпочитаем сотрудничать с ЕС.

Швейцария не является членом НАТО, но все ее страны-соседи, кроме Австрии, являются членами НАТО. Так что мы формируем некий островок «Швейцария — Австрия», который окружен НАТО. Мы не можем действовать абсолютно независимо от НАТО. Если нам надо решить какую-то крупную проблему, то мы должны обратиться к НАТО и согласовать свои действия с ней. В то же время мы обладаем и независимостью. На рис. 1 показан вид Цюриха. Цюрих находится в центре Швейцарии. На

Рис. 1. Вид Цюриха на фоне озера, холмов и гор

переднем плане вы видите здания и озеро г. Цюрих, за ними лежат холмы, а на заднем фоне вы можете увидеть горы. Эти горы пролегают с Востока на Запад или наоборот. Так что если вы хотите торговать с северной или южной Германией или с Италией, вам придется проделать это через горы. К сожалению, в Альпах не так много хороших дорог. Через Швейцарию проходит одна из исторических дорог, которая называется Готтард. По бо-

кам этой дороги лежат горы, и если в начале дорога довольно простая, то потом начинаются повороты. Левая часть дороги ведет в равнину, а правая в Милан. Разумеется, теперь мы построили туннель, но движение по дороге очень интенсивное, поэтому очень часто с севера на юг возникают пробки.

Какова политическая обстановка в Швейцарии, где нам предстоит построить систему, которая смогла бы защитить малый и средний бизнес? А политическая обстановка следующая. На вершине власти находится народ. Это верховная власть. Народ обладает властью говорить парламенту и правительству, как следует работать. Народ избирает парламент, а тот в свою очередь избирает правительство и Верховный суд, который должен следить за тем, чтобы все работало, как этого желает народ. В правительство входят семь министерств во главе с семью министрами, которые занимают свои позиции довольно долгое время. Это следующие министерства: Министерство иностранных дел, Министерство внутренних дел, Министерство юстиции и полиции, Министерство финансов, Министерство экономики, Министерство обороны, и Министерство окружающей среды, транспорта, и связи. В правительство также входит Федеральная канцелярия. Президентом Швейцарии избирается каждый из семи министров. Хотя его функции скорее носят репрезентативный характер.

Кто мог бы войти в команду быстрого реагирования на нарушения компьютерной безопасности? Естественно, прежде всего, это полиция. Полиция должна также следить, чтобы ничего не случилось с информационной безопасностью или в информационном пространстве. В команду также надо включить какое-нибудь министерство. Прежде всего, Министерство финансов. Наверное, это вас удивит, но именно министерство финансов — это главный поставщик информационных технологий для администрации. И хотя на них работают специалисты в области информационных технологий (ИТ), но как я уже упоминал раньше, у нас, в основном, развит малый и средний бизнес. Поэтому, армия должна защищать экономику Швейцарии от атак на киберпространство страны. И последняя это Федеральная канцелярия, так как именно эта организация занимается обеспечением конфиденциальности данных в Швейцарии. Она должна охранять конфиденциальность личных данных людей.

Если вы хотите создать команду быстрого реагирования на нарушения компьютерной безопасности, то главная проблема, которая здесь возникает, связана с тем, чтобы не злоупотребить данными, не нарушить право людей на конфиденциальность.

В Швейцарии есть и признаки федералистской системы. Мы очень маленькая страна, но в нашей маленькой стране признаются четыре государственных языка. Мы говорим по-немецки, по-французски, по-итальянски,

и по-ретроромански. И каждый официальный документ должен быть опубликован на всех четырех языках. В нашей маленькой стране 26 кантонов или, как вы их называете в России, областей. Хотя кантоны очень маленькие, они довольно-таки автономны. Они обладают своими собственными конституциями, которые не противоречат национальной конституции, у них есть свои парламенты, правительства, и суды. Полиция тоже относится к обязанностям кантонов, а не государства в целом. В принципе, у нас нет национальной полиции. Хотя делами полиции занимается Министерство юстиции и полиции. Кантоны также собирают налоги с граждан.

Как я вам уже говорил, наша система очень демократична. Народ обладает властью, а правительство не такое уж и сильное. Я не знаю ни одно другое государство, где правительство было бы таким же слабым, как в Швейцарии. Каждый закон, принятый правительством, выносится на референдум. Так что если 50 тысяч граждан подпишут петицию, что хотят вынести тот или иной вопрос на референдум, то вся нация должна проголосовать за или против закона. Большинство определяет, принять закон или нет. У нас также есть, так называемая, народная инициатива. Если 100 тысяч граждан потребуют внести изменения в конституцию, то необходимо провести референдум, чтобы решить вносить изменения или нет.

Политические деятели и правительство очень внимательно следят за тем, чего желает народ. Если они хотят что-то сделать и не уверены, согласится ли с этим большинство, то они должны провести референдум или народную инициативу.

Теперь о швейцарской армии. У нас действует обязательная воинская повинность. То есть, в принципе, каждый мужчина в возрасте от 20 до 33 лет должен раз в год на несколько недель уходить в армию. Он хранит свое оружие и даже боеприпасы дома. Кстати, не так давно парламент дал на это добро. Это пожелание людей хранить оружие дома. С другой стороны, это показывает, что правительство доверяет народу, а также то, что власть находится в руках граждан. Это также является доказательством того, что швейцарская армия и народ едины. Так что получается, что руководство промышленности и бизнеса в армии, а командиры армии в промышленности, то есть они все работают совместно, как одна семья.

Мы очень маленькая страна, поэтому еще давным-давно мы поняли, что нам надо быть нейтральными. Мы сохраняем нейтралитет, то есть мы не поддерживаем ни ту, ни другую сторону ни в конфликте, ни в войне. Швейцария всегда пытается соблюдать нейтралитет и одинаково поддерживает обе стороны. Это помогло нам избежать участия в первой и второй мировых войнах. Мы были окружены фашистскими Германией и Италией, но мы сохраняли нейтралитет и избежали участия в войне. Но сегодняш-

ние проблемы глобальные, и нам необходимо сотрудничать с другими организациями, в первую очередь, с НАТО, ЕС, ООН и т. д. Мы пытаемся сотрудничать так, чтобы при этом сохранять нейтралитет.

Какие действия мы предприняли за последнее время? Во-первых, на нашу политику сильно повлияло, так называемое, дело Фишена. Это был огромный скандал в политической жизни Швейцарии. В 1988 году общественности стало известно, что швейцарская администрация собирала данные на 900 тысяч граждан и продолжает собирать материалы на граждан. В основном, администрации удалось собрать информацию о Социалистической партии и о профсоюзах. Я уверен, что мои поездки в Восточную Европу тоже были зафиксированы в этих документах. И хотя в Швейцарии наличие таких документов особого значения не играет, но все равно такой скандал имел место быть. Так что с тех пор конфиденциальность очень важна. В 1997 году правительство столкнулось с новой угрозой. В том же году были проведены стратегические маневры. Правительство поставило целью определить, применимы ли имеющиеся процессы для борьбы с угрозами информационной безопасности, угрозами в киберпространстве. Все министры и большая часть администрации участвовали в этих маневрах. В результате оказалось, что Швейцария нуждается в обеспечении информационной безопасности. Нам необходим кризисный штаб, который мог координировать работу в случае кризиса в области информационной безопасности. Такой штаб был организован в 2001 году и были проведены первые маневры с тем, чтобы посмотреть, какова будет реакция людей и какие меры надо принять в случае кризисной ситуации. В 2001 году 150 человек встретились специально для проведения этих маневров. Это были представители администрации, частного бизнеса (волонтеры) и исследователи (волонтеры). Они хотели узнать, если швейцарские организации будут атакованы, то обладают ли они достаточными средствами, чтобы дать отпор. В результате выяснилось, что для обеспечения информационной безопасности необходимо создать еще две организации, помимо кризисного штаба. Эти организации назвали «Соня» и «Мелани». Да, это женские имена, но у них есть другое значение. «Мелани» означает сигнальный и аналитический центр по информационной безопасности. Это организация, в которую должны обращаться люди при возникновении проблем. Если у организации, компании или обычного человека возникают проблемы, то они могут обратиться в этот центр с тем, чтобы их проблемы детально рассмотрели. Главная цель этой организации следить за тем, что происходит в информационном пространстве. «Мелани» должна предупреждать правительство в случае киберкризиса. Но это организация должна быть реагирующей, а не деятельной. Она должна ждать, пока что-то не случится. Ясно, что эта организация должна работать совместно с командой быстрого реагиро-

вания на нарушения компьютерной безопасности, но она не должна быть деятельной, пока этого не потребуют обстоятельства. Она должна слушать, но не предпринимать действий. Деятельной должна быть «Соня» — специальная организация по обеспечению безопасности. Штаб этой организации должен разработать рекомендации для правительства и администрации, и информировать всех заинтересованных лиц: кантоны, компании и т. д. Она должна координировать действия. В штаб вошли представители администрации и бизнеса, которые символизируют швейцарское общество. Так что вот две организации, которые у нас существуют. Они очень близки по своему смыслу команде быстрого реагирования на нарушения компьютерной безопасности НАТО. Мы считаем, что таким образом нам удастся сохранить конфиденциальность частной информации.

Некоторые методологические и организационные проблемы обнаружения и предупреждения компьютерных атак на критически важные объекты информационной инфраструктуры Российской Федерации

А. М. Ивашко

В современных условиях нормальное и эффективное функционирование объектов критически важной инфраструктуры государства существенно зависит от информационных систем, обеспечивающих их деятельность. Устойчивое функционирование таких информационных систем, получивших название «объекты критически важной информационной инфраструктуры» (КИИ), является важным для успешного экономического и социально-политического развития общества, обороноспособности и безопасности любого государства.

На основании изложенного объективно существующие угрозы информационной безопасности критически важной инфраструктуры государства требуют осуществления как практических шагов по выработке адекватных мер защиты, так и создания соответствующей нормативной и правовой базы, определяющей политику государства в данной области, включая вопросы международного сотрудничества.

Обозначенный круг проблем активно исследуется научными, политическими и бизнес кругами разных стран. Например, в Швейцарии Центром изучения безопасности при Национальном технологическом институте (`www.ethz.ch`) регулярно публикуются исследования по проблеме защиты критических инфраструктур в различных странах. В материалы Центра за 2006 год впервые включена Российская Федерация. В США Центр стратегических и международных исследований (CSIS) проводит семинары в рамках Программы по защите национальных критических инфраструктур (`www.csis.org`). Странами-участницами ASEAN, Китаем, Россией и США ежегодно проводится семинар по вопросам борьбы с кибертерроризмом и защите национальных критически важных инфраструктур (`www.aseanregionalforum.org`).

Анализируя материалы этих семинаров, можно сделать вывод о том, что меры по защите объектов критически важной информационной инфраструктуры в разных странах сходны. К их числу относятся следующие:

- *выделение критических секторов* (обычно определяется законом или доктриной национальной безопасности);
- *назначение государственного органа* (*органов*), *ответственного за обеспечение безопасности в выделенных секторах* (как правило — это силовое ведомство, но может быть и межведомственный орган);
- *создание стандартов и методик обеспечения безопасности КИИ* (как правило, для государственного сектора использование стандартов обязательно, для частного сектора они носят рекомендательный характер);
- *создание системы обнаружения и предупреждения компьютерных атак* (*КА*) (Такие системы, также называемые системами реагирования, обычно рассматриваются в широком смысле и включают в себя сбор и анализ фактов компьютерных атак, организацию первичного расследования, ликвидацию последствий, а в некоторых случаях и прямой контроль за обеспечением безопасности конкретных критических систем);
- *организация взаимодействия государственных органов*, *частного сектора и общественных организаций* с целью полного охвата имеющихся информационных ресурсов и привлечения частного сектора и граждан к решению вопросов защиты национальной КИИ.

В этом отношении Российская Федерация не является исключением. Важным современным этапом формирования нормативной правовой базы для реализации перечисленных выше мер является, осуществляемая в настоящее время, разработка проекта федерального закона «*Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры*» (`www.duma.gov.ru`). Данный законопроект в качестве законодательной инициативы внесен рядом депутатов Государственной Думы Федерального Собрания Российской Федерации (М. И. Гришанковым, Ю. Г. Медведевым и другими). Целью законопроекта является установление организационно-правовых механизмов обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры различных видов собственности.

В проекте Закона впервые вводятся такие понятия как:

- критически важный объект информационной и телекоммуникационной инфраструктуры;
- критически важная система;
- критически важный сегмент.

В настоящее время законопроект находится только на начальной стадии обсуждения. Необходим тщательный анализ, как самого текста законопроекта, так и всей нормативной правовой базы в области информационной безопасности. Вместе с тем есть основания полагать, что принятие данного закона позволит решить или определит предпосылки к решению таких организационных и методологических проблем как:

- *определение угроз* информационной безопасности критически важных объектов информационной инфраструктуры;
- *оценка уязвимости таких объектов* от актов незаконного вмешательства и деструктивных информационных воздействий;
- *категорирование критически важных объектов* информационной инфраструктуры в зависимости от негативных последствий, возникающих вследствие прекращения или нарушения их функционирования;
- *разработка требований и реализация мер по обеспечению информационной безопасности* критически важных объектов;
- *создание и функционирование системы обнаружения и предупреждения компьютерных атак*.

Вместе с тем, для создания и функционирования реального объекта, какой должна стать система обнаружения и предупреждения компьютерных атак на КИИ Российской Федерации, требуют своего решения ряд проблем как базового научно-технического и методологического плана, так и организационных.

К базовым проблемам на пути её создания можно отнести следующие:

- *Разработка и обоснование архитектуры эффективной системы обнаружения и предупреждения КА на КИИ*. Необходимо провести анализ КИИ Российской Федерации и на его основе предложить обоснованную архитектуру, эффективную для обнаружения, в том числе, и сложных распределенных во времени и пространстве КА, устойчивую к воздействиям на нее, с приемлемыми порогом ложного срабатывания и временем латентности.

- *Создание верифицированных математических моделей, описывающих процессы взаимодействия сегментов КИИ, а также их реакцию на различные внешние и внутренние воздействия*. Это сложная и ресурсоемкая задача. В случае ее приемлемого решения появится возможность прогнозировать последствия КА и разрабатывать стратегии по их обнаружению и предотвращению.
- *Создание математически обоснованных алгоритмов взаимодействия средств обнаружения и средств защиты*. На первый взгляд простая задача таит в себе много «подводных камней». К ним, в частности, можно отнести DOS-атаки, реализуемые с использованием средств защиты и приводящие к потере значимого функционала защищаемой системы.
- *Разработка математического аппарата, который позволит получать обоснованные численные оценки эффективности методов и средств обнаружения КА*. Понятно, что для реальной оценки эффективности средств обнаружения подходы, основанные на оценке процента выявления опубликованных КА, не подходят. Требуется также найти и обосновать баланс применения сетевых и хостовых средств обнаружения.

Одним из путей предупреждения компьютерных атак на информационные системы является создание комплексной многоуровневой защиты, позволяющей гарантировать с определенным уровнем доверия безопасность системы. Однако реализация такой защиты длительный и, главное, дорогостоящий процесс, практически не реализуемый при массовом информационном обмене, тем более при интеграции разнокатегорийных информационных систем и множественности сервисов. По этой причине применение средств обнаружения компьютерных атак, позволяющих гибко перестраивать имеющиеся, доступные для массового потребителя средства защиты информации в сочетании с налаженной системой реагирования на компьютерные инциденты является разумным компромиссом между гарантированием информационной безопасности и эффективностью функционирования информационной системы.

Данный подход требует *разработки и обоснования требований информационной безопасности систем с учетом применения в них подсистем обнаружения и предупреждения компьютерных атак*.

Сегодня профессиональный поиск компьютерных вирусов (КВ) и их проявлений является отдельной трудоемкой задачей. Современные КВ для маскировки и достижения своих целей широко используют слабости сигнатурных и эвристических анализаторов антивирусных средств (АВС). Видна устойчивая тенденция использования модификаций известных КВ. Так,

например, только КВ семейств MyDoom, Beagle, NetSky насчитывают десятки модификаций в том числе и с использованием различных алгоритмов динамического сжатия и обфускации.

В ближайшее будущее важнейшей научной задачей в этой области будет *создание математически обоснованных алгоритмов выявления модификаций КВ*. Для модификаций КВ применение математических методов по всей видимости даст хорошие решения, однако для выявлении *новых вирусов*, которых стало в этом году на 10 % больше по отношению к 2005 году, построение универсальных методов не так очевидно.

Перейдем к организационным проблемам. Зачастую для нанесения ущерба используется следующая тактика: проникновение на компьютер посредством преодоления сигнатурных и эвристических методов, выполнение деструктивных функций и удаление следов пребывания вредоносного программного обеспечения. Такую тактику использовало, например, семейство троянских программ Encoder. Экземпляры данного семейства с целью финансового шантажа шифровали файлы пользователей. После выполнения указанных действий троянские программы самостоятельно удаляли себя с целевого компьютера. В данной ситуации использование АВС по факту обнаруженного воздействия не даст результатов, так же не принесут желаемого результата и стандартные действия по локализации и восстановлению. Очевидно, что требуется *разработка новых стратегий обнаружения и предупреждения КА и организационных форм для их реализации*.

Эффективность средств обнаружения и предупреждения КА напрямую зависит от используемой технологии процесса обновления баз данных КА.

Обновление связано с решением следующего комплекса задач:

- обеспечение целостности в процессе передачи по каналам связи, аутентификация и идентификация источников информационного обмена;
- оперативность проведения обновления и доступность информационных ресурсов, с которых это обновление производится.

Для реализации системы обновления *достаточно современных средств и методов с использованием криптографии*.

К текущим организационным проблемам обнаружения и предупреждения КА в Российской Федерации следует отнести:

- *взаимодействие с пользователями*, *владельцами систем и сетевыми операторами для получения информации об инцидентах* (*превалирует практика умалчивания об инцидентах*);

- *обеспечение реализации услуг на размещение информационных ресурсов с контролем их использования, в качестве фишинг-страниц или распространителей вирусов*;
- *оказание оперативной и квалифицированной помощи пользователям и администраторам.*

Перечисленные организационные проблемы могут быть решены в рамках партнерства с негосударственными организациями и бизнес сообществом.

В Российской Федерации такие структуры есть. Одной из них является национальная группа реагирования на компьютерные инциденты RU-CERT (`www.ru-cert.ru`). Группа является важной компонентой и активным участником международного форума групп реагирования на инциденты FIRST и европейского агентства сетевой безопасности ENISA. Группа RU-CERT является единой точкой контактов и координатором заинтересованных групп реагирования (CSIRT — Computer Security Incident Response Team) для Российской Федерации.

В функции RU-CERT входит:

- *сбор и анализ фактов компьютерных инцидентов*, имеющих отношение к сетевым ресурсам, расположенным на территории Российской Федерации;
- *реагирование на компьютерные инциденты* с целью их прекращения, предотвращения, восстановления и сбора доказательств;
- *содействие пользователям* в обращении к Интернет-провайдерам и официальным структурам, отвечающим за расследование компьютерных преступлений;
- *взаимодействие с доверенными CSIRT* с целью отслеживания источника атаки и ее прекращения, связь с центрами реагирования производителей (PSIRT и т. д.).

По данным RU-CERT структура инцидентов в российском сегменте сети Интернете в 2006 году выглядит следующим образом:

- 70 % — фишинг;
- 20 % — распространение вредоносных программ и сбор данных;
- 9 % — сканирование или другая активность;
- 1 % — прочее.

Другой организацией, которую можно отнести к числу отраслевых, является созданная общественно-государственным объединением «Ассоциация документальной электросвязи» Межоператорская группа анали-

за инцидентов, сокращенно «МЕГА» (`www.rans.ru`). Она создана летом 2006 года и в настоящее время идет процесс становления.

Среди основных задач «МЕГА» необходимо выделить следующие:

- *формирование и рассылка действенных рекомендаций для операторов*;
- *экспертиза и мониторинг конкретных информационных и телекоммуникационных систем операторов* на предмет уязвимостей и выдача рекомендации по их устранению;
- *круглосуточный прием обращений операторов по поводу инцидентов безопасности*, в том числе, жалобы от любых лиц на действия пользователей, самого оператора-участника или на инциденты, в которых тем или иным образом замешаны средства связи оператора;
- *расследование зафиксированных инцидентов*, взаимодействуя с операторами, производителями, государственными органами;
- *разработка оперативных рекомендаций* по устранению угроз, разрешению инцидентов, ликвидации их последствий и т. п.

В заключение хотелось бы отметить, что, по оценке экспертов, российский рынок информационных технологий растет динамично. Этот факт свидетельствует о том, что решение перечисленных выше проблем очень актуально, в том числе и для развития средств защиты КИИ Российской Федерации.

Комплекс активного аудита распределенных многопользовательских систем

А. В. Галатенко

Аннотация

В работе рассматривается подход к построению системы активного аудита на основе модульной архитектуры с единым управляющим ядром. Описываются компоненты системы, возникшие математические модели и открытые задачи.

1. Введение

В распределенных информационно-вычислительных комплексах, которые созданы на базе практически значимых сетей, необходимым условием эффективности системы их защиты является ее эшелонированность. Необходимость такого подхода к построению системы защиты вызвана целым рядом причин, в том числе:

- отсутствием должного (адекватного современным потребностям) набора механизмов безопасности, заложенных в операционные системы (ОС) на этапе проектирования;
- наличием ошибок в реализации программного обеспечения (ПО) и администрировании системы;
- постоянным появлением новых атак, которые оказываются непредусмотренными, неучтенными или не полностью учтенными при формировании политики безопасности комплекса.

Разумным дополнительным эшелоном защиты представляется система активного аудита. Такие системы предназначены для выявления аномального поведения информационно-вычислительных комплексов, вызванного деятельностью злоумышленников, ошибками легальных пользователей, сбоями программных или аппаратных компонент и других подобных им причин.

Отметим, что системы активного аудита позволяют, во-первых, выявлять атаки на ранних стадиях и предотвращать ущерб и, во-вторых, выявлять успешные атаки, таким образом минимизируя ущерб. Важным следствием выявления атак на ранней стадии является возможность изучения

взаимосвязности различных злоумышленных действий и выявления скоординированных попыток деструктивного воздействия. Подобная функциональность важна при отражении массированных атак на информационно-вычислительные комплексы, в том числе и попыток кибертеррористических воздействий. Выявление успешных атак позволит ограничить область проникновения злоумышленников вглубь системы, таким образом сохраняя ядро информационно-вычислительных комплексов целостным.

Большинство существующих систем активного аудита реализовано как монолитная программа, ориентированная на анализ информации о сетевом трафике на основе выявления сигнатур известных атак (в качестве примера можно привести snort — одну из самых популярных систем активного аудита с открытым исходным текстом [7]). Недостатки такого подхода отмечались, например, в [4]. С другой стороны, существующие системы можно считать хорошим решением подзадачи активного аудита — выявлении ряда сетевых атак. Как следствие, возникает необходимость реализации более общей системы активного аудита, в которую в качестве подкомпонент можно было бы встраивать существующие системы.

Дополнительное требование, которое необходимо предъявить к системе активного аудита — устойчивость к сбоям отдельных программных или аппаратных компонент.

2. Архитектура системы

Рассмотрим два уровня представления архитектуры системы активного аудита: микроуровень и макроуровень.

На микроуровне представим систему активного аудита в виде совокупности модулей четырех типов, к которым относятся модули сбора, преобразования, анализа информации, а также реагирования ([4]).

Опишем функционирование системы на микроуровне. Модули сбора производят извлечение информации из комплекса, который подлежит защите. В качестве источников информации могут служить данные о сетевой активности, регистрационные журналы, следы системных вызовов, данные о загрузке и функционировании отдельных устройств и другие. Собранные данные передаются модулям преобразования. Модули преобразования ориентированы прежде всего на унификацию и фильтрацию поступающих данных для упрощения функционирования наиболее ресурсоемких (интеллектуальных) компонент, которыми являются модули анализа. Модули анализа обрабатывают поступающие на вход отфильтрованные и унифицированные данные и выдают оценку аномальности поведения системы, в идеале указывая на источник аномалии. Отметим, что очень желательна

обратная связь между анализаторами и преобразователями для управления уровнем фильтрации. По результатам анализа возможна та или иная реакция, например уведомление администратора, блокирование сегмента сети, отключение сервиса.

Одной микрокомпоненты системы активного аудита может оказаться недостаточно для контроля большого распределенного комплекса (например, из-за слишком большого объема информации, которую необходимо проанализировать). Как следствие, возникает необходимость введения макроструктуры, позволяющей проводить декомпозицию системы активного аудита на несколько микрокомпонент. Декомпозиция может быть как чисто иерархической, с древовидной структурой, так и допускать циклы (например, для обмена данными между подсистемами одинакового ранга декомпозиции).

Представляется разумным реализовать макроструктуру системы активного аудита средствами микроструктуры. Действительно, модули анализа могут также рассматриваться как источники информации. Таким образом, результаты анализа могут передаваться преобразователям (и далее — анализаторам) других микрокомпонент. Управление на макроуровне разумно реализовать посредством специальной сущности (управляющего ядра).

Структура модулей системы задается в конфигурационном файле. Управляющее ядро отображает содержимое конфигурационного файла в граф системы. По желанию администратора системы может быть проведена оптимизация графа, ориентированная на снижение дублирования передаваемой между модулями информации. В случае сбоя одного из модулей разрушенные связи должны восстанавливаться с помощью других модулей системы. В текущей версии модули реагирования интегрированы с анализаторами; как следствие, задача естественно отображается на графовую модель и сводится к поддержанию связности компонент трехдольного графа ([9]). Действительно, модули могут быть отображены на множество вершин графа. Пара вершин соединяется ребром в том и только том случае, если соответствующие модули осуществляют обмен информацией. Так как связи возможны только между сборщиками и преобразователями и между преобразователями и анализаторами, можно считать, что граф трехдольный. В систему активного аудита может быть привнесена избыточность, реализованная за счет модулей с дублирующейся функциональностью и нескольких путей передачи информации между модулями (в модели различным путям соответствуют кратные ребра). Введем на множестве вершин отношение эквивалентности. Скажем, что две вершины эквивалентны, если соответствующие им модули имеют одинаковую функциональность. Легко увидеть, что данное отношение обладает свойствами симметричности, рефлексивности и транзитивности. Следовательно

можно считать, что каждая доля является объединением непересекающихся классов эквивалентных вершин. Рассмотрим семейство максимальных трехдольных подграфов, порожденных классами эквивалентности. Назовем подграф связным, если в нем есть путь от одной из вершин первого яруса до одной из вершин третьего яруса. Назовем подграф n-связным, если он остается связным после удаления $n-1$ вершины или ребра. Будем рассматривать только связные подграфы. При правильном функционировании системы активного аудита связность выделенных подграфов не должна нарушаться. В случае выхода из строя модулей (удаления вершин) или соединений (удаление ребер) связность может нарушиться. В этом случае необходимо активизировать одну из оставшихся вершин или одно или несколько из оставшихся ребер для восстановления связности. n-связность обеспечивает необходимую для отказоустойчивости избыточность.

Легко видеть, что для достижимости n-связности в максимальном трехдольном подграфе необходимо, чтобы вершин каждого яруса было по крайней мере n (это следует из того, что выход из строя всех вершин одного яруса нарушает связность подграфа).

Также легко понять, что это условие является и достаточным. Действительно, можно произвольным образом занумеровать вершины, соответствующие каждому классу эквивалентности, а затем активизировать связи между j-й вершиной первого яруса подграфа и j-й вершиной второго яруса подграфа, а также между j-й вершиной второго яруса и j-й вершиной третьего яруса подграфа ($j = 1, 2, \ldots, n$). Полученная конфигурация подсистемы, порожденной подграфом, будет обеспечивать n-связность, при этом задействуется минимальное число вершин и ребер (то есть любая конфигурация, в которой активным является меньшее число вершин и/или ребер, не обеспечивает n-связности).

Так как нумерация вершин в классах эквивалентности фиксирована (зависит лишь от класса и не зависит от рассматриваемого подграфа), утверждение о минимальности задействованного числа вершин и ребер остается верным и для всей системы в целом.

В случае, когда вершин в некоторых классах эквивалентности недостаточно, n-связность не может быть достигнута, в этом случае имеет смысл получить максимально возможную избыточность. Например, если в первом ярусе вершин ровно $n/2$, а во втором и третьем по крайней мере n вершин, имеет смысл активизировать связи между j-й вершиной первого яруса и вершинами $2j-1$, $2j$ второго яруса (а активные связи между вторым и третьим ярусом выбирать так же, как это делалось выше). В этом случае подграф будет оставаться связным после удаления любых $n-1$ ре-

бер, а также при сбое любой $n/2 - 1$ вершины (причем последнее число не может быть увеличено ни при каком выборе активных связей).

После инициализации графа системы происходит регистрация и именование используемых модулей, затем каждый модуль получает от управляющего ядра информацию о том, откуда получать необходимую для работы информацию и куда пересылать результаты. После этого происходит установка соединений между модулями, и система начинает непосредственное функционирование, в процессе которого управляющее ядро периодически производит контроль функционирования модулей.

В основу коммуникационной подсистемы разумно заложить следующие принципы:

1. Коммуникационная система отделена от подсистем, реализующих, например, логику работы модуля или обработку конфигурационного файла.
2. Алгоритм функционирования одинаков для всех модулей.
3. Взаимодействие между модулями осуществляется на основе глобальной конфигурационной структуры.

Такие принципы дают три следующих важных преимущества системе в целом:

- модуль «не заботится» о судьбе отправленных пакетов;
- единообразие кода позволяет проводить тестирование и верификацию один раз;
- возможно практически любое изменение формата и/или протокола передачи данных без изменения логики работы модулей (например, изменение алгоритмов криптографической аутентификации передаваемых данных).

Обмен контрольными сообщениями в системе происходит только между модулями и ядром. Информационные потоки от модуля к модулю динамически создаются и уничтожаются по командам управляющего ядра системы.

На настоящем этапе реализации системы контрольный протокол обмена сообщениями включает в себя перечисленные типы.

1. REGISTER-сообщение передается от модуля к ядру. При передаче сообщения модуль сообщает свой тип, подтип, имена (кроме зарезервированных) и другие регистрационные параметры. В случае успешной регистрации входящего сообщения ядро отвечает сообщением REGISTER.

2. ACQUIRE-сообщение передается модулем ядру. В сообщении модуль запрашивает взаимодействие с модулем более низкого уровня, указывая необходимый подтип. Сообщение UNACQUIRE уведомляет ядро о необходимости разорвать информационный канал между модулями.
3. BIND-передается от ядра к модулю и устанавливает информационный канал между двумя модулями системы. В сообщении ядро передает модулю всю необходимую для взаимодействия информацию (например, IP-адрес и номер порта или имя unix сокета при локальном взаимодействии). После того, как оба модуля подтвердят получение команды, ядро считает, что информационный канал обмена сообщениями между модулями создан. Для уничтожения информационного канала используется сообщение с типом UNBIND. При создании канала первым уведомляется модуль верхнего уровня, при уничтожении — нижнего (как следствие, не происходит лишних пересылок и потери информации). Модуль обязан подтвердить получение команды BIND сообщением типа BIND.
4. PING-сообщение проверки канала. Такое сообщение может идти как от модуля к ядру, так и от ядра к модулю. Модуль передает идентификатор сущности системы, доступность которой нуждается в проверке. Если данная сущность зарегистрирована в системе, ядро перенаправляет запрос на нее. При получении сообщения от ядра, модуль отвечает сообщением с кодом PONG, которое может быть перенаправлено на модуль, породивший исходное сообщение.

Создание информационных каналов может быть инициировано как модулем (через сообщение ACQUIRE), так и ядром (непосредственно сообщением BIND). В случае конфликтов приоритет имеет команда ядра.

Отметим, что для встраивания существующих систем активного аудита в управляющий каркас потребуется всего лишь добавить модуль сбора информации, который будет осуществлять разбор результатов анализа и поддержку коммуникационного протокола, причем поддержка коммуникационного протокола одинакова для всех таких модулей.

Отметим необходимость обеспечения конфиденциальности и целостности трафика самой системы активного аудита. В связи с этим разумным решением является использование методов криптографии.

3. Модули системы активного аудита

Для максимизации эффективности функционирования системы активного аудита необходимо работать как с сетевыми, так и хостовыми данны-

ми. Как следствие, возникает необходимость создания сборщиков, собирающих информацию о заголовках и/или телах сетевых пакетов, об интегральных характеристиках сетевого трафика, о состоянии регистрационных журналов операционной системы, о состоянии системы (например, о загруженности различных компонент). Преобразователи должны реализовывать все необходимые преобразования из формата данных сборщиков в формат данных анализаторов.

Рассмотрим ключевой с точки зрения функционирования системы активного аудита тип модулей — анализаторы. Подавляющее большинство существующих анализаторов ориентировано на сигнатурный анализ и основано на эвристических соображениях. Для информационно-вычислительных комплексов с повышенными требованиями к безопасности желательно наличие анализаторов различных типов (и сигнатурных, и статистических, и нейросетевых), а также формальные доказательства правильности работы модулей в рамках выбранных математических моделей. Результаты в области статистического и нейросетевого анализа докладывались в рамках конференции МаБИТ ([2], [1], [3], [8]). Для исследования свойств сигнатурных анализаторов был создан аппарат на основе теории формальных языков. Показана универсальность такого аппарата, исследованы свойства порождаемых языков, их связь с регулярными языками. Для исследования свойств статистических анализаторов предложена модель, позволяющая по заданному алгоритму анализа и профилю оценивать отклонение от типичного поведения, гарантированно приводящее к обнаружению атаки.

Подробнее остановимся на следующей автоматной модели. Рассмотри автоматную систему, часть состояний которой объявляется безопасной. Исследуем языки, не выводящие автомат из класса безопасных состояний или выводящие из класса безопасных состояний не более, чем на ε.

Под конечным автоматом мы будем понимать четверку $V = (A,\ Q,\ \varphi,\ q_0)$, где A — конечное множество входных символов, Q — конечное множество состояний, $\varphi : A \times Q \to Q$ — функция переходов, $q_0 \in Q$ — начальное состояние. Пусть $Q = S \cup I$, причем $S \cap I = \emptyset$. Состояния из S назовем безопасными, состояния из I — небезопасными. Далее будем предполагать, что начальное состояние является безопасным.

Обозначим через A^* множество всех конечных слов в алфавите A. Функция φ может быть продолжена на множество $A^* \times Q$ по мультипликативности. Подмножество A^* называется языком. Каждому слову $\alpha \in A^*$ соответствует слово $\varkappa(\alpha) \in Q^*$, $\varkappa(\alpha) = \varphi(\alpha,\ q_0)$. Назовем слово $\alpha \in A^*$ безопасным, если $\varkappa(\alpha) \in S^*$. Назовем язык $\mathcal{A} \subseteq A^*$ безопасным (S-языком), если все слова, составляющие $\mathcal{A}$, безопасны, и не существует безопасных слов, не принадлежащих $\mathcal{A}$.

Содержательно безопасный язык может интерпретироваться несколькими способами:

- в системах активного аудита (см. например [4]), как описания легального поведения пользователей (в этом случае выход из множества безопасных состояний трактуется как атака);
- при задании моделей злоумышленника (в этом случае выход из множества безопасных состояний может трактоваться как обнаружение злоумышленника);
- при построении моделей гарантированно защищенных систем (см. например [10], [5]; в таких моделях доказательства как правило проводятся индуктивно, а приведенная ниже лемма 2 означает, что S-языки как раз описывают все регулярные языки, для которых проходит индуктивное доказательство).

Сформулируем ряд утверждений о свойствах S-языков.

Лемма 1. *Если $\mathcal{A}$ является S-языком, то $\mathcal{A}$ регулярен.*

Пусть $\mathcal{A}$ — некоторый язык. Обозначим через $[\mathcal{A}]$ множество всех непустых начал слов, принадлежащих $\mathcal{A}$.

Лемма 2. *Язык $\mathcal{A}$ является S-языком для некоторого автомата V тогда и только тогда, когда выполнены следующие условия:*

1. *$\mathcal{A}$ непуст;*
2. *$\mathcal{A}$ регулярен;*
3. $[\mathcal{A}] \subseteq \mathcal{A}$.

Лемма 3. *Автоматно перечислимые языки (см. [6]) являются S-языками, но, вообще говоря, не наоборот.*

Оценим число S-языков, генерируемых одним автоматом. Будем предполагать, что все состояния автомата достижимы из q_0. Обозначим через NS_V число S-языков, которые можно задать в автомате V.

Лемма 4. *Для конечного автомата V с n состояниями имеет место $NS_V \geqslant n$, и эта оценка неулучшаема.*

Определим функцию Шеннона $LS(n)$ числа S-языков, задаваемых автоматами с n состояниями, следующим образом. $LS(n) = \max\limits_{\{V:|Q|=n\}}(NS_V)$.

Теорема 1. *Для любого $\varepsilon > 0$ существуют константы C_1, C_2, D и N такие, что*

$$C_1 \times D^{|A| \times log_{|A|}(n)} \leqslant LS(n) \leqslant C_2 \times (D \times (1+\varepsilon))^{|A| \times log_{|A|}(n)}.$$

для всех $n \geqslant N$.

Рассмотрим произвольное $\varepsilon > 0$. Введем функции $s : Q^* \to \mathbb{N} \cup \{0\}$ и $i : Q^* \to \mathbb{N} \cup \{0\}$ следующим образом. Пусть $\varkappa \in Q^*$. $s(\varkappa)$ равняется числу

букв $\varkappa$, содержащихся в S, $i(\varkappa)$ равняется числу букв $\varkappa$, содержащихся в I. Обозначим через $|\varkappa|$ число букв в слове $\varkappa$. Назовем слово $\varkappa$ ε-безопасным, если $\frac{i(\varkappa)}{|\varkappa|} < \varepsilon$. Назовем язык $\mathcal{A}$ ε-безопасным (S_ε-языком), если все слова из $\mathcal{A}$ ε-безопасны, и не существует ε-безопасных слов, не принадлежащих $\mathcal{A}$.

S_ε-языки являются естественным обобщением S-языков. Содержательно рассмотрение возможности выхода из множества безопасных состояний может интерпретироваться как признание ущерба, не превышающего некоторого порога, допустимым. Отметим, что свойства S_ε-языков существенно отличаются от свойств S-языков.

Теорема 2. *Если* $\varepsilon \in \mathbb{Q}$, $0 < \varepsilon < 1$, *то существует конечный автомат* V *такой, что определяемый им* S_ε*-язык является контекстно-свободным, но не регулярным, и существуют конечные языки, не являющиеся* S_ε*-языками ни при каких* $\varepsilon \in \mathbb{Q}$.

Замечание. При $\varepsilon = 0$ мы остаемся в множестве S-языков. $S_1 = A^*$.

Теорема 3. *Если* $\varepsilon_1, \varepsilon_2 \in \mathbb{Q}$, $0 \leqslant \varepsilon_1 < \varepsilon_2 \leqslant 1$, *то существует язык, являющийся* S_{ε_1}*-языком, но не являющийся* S_{ε_2}*-языком.*

Литература

[1] *Васенин В. А.*, *Галатенко А. В.*, *Корнеев В. В.*, *Макаров А. А.* Математическое и программное обеспечение активного аудита больших распределенных систем // Материалы конференции «Математика и безопасность информационных технологий». Москва, 2004. С. 99–117.

[2] *Васенин В. А.*, *Галатенко А. В.*, *Макаров А. А.* Анализ отдельных компонент трафика в системах активного аудита компьютерных сетей // Материалы конференции «Математика и безопасность информационных технологий» (МаБИТ-03). Москва, 2003. С. 352–364.

[3] *Васютин С. В.* Использование нейронных сетей для выявления и классификации атак в ОС UNIX // Материалы конференции «Математика и безопасность информационных технологий». Москва, 2003. С. 365–369.

[4] *Галатенко А. В.* Активный аудит // JetInfo, №8, 1999, `http://www.jetinfo.ru/1999/8/1/article1.8.1999.html`.

[5] *Галатенко А. В.* Об автоматной модели защищенных компьютерных систем // Интеллектуальные системы. 1999. Т. 4, вып. 3–4. С. 263–270.

[6] *Кудрявцев В. Б.*, *Алешин С. В.*, *Подколзин А. С.* Введение в теорию автоматов. М.: Наука, 1985.

[7] Материалы по системе активного аудита Snort `http://www.snort.org`

[8] *Райх В. В.* Применение нейронных сетей для решения задач кластеризации в процессе мониторинга информационной безопасности // Материалы конфе-

ренции «Математика и безопасность информационных технологий». Москва, 2003. С. 321–326.

[9] *Харари*. Теория графов. М.: Мир, 1973.

[10] *Moskowitz I. S.*, *Costich O. L.* A Classical Automata Approach to Noninterference Type Problems. Department of the Navy, Naval Research Laboratory, 1992.

On the Social Application of Cryptography and its Development

Lu Shuwang

In an age of knowledge economy, the aspects of human security are different from the past years. The knowledge security has become an important base of human security, besides the political safety and the economic safety. The knowledge security focuses on the generation of the knowledge, and its spreading, inheritance, preservation, protection and disappearance.

Information security study has been given enough attentions to the world, today. The management of knowledge, its audit, digging-up and computing, have been starting development step by step.

In China, I have set up the Peking Knowledge Security Engineering Center, I also work for Chinese Academy of Science. The objective is to study all aspects of matters mentioned above, under the framework of knowledge security.

On this conference, I am not going to discuss the matters of knowledge security. The only thing that I want to introduce is the a block-cipher algorithm which is issued by our country's cryptograph management authorities. It is prepared for WAPI, our country's local wireless area network.

From the security of data and communications, information security, to knowledge security, cryptograph always plays a role of a basic technology in the field of security.

In the age of knowledge security, cryptograph is used to solved many bagatelles about the national economy and the people's livelihood, such as buying an envelop, a lock, a safe-cabinet, a purse and the like, at Cyberspace.

Hereinafter, I would like to make an expatiation of SMS4 algorithm used in local wireless area network. This SMS4 is a first one which is officially published by China, indicating a great change in our cryptograph management policy. All the comments from the attending representatives are welcomed.

SMS4 Cryptographic Algorithm and WAPI

The disposition of cryptographic algorithms in WAPI Proposal (1N904) fully conforms to ISO regulation: 1N7904 DOES NOT force any specific

cryptographic algorithms to be adopted, instead give the right of choosing specific cryptographic algorithms to national bodies. National bodies can choose specific algorithms according to market requirement and local regulations.

The cryptographic algorithms adopted in China are fully open to public.

The infrastructure of the WAPI security protocol is fixed, and the cryptographic algorithms used in WAPI are optional and adoptable modules. Security protocol and cryptographic algorithms are not bound, and WAPI security protocol is applicable to multiple appropriate cryptographic algorithms. Cryptographic algorithms are only adoptable modules. Which algorithm to be applied is subject to the user's requirement and national/regional regulations.

1N7904 doesn't force to adopt any specific cryptographic algorithms (including symmetric algorithm and the parameters of ECC), even China's algorithms. In 1N7904, which algorithms to be applied are optional. Every national body can choose specific algorithms according to requirement and local regulations, and this makes ISO standards furthest applicable without any barrier.

The disposition of cryptographic algorithms in WAPI Proposal (1N904) fully conforms to ISO's common regulation of cipher algorithm. It is different from the disposition of cryptographic algorithms in 1N7903 (IEEE 802.11i). In 1N7903, the implementation of AES algorithm is compulsive.

If there is a will, it is OK for other countries to use the China's algorithms. The Annex I of 1N7904 describes clearly the cryptographic algorithm and ECC parameters adopted in China, and the way of how to get them.

Besides, the specific symmetric algorithm (SMS4) and ECC parameters are fully open to public. And the web link is:

`http://www.oscca.gov.cn/Doc/6/News_1106.htm`,

`http://www.oscca.gov.cn/Doc/6/News_1107.htm`.

As a conclusion, the point of view "the cryptographic algorithms are not disclosed in WAPI proposal" is wrong. And it misled the international community.

SMS4 Cryptographic Algorithm used in WLAN products

SMS4 cryptographic algorithm is a block cipher. The block size is 128 bits and the key length is 128 bits too. The encryption algorithm and key expansion algorithm adopt nonlinear and 32 iteration round structure. The structure of decryption algorithm is the same as the structure of encryption algorithm. Their only difference is the order of round keys , i.e., the order of the round keys in the decryption process is reversed to that in the encryption process.

1. Terms specification

1.1. Word and byte. We use Z_2^e to represent the set of e-bit vectors. An element in Z_2^{32} is called a word ,and an element in Z_2^8 is called a byte.

1.2. S box. S box is a fixed permutation of 8 bits input and 8 bits output, noted as $\mathrm{Sbox}(\cdot)$.

1.3. Basic operations. We use the following basic operations in this algorithm:

- $\oplus$ is the 32 bits EXCLUSIVE-OR;
- $\lll i$ is the i bits left circular shift in a 32-bit vector.

1.4. Key and parameters. The key length in the encryption is 128 bits, which is represented by $\mathrm{MK} = (\mathrm{MK}_0, \mathrm{MK}_1, \mathrm{MK}_2, \mathrm{MK}_3)$, hereinto MK_i $(i = 0, 1, 2, 3)$ is a word.

Round keys is represented by $(\mathrm{rk}_0, \mathrm{rk}_1, \ldots, \mathrm{rk}_{31})$, hereinto rk_i $(i = 0, 1, 2, 3, \ldots, 31)$ is a word. Round keys are produced by encryption keys.

$\mathrm{FK} = (\mathrm{FK}_0, \mathrm{FK}_1, \mathrm{FK}_2, \mathrm{FK}_3)$ is system parameter, $\mathrm{CK} = (\mathrm{rk}_0, \mathrm{rk}_1, \ldots, \mathrm{rk}_{31})$ is fixed parameter, hereinto FK_i $(i = 0, 1, 2, 3)$, CK_i $(i = 0, 1, \ldots, 31)$ is a word. They are used for key expansion algorithm.

2. Round Function

This algorithm uses nonlinear iteration structure and uses words as its units for transformation. One iteration of transformation is called one round.

We suppose input as $(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$, round key as $\mathrm{rk} \in Z_2^{32}$, then the round function is

$$F(X_0, X_1, X_2, X_3, \mathrm{rk}) = X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus \mathrm{rk}).$$

2.1. Combination Replacement *T*. $T\colon Z_2^{32} \to Z_2^{32}$ is a reversible transform which is combined from nonlinear transform τ and linear transform L, namely $T(\cdot) = L(\tau(\cdot))$.

2.1.1. Nonlinear Transform τ. τ consists of 4 parallel S boxes.

We suppose that the input is $A = (a_0, a_1, a_2, a_3) \in (Z_2^8)^4$, the output is $B = (b_0, b_1, b_2, b_3) \in (Z_2^8)^4$, then

$$(b_0, b_1, b_2, b_3) = \tau(A) = (\mathrm{Sbox}(a_0), \mathrm{Sbox}(a_1), \mathrm{Sbox}(a_2), \mathrm{Sbox}(a_3)).$$

2.1.2. Linear Transform *L*. The output of nonlinear transform τ is the input of linear transform L. We suppose that the input is $B \in Z_2^{32}$, output is $C \in Z_2^{32}$, then

$$C = L(B) = B \oplus (B \lll 2) \oplus (B \lll 10) \oplus (B \lll 18) \oplus (B \lll 24).$$

2.2. S Box. The data in S box are presented as hex in Table 1.

Table 1

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	d6	90	e9	fe	cc	e1	3d	b7	16	b6	14	c2	28	fb	2c	05
1	2b	67	9a	76	2a	be	04	c3	aa	44	13	26	49	86	06	99
2	9c	42	50	f4	91	ef	98	7a	33	54	0b	43	ed	cf	ac	62
3	e4	b3	1c	a9	c9	08	e8	95	80	df	94	fa	75	8f	3f	a6
4	47	07	a7	fc	f3	73	17	ba	83	59	3c	19	e6	85	4f	a8
5	68	6b	81	b2	71	64	da	8b	f8	eb	0f	4b	70	56	9d	35
6	1e	24	0e	5e	63	58	d1	a2	25	22	7c	3b	01	21	78	87
7	d4	00	46	57	9f	d3	27	52	4c	36	02	e7	a0	c4	c8	9e
8	ea	bf	8a	d2	40	c7	38	b5	a3	f7	f2	ce	f9	61	15	a1
9	e0	ae	5d	a4	9b	34	1a	55	ad	93	32	30	f5	8c	b1	e3
a	1d	f6	e2	2e	82	66	ca	60	c0	29	23	ab	0d	53	4e	6f
b	d5	db	37	45	de	fd	8e	2f	03	ff	6a	72	6d	6c	5b	51
c	8d	1b	af	92	bb	dd	bc	7f	11	d9	5c	41	1f	10	5a	d8
d	0a	c1	31	88	a5	cd	7b	bd	2d	74	d0	12	b8	e5	b4	b0
e	89	69	97	4a	0c	96	77	7e	65	b9	f1	09	c5	6e	c6	84
f	18	f0	7d	ec	3a	dc	4d	20	79	ee	5f	3e	d7	cb	39	48

3. Encryption/Decryption Algorithm

We defined counter sequence transform R as:

$$R(A_0, A_1, A_2, A_3) = (A_3, A_2, A_1, A_0, \quad A_i \in (Z_2^{32})^4, i = 0, 1, 2, 3.$$

We suppose that the plain text input is $(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$, cipher text output is $(Y_0, Y_1, Y_2, Y_3) \in (Z_2^{32})^4$, round key is $\mathrm{rk}_i \in Z_2^{32}$, $i = 0, 1, 2, \ldots$ $\ldots, 31$.Then the encryption transformation of this algorithm is

$$\begin{aligned} X_{i+4} &= F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, \mathrm{rk}_i) = \\ &= X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus \mathrm{rk}_i), \quad i = 0, 1, \ldots, 31; \\ (Y_0, Y_1, Y_2, Y_3) &= R(X_{32}, X_{33}, X_{34}, X_{35}) = (X_{35}, X_{34}, X_{33}, X_{32}). \end{aligned}$$

The configuration of the decryption transform of this algorithm is the same as the encryption transform of this algorithm. The difference is merely the usage order of round key.

When encryption occur the usage order of round key is $(\mathrm{rk}_0, \mathrm{rk}_1, \ldots, \mathrm{rk}_{31})$.

When decryption occur the usage order of round key is $(\mathrm{rk}_{31}, \mathrm{rk}_{30}, \ldots$ $\ldots, \mathrm{rk}_0)$.

4. Key Expansion Algorithm

In this algorithm the round key of encryption algorithm is produced by encryption key through key expansion algorithm.

Encryption key $\mathrm{MK} = (\mathrm{MK}_0, \mathrm{MK}_1, \mathrm{MK}_2, \mathrm{MK}_3)$, $\mathrm{MK}_i \in Z_2^{32}$, $i = 0, 1, 2, 3$.

We order $K_i \in Z_2^{32}$, $i = 0, 1, \ldots, 35$, round key is $\mathrm{rk}_i \in Z_2^{32}$, $i = 0, 1, \ldots, 31$, then the produce way of round key is:

Firstly,

$$(K_0, K_1, K_2, K_3) = (\mathrm{MK}_0 \oplus \mathrm{FK}_0, \mathrm{MK}_1 \oplus \mathrm{FK}_1, \mathrm{MK}_2 \oplus \mathrm{FK}_2, \mathrm{MK}_3 \oplus \mathrm{FK}_3).$$

Then, to $i = 0, 1, 2, \ldots, 31$:

$$\mathrm{rk}_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus \mathrm{CK}_i).$$

Illustration:

1. T' transformation is almost the same as T in encryption algorithm round function. The only difference is to change linear transformation L to the following L':

$$L'(B) = B \oplus (B \lll 13) \oplus (B \lll 23).$$

2. Adopting hex to express the value of system parameter as:

$$\mathrm{FK}_0 = (\texttt{A3B1BAC6}), \quad \mathrm{FK}_1 = (\texttt{56AA3350}),$$
$$\mathrm{FK}_2 = (\texttt{677D9197}), \quad \mathrm{FK}_3 = (\texttt{B27022DC}).$$

3. The method of defining the value of fixed parameter CK is:
   We suppose ck_{ij} as the j byte ($i = 0, 1, \ldots, 31$; $j = 0, 1, 2, 3$), namely $\mathrm{CK}_i = (\mathrm{ck}_{i,0}, \mathrm{ck}_{i,1}, \mathrm{ck}_{i,2}, \mathrm{ck}_{i,3}) \in (Z_2^8)^4$.
   Then $\mathrm{ck}_{ij} = (4i + j) \times 7 \pmod{256}$. 32 fixed parameters ck_i, their hex are expressed as:

```
00070e15, 1c232a31, 383f464d, 545b6269,
70777e85, 8c939aa1, a8afb6bd, c4cbd2d9,
e0e7eef5, fc030a11, 181f262d, 343b4249,
50575e65, 6c737a81, 888f969d, a4abb2b9,
c0c7ced5, dce3eaf1, f8ff060d, 141b2229,
30373e45, 4c535a61, 686f767d, 848b9299,
a0a7aeb5, bcc3cad1, d8dfe6ed, f4fb0209,
10171e25, 2c333a41, 484f565d, 646b7279.
```

5. Encryption Examples

The following are the calculation examples which use this algorithm as ECB operation methods in order to verify the correctness of encryption algorithm. Hereinto data are expressed in hex.

Example 1. Encrypting a group of plain text once by key.

Plain text: `01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10`.

Encryption key: `01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10`.

Round key and output status of every round:

```
rk[ 0] = f12186f9 X[ 0] = 27fad345
rk[ 1] = 41662b61 X[ 1] = a18b4cb2
rk[ 2] = 5a6ab19a X[ 2] = 11c1e22a
rk[ 3] = 7ba92077 X[ 3] = cc13e2ee
rk[ 4] = 367360f4 X[ 4] = f87c5bd5
rk[ 5] = 776a0c61 X[ 5] = 33220757
rk[ 6] = b6bb89b3 X[ 6] = 77f4c297
rk[ 7] = 24763151 X[ 7] = 7a96f2eb
rk[ 8] = a520307c X[ 8] = 27dac07f
rk[ 9] = b7584dbd X[ 9] = 42dd0f19
rk[10] = c30753ed X[10] = b8a5da02
rk[11] = 7ee55b57 X[11] = 907127fa
rk[12] = 6988608c X[12] = 8b952b83
rk[13] = 30d895b7 X[13] = d42b7c59
rk[14] = 44ba14af X[14] = 2ffc5831
rk[15] = 104495a1 X[15] = f69e6888
rk[16] = d120b428 X[16] = af2432c4
rk[17] = 73b55fa3 X[17] = ed1ec85e
rk[18] = cc874966 X[18] = 55a3ba22
rk[19] = 92244439 X[19] = 124b18aa
rk[20] = e89e641f X[20] = 6ae7725f
rk[21] = 98ca015a X[21] = f4cba1f9
rk[22] = c7159060 X[22] = 1dcdfa10
rk[23] = 99e1fd2e X[23] = 2ff60603
rk[24] = b79bd80c X[24] = eff24fdc
rk[25] = 1d2115b0 X[25] = 6fe46b75
rk[26] = 0e228aeb X[26] = 893450ad
rk[27] = f1780c81 X[27] = 7b938f4c
rk[28] = 428d3654 X[28] = 536e4246
rk[29] = 62293496 X[29] = 86b3e94f
rk[30] = 01cf72e5 X[30] = d206965e
rk[31] = 9124a012 X[31] = 681edf34
```

Cipher text: `68 1e df 34 d2 06 96 5e 86 b3 e9 4f 53 6e 42 46.`

Example 2. Encrypting one group of 明文 again and again for 1000000 times using the same encryption key.

Plain Text: `01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10.`

Encryption key: `01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10.`

Cipher Text: `59 52 98 c7 c6 fd 27 1f 04 02 f8 04 c3 3d 3f 66.`

Применение конечных автоматов для спецификации подозрительного поведения программ как элемент контролируемого выполнения

В. Б. Бетелин, В. А. Галатенко, К. А. Костюхин, Н. В. Шмырев

1. Контролируемое выполнение и ассоциированные понятия

Под *контролируемым выполнением* [1, 2] понимается специально организованный процесс функционирования программно-аппаратных систем, целью которого является выполнение системами своих задач, несмотря на возможное проявление ошибок, атаки и отказы. Основными положениями концепции контролируемого выполнения являются (рис. 1):

- интеграция средств информационной безопасности, отладки и управления;
- распространение контролируемого выполнения на все этапы жизненного цикла систем;
- целостность набора средств контролируемого выполнения, различающихся по степени воздействия на целевые системы, возможность взаимодействия между этими средствами.

Частными случаями контролируемого выполнения являются:

- применение средств управления информационными системами;
- интерактивная отладка;
- мониторинг систем;
- самоконтроль систем;
- воспроизведение предыдущих сеансов работы систем;
- автоматизированное управление поведением системы с помощью средств высокоуровневого описания на основе конечных автоматов.

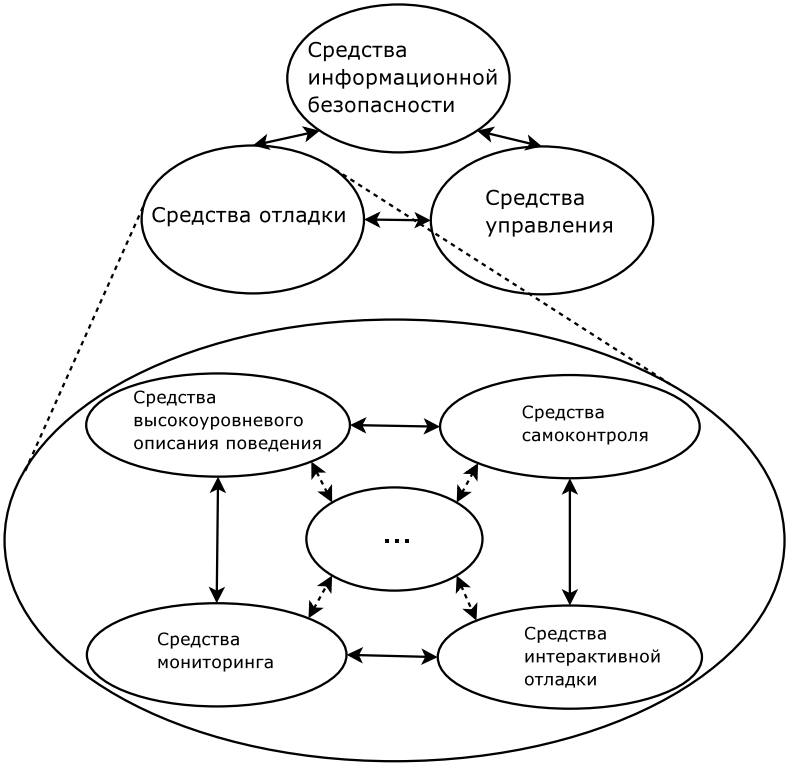


Рис. 1. Целостность набора средств контролируемого выполнения

Средства управления информационными системами ориентированы на такие крупные сущности, как сети, узлы сетей, хосты, устройства, приложения. Эти средства применяются на этапе эксплуатации систем.

Под интерактивной отладкой понимается поиск ошибок (когда известно об их наличии и, возможно, проявлениях) путем запуска программ в режиме диалога с пользователем, который может расставлять точки прерывания, выполнять программу в пошаговом режиме, просматривать и/или изменять значения переменных и производить другие подобные действия. Интерактивную отладку применяют на этапах разработки, тестирования и, возможно, опытной эксплуатации систем.

Под мониторингом системы понимается сбор и анализ (в реальном времени или постфактум) информации о ходе ее функционирования. Мониторинг может являться составной частью как управления на этапе эксплуатации, так и тестирования и (неинтерактивной) отладки на этапах разра-

ботки и тестирования. Важно отметить, что на этапе эксплуатации обычно осуществляется мониторинг описанных выше крупных сущностей. На этапах разработки и тестирования он может носить сколь угодно детальный характер, определяемый потребностями тестирования и отладки.

Самоконтроль систем состоит в проверке значений параметров, отражающих уровень безопасности состояния, в котором находится система (в частности, могут проверяться условия, истинность которых зависит от корректности функционирования системы), а также реагировании, если состояние оказалось небезопасным (некорректным).

Воспроизведение предыдущих сеансов работы систем организуется на основе накопленной трассировочной информации и служит целям выдвижения гипотез о причинах и местах ошибок для последующей эффективной отладки.

Средства высокоуровневого описания поведения полезны для задания шаблонов корректного и некорректного функционирования системы.

2. Роль контролируемого выполнения и его составляющих

Информационные системы создаются для решения определенных задач, достижения заданных целей. Для краткости будем говорить, что у каждой системы есть *миссия*.

У миссии есть несколько относительно независимых аспектов, к которым, помимо предоставляемой функциональности, принадлежит обеспечение определенного уровня информационной безопасности. В свою очередь, основными аспектами (гранями) информационной безопасности являются конфиденциальность, целостность и доступность. В настоящей работе сосредоточимся исключительно на доступности.

Контролируемое выполнение направлено на то, чтобы помочь системе выполнить свою миссию, повышая ее (системы) доступность, понимаемую как способность за заданное время предоставлять заданные информационные сервисы.

Факторами, способными привести к некорректному функционированию и/или понизить доступность систем ниже минимально допустимых пределов и, тем самым, помешать выполнению миссии (в терминологии информационной безопасности — рисками по отношению к доступности), в частности, являются:

- аппаратные и программные ошибки;
- сбои и отказы аппаратуры;
- ошибки пользователей и обслуживающего персонала;

- нарушение эксплуатационных требований и регламентов;
- злоумышленные действия

и другие, аналогичные им. Какими средствами нейтрализовывать перечисленные риски — вопрос экономической и технической целесообразности (в терминологии информационной безопасности соответствующие процедуры называются анализом рисков и выбором контрмер).

Корректное функционирование — необходимое условие выполнения миссии. Средства отладки (интерактивная отладка, мониторинг и воспроизведение предыдущих сеансов работы систем) помогают в поиске ошибок и их исправлении. В то же время, цель, состоящая в выявлении и исправлении всех ошибок, при существующей технологии программирования представляется недостижимой. Следовательно, помимо средств отладки, для выполнения миссии необходимо привлечение дополнительных механизмов. В настоящей работе на эту роль предлагаются средства контроля поведения программ.

Сделаем еще несколько замечаний, относящихся к средствам отладки.

Из приведенного выше перечня видно, что наличие аппаратных и программных ошибок — не единственная угроза корректности функционирования и доступности систем. Даже в том случае, если бы удалось их полностью ликвидировать, необходимо обеспечить устойчивость по отношению к непреднамеренному или умышленному агрессивному потреблению ресурсов, аппаратным сбоям, отказам и другим подобным ситуациям. Отсюда следует, что средства отладки сами по себе принципиально недостаточны, чтобы гарантировать выполнение миссии.

Традиционно отладку и мониторинг в рассматриваемом контексте используют на этапах разработки, тестирования и отладки сложных систем. Широкое распространение программного обеспечения с открытыми исходными текстами по крайней мере в принципиальном плане дает возможность распространить отладку и на этап эксплуатации. Разумеется, чтобы подобное решение стало разумным, необходимо изменения взгляда на эксплуатационную документацию к программным системам, а также на информацию, доступную во время выполнения. Их следует дополнить, предоставив пользователям и отладчику достаточно сведений для анализа нештатных ситуаций и их разрешения.

Для сложных, ответственных систем, особенно систем реального времени, целесообразно постоянно контролировать характер их функционирования, по возможности выявляя и ликвидируя проблемные вопросы и «узкие места» на ранних стадиях их появления. Поведение таких систем определяется не только программными компонентами, но и темпом поступления внешних событий, наличием ресурсов и другими факторами. Если

не располагать регистрационной информацией, то на практике не удастся воспроизвести ситуацию, которая привела к ошибке и, соответственно, не удастся организовать отладку.

Ошибки, особенно типичные, зависят от классов систем. При отладке целесообразно в первую очередь проверить гипотезы, связанные с типичными для класса ошибками. Для параллельных систем с общей памятью это в первую очередь конкуренция за данные, несинхронизированные операции записи/чтения (недетерминизм по данным). Для распределенных систем типичны ошибки, связанные с получением сообщений без ожидания или от произвольного отправителя (недетерминизм приемника). Детерминированное воспроизведение позволяет сколь угодно детально исследовать ошибочные ситуации, проверять гипотезы, связанные с проявлением недетерминизма в поведении отлаживаемых программ.

Очевидно, что применение средств отладки влияет на поведение систем, например, меняются временные характеристики, распределение памяти. Ошибка, проявившаяся при работе системы, в отладочном режиме может не воспроизводиться. Отмеченное обстоятельство позволяет сделать два вывода.

- Необходимо минимизировать возмущение, вносимое средствами отладки в поведение систем.
- Если накладные расходы на средства отладки невелики (приемлемы), эти средства целесообразно оставить в эксплуатационном варианте, так как их изъятие также повлияет на поведение, возможно, сделав его некорректным, а отладку — невозможной. Этот факт — еще одна причина, по которой средства отладки могут присутствовать на этапе эксплуатации системы.

При интерактивной отладке и мониторинге сложных систем вопрос о том, является ли некоторое состояние, достигнутое в процессе функционирования, корректным, или какая-либо ошибка уже проявилась, может оказаться весьма сложным. Для его разрешения может потребоваться анализ не только исходных текстов, но и больших объемов данных. Подобный анализ трудно производить вручную, поэтому целесообразно использование некоторых программных средств. В такой ситуации средства контроля имеют то преимущество, что они записываются на языке, достаточном для автоматической проверки его выразительности, и имеют доступ ко всем необходимым объектам.

Средства контроля можно рассматривать не только как один из инструментов отладки, но и как инструмент защиты от атак на доступность (которая, очевидно, необходима на этапе эксплуатации систем). В такой

трактовке подобные средства можно назвать средствами самозащиты систем.

В начале 1980-х годов Д. Кнут в работе [3] ввел понятие многоаспектного программирования и предложил инструментальные средства для работы с многоаспектными исходными текстами. Идеи аналогичной направленности развивались в инструментальной системе ЭСКОРТ [4]. Средства самозащиты можно рассматривать как отдельный, относительно независимый аспект программы, который может отвечать не только за повышение доступности, но и за другие грани информационной безопасности, такие, например, как контроль целостности программ и данных.

В настоящей работе средствам контроля отведена ключевая роль. Они важны сами по себе. Кроме того, они являются связующим звеном между программой и другими средствами контролируемого выполнения. Реакция на выявление некорректной или подозрительной ситуации может заключаться в инициации или повышении уровня детализации мониторинга, в открытии сеанса интерактивной отладки. Следует отметить, применение средств автоматического контроля поведения систем также позволяет задавать сигнатуры атак, сбоев и ошибок.

3. Требования к средствам контролируемого выполнения и их реализации

В настоящем разделе формулируются требования, предъявляемые к средствам контролируемого выполнения систем со сложной архитектурой.

- Требования к функциональности
  Следование стандартам.
  Должны поддерживаться все возможности отладки и мониторинга, предусмотренные стандартами HPDS [5] и POSIX [6].
  Гибкость воздействия на отлаживаемую систему.
  Средства контролируемого выполнения должны обеспечивать различные уровни воздействия на целевой комплекс от минимального (использование аппаратных средств) до максимального (программная интерактивная отладка).
- Технологические требования
  Расширяемость.
  Архитектура комплекса контролируемого выполнения должна допускать естественные способы наращивания функциональности.
  Настраиваемость и масштабируемость.
  Средства контролируемого выполнения должны содержать механизмы настройки на новые аппаратно-программные платформы. Сред-

ства контролируемого выполнения должны поддерживать любое изменение числа узлов целевого комплекса.

Отказоустойчивость.

Выход из строя нескольких узлов целевого комплекса не должен приводить к сбоям в работе средств контролируемого выполнения.

- Требования к интерфейсу

Развитый, настраиваемый графический интерфейс.

Целевой комплекс может содержать большое число разнородных объектов, которые должны быть представлены пользователю в легко обозримой, удобной для восприятия форме. С этой точки зрения важны такие средства, как поддержка различных уровней детализации в представлении информации о системе, структурированность представления, удобный интерфейс для выполнения действий над объектами.

Полноценный командный язык задания сценариев отладки.

4. Автоматизированное управление процессом выполнения на основе конечных автоматов, как элемент контролируемого выполнения

Для того чтобы дать представление о концепции контролируемого выполнения в действии, рассмотрим пример сценария работы с инструментальным комплексом (рис. 2).

Пусть целевой комплекс состоит из трех узлов: основного (t41), фильтрующего постоянный поток данных; резервного (t42), подключающегося к фильтрации данных, если основной вышел из строя; управляющего (t102), осуществляющего прием отфильтрованных данных и управляющее воздействие на фильтрующие узлы.

В ходе функционирования комплекса основной узел вышел из строя, однако резервный узел не был подключен к фильтрации данных, поскольку управляющий узел продолжал пытаться взаимодействовать с t41. Таким образом, возникла атака типа «Отказ в обслуживании» на управляющий узел, не справляющийся с возросшим потоком неотфильтрованных данных.

Как могла возникнуть подобная ситуация? Допустим, в реализации программного обеспечения на t102 допущена ошибка, которая препятствует правильному отражению изменений в обработке потока данных. Например, в момент поступления заявки на подключение узла t42 к обработке данных некоторый разделяемый ресурс на t102 оказывается захваченным управляющим потоком t41, в результате чего управляющий поток t42 не может принять управление. Подобные ошибки проявляются только в ре-

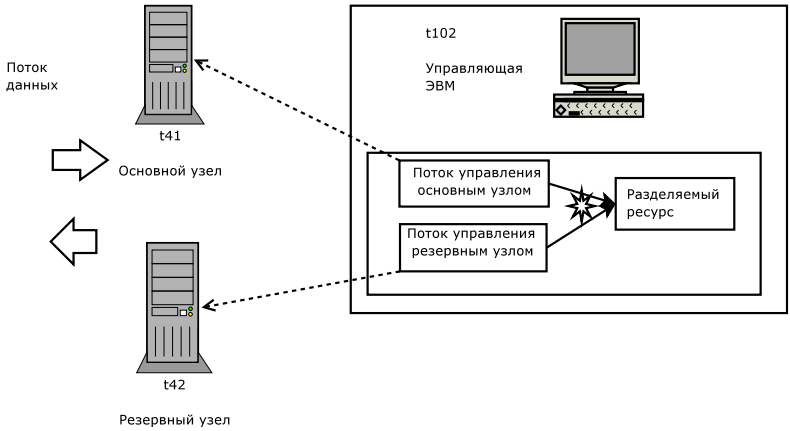


Рис. 2. Пример целевого комплекса

альном режиме работы и плохо воспроизводятся при применении традиционных средств отладки.

Рассмотрим, каким образом разработчик прикладной системы может при помощи инструментального комплекса обнаружить и локализовать подобную ошибку. Первое, что он может сделать, — это включить трассировку событий на узлах t41, t42, t102 и попытаться выявить источник проблемы путем анализа потока событий.

Комплекс позволяет задавать типы регистрируемых событий. Соответственно, разработчик может указать только события, являющиеся с его точки зрения критически важными для правильного функционирования системы (захват и освобождение ресурсов, активация/приостановка работы узла t42 и так далее). Это дает возможность свести к минимуму воздействие средств контролируемого выполнения на функционирование прикладной системы.

Далее, разработчик может построить конечный автомат, моделирующий последовательности событий при передаче управления между узлами t41 и t42 (рис. 3 слева). Данный формализм позволяет обнаруживать ошибки в работе распределенной системы путем выявления логически некорректных последовательностей событий, происходящих при ее функционировании. С состояниями могут быть связаны отладочные действия, например, выдача уведомления на управляющую консоль. С состоянием, которое соответствует некорректному функционированию системы, можно связать ее

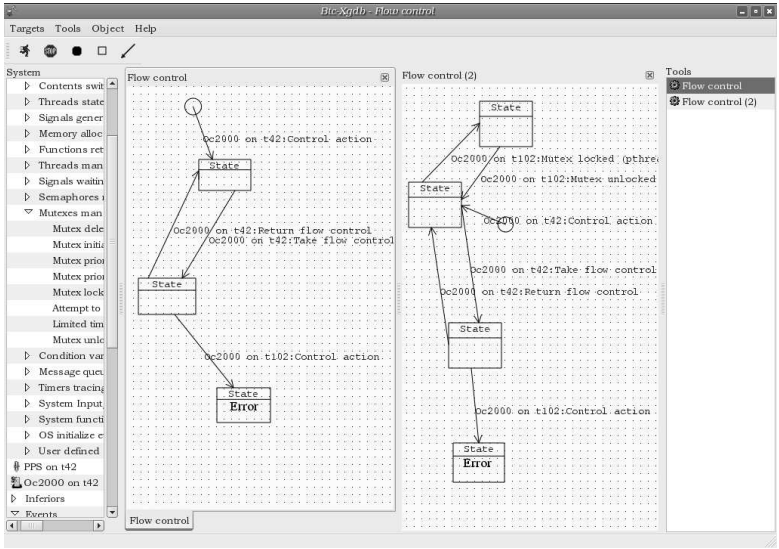


Рис. 3. Шаблоны поведения целевого комплекса

останов с выдачей соответствующего сообщения. После того как процессы прикладной системы остановлены, разработчик может приступить к интерактивной отладке при помощи традиционных средств (просмотр значений переменных, пошаговое выполнение, установка точек останова и других, подобных им).

Допустим, ошибка найдена, однако ее немедленное исправление невозможно. В таком случае при помощи средств быстрой разработки можно создать дополнение к управляющей программе, которое будет корректировать поведение (например, изменять некорректную переменную) программного обеспечения на лету — до того момента, когда необходимые изменения будут внесены в программу на t102.

В принципе, подобные автоматы с минимальным набором отслеживаемых событий могут быть предусмотрены и в эксплуатационном режиме работы с целью повышения надежности функционирования систем и принятия превентивных мер со стороны персонала при первых признаках неблагополучия.

Механизм конечных автоматов позволяет управлять выполнением системы в целом, с учетом событий, происходящих во всей совокупности входящих в нее процессов (потоков). Автомат задается разработчиком прикладной системы (или лицом, отвечающим за ее эксплуатацию), как

элемент контроля функционирования системы. Он может, например, использоваться для задания поведения системы в случае определения вторжения, или с целью отладки, если в работе системы наблюдаются трудно воспроизводимые сбои. Может быть определено одновременно несколько автоматов, контролирующих работу системы.

Множество состояний **S** такого автомата состоит из некоторых логических состояний целевой системы. Входным алфавитом **X** является множество событий целевой системы. Выходным алфавитом **Y** является множество управляющих действий (например, останов системы, выдача сообщения пользователю, продолжение потока, остановленного на точке слежения). В качестве начального состояния $\mathbf{s_0}$ всегда используется точка начала контроля функционирования целевого комплекса, что, как правило, совпадает с началом работы целевого комплекса. Для задания функции переходов (δ) и выходов (λ) в инструментальном комплексе предусмотрены средства визуального редактирования.

Таким образом мы пришли к следующему определению конечного автомата управления процессом функционирования целевой системы.

Определение 1. Конечный автомат управления процессом функционирования программно-аппаратного комплекса — это определенная выше шестерка $\{\mathbf{S}, \mathbf{X}, \mathbf{Y}, \mathbf{s_0}, \delta, \lambda\}$, где **S** — множество состояний, **X** — входной алфавит, **Y** — выходной алфавит, $\mathbf{s_0}$ — начальное состояние, $\delta\colon \mathbf{S} \times \mathbf{X} \to \mathbf{S}$ — функция переходов, $\lambda\colon \mathbf{S} \times \mathbf{X} \to \mathbf{Y}$ — функция выходов.

Способ задания автомата, построенного для контроля поведения целевого комплекса был приведен на рисунке 3. Кружок в изображении автомата обозначает точку входа $\mathbf{s_0}$, то есть начало работы комплекса. Прямоугольники обозначают состояния, а стрелки соответствуют событиям, на которых работает функция перехода δ. Действие, ассоциированное с состоянием и соответствующим событием (результат работы функции λ), задается внутри прямоугольника (тип действия отделяется от аргумента, его конкретизирующего, символом ':'). Надписи, привязанные к стрелкам, обозначают события. Если стрелка не имеет надписи, то ей соответствует любое событие (кроме событий, ассоциированных с другими стрелками, исходящими из того же состояния). События, не отраженные в определении автомата, игнорируются при его отработке. В данном случае верхний прямоугольник соответствует состоянию, когда поток данных полностью обрабатывается узлом t41. Средний прямоугольник соответствует состоянию системы, когда t42 берет обработку на себя. В этом состоянии должно быть выполнено управляющее действие потоком t42 на узле t102. Возникновение в этом состоянии события, соответствующего управляющему действию со стороны потока t41, свидетельствует об ошибочном функционировании системы. Это событие переводит систему в состояние, обозна-

ченное нижним прямоугольником, с которым связано действие по выдаче сообщения об ошибке.

Если гипотеза подтвердилась, то есть сообщение об ошибке было получено, разработчик может попытаться уточнить источник ошибки при помощи более детального автомата. На рис. 3 справа показан автомат, в котором добавлено состояние, соответствующее ситуации, когда разделяемый ресурс на t102 захвачен потоком t41. Если в данном состоянии происходит событие, соответствующее активации узла t42, то этот факт свидетельствует об ошибке в организации доступа к данному разделяемому ресурсу.

Отметим, что необходимое действие для поддержание работоспособности целевого комплекса, а именно, принудительное переключение управляющих потоков может быть сделано автоматически средствами инструментального комплекса.

5. Заключение

Распространенные в настоящее время средства отладки не позволяют в полной мере решить вопросы, возникающие в ходе функционирования распределенных систем, что существенно влияет на уровень их безопасности. В основном это происходит по той причине, что существующие средства ориентированы на контроль отдельных сущностей (потоков, процессов), а не системы в целом.

При проектировании отладочного комплекса в НИИСИ РАН за основу был взят подход, который назван контролируемым выполнением. Его суть заключается в интеграции возможностей современных систем управления и методов традиционной отладки. В качестве программной модели при реализации комплекса использовалась типичная для систем управления объектно-компонентная модель, имеющая ряд важных преимуществ, таких как масштабируемость, расширяемость и настраиваемость.

В составе отладочного комплекса особое место занимают средства автоматизированного контроля выполнения распределенных программ. Использование конечных автоматов для задания шаблонов поведения целевых систем позволяет осуществлять контроль выполнения программ в штатном режиме их работы.

Наличие графического инструмента для определения конечных автоматов обеспечивает простоту и удобство использования средств автоматизированного контроля поведения программ. С их помощью можно также задавать сигнатуры различных ошибок, оперативно реагируя на их возникновение.

Литература

[1] *Галатенко В. А.*, *Костюхин К. А.* Отладка и мониторинг распределенных разнородных систем. Вопросы кибернетики / под ред. В. Б. Бетелина. М.: НИИСИ РАН, 2001.

[2] *Вьюкова Н. И.*, *Галатенко В. А.*, *Костюхин К. А.*, *Шмырев Н. В.* Организация отладочного комплекса для целевых систем со сложной архитектурой. М.: НИИСИ РАН, 2004.

[3] *Knuth D. E.* Literate programming. CSLI, 1992.

[4] *Бетелин В. Б.*, *Галатенко В. А.* ЭСКОРТ — инструментальная среда программирования. Юбилейный сборник трудов институтов Отделения информатики РАН, 1993, Т. II.

[5] High Perfomance Debugging Forum. Review of HPDF standard. `http://www.ptools.org/hpdf/article.html`.

[6] Institute of Electrical and Electronic Engineers. The Open Group Base Specifications Issue 6. IEEE Std 1003.1, 2001.

Модель хостовой системы обнаружения вторжений

П. Д. Зегжда, С. С. Корт

Аннотация

В статье рассматривается модель хостовой системы обнаружения вторжений. На основании модели вычислительной системы, основанной на семантическом графе, систематизируются возможные механизмов нарушения безопасности в вычислительной системе. После этого предлагаются принципы построения модуля анализа, основанного на модели динамического мониторинга безопасности состояний системы. В заключении статьи приведены подходы к разработке модуля сбора данных хостовой системы обнаружения вторжений.

1. Модель вычислительной системы

Компьютерную систему предлагается моделировать G-графом с иерархической конструкцией с именованными вершинами функциональными дугами [1, 2].

При этом объект представляется системой, состоящей из простых объектов O, не имеющих структуры и представляемых в виде набора признаков $\Pi = \langle p_1 \dots p_n \rangle$. Простые объекты на каждом уровне иерархии могут быть отнесены к одному из K классов. Например, для рассматриваемой области такими классами могут являться файлы, записи, запросы, поля базы данных и т.д., вплоть до сегментов памяти на твердом диске. Непосредственно анализируемый объект представляется семантическим графом SG, который является структурой, содержащей вершины двух типов — объектные — I_n и предикатные (процедурные) — Y, что соответствует декларативному и процедурному способам представления знаний в виде

$$SG = \langle I,\ Y,\ G \rangle,$$

где Y — структурные связи между вершинами.

Объектная вершина i задается тройкой множеств $\langle L,\ K,\ P \rangle$, где

- L — тип данного объекта O;

- K — имя класса, к которому он принадлежит;
- P — совокупность признаков, определяющих состояние объекта.

Каждой объектной вершине i соответствует один вход из множества $\{P\}$, задающий свойства и размеры элемента и множества связей с предикатами вершинами $y \in Y$, определяющими структурные связи между простыми объектами.

Множество типов Y определяется с помощью набора характеристических функций

$$g_{i_1}^{(g)},\ g_{i_2}^{(g)},\ \ldots g_{i_m}^{(g)},$$

сопоставляющих типы связей g между объектами вершинами $i_1,\ i_2,\ \ldots i_m$.

Функция $g_{i_m}^{(g)}$ принимает значение 1, если отношение, в общем случае, r-ое типа $\langle g \rangle$ выполняется для набора $i_1,\ i_2,\ \ldots i_m$ вершин, относящихся к классам $K_1,\ \ldots,\ K_N$, в противном случае $g_1^{(g)} = 0$. Если отношение g_1^g выполняется для вершины i, в графе SG существует предикатная вершина g и соединение с объектными вершинами $i = 1$. Множество связей образуют дуги $p \in \Gamma$.

Дуги помечены именами отношений g и задаются функцией преобразования как возможные действия (чтение, запись, уничтожение, назначение прав). Отношения определяются в зависимости от типа объекта и уровня иерархии. Выполняемая операция может быть формализована в виде бинарного отношения между взаимодействующими объектами в виде $Oi,\ kRkOi + 1,\ k,\ k \in K$. В общем случае операция может быть записана в виде цепочки отношений $Oi,\ kRi,\ k\ \ldots.\ Rj,\ kOj,\ k,\ k \in K$. Цепочки отношений строятся с использованием объектного подхода с использованием принципов наследования, инкапсуляции, полиморфизма. В зависимости от выбранного уровня иерархии такими операциями могут быть операции над файлами, выполнение запроса, формирование транзакций.

Утверждение 1. *Множество классов K, определенное для объектов O, является частично упорядоченным.*

Утверждение 2. *Множество имен отношений g является частично упорядоченным. Наименьший уровень, определенный на множестве отношений, соответствует операциям чтения и записи.*

Данные утверждения используются в третьем разделе настоящей статьи для рассмотрения требований к модулю сбора данных.

В системе определена политика безопасности, определяющая допустимые цепочки отношений и недопустимые. При этом ограничения могут устанавливаться как операционной системой, так и политикой безопасности системы. В модели системы это отображается в виде ограничения на определенные функции дуг и контроля за состоянием.

Применительно к задаче компьютерной безопасности состояние системы определяется на каждом уровне иерархии следующим набором множеств

$$\langle O,\ R,\ Rul,\ L_{ij}\rangle, \tag{1}$$

где

- O — множество допустимых объектов $\{O_{ik}\}$;
- R — множество отношений, построенное по бинарному принципу $\{R_{ij}\}$;
- Rul — правила контроля цепочки отношений в соответствии с политикой безопасности; множество правил основывается на типах объектов и операций, а также на уровне иерархии представления объектов и операций $\{Rul_{ij}\}$;
- L_{ij} — функциии передачи от объекта к объекту, построенные на типе отношений R_{ij}; включают: запись, чтение, изменение и т.д.

Изменение состояния происходит одним из следующих способов:

- путем изменения множества $\{O_{ik}\}$;
- путем реализации отношений R_{ij};
- путем построения цепочки $R \times R$, что приводит к действиям над объектом O или изменению $\{O_{ik}\}$.

Функции L_{ij}, реализуемые на отношениях R_{ij}, могут быть систематизированы следующим образом:

- функции, изменяющие объект L^{new}, что приводит к изменению $\{O_i\}$;
- функции, не изменяющие (чтение, копирование), что сохраняет $\{O_i\}$, но может привести к нарушениям Rul;
- функции L_{ij}, включающие функции безопасности, такие как: идентификация O_i; аутентификация O_iRO_j; фильтрация O_iRO_j и др.

1.1. Систематизация возможных механизмов нарушения безопасности

Нарушение безопасности может происходить по одному из следующих механизмов.

1. Изменение множества объектов O:
   - создание нового объекта, не подчиняющегося ограничениям Rul для данного типа объектов. Данное утверждение описывает вторжения, целью которых является внедрение в систему РПС;

- изменение параметров, свойственных существующему объекту. Данное утверждение описывает вторжения, основанные на изменении параметров механизмов защиты, в том числе:
- удаление объекта O;

2. Изменение множества отношений R.
   - возникновение новых отношений между объектами. Возникновение новых отношений может не противоречить (не контролироваться) политикой информационной безопасности, что является недостатком средств контроля;
   - изменение существующих отношений между объектами. или признаком уязвимости, т.е. Rul не изменяется;
   - удаление существующих отношений между объектами. Удаление существующих отношений может появляться при временном отключении защиты.
3. Изменение множества ограничений Rul.
   - добавление нового правила Rul;
   - изменение существующего правила Rul;
   - удаление существующего правила Rul.

В рамках используемой модели эти признаки образуют полное множество. Предложенная систематизация возможных механизмов нарушений позволяет определить термины уязвимости, атаки и вторжения. Кроме того, в рамках предложенных определений можно отделить атаки, связанных с нарушением политики информационной безопасности, от атак, связанных с использованием уязвимостей.

2. Модель динамического мониторинга безопасности состояний системы

В предлагаемой модели СОВ определено множество неопределенной меры вторжений $\{A_k\}$ и счетное множество моделей их описания $\{M_l\}$. Множество моделей описания вторжения используется модулем анализа и определяет возможность нежелательных действий, которые система в состоянии выявить. Множество атак, не описываемых моделями, определяет полноту обнаружения системой обнаружения вторжений, связанную с возможностью выявления нарушений безопасности.

Основным подходом, используемым для описания модели системы при исследовании ее безопасности в процессе проектирования, является анализ состояний системы. В данной статье предлагается описание подхода к анализу безопасности состояний с целью выявления нарушений инфор-

мационной безопасности вычислительной системы в процессе ее функционирования. Подсистема динамического мониторинга безопасности состояний системы должна обнаруживать переходы системы в небезопасные состояния, вызванные выполнением некорректных операций пользователя в системе или вторжениями в систему.

Таким образом, задача динамического мониторинга безопасности состояний системы [3] состоит в:

- обнаружении состояний, противоречащих определенной в системе политике безопасности, — небезопасных состояний;
- выявлении причин, приведших систему в небезопасное состояние;
- оценке безопасности системы, в которую осуществляется вторжение.

Предлагаемый подход должен учитывать нарушения безопасности системы, вызванные как невыполнением политики безопасности, так и атаками на систему, что ведет к необходимости описания двух моделей. При этом обе модели должны быть описаны на базе единого математического формализма, позволяющего в дальнейшем провести объединение моделей. В качестве такого формализма в работе выбран автомат конечных состояний, описывающий поведение субъекта системы.

2.1. Модель системы, учитывающая нарушения политики безопасности

Введем определения понятий, используемых в дальнейших рассуждениях. $\{S\}$ — множество субъектов; $\{O\}$ — множество объектов; $\{Op\}$ — множество операций; $\{Prg\}$ — множество сервисов, используемых субъектом (программ или программных интерфейсов). Введение данного множества в описание модели системы обосновано тем фактом, что операции субъекта системы над объектами выполняются с использованием сервисов. Тогда матрица доступа субъектов системы к объектам может быть определена следующим образом: $M'(s, prg, o)$ — матрица доступа программ, используемых от имени субъектов для выполнения операций с объектами системы.

Тогда автомат $A = \{\sigma, t, Out, \sigma_0, \delta, \lambda\}$, представляющий безопасность функционирования пользователя по отношению к политике безопасности, определенной в системе, может быть описан следующим образом:

$$\sigma = \{op_1(prog_1, 0_1), \ldots, op_i(prog_i, 0_i)\}$$

— состояния автомата, описывающие операции, выполненные субъектом системы над объектами; множество состояний является частично упорядоченным;

$$t \in Op(prg_i, o_j)$$

— управляющие символы автомата, соответствующие операциям, выполненным субъектом над объектами системы с использованием программ.

Под безопасным состоянием понимается состояние, описывающее операции, выполненные субъектом и не противоречащие политике безопасности. Таким образом, оценка безопасности состояния описывает выход автомата как $Out = \{Sec,\ UnSec\}$. Автомат заканчивает свою работу, если он переходит в небезопасное состояние.

Тогда функция перехода δ может быть описана следующим образом:

$$\forall t = op_i \exists op_i(prog_i,\ 0_i) \in \sigma_i = t \to \sigma_{i+1} = \sigma_i,$$
$$\forall t = op_i ! \exists op_i(prog_i,\ 0_i) \in \sigma_i = t \to \sigma_{i+1} = \sigma_i \cup t.$$

Функция выхода автомата λ может быть записана следующим образом:

$$\forall t = op_i(op_i(prog_i,\ 0_i) \in \sigma_i) \vee (op_i(prog_i,\ 0_i) \in M'(s,\ prg,\ o)) \to Out = Sec,$$
$$\forall t = op_i(op_i(prog_i,\ 0_i) \in \sigma_i) \vee (op_i(prog_i,\ 0_i) \notin M'(s,\ prg,\ o)) \to$$
$$\to Out = UnSec.$$

2.2. Модель обнаружения вторжений

После того, как описана модель, соответствующая контролю функционирования системы в соответствии с политикой безопасности, рассмотрим модель, описывающую возможные атаки на систему.

Атаки на систему идентифицируются с использованием сигнатур атак $\{Sgt_m\}_{m=1}^{M}$. Множество сигнатур, описывающих атаки, может быть разбито на подмножества в соответствии со свойством PROPERTY. Свойство PROPERTY отображает множество сигнатур атак во множество prp_n, $n \in \in 1 : N$, описывающие цели атаки. Каждый элемент множества prp_n отражает цели атаки, связанной с использованием сигнатуры. Множество $\{prp_n\}_{n=1}^{N}$ является частично упорядоченным.

Важным является тот факт, что нарушитель, выполняющий вторжение продвигается в своих действиях, реализуя (успешно или нет) различные атаки на систему. Тогда множество сигнатур может быть упорядоченным в соответствии с этапом вторжения следующим образом: $\{Sgt_{i_1}\}_{i_1=1}^{M_1} \dots \{Sgt_{i_k}\}_{i_k=1}^{M_k}$, причем $\sum_{j=1}^{K} m_j = M$.

При этом сценарии нарушения безопасности (вторжения) могут быть описаны как $Scen = (Sgt_0,\ Sgt_1,\ \dots,\ Sgt_k)$, $k \leqslant M$, при условии, что:

1. $\forall i,\ j \in 1 : k,\ i \neq j \to Sgt_i \neq Sgt_j$.
2. $\forall i,\ j \in 1 : k,\ i \leqslant j \to prp(Sgt_i) \leqslant prp(Sgt_j)$.

Автомат, описывающий нарушения безопасности системы, может быть представлен с использованием следующих понятий:

- $\sigma = \{Sgt_m\}$ — состояния автомата, описываемые сигнатурой, соответствующей наибольшему достигнутому нарушителем этапу вторжения;
- $t \in Sgt_i$ — управляющие символы автомата;
- $prp(\sigma_i)$ для текущего состояния автомата — выход автомата;
- $\sigma_0 \in \sigma$ — начальное состояние, в котором субъект начинает работу с системой.

Функция перехода δ автомата может быть описана так:

$$\forall t = Sgt_j \exists Sgt_i \in \sigma_i \colon prp(Sgt_j) \leqslant prp(Sgt_i) \to \sigma_{i+1} = \sigma_i,$$
$$\forall t = Sgt_j ! \exists Sgt_i \in \sigma_i \colon prp(Sgt_j) \leqslant prp(Sgt_i), \to \sigma_{i+1} = \sigma_i \cup Sgt_i.$$

Функция выхода λ описывается следующим образом:

$$\forall t = Sgt_i Out = prp(\delta(\sigma_i,\, t)).$$

2.3. Объединенная модель

Компоненты, описывающие модель системы могут быть описаны с использованием единой структуры. В этой структуре состояния автомата будут описываться следующим образом:

$$\sigma = \{\{op_1(prog_1,\, 0_1),\, \ldots,\, op_i(prog_i,\, 0_i)\},\, Sgt_m(Scen_l)\}.$$

Входом объединенного автомата является операция, выполненная пользователем с использованием сервиса, или атака, выполненная пользователем на систему с использованием сервиса. Таким образом, $t \in \in (Op(prg_i,\, o_j) \vee Sgt_m)$ — управляющие символы автомата.

Функция перехода δ объединенного автомата описывается так:

$$\forall t = Sgt_j \quad \exists Sgt_i \in \sigma_i : prp(Sgt_j) \leqslant prp(Sgt_i) \to \sigma_{i+1} = \sigma_i,$$
$$\forall t = Sgt_j \quad ! \exists Sgt_i \in \sigma_i : prp(Sgt_j) \leqslant prp(Sgt_i) \to \sigma_{i+1} = \sigma_i \cup Sgt_i,$$
$$\forall t = op_i \quad \exists op_i(prog_i,\, 0_i) \in \sigma_i = t \to \sigma_{i+1} = \sigma_i,$$
$$\forall t = op_i \quad ! \exists op_i(prog_i,\, 0_i) \in \sigma_i = t \to \sigma_{i+1} = \sigma_i \cup t.$$

Выходом автомата является характеристика состояния объединенного автомата. В соответствии с определениями, приведенными выше, состояния могут быть: безопасными, небезопасными и состояниями с признаками атаки.

Функция выхода объединенного автомата λ описывается так:

$$\forall t = Sgt_i Out = prp(\delta(\sigma_i,\ t)),$$
$$\forall t = op_i(op_i(prog_i,\ 0_i) \in \sigma_i) \vee (op_i(prog_i,\ 0_i) \in M'(s,\ prg,\ o)) \rightarrow Out = Sec,$$
$$\forall t = op_i(op_i(prog_i,\ 0_i) \in \sigma_i) \vee (op_i(prog_i,\ 0_i) \notin M'(s,\ prg,\ o)) \rightarrow$$
$$\rightarrow Out = UnSec.$$

Таким образом, в настоящей статье предлагается автоматная модель, позволяющая осуществить динамический мониторинг безопасности состояний системы. На основании динамического мониторинга безопасности состояний системы можно выявлять различные нарушения безопасности в вычислительной системы.

Предлагаемый подход к обнаружению вторжений был использован в следующих работах, выполненных в СПбГПУ:

- система антивирусного мониторинга; применительно к модели вычислительной системы
- система динамического анализа безопасности программного обеспечения;
- анализатор сетевых вторжений.

В таблице 1 приведены аспекты модели, предложенной выше, применительно к разработанным системам.

Как показано в таблице, все разработанные системы, укладываясь в единую модель динамического мониторинга безопасности состояний системы, являются ее частными случаями вследствие особенностей назначения.

3. Особенности разработки модуля сбора данных

Описанная в первом разделе статьи модель вычислительной системы позволяет принять решение о нарушении безопасности на некотором, достаточно высоком уровне иерархии. При этом сами атаки и вторжения зачастую описываются в более низкоуровневых терминах. Заполнить этот пробел должен адекватный метод сбора данных и возможное преобразование полученных данных к более высоким уровням представления.

Хотя для сбора данных в хостовых СОВ могут использоваться стандартные средства аудита операционной системы, желательна разработка специализированных модулей сбора данных. Это связано с тем, что стандартные средства аудита часто собирают информацию, бесполезную для определения нарушения безопасности системы, тогда как важная информация зачастую не фиксируется.

Таблица 1. Системы, разработанные на базе предложенного подхода к динамическому мониторингу безопасности состояний системы

Назначение	Система антивирусного мониторинга	Система динамического анализа безопасности программного обеспечения	Анализатор сетевых вторжений
Год разработки	2001	2004	2004
Обнаружение нарушений безопасности применительно к модели, описанной в первом разделе статьи	Модификация параметров объекта O Создание или удаление объекта O	Возникновение новой цепочки R Создание или удаление объекта O Создание, удаление или модификация правила Rul Удаление отношения R	Модификация параметров объекта O Модификация отношения R Создание или удаление объекта O Создание, удаление или модификация правила Rul Удаление отношения R Возникновение новой цепочки R
Управляющие символы	$\{Sgt_m\}_{m=1}^{M}$	$\{Op\}$	$Op(prg_i, o_j) \vee Sgt_m$
Состояние	Sgt_m	$\{op_1, (prog_1, 0_1), \ldots, op_i, (prog_i, 0_i)\}$	$\{\{op_1, (prog_1, 0_1), \ldots, op_i, (prog_i, 0_i)\}, \}$
Выходные данные	Попытка перехода в атакующее состояние	Попытка перехода в запрещенное состояние	Попытка перехода в запрещенное или атакующее состояние
Источник входных данных (Prog)	Сменные носители, сетевые интерфейсы	Программы, выполняемые локально, системные вызовы	Сетевые интерфейсы
Обнаружение неизвестных атак	Нет	Да	Да
Обнаружение известных атак	Да	Да (без их идентификации по имени)	Да
Обнаружение некорректного использования системы	Нет	Да	Да

Таким образом, для эффективного отслеживания вторжений необходимо выбрать уровень представления системы, на котором наиболее целесообразно собирать исходные данные. Выбор уровня определяется двумя противоречивыми факторами — удобством сбора информации и однозначностью принятия решения.

Для раскрытия элементов множеств допустимых объектов и отношений, рассмотренных в представлении модели вычислительной системы необходимо описать представление объектов и операций системы, описанных в выражении (1) на различных уровнях иерархии — Lev. При этом

предполагается, что описание системы на более низком уровне раскрывает описание системы на более высоком уровне, а все отношения, записанные в форме (1) наследуются сверху вниз.

Функция $Level(M_k) = \{LevMod_m\}$ возвращает множество уровней описания операций и объектов, используемое при описании модели вторжения j.

Предположим, что модуль сбора данных собирает данные на уровне $LevData$. Обозначим представление объектов и операций системы на уровне модуля сбора данных как $O_{LevData}$, $R_{LevData}$, а на уровне модели — как O_{LevMod}, R_{LevMod}.

Тогда предлагаемая модель позволяет описать основные свойства СОВ, определяемые модулем сбора данных.

1. *Корректность СОВ.* Модуль сбора данных должен функционировать на минимальном уровне представления операций и объектов, представленных во множестве моделей, описывающих атаки $\forall M_j LevData \leqslant \min(\min(LevMod(M_j)))$. В том случае, если данное требование не выполняется, модуль сбора данных не может предоставить полную информацию модулю анализа о событиях в системе, и работа СОВ некорректна.
2. *Совместимость модулей СОВ.* Данные, полученные модулем сбора данных СОВ хоста, должны быть приведены к единому формату, используемому модулем анализа СОВ $\forall M_j \exists! F,\ G : OLevMod = F(OLevData),\ RLevMod = G(RLevData)$. Существование единственных преобразований F и G и их сложность определяет возможность идентификации объектов и операций на уровне представления модели вторжения, а также сложность разработки.
3. *Совместимость СОВ с вычислительной системой.* В идеале СОВ должна быть прозрачной для пользователя и не вносить новых отношений в модель компьютерной системы, описанной выражением (1).

Для того чтобы оценить различные схемы аудита построим классификацию методов, используемых при построении модуля сбора данных СОВ хоста, приведенную на рис. 1. Данная классификация не зависит от операционной системы хоста, на котором функционирует СОВ.

Используя приведенную на рисунке классификацию, рассмотрим ожидаемые сравнительные характеристики различных методов построения модуля сбора данных с точки зрения приведенных выше требований.

С точки зрения полноты СОВ рациональным является модуль сбора данных, контролирующий поведение всей системы. Вместе с тем, модуль, построенный по этому принципу, может быть неэффективным, т. к. объем

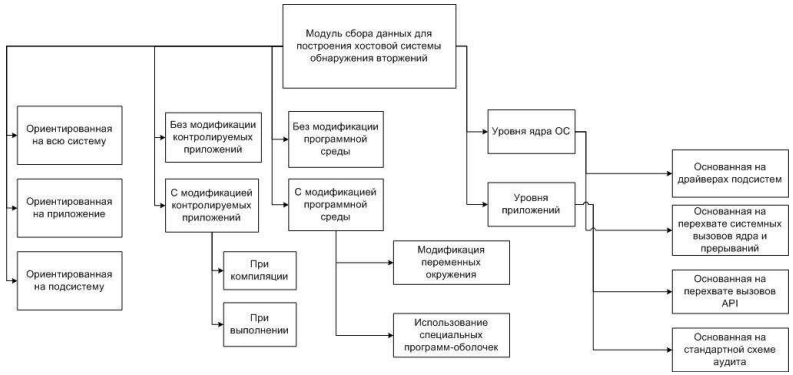


Рис. 1. Классификация методов сбора данных, используемых для построения хостовых СОВ

собираемых для анализа данных может быть избыточен. Использование сбора данных о событиях в отдельной подсистеме может быть целесообразно с точки зрения обнаружения атак на подсистему, что ограничивает количество используемых моделей и уменьшает полноту СОВ. Таким образом, компромиссным является вариант, отслеживающий события подсистем, критичных для безопасности системы.

В соответствии с требованиями, модификация программной среды может повлиять на совместимость модуля сбора данных с вычислительной системой. Как следствие этого, рекомендуется использовать СОВ без модификации программной среды или с использованием модификации переменных окружения.

Как было показано, выбор уровня, на котором функционирует модуль сбора данных, в свою влияет на корректность СОВ и совместимость ее модулей. При этом рациональными являются схемы построения модуля сбора данных, связанные с перехватом системных вызовов и вызовов API.

В таблице 2 приведено сравнение наиболее популярных методов построения модуля сбора данных хостовых СОВ для семейства ОС Windows.

Необходимо отметить, что указанные в таблице значения для различных сравнительных признаков применительно к методу построения модуля сбора данных хостовых СОВ, будут характерны не только для ОС Windows, но и для других операционных систем.

Исходя из таблицы 1, наиболее перспективными методами построения модуля сбора данных являются метод, основанный на перехвате системных вызовов (библиотечных функций) и метод, основанный на использовании драйверов подсистем.

Таблица 2. Сравнение методов построения модуля сбора данных хостовых СОВ в ОС Windows

	Метод либо средство сбора информации				
Критерии сравнения	Стандартный аудит	Перехват системных вызовов (библиотечных функций)	Специализированные драйверы для подсистем ОС	Специальные оболочки	Средства анализа производительности
Эффективность					
Высокая степень информативности	–	+	+	+/–	+/–
Возможность собирать информацию со всех процессов, работающих в системе	+	+/–	–	+	+
Сигнатурный метод обнаружения атак	–	+	+	+	–
Метод выявления аномалий	+/–	+	+	+	+
Анализ операций над объектами в системе	+/–	+	+	+	–
Универсальность					
Применимость единого метода для всех подсистем	+	+	–	–	–
Возможность использования собранной информации для динамического анализа во внешней системе	+	+	+	–	–
Совместимость					
Прозрачность для пользователя (отсутствие оболочки)	+	+	+	–	–
Не требует вмешательства пользователя в процесс сбора информации	+	+	+	–	–
Не требует модификации среды или программного обеспечения	+	+/–	+/–	–	+
Защищенность					
Сложность обхода системы защиты	–	+/–	+	–	–

Использование методов, основанных на перехвате системных вызовов, является менее трудоемким (при одинаковой информативности) по сравнению с методом, основанным на использовании драйверов подсистем. Вместе с тем, использование методов, основанных на перехвате системных вызовов, требует больших усилий направленных на обеспечение защищенности по сравнению с методами, основанными на использовании драйверов подсистем.

Как видно из таблицы 2, у методов, основанных на перехвате системных вызовов, могут быть также проблемы, связанные с требованием совместимости. В качестве примера приведем сравнение различных методов перехвата вызовов функций в ОС Linux, приведенное в таблице 3.

Таблица 3. Сравнение методов перехвата вызовов функций в ОС Linux

	Метод сбора информации				
Критерии сравнения	LD_PRELOAD	PLT Injection	Linux Kernel Hooker	Link-Time Method	модификация sys_call_table
Совместимость					
Отсутствие изменения переменных окружения	-	+	+	+	+
Отсутствие модификации исполняемых файлов на диске	+	-	+	+	+
Отсутствие модификации исполняемых модулей в памяти	+	+	-	+	+
Не требует исходных текстов и перекомпиляции программ	+	+	+	-	+
Эффективность					
Возможность динамической отмены перехвата функций	-	-	+	-	+
Возможность динамического перехвата (возможность «на лету» выбрать множество перехватываемых функций)	-	-	+	-	+
Возможность собирать информацию со всех процессов, работающих в системе	-	-	+	-	+

На основании данной таблицы видно, что в соответствии с требованиями целесообразным для реализации модуля сбора данных СОВ хоста

под ОС Linux, основанной на перехвате системных вызовов (библиотечных функций) является модификация таблицы системных вызовов.

Таким образом, предлагаемая модель позволяет обосновать выбор метода построения модуля сбора данных СОВ хоста, а при оценке (сертификации) системы упрощают анализ возможностей СОВ.

Литература

[1] *Zegzhda P. D.* General model of design process in intellectual system // European simulation multiconference. Barcelona, 1996.

[2] *Зегжда П. Д.*, *Зегжда Д. П.* Методология динамической защиты// Материалы международной научной конференции по проблемам безопасности и противодействия терроризму, 2005. М.: МЦНМО, 2006.

[3] *Корт С. С.* Модель динамического мониторинга состояний системы// Материалы международной научной конференции по проблемам безопасности и противодействия терроризму, 2005. М.: МЦНМО, 2006.

Вероятностные модели псевдослучайных последовательностей в криптографии

А. М. Шойтов

1. Введение

Большинство современных криптографических систем предполагает использование псевдослучайных последовательностей (ПСП). В частности, они используются в качестве ключей шифрования для симметричных и ассиметричных шифрсистем, а также в качестве выходных и промежуточных последовательностей электронных шифраторов. В соответствии с [26] под псевдослучайной последовательностью понимают последовательность, порожденную генератором ПСП, т. е. детерминированным устройством или программой. Важной задачей является построение ПСП, обладающими свойствами, близкими к свойствам реализаций идеальных случайных последовательностей, т. е. последовательностей, полученных в соответствии со случайной равновероятной схемой (СРС).

Типичный генератор ПСП строится путем комбинирования базовых блоков гарантирования периода и различных функций усложнения. В качестве наиболее распространенных базовых блоков выделим линейный конгруэнтный генератор (см. [8]) и линейные рекуррентные последовательности (ЛРП) над конечным полем (см. [10]).

Основной особенностью криптографических требований к ПСП является то, что отклонения от СРС не могут быть обнаружены или использованы для построения эффективных криптоаналитических методов. Так, шифр модульного гаммирования с использованием случайной равновероятной гаммы является совершенным по Шеннону, однако, если гамма является неравновероятной или в ней присутствуют зависимости (отклонения от случайности), то могут быть предложены криптоаналитические методы лучшие, чем тотальный перебор. Поэтому решение задачи оценки качества ПСП и ряда других криптографических задач предполагает, в частности, построение адекватных теоретико-вероятностных моделей ПСП.

В докладе предлагается новый подход к оценке криптографического качества ПСП на основе использования общих теоретико-вероятностных

моделей ПСП. Также представлен краткий обзор результатов исследований асимптотического поведения случайных величин, характеризующих один важный тип вероятностных моделей ПСП (вероятностные модели ПСП с подстановочной зависимостью цепочек).

2. Теоретико-вероятностные модели псевдослучайных последовательностей

Выделим два типа вероятностных моделей ПСП:

I. Вероятностные модели (ВМ) ПСП, применяемые при разработке методов (возможно конкретного метода) анализа узлов криптографических схем, при этом предполагается, что способ образования ПСП известен. При построении таких моделей учитывается одна или несколько достаточно конкретных закономерностей, присущих способу образования ПСП и существенно отличающих их от случайных последовательностей. Под адекватностью ВМ ПСП первого типа следует понимать соответствие алгоритма образования ПСП достаточно конкретному способу образования (конкретность ВМ). Под ВМ ПСП первого типа часто понимают вероятностную модель вырабатывающего ее генератора.

В качестве наиболее известных ВМ ПСП первого типа выделим модели искаженных ЛРП над конечным полем (с известными минимальными многочленами и вероятностями искажения), выходных последовательностей линейного регистра сдвига (РС) с неравномерным движением информации по накопителю (известна обратная связь регистра и распределение шагов движения), а также различные виды цепей Маркова (с известной матрицей переходных вероятностей) или их усложнения.

Проблематика вероятностных моделей ПСП первого типа хорошо изучена и освещена в отечественной и зарубежной литературе (см., например, сборник «Труды по дискретной математике» Академии криптографии Российской Федерации и «Journal of Cryptology» International Association for Cryptologic Research), поэтому далее будем говорить только о вероятностных моделях второго типа, предварительно отметив ряд отечественным математиков и криптографов, работы которых связаны с построением и использованием ВМ ПСП первого типа: А. С. Амбросимов, Г. В. Балакин, П. Ф. Беляев, С. М. Буравлев, А. М. Зубков, В. А. Иванов, Г. И. Ивченко, В. А. Копытцев, Ю. И. Максимов, Ю. И. Медведев, В. Г. Михайлов, А. Ф. Ронжин, В. Н. Сачков, Б. А. Севастьянов, В. Е. Степанов, В. П. Чистяков.

II. Вероятностные модели ПСП, возникающие при оценке криптографического качества псевдослучайных последовательностей. Для ВМ ПСП

второго типа считается, что способ образования ПСП не известен, что предполагает поиск в ней любых отклонений от СРС.

Теоретические исследования общих методов оценки «степени» случайности последовательности, которые проводятся в рамках алгоритмического подхода Мартин-Лефа и сложностного подхода Колмогорова (см., например [28]), пока не привели разработке подходящих для прикладных криптографических применений средств, поэтому в настоящее время в качестве инструмента оценки качества ПСП используются так называемые универсальные статистические тесты на случайность.

Первым известным набором универсальных статистических тестов на случайность был набор статистических тестов Д. Кнута, описанный им в монографии [8], а первой программной реализацией такого набора явился пакет статистических тестов «DIEHARD» Д. Марсалья (см. [46], [47]). В настоящее время известно достаточно много таких пакетов: пакет «NIST Statistical Test Suite» (см. [49]) Национального института стандартов и технологий США, пакет «Crypt-SX» (см. [44]), TestU01 и пр. Известные пакеты содержат порядка 15 тестов на случайность. Классификацию тестов подобных пакетов, можно найти например в книге [29]. Оценка результатов работы тестов основана на вычислении значений так называемых p-уровней (p-value), характеризующих согласованность экспериментов с СРС. Гипотеза о СРС принимается с помощью критерия Колмогорова—Смирнова (KS-test), если значения p-value равномерно распределены на интервале (0,1), то есть предполагается, что все тесты пакета являются равноправными, и для оценки их результата используется критерий согласия.

Для оценки криптографического качества ПСП предлагается новый подход, основанный на использовании ВМ ПСП второго типа. В результате статистического тестирования принимается одна из гипотез, соответствующих вероятностным моделям ПСП второго типа, среди которых содержится гипотеза о случайном равновероятном способе образования. В случае, когда принимается гипотеза о СРС, то ПСП считается успешно прошедшей тестирование, если принимается какая-нибудь другая гипотеза, то ПСП не проходит тестирование, причем степень отклонения от СРС характеризуется степенью соответствия ПСП принятой гипотезе. Под адекватностью ВМ ПСП второго типа следует понимать степень ее соответствия результатам статистического тестирования, при этом, в отличии от ВМ первого типа, по сути рассматривается вероятностная модель ПСП, а не генератора ПСП.

Кроме нового подхода к оценке результатов работы пакетов универсальных тестов на случайность идея использования ВМ ПСП приводит к другому способу выбора состава этих пакетов: в пакет включаются тесты,

предназначенные для выявления определенных вероятностных моделей. Также и качество отдельных тестов оценивается по их способности эффективно выявлять ВМ ПСП. При этом устраняется определенная некорректность (с точки зрения математической статистики) проверки гипотезы об использовании генератора ПСП против СРС, так как при использовании ВМ ПСП статистические отклонения интерпретируются в терминах вероятностной модели и имеет место традиционная проверка статистических гипотез.

Прежде чем переходить к описанию различных типов ВМ ПСП второго типа выделим исследовательские задачи, связанные с их применением в целом:

1. Выбор и исследование вероятностных моделей ПСП второго типа.

2. Исследование (возможно экспериментальное) свойств статистик универсальных тестов на случайность применительно к последовательностям, полученных по различным вероятностным моделям ПСП.

3. Разработка методов проверки гипотез о применимости конкретной вероятностной модели (в том числе СРС), а также методов различения соответствующих гипотез между собой.

Вероятностные модели ПСП второго типа можно строить на основе известных вероятностных моделей первого типа, заменяя соответствующие простые гипотезы на сложные:

1. Марковские модели: Простые и сложные (например, цепи Маркова-Брунса) цепи Маркова (с неизвестной матрицей переходных вероятностей), различные виды усложнений цепей Маркова, например, цепи Маркова со случайной заменой символов и/или со случайным удалением символов (неизвестным усложнением), стохастические регистры сдвига (с неизвестной обратной связью).

2. Стационарные случайные последовательности со следами линейной рекуррентной зависимости: искаженные ЛРП (с неизвестным минимальным многочленом и, возможно, вероятностью искажения), выходные последовательности линейных регистров сдвига с неравномерным движением (с неизвестной обратной связью, распределением шагов движения), стохастические регистры сдвига.

Рассмотрим другой подход к построению ВМ ПСП второго типа. Большинство известных тестов построены как статистики от частот встречаемости значений функции от неперекрывающихся s-цепочек: тест частот встречаемости s-грамм, покер тест, тест линейной сложности, тест ранга случайной матрицы, тест интервалов и др. При этом исходная ПСП $\{X_1, \ldots, X_n, \ldots\}$ разбивается на s-цепочки $Y_i(s) = (X_i, \ldots, X_{i+s-1})$, $i = 1, 2, \ldots, n$, и для выбранной функции f строится последовательность

значений этой функции от цепочек

$$\mathbf{F} = \{F_1, F_2, \ldots, F_n\}, \quad F_i = f(Y_i(s)), \quad i = 1, 2, \ldots, n,$$

к которой применяется критерий хи-квадрат (обычно критерий применяется к последовательности значений функции от неперекрывающихся s-цепочек).

В качестве альтернативного способа построения статистик тестов на случайность рассмотрим следующую конструкцию. Для натурального $k \geqslant 2$ определим статистику

$$\mathbf{Z}_{n,k}(\mathbf{F}) = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} \mathbf{I}\{F_{i_1} = F_{i_2} = \ldots = F_{i_k}\},$$

равную числу k-кратных повторений в последовательности $\mathbf{F}$.

Эта статистика является обобщением известной статистики, равной числу точных повторений s-цепочек в последовательности (значения функции совпадают только для одинаковых цепочек), исследованной в работах Б. А. Севастьянова, А. М. Зубкова, В. Г. Михайлова, H. M. Gustafson, E. P. Dawson, J. Dj. Golic и др. (см., например, [6], [43]). Близкой тематике посвящены работы П. Ф. Беляева, Ю. И. Медведева, В. Е. Степанова (см., например, [2], [11], [27]).

Статистики типа $\mathbf{Z}_{n,k}(\mathbf{F})$ обладают рядом преимуществ перед известными статистиками типа хи-квадрат применительно к выявлению определенных видов зависимостей, характерных для ПСП. Говоря о статистике точных повторений, в качестве основного преимущества может быть выделена способность статистики эффективно обнаруживать некоторые формы далеких, но сильных зависимостей, характерных для ПСП. Определим две новые вероятностные модели ПСП второго типа.

3. Стационарные случайные последовательности с нестандартным профилем повторений цепочек (число повторений цепочек различных длин не соответствует СРС). В качестве примеров генераторов, порождающих последовательностей с такими зависимостями, выступают линейные рекуррентные последовательности над полями и над кольцами вычетов и их усложнения, модели полноцикловых генераторов (что соответствует выборке без возвращения).

4. Стационарные случайные последовательности с подстановочной зависимостью цепочек (число цепочек в ПСП, связанных взаимнооднозначным отображением из некоторого множества, отлично от СРС). Более формально, пусть последовательность $\{X_1, \ldots, X_n, \ldots\}$ состоит из символов алфавита $A = \{1, \ldots, N\}$, s - фиксированное натуральное число. Предположим, что на множестве A^s действует группа подстановок Γ, которая является подгруппой симметрической группы подстановок $S(A^s)$.

Будем говорить, что две цепочки $(X_i, \ldots, X_{i+s-1})$ и $(X_j, \ldots, X_{j+s-1})$ подстановочно зависимы (подстановочно эквивалентны) относительно группы Γ (Γ-эквивалентны), если найдется такая подстановка $g \in \Gamma$, что справедливо равенство

$$g(X_i, \ldots, X_{i+s-1}) = (X_j, \ldots, X_{j+s-1}).$$

Отношение Γ-эквивалентности осуществляет разбиение множества A^s на классы эквивалентности. Определим функцию $f(\Gamma)$ на множестве A^s так, чтобы она принимала одинаковые значения на s-цепочках, принадлежащих к одному классу Γ-эквивалентности, и только на них. Для определения подстановочной зависимости s-цепочек относительно группы Γ в последовательности $\{X_1, \ldots, X_n, \ldots\}$ может быть использована статистика $\mathbf{Z}_{n,k}(\mathbf{F})$, построенная на основе функции $f(\Gamma)$. В качестве примеров генераторов, порождающих последовательности с подстановочной зависимостью цепочек, можно выделить (как и для предыдущей модели), линейные рекуррентные последовательности над полями и кольцами, однако подстановочные зависимости возникают раньше точных повторений цепочек, что связано с наличием у ЛРП мультипликатора (см. [5] и [10]).

3. Повторения значений дискретной функции от цепочек последовательности независимых испытаний

Для использования вероятностной модели подстановочной зависимости цепочек необходимо знать точные или предельные распределения статистик $\mathbf{Z}_{n,k}(\mathbf{F})$, характеризующих различные виды подстановочной зависимости, применительно к последовательностям, полученным при помощи СРС. Введем обозначения.

Пусть $\mathbf{X} = \{X_1, \ldots, X_n, \ldots\}$ — последовательность независимых одинаково распределенных случайных величин, $\mathbf{Y} = \{Y_1(s), \ldots, Y_n(s), \ldots\}$ — последовательность s-цепочек ($s \in \mathbb{N}$) последовательности $\mathbf{X}$, где $Y_i(s) = (X_i, \ldots, X_{i+s-1})$, $i = 1, 2, \ldots, n$. Пусть $f : \mathbb{R}^s \longrightarrow \mathbb{N}$ — борелевская функция, принимающая натуральные значения, $\mathbf{F} = \{F_1, F_2, \ldots, F_n, \ldots\}$ — последовательность значений функции f от s-цепочек последовательности $\mathbf{X}$, $F_i = f\big(Y_i(s)\big)$, $i = 1, 2, \ldots, n$.

Для натурального $k \geqslant 2$ определим случайные величины

$$\mathbf{Z}_{n,k}(\mathbf{F}) = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} \mathbf{I}\{F_{i_1} = F_{i_2} = \ldots = F_{i_k}\},$$

равную числу k-кратных повторений символов на отрезке длины n последовательности $\mathbf{F}$, и

$$\mathbf{Z}'_{n,k}(\mathbf{F}) = \sum_{1 \leqslant i_1 < i_1+s \leqslant i_2 < \ldots < i_{k-1}+s \leqslant i_k \leqslant n} \mathbf{I}\{F_{i_1} = F_{i_2} = \ldots = F_{i_k}\},$$

равную числу k-кратных повторений значений функции f от неперекрывающихся s-цепочек отрезка последовательности $\mathbf{X}$ длины $n+s-1$.

Основные математические результаты, представленные в докладе:

Новые достаточные условия сходимости распределений $\mathbf{Z}_{n,k}(\mathbf{F})$ *и* $\mathbf{Z}'_{n,k}(\mathbf{F})$ *к возможным предельным распределениям: распределению Пуассона, сложному распределению Пуассона, нормальному распределению и распределению типа хи-квадрат.*

Основные результаты формулируются в терминах следующих вероятностей

$$\varkappa_s(f) = \max_{a \in \mathbb{N}} \mathbf{P}\{F_1 = a\}, \;\; \pi_s^{(m)}(f) = \sum_{a \in \mathbb{N}} \mathbf{P}^m\{F_1 = a\},$$

$$\varkappa_r(f) = \max_{a,b \in \mathbb{N}} \mathbf{P}\{F_1 = a | F_{1+r} = b\}, \;\; \pi_r(f) = \mathbf{P}\{F_1 = F_{1+r}\},$$

где $r = 0, \ldots, s-1, \;\; m = 2, 3, \ldots$

Для функции f указанного выше вида определим отношение эквивалентности $\underset{f}{\sim}$ на множестве s-цепочек. Если $\overline{a}, \overline{b} \in \mathbb{R}^s$, то

$$\overline{a} \underset{f}{\sim} \overline{b} \iff f(\overline{a}) = f(\overline{b}),$$

т. е. две цепочки $\underset{f}{\sim}$-эквивалентны тогда и только тогда, когда совпадают значения функции f от этих цепочек. Это замечание позволяет применить общие предельные теоремы для случайных величин $\mathbf{Z}_{n,k}(\mathbf{F})$ и $\mathbf{Z}'_{n,k}(\mathbf{F})$ для описания достаточных условий сходимости к соответствующим предельным распределениям для числа наборов подстановочно эквивалентных цепочек полиномиальной схемы, для различных наиболее интересных с прикладной точки зрения отношений подстановочной эквивалентности.

Следствия из основных результатов:

Предельные теоремы сходимости к указанным выше распределениям для распределений таких случайных величин как число точных повторений s-цепочек полиномиальной схемы, число $\mathbf{H}$*-эквивалентных и число* $\mathbf{G}$*-эквивалентных s-цепочек полиномиальной схемы с конечным (возможно растущим) числом исходов и, в некоторых случаях, для числа* $\mathbf{GH}$*-эквивалентных s-цепочек.*

Пусть последовательность $\mathbf{X}$ получена по полиномиальной схеме испытаний с вероятностями исходов $p_m = \mathbf{P}\{X_1 = m\}$, $m \in \mathbb{N}$. Точное повторение s-цепочек

$$\delta_{n,k} = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} \mathbf{I}\{Y_{i_1}(s) = Y_{i_2}(s) = \ldots = Y_{i_k}(s)\}.$$

Пусть последовательность $\mathbf{X}$ получена по полиномиальной схеме испытаний с исходами в множестве $A = \{1, \ldots, N\}$ с вероятностями исходов $p_m = \mathbf{P}\{X_1 = m\}$, $m \in A$. Повторение с точностью до $\mathbf{G}$-эквивалентности

$$\zeta_{n,k}(\mathbf{G}) = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} \mathbf{I}\{Y_{i_1}(s)\mathbf{G}Y_{i_2}(s)\mathbf{G}\ldots\mathbf{G}Y_{i_k}(s)\}.$$

Повторение с точностью до $\mathbf{H}$-эквивалентности

$$\xi_{n,k}(\mathbf{H}) = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} \mathbf{I}\{Y_{i_1}(s)\mathbf{H}Y_{i_2}(s)\mathbf{H}\ldots\mathbf{H}Y_{i_k}(s)\}.$$

Пусть $\mathbf{H}$ — подгруппа симметрической группы подстановок S_N, а $\mathbf{G}$ — подгруппа S_s. Две s-цепочки $\overline{a} = (a_1, \ldots, a_s)$ и $\overline{b} = (b_1, \ldots, b_s)$ из A^s будем называть $\mathbf{GH}$-эквивалентными (см. монография [24]) и писать $\overline{a}\mathbf{GH}\overline{b}$, если

$$\exists g \in \mathbf{G}, \ \ \exists h \in \mathbf{H}: \ h(a_{g(j)}) = b_j, \ \ \forall j = 1, \ldots, s.$$

Если $\mathbf{H} = \{e\}$ ($\mathbf{G} = \{e\}$), то $\mathbf{GH}$ -эквивалентные цепочки $\overline{a}$ и $\overline{b}$ будем называть $\mathbf{G}$-эквивалентными ($\mathbf{H}$-эквивалентными) и писать $\overline{a}\mathbf{G}\overline{b}$ ($\overline{a}\mathbf{H}\overline{b}$). Отношения S_N-эквивалентности и S_s-эквивалентности называют еще отношениями структурной и перестановочной эквивалентности соответственно (см. обзор [22]).

История задачи:

Исследования асимптотического поведения $\delta_{n,k}$ посвящены работы ряда авторов, наиболее известны результаты А. М. Зубкова и В. Г. Михайлова (см., например, [6], [7]). Исследование $\xi_{n,k}(\mathbf{H})$ начаты С. М. Буравлевым в случае структурной эквивалентности ($\mathbf{H} = S_N$) и в случае, когда нижние строки подстановок из $\mathbf{H}$ образуют латинский прямоугольник ([3], [4]). Исследования продолжены В. Г. Михайловым и автором (см., например, [22]). Случайные величины $\zeta_{n,k}(\mathbf{G})$ введены и исследованы автором доклада.

Случайные величины $\mathbf{Z}_{n,k}(\mathbf{F})$ могут рассматриваться как индикаторные U-статистики от последовательности $(s-1)$-зависимых случайных величин (см. [1], [9]) или как сумма индикаторов с малым числом зависимостей (см. [16]). Общие условия асимптотической нормальности таких величин получены, например, в работах [12], [14], [15], [23] и [45]. В [31] доказана

многомерная (по различным функциям f) центральная предельная теорема для случайных величин $\mathbf{Z}_{n,k}(\mathbf{F})$ в ситуации, когда растет лишь длина последовательности $\mathbf{X}$.

1. Закон Пуассона

Пусть $\mathrm{Po}(\lambda)$ - распределение Пуассона с параметром λ, $L(\gamma)$ - функция распределения случайной величины γ и

$$\rho(\Psi, \Gamma) = \frac{1}{2}\sum_{m=0}^{\infty} |\Psi\{m\} - \Gamma\{m\}|$$

расстояние по вариации между распределениями Ψ и Γ, сосредоточенными на множестве $\{0, 1, \ldots\}$,

Теорема 1 ([36] (метод Чена—Стейна см. [42], [16], [40])). *Пусть $n \geqslant 2s+1$. Тогда*

а) $\rho\Big(\mathcal{L}\big(\mathbf{Z}'_{n,2}(\mathbf{F})\big),\ \mathrm{Po}\big(C^2_{n-2s+1}\pi_s(f)\big)\Big) \leqslant sn\Big(5\pi_s(f) + 4\varkappa_s(f)\Big) + 4\sum\limits_{r=1}^{s-1} r\varkappa_r(f)$;

б) $\rho\Big(\mathcal{L}\big(\mathbf{Z}_{n,2}(\mathbf{F})\big),\ \mathcal{L}\big(\mathbf{Z}'_{n,2}(\mathbf{F})\big)\Big) \leqslant n\sum\limits_{r=1}^{s-1}\pi_r(f)$.

В качестве следствия из теоремы 1 выводятся новые достаточные условия сходимости к закону Пуассона распределения числа точных повторений цепочек полиномиальной схемы, которые являются несколько более слабыми, чем известные условия, полученные в работах А. М. Зубкова и В. Г. Михайлова (см., например, [6], [7]).

Первый результат о сходимости случайных величин $\xi_{n,k}(\mathbf{H})$ к закону Пуассона, полученный С. М. Буравлевым, имеет следующий вид.

Теорема 2 ([3] (метод Б. А. Севастьянова, см. [25])). *Пусть случайные величины X_i независимы и распределены на множестве A равновероятно и $sN^{-1} \geqslant \ln N + 1$. Тогда*:

а) *выполняется неравенство*

$$\lambda(s, n) = \frac{C_n^2}{N^{2s}}\sum_{m=1}^{N}\sigma(s, m)((N)_m)^2 < C_n^2\frac{N!}{N^s},$$

где $\sigma(s, m)$ — числа Стирлинга второго рода;

б) *если $n, N, s \to \infty$ так, что $\lambda(s, n) \to \lambda > 0$, то*

$$\mathbf{P}\{\xi_{n,2}(S_N) = k\} \to \frac{\lambda^k}{k!}e^{-\lambda}, \quad k = 0, 1, \ldots$$

При этом, если $sN^{-1} - \ln N \to \infty$, то $\lambda(s, n) = C_n^2 N! N^{-s}(1 + o(1))$.

Условие $sN^{-1} \geqslant \ln N + 1$ обеспечивает отсутствие случайных s-цепочек, содержащих не все символы алфавита A. Этот результат был улучшен В. Г. Михайловым.

Теорема 3 ([19] (метод Чена — Стейна)). *Пусть случайные величины X_t независимы и имеют на множестве $\{1, \ldots, N\}$ равномерное распределение, параметры n, s, $N \to \infty$ так, что $n \geqslant 2s - 1$ и выполнены условия*

$$\mathbf{E}\xi_{n,2}(S_N) \to \lambda, \quad 0 < \lambda < \infty,$$

$$sN^{-1} - 0.25 \ln N \to \infty.$$

Тогда распределение случайной величины $\xi_{n,2}(S_N)$ сходится к распределению Пуассона с параметром λ.

Условие $sN^{-1} - 0.25 \ln N \to \infty$ допускает отсутствие в случайных и равновероятных s-цепочках отдельных знаков.

Из теоремы 1 вытекает

Следствие 1. *Пусть случайные величины X_t независимы и имеют на множестве $\{1, \ldots, N\}$ равномерное распределение, параметры n, s, $N \to \infty$ так, что $n \geqslant 2s - 1$ и выполнены условия*

$$\mathbf{E}\xi_{n,2}(S_N) \to \lambda, \quad 0 < \lambda < \infty; \qquad s \geqslant N + 2.$$

Тогда распределение случайной величины $\xi_{n,2}(S_N)$ сходится к распределению Пуассона с параметром λ.

Допускается отсутствие в случайных и равновероятных s-цепочках доли знаков знаков алфавита A пропорциональной его мощности N.

Теорема1 позволяет распространить приведенные выше результаты на случай полиномиальной схемы общего вида, а также на случай произвольной группы $\mathbf{H}$ (см. также [20], [21], [32]).

Из теоремы1 вытекают достаточные условия сходимости к распределению Пуассона распределения числа пар нереперекрывающихся $\mathbf{G}$-эквивалентных цепочек.

Следствие 2 ([37]). *Если последовательность $\mathbf{X}$ получена по равновероятной схеме и при $n \to \infty$ параметры N, s и группа $\mathbf{G} \subseteq S_s$ меняются так, что $N \to \infty$, $\mathbf{E}\,\zeta'_{n,2}(\mathbf{G}) \to \lambda$, $0 < \lambda < \infty$, и выполнено одно из двух следующих условий*

$$s^2|\mathbf{G}|^2 N^{-s} \to 0,$$

$$\frac{|\mathbf{G}|s^q}{s!} \to \infty \text{ для некоторого натурального } q,$$

то

$$\lim_{n\to\infty} \mathbf{P}\{\zeta'_{n,2}(\mathbf{G}) = m\} = \frac{\lambda^m}{m!}e^{-\lambda}, \qquad m = 0, 1, \ldots$$

Теорема1 позволяет распространить результат следствия 2 на случай полиномиальной схемы общего вида.

2. Сложный закон Пуассона

Пусть $\Lambda = \{\lambda_1, \lambda_2, \ldots\}$ - последовательность неотрицательных действительных чисел, $\sum\limits_{r=1}^{\infty} \lambda_r < \infty$, $\{N_1, N_2, \ldots\}$ - последовательность независимых случайных величин, где $N_r \sim \mathrm{Po}(\lambda_r)$, $r = 1, 2 \ldots$ Сложное распределение Пуассона случайной величины $\sum\limits_{r=1}^{\infty} rN_r$ обозначим через $\mathrm{CP}(\Lambda)$, распределению $\mathrm{CP}(\Lambda)$ соответствует производящая функция

$$\mathbf{E}z^{\mathbf{N}} = \exp\Big(\lambda_0\big(\sum_{k=1}^{\infty} z^k \lambda_k \lambda_0^{-1} - 1\big)\Big), \quad \lambda_0 = \sum_{k=1}^{\infty} \lambda_k.$$

Пусть множество Γ^{vs} состоит из индексов цепочек $\big((i_1, i_2), (j_1, j_2)\big)$ для которых события $\{F_{i_1} = F_{i_2}\}$ и $\{F_{j_1} = F_{j_2}\}$ могут быть зависимы (подробное и формальное определение множества Γ^{vs} см. [38]). Выбор множества Γ^{vs} зависит от f и однозначно определяет выбор параметров сопутствующего распределению случайной величины $\mathbf{Z}'_{n,2}(\mathbf{F})$ сложного распределения Пуассона, а также значение величины $\psi(\Gamma^{vs})$ (см. теорему4 ниже).

Теорема 4 ([38] (метод Стейна [41], [48])). *Если при $n \to \infty$ параметр s, функция f, параметры случайной последовательности $\mathbf{X}$ и множество Γ^{vs} меняются так, что существуют пределы*

$$\lambda_r = \lim_{n\to\infty} \lambda_r(\Gamma^{vs}), \quad r = 1, 2, \ldots,$$

$$\lambda_0 = \lim_{n\to\infty} \sum_{r=1}^{(2s-1)^2} \lambda_r(\Gamma^{vs}), \quad 0 < \lambda_0 < \infty,$$

и выполнено условие

$$\mathbf{E}\mathbf{Z}'_{n,2}(\mathbf{F}) sn\varkappa_s(f) + \psi(\Gamma^{vs}) \to 0,$$

то распределение случайной величины $\mathbf{Z}'_{n,2}(\mathbf{F})$ сходится к распределению $CP(\Lambda)$, определяемому последовательностью $\{\lambda_1, \lambda_2, \ldots\}$.

Удается также получить оценку расстояния по вариации между распределением случайной величины $\mathbf{Z}'_{n,2}(\mathbf{F})$ и распределением $\mathrm{CP}(\Lambda_n(\Gamma^{vs}))$, а также нормальную предельную теорему для распределения $\mathbf{Z}'_{n,2}(\mathbf{F})$ в зоне смежной со сложнопуассоновской зоной. Пусть $P_2 = \sum\limits_{m=1}^{\infty} p_m^2$.

Следствие 3 ([18] (метод Стейна)). *Если при $n \to \infty$ параметр s и вероятности $p_1, p_2, \ldots$ меняются так, что*

$$P_2 \to \rho, \ \ 0 \leqslant \rho < 1, \quad C_n^2 P_2^s \big(1-\rho\big) \to \lambda, \ \ 0 < \lambda < \infty$$

и выполнено условие

$$ns\big(\max_{m\in\mathbb{N}} p_m\big)^s \to 0,$$

то

$$\mathbf{E}z^{\delta_{n,2}} \to \exp\left\{\lambda\left(\frac{(1-\rho)z}{1-\rho z} - 1\right)\right\}.$$

В доказательстве следствий 3 и 4 полагается $\Gamma^{vs} = \{i_1 - j_1 = i_2 - j_2\}$, что определяется для $\delta_{n,2}$ и $\xi_{n,k}(\mathbf{H})$ сходимостью к распределению суммы пуассоновского числа независимых случайных величин, каждая из которых имеет геометрическое распределение. При этом для $\xi_{n,k}(\mathbf{H})$ наблюдается явление редукции (см. [33]).

Следствие 4 ([35]). *Пусть параметры N, k, группа $\mathbf{H}$ и вероятности $p_a > 0$, $a = 1, \ldots, N$, фиксированы, n и s стремятся к бесконечности так, что*

$$C_n^2 P_2^s (1-P_2)|\mathbf{H}_{\mathcal{P}}| \to \lambda, \quad 0 < \lambda < \infty.$$

Тогда

$$\lim_{n\to\infty} \mathbf{E}z^{\xi_{n,2}(\mathbf{H})} = \exp\left\{\frac{\lambda(z-1)}{1-P_2 z}\right\}.$$

Впервые сходимость распределения $\xi_{n,2}(\mathbf{H})$ к сложному распределению Пуассона была установлена С. М. Буравлевым в случае, когда подстановки из $\mathbf{H}$ образуют латинский прямоугольник (см. [4]).

Также из теоремы 4 могут быть выведены достаточные условия сходимости к сложному распределению Пуассона для числа пар неперекрывающихся $\mathbf{G}$-эквивалентных цепочек, причем тип этого распределения зависит от типа группы подстановок $\mathbf{G}$.

Следствие 5 ([34]). *Если $\mathbf{X}$ получена по равновероятной схеме, $n \to \infty$, параметр N фиксирован, $s \to \infty$ так, что $C_n^2(1-N^{-1})^2 sN^{-s} \to$ $\to \lambda$, 0) сходится к распределению суммы*

$$u_1 v_1 + u_2 v_2 + \ldots + u_\pi v_\pi,$$

где случайные величины π, u_k и v_k независимы, величина π распределена по закону Пуассона с параметром λ, а величины u_l и v_l имеют геометрическое распределение с вероятностью успеха $1 - N^{-1}$.

В следствии 5 группа подстановок T_s состоит из подстановок циклического сдвига, т. е.

$$T_s = \left\{ \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 1 & 2 & \dots & n-1 & n \end{pmatrix}, \dots, \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & 1 & \dots & n-2 & n-1 \end{pmatrix} \right\}.$$

Множество Γ^{vs} выбирается в последнем случае не так как в случае точных повторений и цепочек с одинаковой структурой, что объясняется различием предельных распределений в следствиях 3, 4 и в следствии 5.

Теорема 4 также позволяет исследовать предельное распределение числа цепочек полиномиальной схемы с одинаковыми частотами встречаемости символов. В этом случае группа $\mathbf{G}$ совпадает со всей симметрической группой подстановок S_s.

3. Нормальный закон и распределения типа хи-квадрат

Теорема 5 ([39] (метод Янсона — Михайлова см. [45], [15])). *Если при $n \to \infty$ параметр $k \geqslant 2$ фиксирован, а параметр s, функция f и параметры случайной последовательности $\mathbf{X}$ меняются так, что для некоторого числа α, $0 < \alpha \leqslant 2/3$, выполнено условие*

$$\frac{(\mathbf{E}\mathbf{Z}_{n,k}(\mathbf{F}))^{\alpha}(s(n\varkappa_s(f)+s)^{k-1})^{2-\alpha}}{\mathbf{D}\mathbf{Z}_{n,k}(\mathbf{F})} \to 0,$$

то моменты и распределение случайной величины $\dfrac{\mathbf{Z}_{n,k}(\mathbf{F}) - \mathbf{E}\mathbf{Z}_{n,k}(\mathbf{F})}{\sqrt{\mathbf{D}\mathbf{Z}_{n,k}(\mathbf{F})}}$ *сходятся к моментам и распределению стандартного нормального закона.*

Применение известной теоремы работы [12] о k-кратных повторениях в последовательности s-зависимых случайных величин для описания достаточных условий асимптотической нормальности распределения $\mathbf{Z}'_{n,k}(\mathbf{F})$ дает худший результат, чем теорема 5.

Следствие 6 ([39]). *Пусть при $n \to \infty$ параметр $k \geqslant 2$ фиксирован, а параметр s и вероятности p_1, p_2, ... меняются так, что*

$$\frac{\left(\mathbf{E}\delta_{n,k}\right)^{\alpha} s^{2-\alpha}\left(n(\max\limits_{m\in\mathbb{N}} p_m)^s + s\right)^{(2-\alpha)(k-1)}}{\mathbf{D}\delta_{n,k}} \to 0, \quad 0 < \alpha \leqslant 2/3.$$

Тогда распределение случайной величины $\dfrac{\delta_{n,k} - \mathbf{E}\delta_{n,k}}{\sqrt{\mathbf{D}\delta_{n,k}}}$ *сходится к стандартному нормальному закону.*

В работе В. Г. Михайлова [13] получены близкие условиям теоремы 5 по форме достаточные условия для сходимости распределения числа точ-

ных повторений наборов из k цепочек к нормальному закону:

$$\frac{(s+np^s)^{2k}}{\mathbf{D}\delta_{n,k}} + \frac{(s+np^s)^{4k}(\mathbf{E}\delta_{n,k})^2}{(\mathbf{D}\delta_{n,k})^3} \to 0.$$

Нетрудно убедиться, что условие теоремы5 является более слабым.

Проверка условий теоремы5 для конкретных функций f связана с оценкой снизу дисперсии $\mathbf{Z}_{n,k}(\mathbf{F})$. При этом асимптотическое поведение величины $\mathbf{D}\mathbf{Z}_{n,k}(\mathbf{F})$ определяется соотношением величин s и $n\varkappa_s(f)$. Если $n\varkappa_s(f)s = o(1)$, то мы попадаем в нормальные зоны, смежные с пуассоновской и сложнопуассоновской зонами (см. выше).

Если $s = O(n\varkappa_s(f))$, то нижние и асимптотические оценки для $\mathbf{D}\mathbf{Z}_{n,k}(\mathbf{F})$ удается получить, если наложить ограничение на вид f:

$$f(x_1, x_2, \ldots, x_s) = f(x'_1, x'_2, \ldots, x'_s) \Leftrightarrow$$

$$\Leftrightarrow f(x_2, \ldots, x_s, x_1) = f(x'_2, \ldots, x'_s, x'_1). \quad (*)$$

Лемма 1. *Пусть* $\mathbf{H}$ *- подгруппа группы* S_N, *а* $\mathbf{G}$ *- такая подгруппа* S_s, *что подстановка циклического сдвига* $(1, 2, \ldots, s)$ *нормализует* $\mathbf{G}$ *в группе* S_s (*т.е.* $(1, \ldots, s)\,\mathbf{G}\,(s, \ldots, 1) = \mathbf{G}$.). *Тогда для функции* f, *для которой отношение* $\underset{f}{\sim}$ *является* $\mathbf{GH}$*-эквивалентностью, выполнено свойство* $(*)$.

Следствиями из этой теоремы 5 являются нормальные предельные теоремы для числа наборов из k $\mathbf{GH}$-эквивалентных цепочек.

Следствие 7 ([39]). *Пусть параметр* $k \geqslant 2$ *фиксирован, параметры* n *и* s *стремятся к бесконечности, а параметр* N *и вероятности* $p_1, p_2, \ldots, p_N$ *фиксированы,* $p_j > 0$, $j = 1, \ldots, N$, *и выполнено одно из условий*

$$\frac{n^{2k-1}}{s^{N(k+1)-1+\varepsilon}} \to \infty, \ \textit{при } k \leqslant \frac{3N}{2}, \quad \varepsilon > 0,$$

$$\frac{n}{s^{(N+1)/2}} \to \infty, \ \textit{при } k \geqslant \frac{3N+1}{2}.$$

Тогда моменты и распределение случайной величины

$$\frac{\zeta'_{n,k}(S_s) - \mathbf{E}\zeta'_{n,k}(S_s)}{\sqrt{\mathbf{D}\zeta'_{n,k}(S_s)}}$$

сходятся к моментам и распределению стандартного нормального закона. Причем

$$\mathbf{E}\zeta'_{n,k}(S_s) = (k!)^{-1} n^k \Big(\prod_{j=1}^{N} p_j\Big)^{(1-k)/2} k^{(1-N)/2} \times$$

$$\big(2\pi s\big)^{(k-1)(1-N)/2}\big(1+o(1)\big),$$

$$\mathbf{D}\zeta'_{n,k}(S_s) = \mathbf{E}\zeta_{n,k}(S_s) k\big((k-1)!\big)^{-1} D'''_k\big(1+o(1)\big),$$

$$D'''_k = n^{k-1} 2\Big(\prod_{j=1}^{N} p_j\Big)^{(1-k)} \big(2\pi s\big)^{(k-1)(1-N)} s d_k\big(1+o(1)\big),$$

$$d_k = \frac{k^{(N-1)/2}}{k-1} \int\limits_{1-k}^{0} \frac{dx}{\big(k^2-x^2\big)^{(N-1)/2}} - k^{(1-N)/2} > 0.$$

Если $\mathbf{E}\mathbf{Z}_{n,k}(\mathbf{F}) \to \infty$, а дисперсия $\mathbf{Z}_{n,k}(\mathbf{F})$ вырождена, то предельным распределением для $\mathbf{Z}_{n,k}(\mathbf{F})$ может быть хи-квадрат (см. [30]).

В заключение отметим некоторые другие (экстремальные) статистики, характеризующие подстановочную зависимость цепочек ПСП, исследования асимптотического поведения которых применительно к последовательностям, полученным по полиномиальной схеме, проводятся на основе представленных выше результатов:

$$\tau_{s,k}(\mathbf{H}) = \min\{n:\ \xi_{n,k}(\mathbf{H}) > 0\},$$

равную минимальной длине отрезка последовательности $\mathbf{X}$ на котором нашелся хотя бы один набор из k $\mathbf{H}$-эквивалентных цепочек,

$$\theta_{n,k}(\mathbf{H}) = \max\{s:\ \xi_{n,k}(\mathbf{H}) > 0\},$$

равную максимальной длине цепочек, составляющих набор из k $\mathbf{H}$-эквивалентных цепочек в отрезке $\mathbf{X}$ длины $n-s+1$.

Установлено (см. [32]), что в качестве предельного распределения для случайной величины $\tau_{s,k}(\mathbf{H})$ может выступать распределение Вейбула—Гнеденко и двойное экспоненциальное распределение, а предельное распределение $\theta_{n,k}(\mathbf{H})$ сосредоточено в одной или в двух точках. Аналогичные результаты получены ранее С. М. Буравлевым (см. [3]) для случая $\mathbf{H} = S_N$ и $k = 2$ и А. М. Зубковым, В. Г. Михайловым для $\delta_{n,k}$ (см., например, [6]).

Рассмотренные в докладе случайные величины $\mathbf{Z}_{n,k}(\mathbf{F})$, $\mathbf{Z}'_{n,k}(\mathbf{F})$, $\zeta'_{n,k}(\mathbf{G})$, $\xi_{n,k}(\mathbf{H})$, $\tau_{s,k}(\mathbf{H})$ и $\theta_{n,k}(\mathbf{H})$ предлагается применять в качестве статистик критериев выявления различных теоретико-вероятностных моделей подстано-

вочной зависимости цепочек ПСП. Описание конкретных типов теоретико-вероятностных моделей подстановочной зависимости цепочек ПСП, соответствия этих моделей различным типам генераторов, а также исследование эффективности применения указанных выше статистик для выявления таких моделей представляет собой отдельную научно-исследовательскую задачу, выходящую за рамки данного доклада.

Литература

[1] *Абдалимов Б.* Асимптотическая нормальность U-статистик для s-зависимых величин. Случайные процессы и смежные вопросы. Ташкент: Фан, 1970, ч. 1. С. 26–30.

[2] *Беляев П. Ф.* О совместном распределении частот длинных s-цепочек в простых однородных цепях Маркова с конечным множеством исходов. // Труды по дискретной математике. 1997. Т. 1. С. 19–42.

[3] *Буравлев С. М.* Повторения с точностью до перестановок в последовательности независимых испытаний // Дискретная математика. 1999. Т. 11, вып. 1. С. 53–75.

[4] *Буравлев С. М.* Повторения с точностью до перестановок, образующих латинский прямоугольник // Дискретная математика. 2000. Т. 12, вып. 1. С. 24–46.

[5] *Глухов М. М.*, *Елизаров В. П.*, *Нечаев А. А.* Алгебра. М.: Гелиос АРВ, 2003. Т. 2, 416 с.

[6] *Зубков А. М.*, *Михайлов В. Г.* Предельные распределения случайных величин, связанных с длинными повторениями в последовательности независимых испытаний // Теория вероятн. и ее применен. 1974. Т. 19, вып. 1. С. 173–181.

[7] *Зубков А. М.*, *Михайлов В. Г.* О повторениях s-цепочек в последовательности независимых величин // Теория вероятн. и ее применен. 1979. Т. 24, вып. 2. С. 267–279.

[8] *Кнут Д.* Искусство программирования для ЭВМ: Получисленные алгоритмы. М.: Мир, 1977. Том 2. 724 с.

[9] *Королюк В. С.*, *Боровских Ю. В.* Теория U-статистик. Киев: Наукова думка, 1989.

[10] *Лидл Р.*, *Нидерайтер Г.* Конечные поля. М.: Мир, 1988. Т. 2. 822 с.

[11] *Медведев Ю. И.* Разделимые статистики в полиномиальной схеме I, II. // Теория вероятн. и ее примен. 1977. Т. 22, вып. 1. С. 3-17. Т. 22, вып. 3. С. 623–631.

[12] *Михайлов В. Г.* Асимптотическая нормальность в схеме конечно-зависи мого размещения частиц по ячейкам // Матем. сб. 1982. Т. 119, № 4. С. 509–520.

[13] *Михайлов В. Г.* Об асимптотической нормальности U-статистик с неотрицательными ядрами // Труды МИАН. 1986. Т. 177. С. 105–113.

[14] *Михайлов В. Г.* Асимптотическая нормальность разделимых статистик от частот m-цепочек // Дискретная математика. 1989. Т. 1, вып. 4. С. 92–103.

[15] *Михайлов В. Г.* Об одной теореме Янсона // Теория вероятн. и ее применен., 1991. Т. 36. С. 168–170.

[16] *Михайлов В. Г.* Явные оценки в предельных теоремах для сумм случайных индикаторов // Обозрение прикл. промышл. матем., сер. «Дискретная математика». 1994. Т. 1, вып. 4. С. 580-617.

[17] *Михайлов В. Г.* Оценка точности сложной пуассоновской аппроксимации по методу Стейна—Чена // Обозрение прикл. промышл. матем., «Дискретная математика». 1996. Т. 3, вып. 4. С. 530-548.

[18] *Михайлов В. Г.* Оценка точности сложной пуассоновской аппроксимации для распределения числа совпадающих цепочек // Теория вероятн. и ее применен. 2001. Т. 46, вып. 4. С. 713–723.

[19] *Михайлов В. Г.* Об асимптотических свойствах распределения числа пар H-связанных цепочек // Дискретная математика. 2002. Т. 14, вып. 3. С. 122–129.

[20] *Михайлов В. Г.* Предельные теоремы пуассоновского типа для числа пар H-связных цепочек // Труды по дискретной математике. Т. 7. М.: ФИЗМАТЛИТ, 2003. С. 138–155.

[21] *Михайлов В. Г.* Об особенностях асимптотического поведения числа пар структурно близких цепочек // Труды по дискретной математике. Т. 8. М.: ФИЗМАТЛИТ, 2004. С. 176–186.

[22] *Михайлов В. Г.*, *Шойтов А. М.* Структурная эквивалентность s-цепочек в случайных дискретных последовательностях // Дискретная матем. 2003. Т. 15, № 4. С. 7–34.

[23] *Ронжин А. Ф.* О предельных теоремах для сумм зависимых случайных величин // Теория вероятн. и ее применен. 1979. Т. 24, вып. 2. С. 542–552.

[24] *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М.: Наука, 1982.

[25] *Севастьянов Б. А.* Предельный закон Пуассона в схеме сумм зависимых случайных величин // Теория вероятностей и ее применения. 1972. Т. 17, вып. 4. С. 333–338.

[26] Словарь криптографических терминов (под редакцией Б. А. Погорелова и В. Н. Сачкова). М.: 2006, МЦНМО. 94 с.

[27] *Степанов В. Е.* Некоторые статистические критерии для цепей Маркова // Теория вероятностей и ее применения. 1957. Т. II, вып. 1. С. 143–144.

[28] *Успенский В. А.*, *Семенов А. Л.*, *Шень А. Х.* // Успехи матем. наук, 1990. Т. 45, вып. 1(271). С. 105–162.

[29] *Харин Ю. С.*, *Берник В. И.*, *Матвеев Г. В.*, *Агиевич С. В.* Основы криптологии. Минск: Новое знание, 2003. 382 с.

[30] *Шойтов А. М.* Предельные распределения числа наборов H-эквивалентных отрезков в последовательности независимых испытаний // Обозрение прикладной и промышленной математики. 1999. Т. 6, вып. 1. С. 218–220.

[31] *Шойтов А. М.* Повторения значений функции от отрезков последовательности независимых испытаний // Дискретная математика. 2000. Т. 12, вып. 3. С. 49–59.

[32] *Шойтов А. М.* Предельные распределения числа наборов H-эквивалентных отрезков в равновероятной полиномиальной схеме серий // Дискретная математика. 2002. Т. 14, вып. 1. С. 82–98.

[33] *Шойтов А. М.* Об одной особенности асимптотического поведения числа наборов H-эквивалентных n-цепочек в неравновероятной полиномиальной схеме // Труды по дискретной математике. Т. 7. М.: ФИЗМАТЛИТ, 2003. С. 227–238.

[34] *Шойтов А. М.* О перестановочной эквивалентности цепочек полиномиальной схемы // Вестник ИКСИ Академии ФСБ РФ, серия «К», специальный выпуск. М., 2003. С. 107–113.

[35] *Шойтов А. М.* Предельные распределения случайных величин, характеризующих связь цепочек полиномиальной схемы структурной эквивалентностью // Труды по дискретной математике. Т. 8. М.: ФИЗМАТЛИТ, 2004. С. 312–326.

[36] *Шойтов А. М.* Пуассоновское приближение для числа повторений значений дискретной функции от цепочек // Дискретная математика, 2005. Т. 17, вып. 2. С. 56–69.

[37] *Шойтов А. М.* Повторения неперекрывающихся цепочек полиномиальной схемы с точностью до перестановочной эквивалентности // Труды по дискретной математике. Т. 9. М.: ФИЗМАТЛИТ, 2006 (в печати).

[38] *Шойтов А. М.* Сложное распределение Пуассона для числа повторений значений дискретной функции от цепочек // Дискретная математика, 2007 (в печати).

[39] *Шойтов А. М.* Нормальное приближение в задаче об эквивалентных цепочках // Труды по дискретной математике. Т. 10. М.: ФИЗМАТЛИТ, 2007 (в печати).

[40] An introduction to Stein's method. (redaction Barbour A.D., Chen L.H.D.) Singapore: University Press and World Scientific, 2005, vol. 4.

[41] *Barbour A. D.*, *Chen L. H. Y.*, *Loh W.-L.* Compound poisson approximation for nonnegative random variables via Stein's method // Appl. Probab. 1992. V. 20, No. 4. P. 1843–1866.

[42] *Barbour A. D.*, *Holst L.*, *Janson S.* Poisson Approximation, Oxford: Oxford University Press, 1992.

[43] *Gustafson H. M.*, *Dawson E. P.*, *Golic J. Dj.* Randomness Measures Related to subset occurence, in Lecture Notes in Computer Science 1029; Advances in Cryptology: Proc. Cryptography: Policy and Algorithms, Ed Dawson, J.Golic (Eds.), Brisbane, Queensland, Australia, July 1995, pp. 132–143. Berlin: Springler-Verlag, 1996.

[44] *Gustafson H.*, *et. al.* Statistical test suite Crypt-SX. Available on `http://www.isrc.qut.edu.au/cryptx`.

[45] *Janson Sv.* Normal convergence by higher semiinvariants with applications to sums dependent random variables and random grafs // Ann. Probab. 1998. V. 16, № 1. P. 305–312.

[46] *Marsaglia G.* DIEHARD Statistical Tests. Available on `http://stat.fsu.edu/~geo/diehard.html`.

[47] *Marsaglia G.* The Marsaglia random CDROM with the Diehard Battery of test of randomness, 1996. (доступен в интернет по адресу `hppt://stat.fsu.edu/pub/diehard`)

[48] *Roos M.* Stein method for compound Poisson approximation: The local approach // Ann. Appl. Probab. 1994. V. 4. P. 1177–1187.

[49] *Rukhin A., et. al.* A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22 (with revisions dated May 15, 2001).

Безопасность, верификация и теория конформности

И. Б. Бурдонов, А. С. Косачев, В. В. Кулямин

1. Введение и постановка проблемы

Кризис в индустрии производства программного обеспечения в 2000 году не только отрезвил участников рынка, развеяв множество грандиозных, хотя и несбыточных планов, но и вскрыл возникший перекос в технологиях разработки программ. Они позволяли достаточно быстро и с небольшими затратами создавать программные комплексы такой сложности, которая и не снилась даже большим коллективам разработчиков еще в середине 80-х годов. Однако для проверки их безопасности и корректности работы использовались те же методы, которые были изобретены еще в 60-х годах. Если до кризиса клиента еще можно было убедить отдать деньги за сырой продукт, распаляя его надежды на потрясающие результаты внедрения: снижение издержек, повышение эффективности и прочее, то после ситуация резко изменилась. Теперь руководители проектов должны были, скрепя сердце, тратить драгоценное время и не менее дорогие усилия разработчиков не только на то, чтобы создать нечто новое и невиданное, но и продемонстрировать заказчику, что оно действительно решает нужные ему задачи и делает это правильно. Неожиданно высокая трудоемкость этой второй части работ, на которую раньше и внимания-то особо не обращали, вынудила заняться поисками технологий, позволяющих сделать это более эффективно.

В новых обстоятельствах внезапно пригодилась «нерыночная» увлеченность программистов первой волны, уже ставших классиками Computer Science, корректностью работы программ. Стали востребованными созданные на основе их идей техники разработки программного обеспечения, изначально работающего правильно, и методы проверки правильности функционирования произвольно взятой программы. Даже компании, чьи продукты 10 лет назад славились далеко не идеальной стабильностью и надежностью работы, провозглашают курс на повышение надежности и безопасности работы программного обеспечения и проводят для своих

разработчиков и партнеров тренинги по техникам написания корректных и безопасных программ.

Прямо на наших глазах складывается новая дисциплина, стоящая на границе между теоретической информатикой и такими инженерными науками, как инженерия программного обеспечения и системная инженерия, — *тестирование на основе моделей*. Во многом она опирается на работы различных исследователей, выполненные в 80-х и в 90-х годах прошлого века и посвященные проблемам тестирования телекоммуникационных протоколов. Самые первые же статьи, которые с полным правом можно отнести с этой области, появились еще в конце 60-х—начале 70-х годов. Тем не менее, серьезный практический интерес к ее результатам возник только в начале XXI века, в связи с востребованностью эффективных методов контроля и обеспечения качества сложных программных и программно-аппаратных систем в индустрии.

1.1. Безопасность, конформность и тестирование

В первом приближении будем считать, что система безопасна (secure), если при любом взаимодействии с ней она не может себя вести недекларированным образом. Декларированность поведения определяется требованиями к системе. Конформность понимается как соответствие требованиям, то есть отсутствие недекларированного поведения. Верификацией системы называют проверку её соответствия требованиям.

Поведение целевой (исследуемой) системы описывается в терминах её «внешнего», то есть наблюдаемого взаимодействия с окружением. У системы может быть и внутренняя, не проявляющаяся во внешних взаимодействиях, ненаблюдаемая активность. Рассматривается широко распространенный частный случай взаимодействия, при котором система и окружение обмениваются между собой дискретными порциями информации (сообщениями). Такие системы называют системами ввода-вывода [23, 27, 30]. Сообщение, передаваемое из окружения в систему, называется стимулом (input), а сообщение, передаваемое из системы в окружение, — реакцией (output). Следуя нотации алгебры процессов CCS (Calculus of Communicating Systems [25, 26]), обозначим стимулы как $?m$, а реакции — как $!m$, где m — символ сообщения.

Чтобы формально определить соответствие системы требованиям, нужно, прежде всего, формализовать и то и другое. Для этого объекты реального мира отображаются в модельные (математические) объекты. Модель требований называется спецификацией, а модель целевой системы — реализацией. Между объектами-моделями задается отношение конформности как математическое соответствие, то есть подмножество декартового произведения множеств реализаций и спецификаций. Если реализа-

ция как модель системы конформна спецификации как модели требований, то считается, что система конформна требованиям. Верификация проверяет отношение реализации к спецификации, но само моделирование, то есть соответствие системы и требований их моделям, предполагается «правильным» и не проверяется. Точно также предполагается, что отображение реальной конформности в модельное отношение также «правильное», то есть модельное отношение является формализацией интуитивного понимания требований [17].

Спецификация считается известной и заданной. Что касается реализации, то, так называемая, «тестовая гипотеза» предполагает лишь, что модель системы существует, но она может быть как известна, так и неизвестна [1]. Что делать в последнем случае? Если конформность выражается в терминах взаимодействия, становится возможным тестирование как проверка конформности в эксперименте (динамическая верификация). При этом по спецификации генерируется набор модельных тестов и определяется формальное отношение «реализация прошла (passes) тест». Набор тестов называется полным, если реализация конформна спецификации тогда и только тогда, когда реализация проходит каждый тест из набора. После этого модельные тесты транслируются в реализационное представление и пропускаются на целевой системе. Если все они проходят, то конформность системы требованиям считается доказанной. Разумеется, здесь предполагается, что трансляция тестов осуществлена «правильно».

1.2. Композиционная система и запрещённые действия

Целевая система может быть (и, как правило, является) не монолитной, а состоящей из компонентов. В этом случае всякое взаимодействие системы с окружением включает взаимодействие компонентов между собой. Последнее становится внутренней, ненаблюдаемой извне активностью. Возникает вопрос: можно ли построить безопасную систему из опасных компонентов? Можно, если учитывать, что окружение каждого компонента не произвольно, а ограничено, частично или полностью, другими компонентами, поведение которых определяется требованиями к ним.

В этом случае под опасным компонентом следует понимать не любой компонент, а такой, поведение которого определено, но частично. Для этого спецификация должна описывать не только декларированное поведение, но и случаи, когда поведение «имеет право» быть любым, включая заведомо не разрешенное [9, 24]. Такое поведение будем называть «запрещенным» и обозначать в спецификации символом γ. Компонент, конформный такой спецификации, будем называть условно-безопасным. Если условно-безопасный компонент конформен своей спецификации, то он может иметь опасное поведение, но нам известно, при каком взаимодействии этого ком-

понента с его окружением это возможно, а при каком нет. Композиционная система, построенная из условно-безопасных компонентов, безопасна, если запрещенное поведение в любом компоненте окажется недостижимо при любом взаимодействии композиционной системы с её окружением.

Приведём примеры запрещенного поведения.

1. В системах динамического распределения памяти поведение процедуры освобождения памяти не декларировано для освобождения незахваченной ранее памяти.
2. «Кнопка запуска ракеты» в некоторых случаях явно не разрешается.

1.3. Системы размеченных переходов

В качестве моделей (реализаций и спецификаций) выберем достаточно традиционные системы размеченных переходов — LTS (Labelled Transition System). Одна из причин такого выбора заключается в том, что для таких систем определены операции композиции, заимствуемые из алгебр процессов.

LTS — это ориентированный граф, в котором вершины называются состояниями, выделено одно начальное состояние, дуги помечены символами действий и называются переходами. Действием может быть передача стимула или реакции из заданного вместе с LTS алфавита L внешних действий, а также внутреннее, ненаблюдаемое действие, традиционно обозначаемое символом τ. Дополнительно введем запрещённое действие γ. Переход из состояния s в состояние s' по действию z обозначается $s - z \to s'$. Для дальнейшего нам понадобится понятие стабильного состояния — состояния, в котором нет τ- и γ-переходов. Теперь безопасная система определяется как система, в LTS-модели которой нет γ-переходов, достижимых из начального состояния.

1.4. Композиция LTS

Определим композицию LTS, которая строит LTS-модель композиционной системы по LTS-моделям её компонентов. Такую композицию будем называть . Она соответствует оператору композиции в алгебре процессов CCS. Результат композиции LTS $\boldsymbol{S}_1$ (в алфавите A) и $\boldsymbol{S}_2$ (в алфавите B) — это третья LTS, обозначаемая $\boldsymbol{S}_1 \upharpoonleft\!\upharpoonright \boldsymbol{S}_2$. Её состояния — это пары состояний LTS-операндов, начальное состояние — это пара начальных состояний. Стимул $?m$ и реакция $!m$ называются *противоположными* действиями; определяется операция «подчёркивание»: $\underline{?m} = !m$ и $\underline{!m} = ?m$. В алфавит композиции попадают те внешние действия из алфавита каждого LTS-операнда, для которых в алфавите другого LTS-операнда нет противоположных действий: $A \upharpoonleft\!\upharpoonright B = (A \setminus \underline{B}) \cup (B \setminus \underline{A})$. Композиционные переходы

делятся на асинхронные и синхронные. Асинхронному переходу соответствует переход в одном из LTS-операндов, помеченный внешним действием композиционного алфавита, символом τ или γ; измениться может состояние только одного LTS-операнда. Синхронному переходу соответствует пара переходов в LTS-операндах по противоположным действиям, которая в композиции становится τ-переходом; измениться могут состояния обоих LTS-операндов. Формально композиция переходов определяется следующими правилами вывода:

$$
\begin{array}{lll}
z \in (A \setminus \underline{B}) \cup \{\tau, \gamma\} \ \& \ a - z \to a' & & \vdash ab - z \to a'b; \\
z \in (B \setminus \underline{A}) \cup \{\tau, \gamma\} & \& \ b - z \to b' & \vdash ab - z \to ab'; \\
z \in A \setminus \underline{B} & \& \ a - z \to a' \ \& \ b - z \to b' & \vdash ab - \tau \to a'b'.
\end{array}
$$

1.5. Проблема монотонности композиции и предлагаемое решение

Будем предполагать, что отношение конформности является предпорядком (рефлексивно и транзитивно). Пусть нам заданы спецификации компонентов. Определим свойства, которыми должна обладать «полная» спецификация композиционной системы:

1. *Условие монотонности*: композиция любых реализаций компонентов, конформных своим спецификациям, конформна спецификации системы.
2. *Условие максимальности требований*: спецификация системы предъявляет к системе самые сильные требования среди всех спецификаций, которые удовлетворяют условию монотонности, то есть конформна каждой из них.

Спецификацию, удовлетворяющую условию монотонности, будем называть *корректной* спецификацией. Заметим, что спецификация, разрешающая «всё», заведомо корректна. Если же корректная спецификация удовлетворяет условию максимальности требований, то будем называть её *косой* композицией спецификаций компонентов. Такую косую композицию будем обозначать $\boldsymbol{S}_1 \mathbin{/\!/} \boldsymbol{S}_2$. Проблема заключается в том, что прямая композиция спецификаций компонентов, вообще говоря, не является не только косой композицией, но и вообще корректной спецификацией системы: она может не удовлетворять условию монотонности [18, 10, 11]. В частности, возможно нарушение безопасности: прямая композиция спецификаций безопасна, а композиция конформных реализаций опасна.

Основная идея предлагаемого решения проблемы заключается в том, чтобы косую композицию выполнять как прямую композицию преобразованных спецификаций. Преобразование $\mathcal{T}$: LTS $\to$ LTS, удовлетворяющее

условию $\mathcal{T}(\boldsymbol{S}_1) \upharpoonleft\!\!\upharpoonright \mathcal{T}(\boldsymbol{S}_2) = \boldsymbol{S}_1 \mathbin{/\!\!/} \boldsymbol{S}_2$, будем называть *монотонным преобразованием*. Преобразованная спецификация должна быть эквивалентна исходной спецификации по отношению конформности: множество конформных реализаций сохраняется при преобразовании.

2. Отношение конформности $\mathrm{ioco}_{\beta\gamma\delta}$

Рассматривается отношение конформности, основанное на минимальных тестовых возможностях по управлению реализацией (тестовые воздействия) и наблюдению её поведения. Тест может посылать в реализацию отдельный стимул и наблюдать либо его приём реализацией, либо отказ в приёме стимула. Также тест может принимать любую реакцию от реализации, наблюдая либо выдаваемую реализацией реакцию, либо отсутствие выдаваемых реакций. Отношение конформности формулируется в терминах трасс (последовательностей) наблюдений и складывается из двух условий: 1) гипотеза о безопасности, которая является предусловием тестирования и определяет класс реализаций, при тестировании которых не возникает запрещённых действий, и 2) условие, проверяемое при тестировании реализаций, удовлетворяющих гипотезе о безопасности.

2.1. Трассы наблюдений

Для того чтобы можно было проводить как статическую, так и динамическую верификацию, будем формализовать поведение системы как множество трасс (последовательностей) наблюдений, которые могут быть получены в тестовых экспериментах с системой. Спецификацию также будем понимать как множество трасс, а конформность как отношение между двумя множествами трасс. Поскольку состояния тестируемой системы, как правило, не наблюдаемы при тестировании, не будем рассматривать отношения конформности, основанные на состояниях, такие как изоморфизм и всевозможные симуляции: сильная (strong), слабая (weak), и т.п. В том случае, когда состояния реализации всё же открыты, будем считать, что имеется специальная реакция «сообщение о состоянии» (status message). Предполагается, что эта реакция «достоверна», то есть она выдаётся в том состоянии, о котором она сообщает, и сама не меняет этого состояния. Наблюдения таких специальных реакций, если они есть, также включаются в трассы наблюдений. Можно отметить, что тестирование реализаций с открытыми состояниями существенно упрощается, сводясь, фактически, к обходу графа переходов LTS [24, 4, 5, 6, 20, 7].

Будем рассчитывать на минимальные тестовые возможности управления реализацией, которые сводятся к тестовым воздействиям двух типов: приём реакций от реализации и посылка стимула в реализацию. При этом

будем считать, что тестер не может «выбирать», какую реакцию от реализации ему принять, а какую нет: либо принимается любая реакция, либо никакая не принимается. Стимул, напротив, всегда посылается один: нет совмещения посылки стимула с приёмом реакций или посылкой другого стимула.

Также будем рассчитывать на минимальные тестовые возможности наблюдения, которые сводятся к двум типам: наблюдение внешнего действия (выдача реализацией реакции или приём реализацией стимула) и отказ, понимаемый как отсутствие таких наблюдений. Последнее возможно в том случае, когда во взаимодействии возникает тупик: реализация ничего не может делать и *останавливается* (до следующего тестового воздействия, которое может этот тупик разрешить). Поскольку τ- и γ-действия всегда могут выполняться, тупик возникает только в стабильных состояниях. Для указанных выше типов тестовых воздействий у нас могут быть отказы двух типов:

1. *Стационарность* как отсутствие реакций (quiescent), когда тестер принимает реакции; обозначается символом δ [30, 31]. Соответствующее состояние реализации называется стационарным.
2. *Блокировка стимула* (input refusal) как отказ в приёме данного стимула $?x$, посылаемого в реализацию тестером; обозначается как $\{?x\}$ [28, 29, 22, 2, 8, 16, 14].

Стационарность может наблюдаться, если, например, время ожидания следующей реакции ограничено сверху известным тайм-аутом. Истечение тайм-аута означает, что реакций больше не будет до нового тестового воздействия (посылки стимула). Другой вариант: окружение получает специальное достоверное (безошибочное и, значит, не требующее тестирования) «извещение о прекращении передачи реакций». Блокировка стимула наблюдаема, если посылка стимула в реализацию предусматривает достоверное «уведомление о вручении», которое должно придти за время, ограниченное сверху известным тайм-аутом. Другой вариант: окружение достоверно получает либо «уведомление о вручении», либо «уведомление о невручении».

Наблюдение отказов возможно только, если в LTS нет дивергенции — бесконечной последовательности τ-действий, поскольку в этом случае система не выполняет никаких внешних действий и не останавливается. На каждое тестовое воздействие (наблюдение внешнего действия или отказа) желательно получение ответа, поэтому дивергенцию будем считать запрещенным действием и рассматривать как один из видов γ-действия.

γ-действие будем считать условно-наблюдаемым действием, и включать его в трассу. Как событие γ-действие может возникать при взаи-

модействии, но в дальнейшем ограничимся только таким тестированием, при котором γ-действия не будут выполняться. Тем самым, предполагается, что окружение должно взаимодействовать с реализацией правильно в том смысле, что такое взаимодействие не должно приводить к γ-действиям реализации. Если, например, интерфейс реализации содержит операции с предусловиями, то окружение не должно вызывать эти операции с нарушением предусловий: поведение реализации в этом случае считается нежелательным (неопределённым) и моделируется γ-действием. Иными словами, поскольку мы хотим убедиться в правильности реализации, а не окружения, нас не интересует поведение реализации при вызове её операций с нарушением предусловий, и такое поведение не регламентируется спецификацией. Семантика γ-действия предполагает, что после него любые наблюдения недостоверны, поэтому после γ-действия никакие наблюдения невозможны. Напомним, что наша цель — уметь строить безопасные системы из условно-безопасных компонентов, когда при взаимодействии компонентов γ-действия в них не выполняются.

Для получения всех трасс LTS достаточно в каждом стабильном состоянии добавить петлю, помеченную отказом, который в этом состоянии может возникать. Кроме того, каждый γ-переход перенаправим в добавленное терминальное γ-состояние, и для моделирования дивергенции γ-действием из каждого дивергентного состояния (в котором начинается дивергенция) добавим γ-переход в γ-состояние. После этого нужно взять последовательности символов, кроме символа τ, которыми помечены все конечные цепочки переходов LTS, начинающиеся в начальном состоянии. Множество трасс LTS $\boldsymbol{S}$ будем обозначать как $\mathbf{Traces}(\boldsymbol{S})$ и называть *трассовой моделью*. Заметим, что такие трассы, в которые, кроме внешних действий, входят отказы, являются разновидностью трасс с отказами (failure traces) [12, 13]. Отличие в том, что мы разрешаем только два типа отказов: стационарность и блокировки стимулов.

2.2. Безопасные трассы и гипотеза о безопасности

Будем говорить, что тестирование безопасно, если оно не приводит к γ-действиям (включая дивергенцию). Определим это формально для LTS $\boldsymbol{S}$. Заметим, что все определения безопасности существенно зависят только от трассовой модели $\mathbf{Traces}(\boldsymbol{S})$, то есть LTS с одним множеством трасс эквивалентны с точки зрения безопасности.

Стимул $?x$ и его блокировка $\{?x\}$ безопасны после трассы σ, если $\sigma ?x\gamma \notin \mathbf{Traces}(\boldsymbol{S})$. Все реакции и стационарность безопасны после трассы σ, если ни для какой реакции $!y$ не существует трассы $\sigma !y\gamma \notin \mathbf{Traces}(\boldsymbol{S})$. Множество символов, безопасных в LTS $\boldsymbol{S}$ после трассы σ, обозначается как $\mathbf{SafeSymbols}(\boldsymbol{S}\ \mathbf{after}\ \sigma)$. Заметим, что, если трасса $\sigma \notin \mathbf{Traces}(\boldsymbol{S})$, все

символы безопасны после неё, а если $\sigma \in \mathbf{Traces}(\boldsymbol{S})$, то это не обязательно так. Кроме того, продолжение трассы $\sigma \in \mathbf{Traces}(\boldsymbol{S})$ безопасным символом может принадлежать или не принадлежать множеству трасс LTS. Трасса σ безопасна, если $\gamma \notin \mathbf{Traces}(\boldsymbol{S})$, $\sigma \in \mathbf{Traces}(\boldsymbol{S})$ и любой префикс трассы σ продолжается в ней символом, безопасным после этого префикса. Подмножество безопасных трасс LTS $\boldsymbol{S}$ будем обозначать как $\mathbf{SafeTraces}(\boldsymbol{S})$. LTS безопасна, если все её трассы безопасны: $\boldsymbol{S}$ **secure** $\overset{\text{def}}{\Longleftrightarrow}$ $\mathbf{SafeTraces}(\boldsymbol{S}) = \mathbf{Traces}(\boldsymbol{S})$. Тестирование безопасно, если наблюдаются только безопасные трассы.

Поскольку тестируется неизвестная реализация, не может быть абсолютной уверенности в безопасности тестирования. Поэтому необходимо выдвинуть гипотезу о том, что реализация принадлежит некоторому классу *безопасно-тестируемых* реализаций. Такую гипотезу будем называть *гипотезой о безопасности*. Ограничимся такими отношениями конформности, которые проверяемы при безопасном тестировании, и поэтому желательно, чтобы класс конформных реализаций являлся подклассом класса безопасно-тестируемых реализаций. В этом случае имеется потенциальная возможность удостовериться, является ли любая реализация конформной или нет: если она не удовлетворяет гипотезе о безопасности, она неконформна, а если удовлетворяет, то проводим тестирование. Здесь отношение конформности складывается из двух условий: 1) гипотеза о безопасности, которая является предусловием тестирования, и 2) условие, проверяемое при тестировании реализаций, удовлетворяющих гипотезе о безопасности.

Безотносительно к спецификации реализация безопасно-тестируема только тогда, когда в ней вообще нет γ-действий. Хотя в этом случае любое тестирование безопасно, ни откуда не следует, что такой класс содержит все реализации, конформные данной спецификации. Выход в том, чтобы проводить тестирование не «вообще», а для проверки конформности заданной, известной спецификации. Это уже будет не любое тестирование. Например, нам не нужно сравнивать поведение реализации и спецификации после трассы, которой, согласно спецификации, не должно быть в конформной реализации. Фактически, здесь идёт речь о том, что тестирование проводится, вообще говоря, «до первой ошибки». Таким образом, класс безопасно-тестируемых реализаций зависит от спецификации.

Сформулируем предлагаемую гипотезу о безопасности для выбранных нами тестовых возможностей: реализация $\boldsymbol{I}$ безопасно-тестируема для заданной спецификации $\boldsymbol{S}$, обозначается $\boldsymbol{I}$ **safe for** $\boldsymbol{S}$, тогда и только тогда, когда выполняются два условия:

1) $\gamma \notin \mathbf{Traces}(\boldsymbol{S}) \implies \gamma \notin \mathbf{Traces}(\boldsymbol{I})$;

2) $\forall \sigma \in \mathbf{SafeTraces}(\boldsymbol{S})\, \forall u \in \mathbf{SafeSymbols}(\boldsymbol{S}\ \mathbf{after}\ \sigma)\ u \in \mathbf{SafeSymbols}(\mathbf{I}\ \mathbf{after}\ \sigma)$.

Короче это можно сформулировать, используя тестовые трассы. Трасса называется тестовой, если она безопасна или является продолжением безопасной трассы символом, безопасным после неё. Обозначая множество тестовых трасс LTS $\boldsymbol{S}$ как $\mathbf{TestTraces}(\boldsymbol{S})$, имеем:

$$\boldsymbol{I}\ \mathbf{safe\ for}\ \boldsymbol{S} \iff \mathbf{TestTraces}(\boldsymbol{S}) \cap \mathbf{Traces}(\boldsymbol{I}) \subseteq \mathbf{TestTraces}(\boldsymbol{I}).$$

Тестовые трассы спецификации — это как раз те трассы, которые нужны для проверки конформности любой безопасно-тестируемой реализации.

2.3. Отношение конформности

Правила предлагаемого отношения конформности $\mathbf{ioco}_{\beta\gamma\delta}$ применяются к безопасно-тестируемым реализациям и имеют вид «*Реализация может...только тогда, когда для спецификации это возможно в такой же ситуации, то есть, после той же самой трассы, безопасной в спецификации*», где многоточие означает *символ, оставляющий трассу безопасной в спецификации*, то есть одно из следующих:

- *Правило реакции*: «выдать данную реакцию».
- *Правило стационарности*: «не выдавать никаких реакций».
- *Правило стимула*: «принять данный стимул».
- *Правило блокировки*: «блокировать данный стимул».

Теперь дадим формальное определение (заметим, что оно зависит только от трассовых моделей реализации и спецификации):

$$\begin{aligned}&\boldsymbol{I}\ \mathbf{ioco}_{\beta\gamma\delta}\ \boldsymbol{S} \overset{\text{def}}{\iff} \boldsymbol{I}\ \mathbf{safe\ for}\ \boldsymbol{S}\\ &\quad \&\ \forall \sigma \in \mathbf{SafeTraces}(\boldsymbol{S})\, \forall u \in \mathbf{SafeSymbols}(\boldsymbol{S}\ \mathbf{after}\ \sigma)\\ &\quad (\sigma u \in \mathbf{Traces}(\boldsymbol{I}) \implies \sigma u \in \mathbf{Traces}(\boldsymbol{S})).\end{aligned}$$

В терминах тестовых трасс проверяемое условие записывается короче:

$$\mathbf{TestTraces}(\boldsymbol{S}) \cap \mathbf{Traces}(\boldsymbol{I}) \subseteq \mathbf{Traces}(\boldsymbol{S}).$$

Соответственно:

$$\boldsymbol{I}\ \mathbf{ioco}_{\beta\gamma\delta}\ \boldsymbol{S} \iff \mathbf{TestTraces}(\boldsymbol{S}) \cap \mathbf{Traces}(\boldsymbol{I}) \subseteq \mathbf{Traces}(\boldsymbol{S}) \cap \mathbf{TestTraces}(\boldsymbol{I}).$$

На рис. 1 приведены примеры спецификации и трёх реализаций. Первая реализация конформна спецификации, вторая не удовлетворяет гипотезе о безопасности, третья безопасно-тестируема, но не конформна.

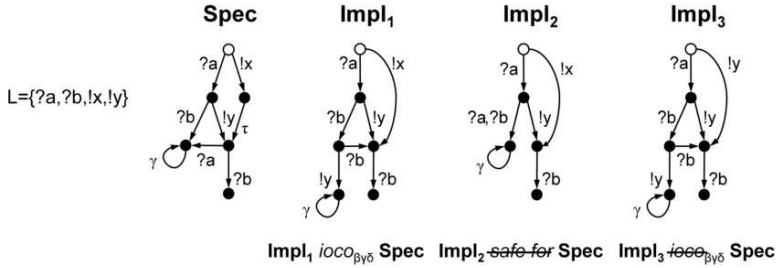


Рис. 1. Конформные и неконформные реализации

Если спецификация безопасна, конформность сводится к вложенности трасс. На рис. 2 приведены примеры безопасной реализации, которая конформна как безопасной, так и опасной спецификациям. Последняя, в силу рефлексивности, конформна сама себе.

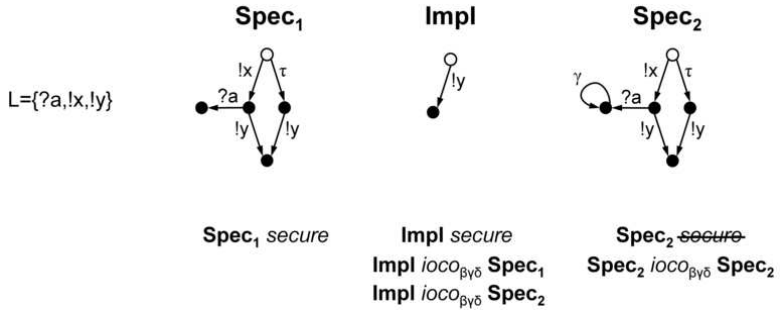


Рис. 2. Безопасные и опасные реализации и спецификации

3. Монотонное преобразование спецификации

Напомним, что целью монотонного преобразования является получение спецификации, эквивалентной исходной спецификации по множеству конформных реализаций, но удовлетворяющей условию монотонности: композиция любых реализаций компонентов, конформных своим спецификациям, конформна композиции преобразованных спецификаций.

3.1. Возможность построения безопасной системы из опасных компонентов

Для проверки безопасности системы, построенной из компонентов, конформных своим спецификациям, нам нужно: 1) построить косую композицию спецификаций компонентов, 2) проверить её безопасность (недо-

стижимость γ-действий). Прежде всего, продемонстрируем возможность этого на простом примере (рис. 3). Здесь косая композиция опасных спецификаций совпадает с их прямой композицией и сама безопасна.

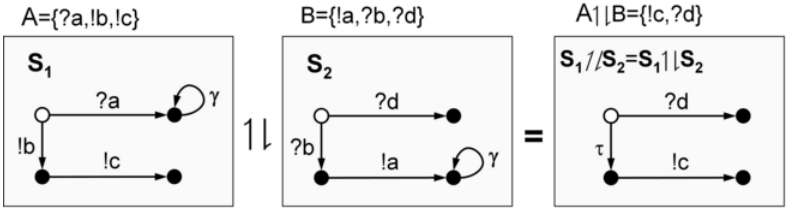


Рис. 3. Безопасная система, построенная из опасных компонентов

3.2. Существование монотонного преобразования

Монотонных преобразований LTS-спецификаций может быть много. Сначала покажем, что такое преобразование существует. Определим объединение множества LTS как новую LTS, которая строится добавлением нового начального состояния и проведением из него τ-переходов во все начальные состояния объединяемых LTS (рис. 4). Трассовая модель объединения LTS совпадает с объединением трассовых моделей объединяемых LTS.

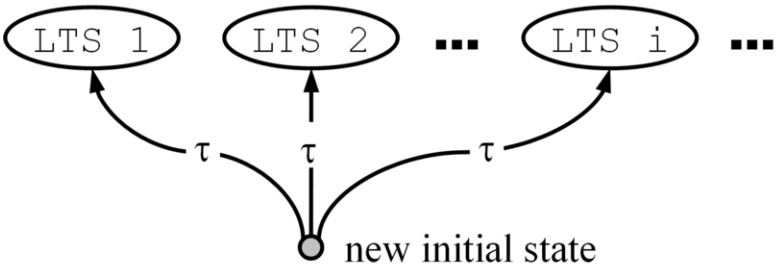


Рис. 4. Объединение LTS

Нетрудно показать, что объединение реализаций, конформных заданной спецификации, является её монотонным преобразованием. Конечно, такое определение преобразования неконструктивно и, как правило, неалгоритмизуемо. В частности, конформных реализаций может быть несчётное множество. Кроме того, объединение конформных реализаций содержит много «лишнего», без чего можно обойтись в монотонно преобразованной спецификации. Поэтому далее дадим конструктивное определение друго-

го монотонного преобразования, которое при некоторых ограничениях на LTS-спецификацию может быть алгоритмизуемо.

3.3. Причины несохранения конформности и нарушения безопасности

Сначала рассмотрим примеры несохранения конформности и нарушения безопасности при композиции. Выделим четыре причины этого и четыре аспекта предлагаемого монотонного преобразования спецификаций.

3.3.1. Полное стабильное состояние. Полное стабильное состояние — это стабильное состояние, в котором определены переходы по всем стимулам и, по крайней мере, по одной реакции, то есть в нём нет блокировок стимулов и стационарности. В примере на рис. 5 у первого компонента

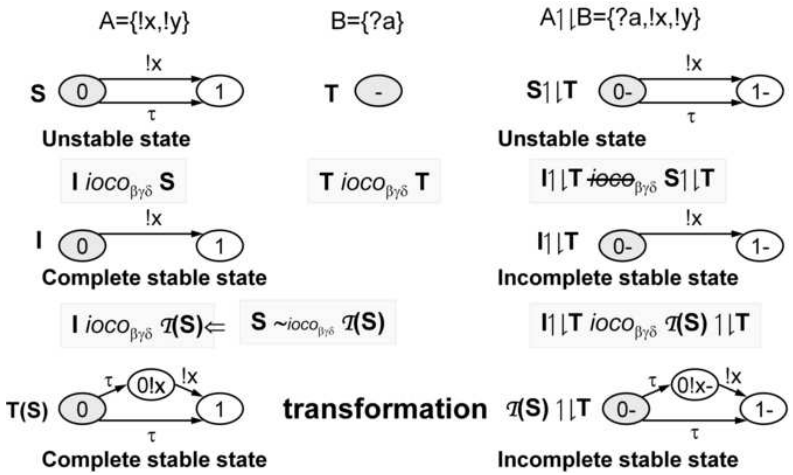


Рис. 5. Полное стабильное состояние

реализация ***I*** конформна спецификации ***S***. Они различаются тем, что в спецификации начальное состояние нестабильное, а в реализации полное стабильное. У второго компонента спецификация и реализация совпадают — это LTS ***T***, которая (по рефлексивности отношения) конформна сама себе. У прямой композиции спецификаций ***S*** $|\!|$ ***T*** начальное состояние нестабильно, а у прямой композиции реализаций ***I*** $|\!|$ ***T*** — неполное стабильное. Из-за этого в композиции реализаций есть трасса $\{?a\}!x$, которой нет в композиции спецификаций. Поскольку γ-действие в композиции спецификаций отсутствует, конформность эквивалентна вложенности трасс. Но в этом примере конформность не сохраняется при прямой композиции спецификаций.

Как сохранить конформность? Рассмотрим преобразование, создающее в спецификации $\boldsymbol{S}$ полное стабильное состояние. Преобразованная спецификация $\mathcal{T}(\boldsymbol{S})$ эквивалентна исходной спецификации $\boldsymbol{S}$, следовательно, $\boldsymbol{I}$ **ioco**$_{\beta\gamma\delta}$ $\mathcal{T}(\boldsymbol{S})$. Но теперь в композиции спецификаций $\mathcal{T}(\boldsymbol{S}) \,\|\!\downarrow\, \boldsymbol{T}$ появилось неполное стабильное состояние, как в реализации $\boldsymbol{I} \,\|\!\downarrow\, \boldsymbol{T}$, и конформность сохраняется.

3.3.2. Сингулярность. Сингулярным состоянием называем стабильное состояние, из которого выходит не более одного перехода, помеченного реакцией. В примере на рис. 6 у первого компонента реализация $\boldsymbol{I}$ конформна спецификации $\boldsymbol{S}$. Они различаются тем, что в спецификации

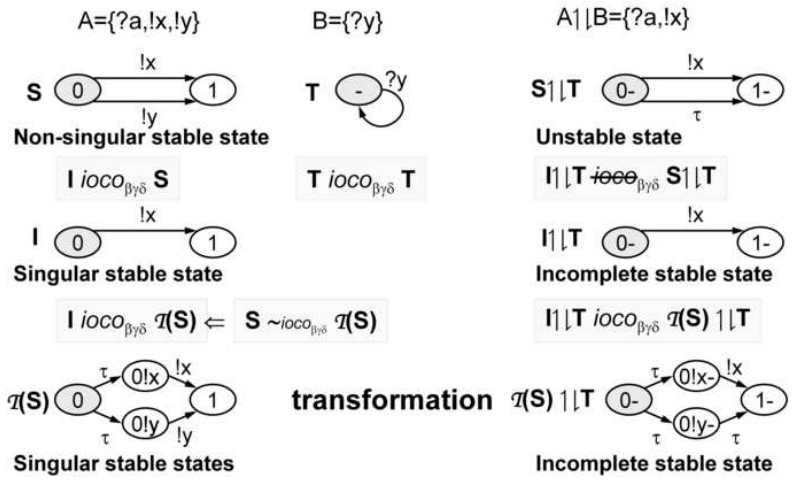


Рис. 6. Сингулярность

начальное состояние несингулярно, а в реализации — сингулярно. У второго компонента спецификация и реализация совпадают — это LTS $\boldsymbol{T}$. Как и в предыдущем примере у прямой композиции спецификаций $\boldsymbol{S} \,\|\!\downarrow\, \boldsymbol{T}$ начальное состояние нестабильно, а у прямой композиции реализаций $\boldsymbol{I} \,\|\!\downarrow\, \boldsymbol{T}$ — неполное стабильное. Из-за этого в композиции реализаций есть трасса $\{?a\}!x$, которой нет в композиции спецификаций. Поскольку γ-действия в композиции спецификаций отсутствуют, в этом примере также конформность не сохраняется при прямой композиции спецификаций.

Для сохранения конформности нужно преобразовать спецификацию, «расщепив» несингулярное состояние на несколько (по числу выходящих реакций) сингулярных состояний. В данном примере несингулярное состояние 0 расщепляется на два сингулярных состояния $0!x$ и $0!y$, из ко-

торых ведутся переходы только по одной реакции $!x$ и $!y$, соответственно. Преобразованная спецификация $\mathcal{T}(\boldsymbol{S})$ эквивалентна исходной $\boldsymbol{S}$, но теперь в композиции спецификаций $\mathcal{T}(\boldsymbol{S}) \parallel \boldsymbol{T}$ появилось неполное стабильное состояние, как в реализации $\boldsymbol{I} \parallel \boldsymbol{T}$, и конформность сохраняется.

3.3.3. Экспонентная LTS. Еще одним аспектом преобразования является преобразование, которое называется *экспоненцированием*. Оно похоже на известное преобразование детерминизации конечного автомата [15] с тем, однако, отличием, что у нас сохраняются τ-переходы. Результат такого преобразования будем называть *экспонентной* LTS. Состояния экспонентной LTS (*экспонентные состояния*) соответствуют трассам исходной LTS $\boldsymbol{S}$ и являются множествами состояний после этих трасс. Для трассы $\sigma \in \mathbf{Traces}(\boldsymbol{S})$ соответствующее экспонентное состояние будем обозначать $[\sigma]$. Начальное экспонентное состояние $[\varepsilon]$ соответствует пустой трассе. В экспонентной LTS проводится переход $[\sigma] - z \to [\sigma z]$, если $z \neq \tau$ и $\sigma z \in \mathbf{Traces}(\boldsymbol{S})$. Здесь $[\sigma z]$ совпадает с множество концов b всех переходов вида $a - z \to b$, где a пробегает множество A. Внутренний переход $[\sigma] - \tau \to [\sigma\rho]$ проводится, если трасса ρ состоит только из отказов и $\sigma\rho \in \mathbf{Traces}(\boldsymbol{S})$. Здесь $[\sigma\rho]$ состоит из тех состояний $s \in [\sigma]$, которые стабильны и порождают все отказы из ρ. Нетрудно показать, что экспонентная LTS эквивалентна исходной по отношению конформности.

На рис. 7 приведён пример частичного экспоненцирования и последующей сингуляризации. Добавляются экспонентные состояния только пустой трассы ε и всех трасс отказов. Кроме того, из экспонентного состояния $[\varepsilon]$ проведены только τ-переходы. В этом примере этого достаточно для монотонности преобразования.

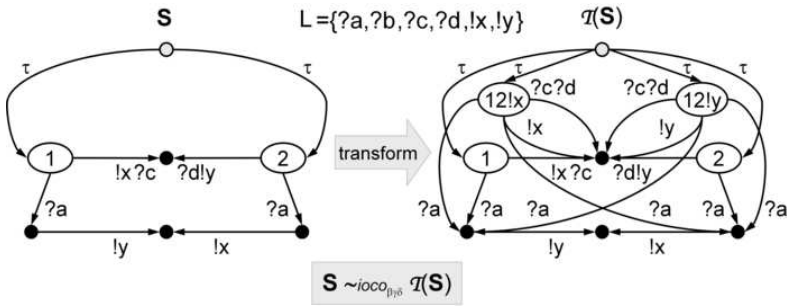


Рис. 7. Экспоненцирование

Покажем необходимость всех экспонентных состояний: $[\{?d\}] = \{1\}$, $[\{?c\}] = \{2\}$ и $[\{?b\}] = \{12\}$, расщепляемого на два сингулярных состояния $\{12!x\}$ и $\{12!y\}$.

Необходимость сохранения состояния {1} показано на рис. 8. Поскольку $\boldsymbol{S}$ **ioco**$_{\beta\gamma\delta}$ $\mathcal{T}(\boldsymbol{S})$ и $\boldsymbol{T}$ **ioco**$_{\beta\gamma\delta}$ $\boldsymbol{T}$, должно быть $\boldsymbol{S} \,\|\!\downarrow\, \boldsymbol{T}$ **ioco**$_{\beta\gamma\delta}$ $\mathcal{T}(\boldsymbol{S}) \,\|\!\downarrow\, \boldsymbol{T}$. Поскольку в спецификации γ-действий нет, должна быть вложенность трасс $\mathbf{Traces}(\boldsymbol{S} \,\|\!\downarrow\, \boldsymbol{T}) \subseteq \mathbf{Traces}(\mathcal{T}(\boldsymbol{S}) \,\|\!\downarrow\, \boldsymbol{T})$. Однако в композиции $\boldsymbol{S} \,\|\!\downarrow\, \boldsymbol{T}$ имеется трасса $\{?b\}?a!y$, которой не было бы в композиции $\mathcal{T}(\boldsymbol{S}) \,\|\!\downarrow\, \boldsymbol{T}$, если бы там не было состояния {1}. Аналогично показывается необходимость сохранения состояния {2}.

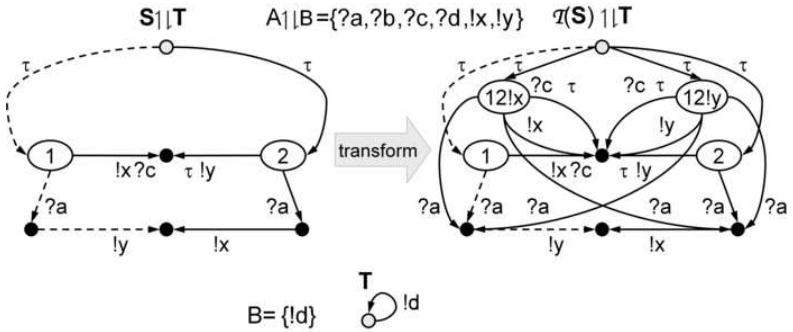


Рис. 8. Экспоненцирование: необходимость сохранения состояния {1}

Необходимость добавления состояния $\{12!x\}$ показано на рис. 9. Поскольку $\boldsymbol{I}$ **ioco**$_{\beta\gamma\delta}$ $\boldsymbol{S}$ и $\boldsymbol{T}$ **ioco**$_{\beta\gamma\delta}$ $\boldsymbol{T}$, должно быть $\boldsymbol{I} \,\|\!\downarrow\, \boldsymbol{T}$ **ioco**$_{\beta\gamma\delta}$ $\mathcal{T}(\boldsymbol{S}) \,\|\!\downarrow\, \boldsymbol{T}$. Заметим, что $\boldsymbol{I} \,\|\!\downarrow\, \boldsymbol{T} \neg$ **ioco**$_{\beta\gamma\delta}$ $\boldsymbol{S} \,\|\!\downarrow\, \boldsymbol{T}$, то есть без преобразования конформность не сохраняется. Поскольку в спецификации γ-действий нет, должна быть вложенность трасс. Однако в композиции $\boldsymbol{I} \,\|\!\downarrow\, \boldsymbol{T}$ имеется трасса $\{?b\}?a!x$,

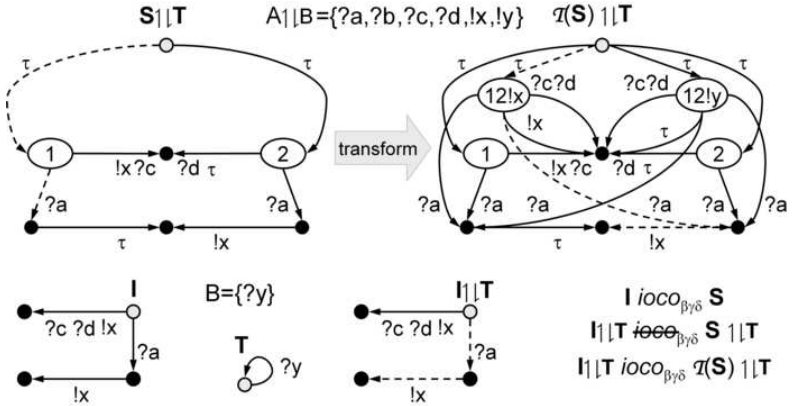


Рис. 9. Экспоненцирование: необходимость добавления состояния $\{12!x\}$

которой нет в композиции $\boldsymbol{S} \upharpoonleft\downharpoonleft \boldsymbol{T}$. В композиции $\mathcal{T}(\boldsymbol{S}) \upharpoonleft\downharpoonleft \boldsymbol{T}$ эта трасса есть, но без состояния $\{12!x\}$ её бы не было. Аналогично показывается необходимость сохранения состояния $\{12!y\}$.

3.3.4. γ-однородность. Состояние называется γ-однородным, если после всех реакций следует γ-действие или все реакции безопасны. На рис. 10 приведён пример, когда начальное состояние спецификации $\boldsymbol{S}$ не γ-однородно: переход по реакции $!x$ приводит к γ-действию, а перехода по реакции $!y$ нет. В конформной реализации $\boldsymbol{I}$, наоборот, нет перехода по реакции $!x$, а переход по реакции $!y$ приводит к γ-действию. Из-за этого композиция спецификаций $\boldsymbol{S} \upharpoonleft\downharpoonleft \boldsymbol{T}$ безопасна, а композиция конформных реализаций $\boldsymbol{I} \upharpoonleft\downharpoonleft \boldsymbol{T}$ опасна, что означает и неконформность.

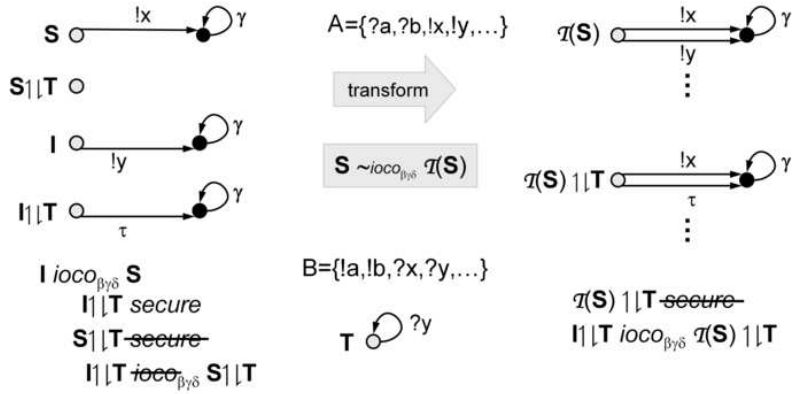


Рис. 10. γ-однородность

Чтобы сохранить конформность, нужно преобразовать спецификацию, сделав все её состояния γ-однородными. Если в состоянии есть переход по реакции, приводящий к γ-действию, добавляем переходы из этого состояния по всем реакциям, ведущие к γ-действию. Будем считать, что все переходы по опасным действиям (действиям, после которых возможно γ-действие) ведут в специальное состояние Г, в котором определена только γ-петля.

Заметим, что при сочетании сингуляризации и γ-однородности из каждого стабильного состояния ведёт либо только один переход по безопасной реакции, либо переходы по всем опасным реакциям в состояние Г, либо ни одного перехода реакциям.

3.4. Формальное определение монотонного преобразования

Теперь можной формально определить предлагаемое монотонное преобразование спецификации. Пусть задана LTS-спецификация $\boldsymbol{S}$ в алфа-

вите L. Состояния преобразованной LTS $\mathcal{T}(\boldsymbol{S})$ строятся на основе экспонентных состояний. Начальным является экспонентное состояние $[\varepsilon]$, соответствующее пустой трассе. Переходы определяются правилами вывода в таблице 1, где $T = \mathbf{Traces}(\boldsymbol{S})$, $S = \mathbf{SafeTraces}(\boldsymbol{S})$, μ — трасса, не заканчивающаяся на отказ, и ρ — непустая трасса отказов.

Таблица 1

1)		$\vdash\ \Gamma - \gamma \to \Gamma;$
2)	$\mu!x \in S$	$\vdash\ [\mu] - !x \to [\mu!x];$
3)	$\exists!y\ \mu!y\gamma \in T$	$\vdash\ [\mu] - !x \to \Gamma;$
4)	$\mu?a \in S$	$\vdash\ [\mu] - ?a \to [\mu?a];$
5)	$\mu?a\gamma \in T$	$\vdash\ [\mu] - ?a \to \Gamma;$
6)	$\forall?b \in L\ \mu?b \in T\ \&\ \mu!x \in S$	$\vdash\ [\mu] - \tau \to [\mu]!x - !x \to [\mu!x];$
7)	-"- -"- -"- -"- -"- & $\mu?a \in S$	$\vdash\ [\mu]!x - ?a \to [\mu?a];$
8)	-"- -"- -"- -"- -"- & $\mu?a\gamma \in T$	$\vdash\ [\mu]!x - ?a \to \Gamma;$
9)	$\forall?b \in L\ \mu?b \in T\ \&\ \exists!y\ \mu!y\gamma \in T$	$\vdash\ [\mu] - \tau \to [\mu]\gamma - !x \to \Gamma;$
10)	-"- -"- -"- -"- -"- & $\mu?a \in S$	$\vdash\ [\mu]\gamma - ?a \to [\mu?a];$
11)	-"- -"- -"- -"- -"- & $\mu?a\gamma \in T$	$\vdash\ [\mu]\gamma - ?a \to \Gamma;$
12)	$\mu\rho!x \in S$	$\vdash\ [\mu] - \tau \to [\mu\rho]!x - !x \to [\mu\rho!x];$
13)	-"- -"- -"- -"- -"- & $\mu\rho?a \in S$	$\vdash\ [\mu\rho]!x - ?a \to [\mu\rho?a];$
14)	-"- -"- -"- -"- -"- & $\mu\rho?a\gamma \in T$	$\vdash\ [\mu\rho]!x - ?a \to \Gamma;$
15)	$\exists!y\ \mu\rho!y\gamma \in T$	$\vdash\ [\mu] - \tau \to [\mu\rho]\gamma - !x \to \Gamma;$
16)	-"- -"- -"- -"- -"- & $\mu\rho?a \in S$	$\vdash\ [\mu\rho]\gamma - ?a \to [\mu\rho?a];$
17)	-"- -"- -"- -"- -"- & $\mu\rho?a\gamma \in T$	$\vdash\ [\mu\rho]\gamma - ?a \to \Gamma;$
18)	$\forall!y \in L\ \mu!y \notin T\ \&\ \mu\rho \in S$	$\vdash\ [\mu] - \tau \to [\mu\rho]\delta;$
19)	-"- -"- -"- -"- -"- & $\mu\rho?a \in S$	$\vdash\ [\mu\rho]\delta - ?a \to [\mu\rho?a];$
20)	-"- -"- -"- -"- -"- & $\mu\rho?a\gamma \in T$	$\vdash\ [\mu\rho]\delta - ?a \to \Gamma.$

Поясним эти правила вывода.

Правило 1 описывает специальное состояние Γ, в котором определяется только γ-петля. В это состояние будут вести все переходы по опасным стимулам и реакциям, как это делалось для получения γ-однородной LTS.

Правила 2–5 описывают переходы по стимулам и реакциям из нестабильного экспонентного состояния $[\mu]$ для безопасной трассы μ.

Правила 6–8 описывают случай, когда реакции безопасны после безопасной трассы μ. Определяются τ-переходы во все сингулярные полные стабильные состояния и переходы из них по стимулам и реакциям. Каждое такое состояние имеет вид $[\mu]!x$, и из него определяется переход только по одной реакции $!x$.

Правила 9–11 описывают случай, когда реакции опасны после безопасной трассы μ. Определяются τ-переходы во все γ-однородные полные стабильные состояния и переходы из них по стимулам и реакциям. Каждое такое состояние имеет вид $[\mu]\gamma$, и из него определяются переходы по всем реакциям в состояние Г.

Правила 12–14 описывают случай, когда безопасная трасса μ безопасно продолжается непустой трассой отказов ρ, и реакции безопасны после трассы $\mu\rho$. Определяются τ-переходы во все сингулярные неполные стабильные состояния и переходы из них по стимулам и реакциям. Каждое такое состояние имеет вид $[\mu\rho!x]$, и из него определяется переход только по одной реакции $!x$.

Правила 15–17 описывают случай, когда безопасная трасса μ безопасно продолжается непустой трассой отказов ρ, а реакции опасны после трассы $\mu\rho$. Определяются τ-переходы во все γ-однородные неполные стабильные состояния и переходы из них по стимулам и реакциям. Каждое такое состояние имеет вид $[\mu\rho]\gamma$, и из него определяются переходы по всем реакциям в состояние Г.

Правила 18–20 описывают случай, когда безопасная трасса μ безопасно продолжается непустой трассой отказов ρ, а $\mu\rho$ не продолжается реакциями в спецификации. Определяются τ-переходы во все стационарные (неполные) стабильные состояния и переходы из них по стимулам. Каждое такое состояние имеет вид $[\mu\rho]\delta$.

За отсутствием места формальное доказательство монотонности этого преобразования опускается.

4. Монотонное преобразование в частных случаях

4.1. Системы без блокировок стимулов

Можно показать, что для важного частного случая спецификаций без блокировок стимулов монотонное преобразование можно существенно упростить. Для этого достаточно только γ-однородности. При отсутствии γ-действий монотонно тождественное преобразование.

При отсутствии блокировок в спецификациях компонентов, если косая композиция безопасна, то она совпадает с прямой композицией спецификаций. Отсюда следует, что для систем без блокировок косая композиция нужна только для проверки безопасности. Безопасность может быть нарушена только из-за дивергенции, которая считается нежелательным поведением и моделируется γ-действием. Такая дивергенция в композиции может порождаться бесконечной цепочкой синхронных переходов. Поэто-

му проверка безопасности, фактически, сводится к проверке дивергенции в композиции LTS.

Заметим, что для спецификаций без блокировок наше отношение $\mathbf{ioco}_{\beta\gamma\delta}$ совпадает с известным отношением **ioco**, которое строится на трассах без блокировок и без γ-действий [30]. Отличие лишь в том, что для отношения **ioco** требуется отсутствие блокировок в каждом состоянии реализации, а для отношения $\mathbf{ioco}_{\beta\gamma\delta}$ — только в тех состояниях, которые достижимы по трассам, безопасным в спецификации.

Также заметим, что отношение **ioco** формально определяется для LTS-спецификаций, в которых могут быть блокировки стимулов, но эти блокировки игнорируются. Из-за этого прямая композиция LTS-спецификаций оказывается, вообще говоря, некорректной и для отношения **ioco**. Вот почему стараются выполнить, так называемое пополнение LTS-спецификаций [9, 24], то есть такое преобразование, которое сохраняет (или почти сохраняет) множество конформных реализаций, но удаляет все блокировки. После такого пополнения (при отсутствии γ-действий) дальнейшее преобразование не требуется для монотонности, то есть само такое пополнение является монотонным преобразованием [11].

Если нет γ-действий, то может оказаться, что трасса в исходной спецификации не продолжалась некоторым стимулом. Это приводит к тому, что для отношения **ioco** вообще не проверяется поведение реализации по поводу этого стимула. Формально конформная реализация может этот стимул блокировать или принимать с любым дальнейшим поведением [11]. Фактически речь идёт о том, что поведение реализации по поводу этого стимула не определено [9, 24]. При нашем подходе, когда допускаются γ-действия, это легко моделируется продолжением такой трассы стимулом и далее γ-действием. В результате получится пополненная спецификация с γ-действиями, которую для монотонности нужно дополнительно привести к γ-однородности.

4.2. Системы без γ-действий

Для систем без γ-действий (но с возможными блокировками) монотонное преобразование не намного проще, чем в общем случае. Отсутствует лишь требование γ-однородности. Однако класс таких LTS-систем имеет тот существенный недостаток, что он незамкнут по композиции. Дело в том, что при композиции может возникать дивергенция, порождаемая бесконечной цепочкой синхронных переходов. Поскольку дивергенция рассматривается как нежелательное поведение и моделируется γ-действием, такие γ-действия могут появляться при композиции и в том случае, когда LTS-операнды не имели γ-действий.

4.3. Алгоритмические проблемы

За отсутствием места не будем рассматривать подробно вопросы алгоритмизации преобразования и последующей прямой композиции. Более точно, речь идёт о тех ограничениях, которые нужно наложить на спецификацию, чтобы преобразование и последующая прямая композиция стали алгоритмическими. Разумеется, и сама LTS-спецификация должна быть задана алгоритмическим способом, то есть алгоритмами, определяющими переходы из каждого состояния LTS. Здесь лишь вкратце укажем на ряд ключевых моментов.

1. Множество состояний после безопасной трассы должно быть конечным. Это необходимо для того, чтобы алгоритмически строить экспонентные состояния и переходы из них. Для этого нужно ограничить степень ветвления LTS. В общем, достаточно потребовать конечности ветвления: в каждом состоянии (достижимом по безопасной трассе) должно быть определено конечное число переходов [21].
2. Поскольку дивергенция моделируется разрушением, нужно уметь алгоритмически распознавать дивергенцию. Такая дивергенция всегда распознаваема, если она является бесконечной цепочкой τ-переходов, порождённой τ-циклом в LTS. С учётом γ-действий достаточно наложить такие ограничения, чтобы при построении τ-замыкания состояния (множества состояний, достижимых из данного состояния по τ-переходам) гарантированно и за конечное время обнаруживался либо τ-цикл, либо γ-переход.
3. Дивергенция в композиционной LTS может быть не только унаследованной от дивергенции от одного из LTS-операндов, но и порождаться бесконечной цепочкой синхронных переходов. Нужно наложить на LTS-операнды такие ограничения, чтобы такая дивергенция также обнаруживалась за конечное время. В общем, эти ограничения сводятся к некоторой «регулярности» LTS-операндов: каждая бесконечная трасса без γ-ответвлений должна порождаться «регулярной» цепочкой переходов, то есть такой цепочкой, которая «укладывается» в конечную под-LTS (проходит через конечное число состояний).

5. Заключение

В данной работе формализуется понятие запрещённого поведения, что позволяет формально определить безопасные системы и условно-безопасные компоненты таких систем. Также вводится понятие косой ком-

позиции спецификаций, которая: 1) корректна, то есть удовлетворяет условию монотонности (конформность сохраняется при композиции), и 2) является самой «сильной» (предъявляющей максимальные требования) среди всех корректных спецификаций. При заданных спецификациях компонентов косая композиция этих спецификаций является точной спецификацией системы и может использоваться при использовании системы внешними клиентами.

В данной работе показано, что при заданных спецификациях компонентов можно получить косую композицию спецификаций как прямую композицию соответствующим образом преобразованных спецификаций.

Это позволяет решить следующие важнейшие проблемы.

1. Если заданы не только спецификации компонентов, но и спецификация системы, можно верифицировать декомпозицию требований (согласованность спецификаций системы и её компонентов). Декомпозиция корректна, если косая композиция конформна заданной спецификации системы.
2. При достаточной полноте тестирования компонентов снимается проблема тестирования системы (на конформность косой композиции и, тем более, заданной спецификации системы, если декомпозиция требований правильна).
3. Если нет уверенности в полноте тестирования компонентов, косая композиция может использоваться для генерации системных тестов.

Данная работа была выполнена в рамках развития технологии тестирования UniTESK [19, 20]. Отдельные части этой работы выполнялись как части исследований, финансируемых грантами РФФИ и контрактами с Президиумом РАН. Результаты докладывались на нескольких конференциях [2, 3, 8].

Литература

[1] *Bernot G.* Testing against formal specifications: A theoretical view // S. Abramsky and T. S. E. Maibaum, editors. Proc. of TAPSOFT'91, v. 2, p. 99–119. Lecture Notes in Computer Science, v. 494, Springer-Verlag, 1991.

[2] *Бурдонов И. Б., Косачев А. С.* Тестирование компонентов распределенной системы. Труды Всероссийской научной конференции «Научный сервис в сети ИНТЕРНЕТ». Изд-во МГУ, 2005. С. 63–65.

[3] *Бурдонов И. Б., Косачев А. С.* Верификация композиции распределенной системы. Труды Всероссийской научной конференции «Научный сервис в сети ИНТЕРНЕТ». Изд-во МГУ, 2005. С. 67–69.

[4] *Бурдонов И. Б.*, *Косачев А. С.*, *Кулямин В. В.* Использование конечных автоматов для тестирования программ. Программирование, 2000, № 2. с. 12–28.

[5] *Бурдонов И. Б.*, *Косачев А. С.*, *Кулямин В. В.* Асинхронные автоматы: классификация и тестирование. Труды ИСП РАН, т. 4, 2003. С. 7–84.

[6] *Бурдонов И. Б.*, *Косачев А. С.*, *Кулямин В. В.* Неизбыточные алгоритмы обхода ориентированных графов. Детерминированнный случай. Программирование, 2003, № 5.

[7] *Бурдонов И. Б.*, *Косачев А. С.*, *Кулямин В. В.* Неизбыточные алгоритмы обхода ориентированных графов. Недетерминированнный случай. Программирование, 2004, № 1.

[8] *Bourdonov I.*, *Kossatchev A.*, *Kuliamin V.* Formal Conformance Testing of Systems with Refused Inputs and Forbidden Actions. Proc. of MBT'2006, Vienna, Austria, March 2006.

[9] *Bochmann G. V.*, *Petrenko A.* Protocol testing: review of methods and relevance for software testing. Proc. of the 1994 International Symposium on Software Testing and Analysis, p. 109–124, August 17–19, 1994, Seattle, Washington, United States.

[10] *Van der Bijl M.*, *Rensink A.*, *Tretmans J.* Component Based Testing with ioco. CTIT Technical Report TR-CTIT-03-34, University of Twente, 2003.

[11] *Van der Bijl M.*, *Rensink A.*, *Tretmans J.* Compositional testing with ioco. In: Formal Approaches to Software Testing: Third International Workshop, FATES'2003, Montreal, Quebec, Canada, October 6th, 2003. Editors: Alexandre Petrenko, Andreas Ulrich ISBN: 3-540-20894-1. LNCS, v. 2931, Springer, p. 86–100.

[12] *Van Glabbeek R.* The linear time — branching time spectrum I; the semantics of concrete, sequential processes, in: Handbook of Process Algebra (J. A. Bergstra, A. Ponse, S. A. Smolka, eds.), 2001, Chapter 1, Elsevier, p. 3–99.

[13] *Van Glabbeek R. J.* The linear time — branching time spectrum II; the semantics of sequential processes with silent moves. Proceedings of CONCUR'93, Hildesheim, Germany, August 1993 (E. Best, ed.). LNCS, v. 715, Springer-Verlag, 1993, p. 66–81.

[14] *Heerink L.* Ins and Outs in Refusal Testing. PhD thesis, University of Twente, Enschede, The Netherlands, 1998.

[15] *Хопкрофт Д.*, *Мотвани Р.*, *Ульман Д.* Введение в теорию автоматов, языков и вычислений, 2-е изд. М.: Вильямс, 2002.

[16] *Heerink L.*, *Tretmans J.* Refusal Testing for Classes of Transition Systems with inputs and Outputs. In: T. Mizuno, N. Shiratori, T. Higashino, A. Togashi, eds. Formal Description Techniques and Protocol Specification, Testing and Verification. Chapman & Hill, 1997.

[17] Revised Working Draft on "Framework: Formal Methods in Conformance Testing", JTC1/SC21/WG1/Project 54/1 // ISO Interim Meeting / ITU-T on, Paris, 1995.

[18] *Jard C.*, *Jéron T.*, *Tanguy L.*, *Viho C.* Remote testing can be as powerful as local testing. In: Formal methods for protocol engineering and distributed systems, FORTE'XII /PSTV XIX'99, Beijing, China, J. Wu, S. Chanson, Q. Gao (eds.), p. 25–40, October 1999.

[19] *Kuliamin V. V.*, *Kossatchev A. S.*, *Petrenko A. K.*, *Pakoulin N. V.*, *Bourdonov I. B.* Integration of Functional and Timed Testing of Real-Time and Concurrent Systems. Perspectives of System Informatics. LNCS, v. 2890, 2003, p. 450–461.

[20] *Кулямин В. В.*, *Петренко А. К.*, *Косачев А. С.*, *Бурдонов И. Б.* Подход UniTesK к разработке тестов. Программирование, 2003, № 6. С. 25–43; *Kuliamin V. V.*, *Petrenko A. K.*, *Kossatchev A. S.*, *Bourdonov I. B.* The UniTesK Approach to Designing Test Suites. Programming and Computer Software, 2003, 6, p. 310.

[21] *König D.* Über eine Schlusswaise aus dem Endlichen ins Unendliche. Acta Litt. Ac. Sci. Hung. Fran. Josep., No. 3, 1927, p. 121–130. См. также К. Куратовский, А. Мостовский. Теория множеств. М.: Мир, 1970.

[22] *Lestiennes G.*, *Gaudel M.-C.* Test de systemes reactifs non receptifs. Journal Europeen des Systemes Automatises, Modelisation des Systemes Reactifs, p. 255–270. Hermes, 2005.

[23] *Lynch N. A.*, *Tuttle M. R.* Hierarchical correctness proofs for distributed algorithms. In: Proceedings of the 6th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, p. 137–151, August 1987.

[24] *Lee D.*, *Yannakakis M.* Principles and Methods of Testing Finite State Machines — A Survey. Proceedings of the IEEE'84, No. 8, p. 1090–1123, 1996.

[25] *Milner R.* A Calculus of Communicating Systems. LNCS, v. 92, Springer-Verlag, 1980.

[26] *Milner R.* Communication and Concurrency. Prentice-Hall, 1989.

[27] *Phalippou M.* Relations d'Implantation et Hypotheses de Test sur des Automates a Entrees et Sorties. PhD thesis, L'Universite de Bordeaux I, France, 1994.

[28] *Segala R.* Quiescence, fairness, testing and the notation of implementation (extended abstract). In: Proceedings of the 4th International Conference on Concurrency Theory (CONCUR'93), Hildesheim, Germany, 1993. LNCS, v. 715.

[29] *Tretmans J.* A Formal Approach to Conformance Testing. PhD. Thesis, University of Twente, Enschede, The Netherlands, 1992.

[30] *Tretmans J.* Test Generation with Inputs, Outputs and Repetitive Quiescence. In: Software — Concepts and Tools, v. 17, issue 3, 1996.

[31] *Vaandrager F.* On the relationship between process algebra and input/output automata. In: Logic in Computer Science, p. 387–398. Sixth Annual IEEE Symposium, IEEE Computer Society Press, 1991.

Математические модели и механизмы логического разграничения доступа в операционной системе Linux: текущее состояние и перспективы развития

В. А. Васенин, К. А. Шапченко, О. О. Андреев

1. Введение

Одним из базовых сервисов в комплексе средств обеспечения безопасности информационных технологий является логическое разграничение доступа (ЛРД). Средства ЛРД определяют действия, которые субъекты (например, пользователи и процессы) могут выполнять над объектами (как правило, информационными активами и процессами) [1]. Кроме того, с помощью механизмов протоколирования подобные средства позволяют обеспечить контроль за корректностью совершения этих действий.

Особенности средств ЛРД, встроенных в ядра операционных систем (ОС), связаны, в первую очередь, с характеристиками контролируемых ОС субъектов и объектов доступа. Как правило, к субъектам, контролируемым ядром, относят процессы, в том числе, действующие от имени некоторого пользователя или обладающие другими атрибутами безопасности. Характерными объектами, доступ к которым разграничивается на уровне ядра ОС, являются объекты файловых систем. К их числу относятся, например, файлы, каталоги, возможно, метаданные и атрибуты файлов. Другими объектами доступа на уровне ядра ОС являются выполняемые процессы, рассматриваемые как объекты доступа, объекты межпроцессного взаимодействия, объекты сетевого взаимодействия, конфигурационные данные подсистем ядра ОС (в том числе, подсистем, ответственных за разграничение доступа). Другой особенностью средств ЛРД, встроенных в ядра ОС, является их «привязка» к системным вызовам, непосредственно реализующим доступ, что приводит к унификации используемых типов доступа.

В качестве примеров задач, которые обычно решаются с помощью средств ЛРД в ядре ОС, можно отнести управление привилегиями пользователей ОС и изоляцию программных сервисов в составе ОС. С позиции

таких задач, средства ЛРД в ядрах ОС можно отнести к низкоуровневым, в отличие от высокоуровневых средств разграничения доступа, внедрение которых может быть оправдано в случае использования некоторых программных сервисов. Например, разграничение прав доступа на основе содержания информационных ресурсов, как правило, технически эффективнее реализуется в программных средствах, расположенных вне ядра ОС.

2. Модели логического разграничения доступа

Учитывая многообразие существующих моделей и построенных на их основе механизмов ЛРД, с необходимостью возникает проблема классификации (хотя бы частичной) существующих моделей ЛРД.

К ключевым классификационным признакам можно отнести, например, следующие отличительные черты моделей ЛРД.

Естественным признаком различия моделей ЛРД является способ задания правил доступа в «статическом срезе» (статическом состоянии) модели ЛРД. В данном случае имеется в виду, что такая конфигурация модели, в которой набор субъектов и объектов доступа неизменен, а действий по модификации правил доступа не производится. Рассмотрение статического среза модели ЛРД оправдано в моделях, не поддерживающих явно зависимость правил доступа от истории произведенных доступов. На основе именно таких моделей построено большинство низкоуровневых механизмов ЛРД в ядрах ОС. Зависимость же правил доступа от их истории и других произошедших событий поддерживается, как правило, через средства протоколирования и активного аудита.

На примере нескольких распространенных моделей ЛРД продемонстрируем различные способы задания правил разграничения доступа в статическом срезе модели ЛРД.

Введем следующие обозначения. Пусть S — множество субъектов доступа, O — множество объектов доступа, A — множество типов доступа (например, доступ на запись, доступ на чтение). Наиболее простым способом задания статического среза модели ЛРД в таких обозначениях является задание матрицы доступа, то есть отображения

$$AM\colon S \times O \to 2^A,$$

определяющего для каждой пары (субъект, объект) множество разрешенных доступов в модели.

Зачастую удобно записывать эту матрицу как набор списков прав доступа, а именно, — отображение

$$acl'\colon O \to 2^{S \times A}.$$

Однако, как правило, для таких моделей ЛРД вводят дополнительное множество U — множество пользователей и отображение $owner\colon S \to U$, позволяющее задать пользователя-владельца для каждого субъекта. Тогда отображение acl' может быть задано как

$$acl\colon O \to 2^{U \times A},$$

а возможность доступа определяется следующим предикатом:

$$\Delta(s,\, o,\, a) \equiv (owner(s),\, a) \in acl(o).$$

Модели ЛРД, основанные на списках доступа получили распространение в дискреционных механизмах доступа, а при некотором расширении (например, при использовании группировки субъектов доступа) — и в механизмах, основанных на ролевом разграничении доступа.

Широким классом моделей ЛРД, используемых в принудительном, мандатном управлении доступом, являются модели, возможность доступа в которых определяется на основе сравнения элементов некоторой решетки. Значимыми примерами моделей разграничения доступа, основанных на решетках, являются модели многоуровневого разграничения доступа, такие как модель Белла—Лападула и модель Биба.

Пусть, как и ранее, O — множество объектов, S — множество субъектов в модели разграничения доступа.

Пусть L — конечная решетка, элементы которой будем называть метками безопасности. Метки безопасности приписываются субъектам и объектам доступа согласно задаваемому отображению $label\colon S \cup O \to L$.

Для определения возможности доступа могут быть использованы следующие правила.

SS-свойство: субъект $s \in S$ может обратиться с доступом на чтение к объекту $o \in O$ только в том случае, если $label(s) \geqslant label(o)$.

$*$-свойство: субъект $s \in S$ может обратиться с доступом на запись к объекту $o \in O$ только в том случае, если $label(s) \leqslant label(o)$.

Строгое $*$-свойство: субъект $s \in S$ может обратиться с доступом на запись к объекту $o \in O$ только в том случае, если $label(s) = label(o)$.

В многоуровневых моделях ЛРД используется следующий способ построения решетки. Пусть R — линейно упорядоченное конечное множество (например, множество уровней секретности), C — конечное множество (множество категорий). Решетка L строится как $L = R \times 2^C$. Операция сравнения на L определяется как $(r_1,\, C_1) \preceq (r_2,\, C_2) \equiv r_1 \leqslant r_2 \wedge C_1 \subset \subset C_2$.

Таким образом, предикат предоставления доступа в многоуровневой модели ЛРД, использующей только доступы на чтение и на запись, а также удовлетворяющей SS- и $*$-свойствам, может быть задан в следующем

виде:

$$\Delta(s,\, o,\, a) \equiv (a = read \wedge label(s) \geqslant label(o)) \vee \\ \vee\, (a = write \wedge label(s) \leqslant label(o)).$$

Приведем основные положения упрощенной модели $RBAC_0$ — базовой ролевой модели ЛРД.

Введем следующие обозначения.Пусть U — множество пользователей, R — множество ролей, P — множество привилегий. Множество P можно задавать, например, как $P \subset O \times A$, где O — множество объектов доступа, A — множество типов доступа.

Отношение $PRA \subset P \times R$ задает привязку ролей к привилегиям, а отношение $URA \subset U \times R$ задает разрешенные роли для пользователей. Введем множество субъектов S и функции $role\colon S \to R$ и $owner\colon S \to U$, задающие роль и пользователя-владельца субъекта соответственно.

В таких обозначениях предикат предоставления доступа запишется в следующем виде:

$$\Delta(s,\, o,\, a) \equiv (owner(s),\, role(s)) \in URA \wedge ((o,\, a),\, role(s)) \in PRA.$$

В общем случае, можно говорить о задании правил доступа в статическом срезе модели ЛРД с помощью предиката предоставления доступа, который зависит от субъекта, объекта и типа доступа. Распространены такие варианты задания предиката, ориентированные на особенности реализации механизмов ЛРД, как определение списков прав доступа, задание групп и ролей (в том числе, с построением ролевой иерархии). Их привязка к субъектам доступа, типизация субъектов и объектов доступа, определение возможности доступа заданного типа через атрибуты безопасности субъектов и объектов доступа (например, метки в многоуровневых, основанных на решетках меток безопасности, моделях).

Отдельно необходимо рассмотрение правил модели ЛРД, описывающих поведение системы при изменении набора объектов и субъектов доступа, например, при добавлении объекта или субъекта доступа, его удалении или модификации его свойств. Если модификация атрибутов безопасности объекта или субъекта доступа может быть отнесена к изменению правил доступа, действующих в статическом срезе модели, то добавление объекта требует задания свойств (таких как, например, метки безопасности) вновь создаваемой сущности. Примерами схем задания такого рода свойств являются принудительное задание, наследование свойств и комбинации этих двух схем.

Другим признаком, характеризующим модели ЛРД, является возможность изменения правил доступа. Поскольку конкретные механизмы и правила изменения правил доступа обычно привязаны к способу задания ста-

тического среза модели ЛРД, уместно выделить общую характеристику возможности изменения правил, например, со следующими градациями: дискреционное разграничение доступа, разделение административных привилегий, мандатное разграничение доступа. К особенностям дискреционного разграничения доступа относится возможность передачи привилегий, причем не только привилегий доступа, но и, как в некоторых вариациях дискреционных моделей, привилегий передачи прав доступа. Мандатное разграничения доступа характеризуется заданием правил доступа на уровне системы (например, через априорное задание меток безопасности), без возможности изменения правил доступа. Разграничение доступа с разделением административных привилегий представляет собой компромиссный вариант механизма изменения правил доступа. Такой вариант позволяет вводить области ответственности администраторов безопасности, тем самым ограничивая возможное изменение правил доступа.

Необходимо заметить, что указанные классификационные признаки в достаточной степени независимы друг от друга. Например, одна и та же схема задания правил доступа в статическом срезе модели ЛРД может быть использована и в дискреционной модели, и в мандатной, приводя при этом к моделям, обладающим существенно разными свойствами.

Тем не менее, традиционно выделяют следующие широко распространенные классы моделей ЛРД, объединяющие перечисленные классификационные признаки: модели дискреционного разграничения доступа, модели мандатного многоуровневого разграничения доступа, ролевые модели разграничения доступа.

Одной из теоретических задач, решаемых в рамках рассмотрения формальных моделей ЛРД, является задача о выражении одной модели с помощью описательных средств другой модели ЛРД. Как правило, утверждения такого характера доказываются в применении к статическому срезу моделей ЛРД [2, 4].

3. Механизмы разграничения доступа в ядре Linux

К широко распространенным механизмам логического разграничения доступа в ядре ОС Linux относятся следующие встроенные в ядро или являющиеся его модификациями механизмы:

- UNIX permissions — традиционный механизм ЛРД в UNIX-подобных системах;
- POSIX Access Control Lists — механизм ЛРД на основе списков прав доступа;

- NSA Security-Enhanced Linux [5, 6] — механизм ЛРД, основанный на типизации объектов и субъектов доступа и поддерживающий использование ролевых и многоуровневых моделей ЛРД;
- Rule-Set Based Access Control [7] — модульный механизм ЛРД, поддерживающий разнообразные модели ЛРД, включающие в себя несколько вариантов дискреционных, многоуровневых и ролевых моделей [8];
- grsecurity [9, 10] — механизм, позволяющий внедрять упрощенные ролевые модели.

Последние три механизма из приведенного списка являются относительно новыми по сравнению с традиционно используемыми первыми двумя. Чтобы пояснить особенности этих механизмов, приведем упрощенные варианты моделей ЛРД, лежащих в их основе.

В качестве основной модели ЛРД в SELinux выбрана модель Type Enforcement (TE), позволяющая задавать типы субъектов и объектов доступа и определять правила разграничения доступа на основании таких типов. Теоретико-множественное описание упрощенной[1)] модели Type Enforcement.

Перечислим следующие базовые множества, определяемые в модели TE, в предположении, что они конечны и непусты:

- A — множество типов доступа, заданных в модели;
- U — множество пользователей, определяемых в модели;
- R — множество ролей, определяемых в модели, $r_o \in R$ — роль, соответствующая `object_r`;
- T — множество типов, определяемых в модели.

С учетом этих обозначений, в модели TE вводится понятие контекста безопасности — тройки (u, r, t), где $u \in U$, $r \in R$, $t \in T$. В модели TE, каждому субъекту или объекту доступа сопоставляется его контекст безопасности таким образом, что возможность доступа определяется для двух контекстов безопасности — субъекта и объекта доступа соответственно.

В модели TE определяются следующие предикаты, определяющие взаимосвязь различных понятий модели:

- $\mu(u, r)$, $u \in U$, $r \in R$ — в модели «пользователю u разрешена роль r», причем выполнено свойство $\forall u \in U \mu(u, r_o)$ для корректной обработки объектной роли;

[1)] Имеется в виду модель TE без смены атрибутов объектов и субъектов доступа, в том числе, без смены роли субъекта и типов объектов и субъектов. Такие изменения могут быть учтены при исследовании динамических свойств моделей ЛРД, но не свойств статического среза модели. Изложение теоретико-множественных описаний модели TE приведено в [4]

- $\rho(r, t)$, $r \in R$, $t \in T$ — в модели «роли r разрешен тип t», причем выполнено свойство $\forall t \in T \rho(r_o, t)$;
- $\alpha(t_1, t_2, c, p)$, $t_1 \in T$, $t_2 \in T$, $a \in A$ — в модели «субъекту с типом t_1 разрешен доступ a к объекту с типом t_2».

В таких обозначениях можно следующим образом записать предикат предоставления доступа a от контекста безопасности (u_1, r_1, t_1) к контексту (u_2, r_2, t_2):

$$\Delta'(u_1, r_1, t_1; u_2, r_2, t_2; a) \equiv \alpha(t_1, t_2, a) \wedge \rho(r_1, t_1) \wedge \rho(r_2, t_2) \wedge \\ \wedge \mu(u_1, r_1) \wedge \mu(u_2, r_2).$$

Предикат Δ' можно переписать как предикат от субъекта, объекта и типа доступа, определив вспомогательные функции, позволяющие восстановить контекст безопасности:

- $user$: $S \cup O \to U$ — функция, определяющая пользователя-владельца субъекта или объекта доступа;
- $role$: $S \cup O \to R$ — функция, определяющая роль субъекта или объекта доступа, причем для любого $o \in O$ выполнено $role(o) = r_o$;
- $type$: $S \cup O \to T$ — функция, определяющая тип, приписанный субъекту или объекту доступа.

С учетом введенных обозначений, предикат предоставления доступа может быть записан в терминах субъектов и объектов доступа следующим образом:

$$\Delta(s, o, a) \equiv \Delta'(user(s), role(s), type(s); user(o), role(o), type(o); a) \equiv \\ \equiv \alpha(type(s), type(o), a) \wedge \rho(role(s), type(s)) \wedge \\ \wedge \rho(role(o), type(o)) \wedge \mu(user(s), role(s)) \wedge \mu(user(o), role(o)).$$

Модель Role Compatibility (RC), используемая в одном из модулей принятия решений о доступе в системе RSBAC, таким же образом может быть описана в своем упрощенном варианте, учитывающем только статическое состояние модели ЛРД [2)].

Как и для модели TE, введем следующие базовые множества, определяемые в модели RC, в предположении, что они конечны и непусты:

- A — множество типов доступа, заданных в модели;
- R — множество ролей, определяемых в модели, $r_o \in R$ — роль, соответствующая объектам доступа («объектная роль»);
- T — множество типов, определяемых в модели.

[2)] Модель RC, учитывающая смену роли и изменение атрибутов объектов доступа, описана в [4]

Ключевым отображением, определяемым в модели RC, является отображение роли в совместимые с ней доступы к объектам определенных типов:

- $CT\colon R \to T \times A$.

Для того, чтобы задать предикат предоставления доступа в зависимости от субъектов и объектов доступа, введем следующие вспомогательные функции:

- $role\colon S \to R$ — функция, определяющая роль субъекта доступа;
- $type\colon O \to T$ — функция, определяющая тип объекта доступа.

С учетом введенных обозначений предикат предоставления доступа записывается следующим образом:

$$\Delta(s,\, o,\, a) \equiv ((type(o),\, a) \in CT(role(s))).$$

Заметим, что в таком определении модели RC возможно определение контекста безопасности по аналогии с моделью TE, например, как пары $(r,\, t)$, где r и t — соответственно роль и тип субъекта или объекта доступа. При таком определении предикат доступа может быть записан как предикат от двух контекстов безопасности и типа осуществляемого доступа.

Используемая в системе grsecurity ролевая модель ЛРД полностью совпадает с упрощенной моделью RBAC_0, описанной ранее в настоящей работе. Отличия модели grsecurity/RBAC от традиционной проявляются при рассмотрении динамических свойств модели, связанных с так называемыми «вложенными субъектами» в grsecurty/RBAC — одним из способов задания правил смены роли субъекта. [3)]

В заключение настоящего раздела коснемся задач сравнения моделей ЛРД, используемых в ядре Linux. Как уже было замечено, отличительной особенностью средств ЛРД, встроенных в ядро, является унифицированность типов доступа. При рассмотрении теоретических моделей, положенных в основу перечисленных механизмов ЛРД, обнаруживается соответствие между субъектами, производящими доступ в различных моделях, а также соответствие между объектами, доступ к которым регулируется средствами ЛРД. В частности, удается теоретически подтвердить эквивалентность ряда схем задания статического среза моделей ЛРД, а при дополнительно наложенных условиях — и эквивалентности поведения моделей ЛРД при изменении набора субъектов и объектов. К таким результатам можно отнести полученные авторами выводы о возможности выражения друг через друга ролевых моделей Type Enforcement из системы

[3)] Подробнее модель grsecurity/RBAC с учетом динамических свойств рассматривается в [4].

SELinux и Role Compatibility из системы RSBAC, а также модели Type Enforcement и ролевой модели из системы grsecurity [4]. При рассмотрении случая статического состояния модели ЛРД, доказанные утверждения переходят в теоремы об эквивалентности моделей ЛРД. В формулировках таких теорем утверждается, что в условиях фиксированных множеств субъектов, объектов и типов доступа одна модель ЛРД всегда может быть записана в правилах другой (таким образом, что предикаты предоставления доступа совпадут), и наоборот. [4)]

4. Перспективы развития моделей ЛРД

Задачи, связанные с моделями ЛРД в целом, удобно разделить на следующие три класса:

- разработка описательных средств моделей ЛРД, в том числе, формальных моделей, привязки моделей к конкретным механизмам ЛРД, а также описательных средств, упрощающих настройку механизмов ЛРД;
- интеграция и согласование моделей ЛРД — построение по одной или нескольким моделям ЛРД новой модели, объединяющей эти модели с учетом правил разграничения доступа, задаваемых в согласуемых моделях ЛРД;
- верификация моделей ЛРД — проверка выполнения в изучаемой модели ЛРД ряда требуемых свойств [4].

В задачах согласования и задачах верификации моделей ЛРД авторами разработан унифицированный подход, основанный на контекстах безопасности в моделях ЛРД. Под контекстом безопасности понимается набор свойств, одинаковый для субъектов и объектов, такой, что решение о доступе с учетом заданной системы правил может быть однозначным образом принято на основании двух контекстов безопасности и типа доступа. Примеры таких контекстов рассмотрены в предыдущем разделе для случаев моделей Type Enforcement и Role Compatibility. В задачах согласования использование контекстов безопасности позволяет унифицировать модели ЛРД и организовать согласование моделей через дополнительные связи или отождествление контекстов безопасности из разных моделей. В задачах верификации, а именно, — проверки свойств моделей ЛРД удобно специфицировать свойства разрешенных информационных потоков между

[4)] При рассмотрении динамических свойств моделей ЛРД различия между моделями приводят к установлению эквивалентности только при наложении дополнительных ограничений, см. [4].

контекстами безопасности. В частности, авторами разработан способ преобразования ряда практически используемых моделей ЛРД (Role Compatibility, Type Enforcement, RBAC_0, моделей многоуровневого разграничения доступа и некоторых дискреционных моделей) к помеченной системе переходов, состояниями которой являются контексты безопасности. В таком представлении возможно задание свойств модели ЛРД, характеризующих информационные потоки, с помощью формул временно́й логики, например, Linear Temporal Logic (LTL) или Computational Tree Logic (CTL). Выполнимость таких свойств в системе переходов может быть проверена с помощью универсальных средств проверки моделей (model checking) [4, 11].

Проверяемые таким способом свойства можно представить следующей схемой. Представим информационный поток как последовательность элементарных информационных потоков, порождаемых доступами [5)], разрешенными заданными правилами исследуемой модели ЛРД:

$$SC_1 \xrightarrow{a_1} SC_2 \xrightarrow{a_2} SC_3 \xrightarrow{a_3} \ldots \xrightarrow{a_{n-1}} SC_n,$$

где $SC_1, \ldots, SC_n$ — контексты безопасности субъектов и объектов доступа, участвующих в информационном потоке; $a_1, \ldots, a_{n-1}$ — типы осуществляемых доступов (например, доступы на чтение и доступы на запись). С помощью формул временно́й логики на такой последовательности удается выделить следующую структуру:

$$s_1^{(1)} \to s_2^{(1)} \to \ldots \to s_{k_1}^{(1)} \to s_1^{(2)} \to \ldots \to s_{k_2}^{(2)} \to \ldots \to s_{k_m}^{(m)},$$

где $s_j^{(i)}$, $i = 1, \ldots, m$, $j = 1, \ldots, k_i$ — состояния системы переходов, в которой проверяется свойство, записанное на языке временно́й логики. Такие состояния в рассматриваемой задаче будут содержать информацию о контексте безопасности и о типе осуществляемого доступа. [6)] Состояния с одинаковым верхним индексом (i) удовлетворяют свойству, заданному с помощью формулы пропозициональной логики от переменных состояния. В рассматриваемой задаче проверки свойств моделей ЛРД к таким переменным можно отнести тип доступа и контекст безопасности, в свою очередь, содержащий данные о субъекте или объекте доступа, например, о пользователе-владельце, роли и типе субъекта или объекта доступа в модели Type Enforcement. Таким образом, представленная выше структура,

[5)] Например, доступ на чтение порождает информационный поток от объекта к субъекта, а доступ на запись — наоборот, от субъекта к объекту.

[6)] Пример построения такой системы переходов для модели Type Enforcement приводится в работе [4].

выделяемая в системе переходов, позволяет задавать свойства последовательного выполнения ряда условий на пути информационного потока, который состоит из последовательности элементарных информационных потоков. Такой способ спецификации свойств позволяет задавать ограничения на информационные потоки, а именно, — прохождение информационного потока только по определенной последовательности субъектов или объектов доступа. К таким ограничениям можно отнести изоляцию двух групп субъектов, когда запрещены информационные потоки от первой группы субъектов ко второй и от второй к первой. Аналогичным ограничением является свойство контролируемых информационных потоков, при котором запрещены информационные потоки от одной группы субъектов к другой, не проходящие через заданную третью группу субъектов доступа.

Отдельной задачей на этом направлении является разработка специализированных средств автоматизированного проектирования моделей логического разграничения доступа, ориентированных на задачи верификации моделей ЛРД в применении к конкретным компьютерным системам и их компонентам. Такие средства должны поддерживать все модели ЛРД, используемые в той или иной компьютерной системе. При этом следует предусмотреть возможность объединения их в единую, согласованную модель, производя анализ отдельных моделей на выполнение ряда свойств, заданных администратором безопасности компьютерной системы. Средства проектирования ЛРД должны быть ориентированы как на изначальное задание конфигурации механизмов ЛРД при развертывании компьютерной системы, так и на безопасное изменение такой конфигурации в процессе эксплуатации системы.

К перспективным задачам уровня ядра ОС можно отнести следующие задачи, носящие более технический характер:

- детализация доступов, контролируемых ядром ОС;
- разработка языков описания моделей ЛРД;
- внедрение новых механизмов ЛРД в ядро.

Внедрение детализированных доступов на уровне ядра ОС может быть реализовано, в том числе, с помощью:

- внедрения дополнительных атрибутов субъектов и объектов доступа;
- расширения набора типов доступа без модификации существующих программных интерфейсов (например, через введение зависимости типа доступа от аргументов системных вызовов);
- переноса ряда высокоуровневых механизмов ЛРД в ядро (например, переноса управления учетными записями пользователей ОС в ядро).

Последние два класса задач взаимосвязаны и с необходимостью объединяют теоретические исследования и программную реализацию. Одним из авторов разработан язык описания моделей ЛРД [3], основанный на явном задании формулой предиката предоставления доступа с помощью формул, определяющих зависимость возможных типов доступа от атрибутов субъектов и объектов доступа. Используя выразительные свойства разработанного языка удается записать на нем правила традиционно используемых многоуровневых и ролевых моделей ЛРД. В разработанной модели поддержка динамического изменения конфигурации производится с помощью так называемых пост-действий — действий, выполняемых после принятия решения о доступе. Такие действия могут изменять отдельные элементы конфигурации модели в зависимости от принятого решения о доступе. Прототип механизма, использующий разработанный язык, был реализован как дополнительный модуль для системы RSBAC с использованием XML-контейнера для хранения правил модели ЛРД — формул, задающих предикаты предоставления доступа. Более подробно разработанная модель ЛРД и язык описания конфигурации представлены в работе [3].

К задачам уровня ближайшего окружения ядра ОС, в первую очередь, относится задача интеграции средств управления механизмами ЛРД с дистрибутивом ОС. Такая интеграция призвана обеспечить решение задач управления правами пользователей и изоляцией сервисов с учетом жизненного цикла компьютерной системы, в рамках которого может потребоваться изменение конфигурации механизмов ЛРД, а безопасность такого изменения также должна быть обеспечена. Существующие механизмы управления конфигурацией средств разграничения доступа не всегда позволяют изменение настроек «на лету». В тех же случаях, когда это возможно, такие механизмы не гарантируют выполнения ряда свойств, например, связанных с допустимыми информационными потоками.

С учетом использования некоторыми программными сервисами средств ЛРД, вынесенных за пределы ядра ОС, требуется решение ряда задач интеграции и согласования моделей ЛРД, поддерживаемых различными механизмами ЛРД. Примером такой задачи является проверка непротиворечивости правил, задаваемых различными моделями. Такая задача включает в себя общие проблемы согласования моделей, а также некоторые частные задачи верификации моделей ЛРД [4].

Необходимо отметить важность задач согласования моделей и их последующей верификации для обеспечения безопасности на операционном уровне. Ключевыми моментами для моделей ЛРД в контексте операционного уровня обеспечения информационной безопасности являются возможности получения общей картины поддерживаемых моделей ЛРД и ав-

томатизированной проверки моделей на предмет выполнения ряда важных свойств, задаваемых администратором безопасности на основе политики информационной безопасности.

Литература

[1] *Васенин В. А.* Проблемы математического, алгоритмического и программного обеспечения компьютерной безопасности в Интернет // Материалы конференции МаБИТ-03, Москва, 2004. С. 111–143.

[2] *Андреев О. О.* Сравнение ролевой и дискреционной модели разграничения доступа // Материалы конференции МаБИТ-04, Москва, 2005. С. 284–291.

[3] *Андреев О. О.* Язык описания моделей разграничения доступа и его реализация в ядре операционной системы Linux // Материалы конференции МаБИТ-05, Москва, 2006. С. 305–321.

[4] *Шапченко К. А.* О некоторых средствах операционных систем для управления доступом при использовании ролевых политик безопасности // Материалы конференции МаБИТ-05, Москва, 2006. С. 257–281.

[5] NSA Security-Enhanced Linux. `http://www.nsa.gov/selinux`.

[6] *Loscocco P*, *Smalley S*. Meeting Critical Security Objectives with Security-Enhanced Linux, Proceedings of the 2001 Ottawa Linux Symposium. `http://www.nsa.gov/selinux/papers/ottawa01.pdf`.

[7] Rule-Set Based Access Control. `http://www.rsbac.org`.

[8] *Ott A*. The Role Compatibility Security Model. Nordic Workshop on Secure IT Systems (NordSec), 2002.

[9] Grsecurity. `http://www.grsecurity.net`.

[10] *Spengler B*. Increasing Performance and Granularity in Role-Based Access Control Systems: A Case Study in Grsecurity. `http://www.grsecurity.net/researchpaper.pdf`.

[11] *Guttman J. D.*, *Herzog A. L.*, *Ramsdell J. D.*, *Skorupka C. W*. Verifying information flow goals in Security-Enhanced Linux // Journal of Computer Security. 2005. V. 13, № 1. P. 115–134.

Обнаружение и разрешение противоречий в политиках безопасности

А. В. Тишков, И. В. Котенко, Е. В. Сидельникова, О. В. Черватюк

1. Введение

Актуальной задачей в системах, основанных на политике безопасности, которые предназначены для защиты крупномасштабных компьютерных сетей, является *обнаружение и разрешение противоречий в политике безопасности*.

Создавая множество правил безопасности, администратор (проектировщик) системы не в состоянии без соответствующего инструментария найти и устранить возможные противоречия между различными категориями политики, особенно в ситуации взаимного влияния правил разных категорий, а также определить возможность реализации этих правил на заданной компьютерной сети.

Существующие исследования в этой области, в большинстве случаев, ограничиваются рассмотрением лишь некоторых категорий правил политики безопасности.

В данной работе рассматривается *подход к построению системы верификации политики безопасности*, *разрабатываемой в настоящее время СПИИРАН*.

Предлагаемый подход основан на учете полного перечня возможных противоречий (в соответствии с разработанной классификацией), включая противоречия между правилами разных категорий и противоречия применения политики к защищаемой системе.

Настоящая статья структурирована следующим образом. *Во втором разделе* представлены основные аспекты подхода к верификации политики безопасности. *Третий раздел* дает представление об используемых языках

)Работа выполняется при финансовой поддержке РФФИ, программы фундаментальных исследований ОИТВС РАН (контракт № 3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза POSITIF (контракт IST-2002-002314) и RE-TRUST (контракт № 021186-2).

описания политики безопасности и системы. Предлагаемая классификация противоречий в политике безопасности рассмотрена *в четвертом разделе*. Архитектура и реализация системы верификации политики безопасности описываются *в пятом и шестом разделах*. *В седьмом разделе* делаются выводы и представляются направления будущих исследований.

2. Основные аспекты подхода к верификации

Программная система верификации политики безопасности получает на вход набор правил политики на *языке описания политики безопасности* (*ЯОП*), а также формализованное описание системы на *языке описания системы* (*ЯОС*), и позволяет «отлаживать» политику.

«Отладка» заключается в обнаружении противоречий и последующем их разрешении (или автоматическом, если возможно, или автоматизированном, работая в диалоге с администратором (проектировщиком).

Основными аспектами, *положенными в основу реализации системы верификации*, являются:

- использование систематического, мощного и гибкого подхода к верификации политики безопасности, основанного на предлагаемой классификации противоречий в политике;
- обнаружение полного перечня возможных противоречий;
- эффективная реализация поиска и разрешения противоречий с использованием как модулей общего назначения, которые позволяют обнаруживать все или большинство противоречий, в том числе динамические, так и специализированных модулей, работающих эффективно на конкретных типах противоречий;
- открытая, гибкая и расширяемая архитектура.

В качестве близких по тематике работ, использованных при разработке представляемой систеы, необходимо отметить исследования по формализации противоречий в политике [1], системы Rei [2] и Ponder [3], подход, основанный на деонтической логике [4]. Интересная система, позволяющая отслеживать состояние противоречия и разрешать его в «критический» момент предложена в [5]. Из других работ отметим подробную классификацию противоречий в политике фильтрации [6], аномалии задания политики IPSec [7], использование исчисления событий для моделирования работы системы защиты [8]. Перечень релевантных исследований, естественно, не исчерпывается представленными работами.

3. Языки описания политики безопасности и системы

Предлагаемая система верификации политики безопасности основана на использовании двух специализированных языков, служащих для описания политики безопасности (ЯОП) и конфигурации защищаемой системы (ЯОС).

Язык описания политики безопасности — это язык, используемый администратором сети для определения желаемого поведения системы безопасности в компьютерной сети или приложениях. Их описание должно быть создано заранее на языке ЯОС. Данный язык основан на стандарте CIM [9] и XML технологиях. Набор сгруппированных классов извлекается из модели в порядке представления различных категорий политики безопасности. ЯОП позволяет задать группировку, приоритет и классификацию категорий политики.

Язык описания политики безопасности содержит *пять категорий правил*:

- аутентификации;
- авторизации (контроля доступа);
- фильтрации;
- защиты каналов (IPSec, SSL/TLS);
- операционные.

Синтаксис каждой из категорий правил задается собственной схемой, основанной на XML-схеме. Схемы ЯОП были получены из xCIM-схем, которые являются представлением CIM с помощью технологии XML-схем.

Правила аутентификации определяют критерии аутентификации для субъекта на узле (объекте) сети. Поддерживается несколько типов аутентификации: аутентификация на основе разделяемых секретных ключей, посредством учетной записи, биометрическая, посредством сетевого идентификатора, открытого и закрытого ключа, Kerberos и др. Примером правила аутентификации является правило, позволяющее задать аутентификацию пользователя для входа на рабочую станцию по биометрическим данным.

Правила авторизации задают разделение доступа к ресурсам сети. Правило состоит из объекта (узла сети), субъекта (пользователь и/или роль), действия и привилегии (разрешения на действия или запрещения). Примером правила авторизации может служить запрет печати на сетевом принтере всем пользователям, находящимся в роли «Студент».

Правила фильтрации определяют условия фильтрации, используемые на сетевых узлах. В условиях обязательно указывать адрес и маску источника, адрес и маску получателя, порт или диапазон значений для портов

источника, порт или диапазон значений для портов получателя, а также тип протокола. Пример правила фильтрации — запрещение доступа с адреса 140.192.37.30 на адрес 161.120.33.40 при использовании порта 80 для источника и получателя и протокола tcp.

Правила защиты каналов позволяют задать, какой способ шифрования используется при передаче данных между определенными участками сети, например, IPSec/SA, IKE, SSL/TLS и др.

Операционные правила обуславливают выполнение определенных действий в зависимости от состояния системы, например, если обнаружен сбой работы сервиса принтера, то необходимо отправить сообщение администратору, или в заданном временном промежутке необходимо выполнить резервирование хранилища данных системы.

Язык описания системы применяется для описания конфигурации сети и ее функциональности. Правила политики должны использовать только те устройства, сервисы и функции, которые указаны в описании сети на ЯОС. Как и ЯОП, язык описания системы базируется на XML-схеме. ЯОС состоит из следующих основных частей:

- описание топологии сети, т.е. какой узел соединен с каким, тип соединения (проводное, беспроводное), тип кабеля и т. п.;
- описание сетевых сервисов, доступных на соответствующих серверах, а также установленных операционных систем;
- описание устройств и интерфейсов, в т.ч. имена, адреса, порты, общее описание назначения, изготовитель и др.

Например, описание сетевого интерфейса компьютера `client2` на ЯОС выглядит следующим образом:

```
<computer id="client2">
  <interface id="eth0" technology="Ethernet">
    <addr type="hw">00:08:02:57:28:EA</addr>
    <addr type="ipv4" netmask="255.255.255.0">192.168.1.254</addr>
  </interface>
  ...
</computer>
```

В следующем примере приведено описание HTTP и FTP сервисов на сервере `server1`:

```
<computer id="server1">
  ...
  <service id="web server">
    <protocol idRef="http"/>
```

```
    <sap addr="192.168.1.17" transport="tcp" port="80"/>
    <sap addr="192.168.1.17" transport="tcp" port="4444"/>
    <software idRef="MyApache"/>
  </service>
  <service id="ftp server">
    <protocol idRef="ftp"/>
    <sap addr="*" transport="tcp" port="21"/>
    <software idRef="Myftpd"/>
  </service>
  ...
</computer>
```

4. Классификация противоречий

Противоречие может возникнуть между правилами политики безопасности, между политикой и описанием системы или в описании системы. Разрабатываемая система верификации предназначена для поиска противоречий между правилами политики и при применении политики к описанию системы.

Авторы выделяют три вида *противоречий* (*несоответствий*) *применения политики безопасности к системе*.

К первому из них относится *отсутствие в описании сети элементов*, *представленных при описании политики безопасности*.

В качестве второго противоречия рассматривается *недостаточность функциональных возможностей для применения политики безопасности*. В ЯОС существует элемент `security_capabilities`, который относится к средствам описания топологии сети, устройств и интерфейсов согласно введенной выше структуре языка. Он отображает, какие узлы являются фильтрующими, какие типы защищенных протоколов поддерживаются, является ли элемент шлюзом для протоколов уровня приложений. Эти данные дают возможность проверять конфликты недостаточности функциональности для политики фильтрации и защиты каналов.

Третьим видом противоречий является *недостижимость узлов сети*. Входными данными для этой задачи является топология сети, получаемая из описания системы, и политики фильтрации, запрещающие или разрешающие трафик между двумя узлами. Все узлы делятся на два типа: имеющие и не имеющие функцию фильтрации. Задача состоит в том, чтобы построить таблицы доступа на узлах, имеющих функцию фильтрации, причем такие, чтобы в результате поддерживались все исходные правила фильтрации. Если такой набор таблиц построить невозможно, то администратор получает сообщение о конфликте.

Противоречия между правилами политики безопасности разделяются на два класса:

- внутри одной категории и
- между различными категориями.

Рассмотрим вначале **противоречия внутри одной категории правил**.

Противоречия между правилами категории аутентификации возникают, если для некоторого субъекта и объекта задан нерелевантный тип аутентификации. Делается допущение, что допустимые правила аутентификации между собой не конфликтуют: если для одной и той же пары субъект-объект заданы два типа аутентификации, считается, что они являются альтернативными способами входа.

Правило категории авторизации состоит в управлении доступом и задается четверкой: «субъект-действие-объект-право доступа» (разрешить (allow) / запретить (deny)). Субъект может представляться ролью или конкретным пользователем. Объект может быть составным и содержать коллекцию подобъектов. Противоречие возникает, если для одной и той же тройки «субъект-действие-объект» разрешение и запрет заданы явно или выводимы по иерархиям ролей и объектов.

Правила категории фильтрации разрешают или запрещают пересылку пакетов с определенным адресом и портом источника и получателя для заданного протокола. В результате процедуры уточнения правила фильтрации приобретают вид набора таблиц доступа, каждая из которых предназначена для определенного узла, обладающего фильтрующими функциями (межсетевого экрана).

Противоречия или аномалии внутри одной таблицы доступа (затенение, обобщение, корреляция, избыточность) и между таблицами доступа различных межсетевых экранах (затенение, фиктивность, корреляция, избыточность) подробно рассмотрены в [6] и обрабатываются в предлагаемой системе.

Внутри одной таблицы доступа возможны следующие аномалии:

- *затенение* — когда правило с большим приоритетом обрабатывает все пакеты, которые удовлетворяют условиям правила с меньшим приоритетом, и привилегии (разрешение/запрет) у этих правил различны. В этом случае правило с меньшим приоритетом никогда не будет активировано;
- *обобщение* — когда множество пакетов, удовлетворяющих условию правила с большим приоритетом, является подмножеством пакетов, удовлетворяющих условию правила с меньшим приоритетом, и при-

вилегии у этих правил различны. Правило с меньшим приоритетом никогда не будет активировано на этом подмножестве;

- *корреляция* — когда пересечение множеств пакетов, задаваемых условиями двух правил, не пусто, в то же время оно не совпадает ни с одним из этих множеств; при этом привилегии у этих правил различны. В этом случае правило с меньшим приоритетом никогда не будет активировано на указанном пересечении;
- *избыточность* — когда пересечение множеств пакетов, задаваемых условиями двух правил не пусто, при этом привилегии у этих правил совпадают. Возможно, такая ситуация связана с ошибкой администратора и одно из правил можно удалить или разделить на части.

Противоречия или аномалии между таблицами доступа также связаны с пересечениями условий правил, но из разных таблиц:

- *затенение* — когда вышестоящий (ближайший) по пути следования пакета межсетевой экран запрещает трафик, разрешенный нижестоящим (дальнейшим). Правило на нижестоящем межсетевом экране никогда не будет активировано;
- *фиктивность* — когда вышестоящий межсетевой экран разрешает трафик, запрещенный нижестоящим. Тогда образом, между межсетевыми экранами будет идти избыточный трафик, который можно было отсечь на вышестоящем межсетевом экране;
- *корреляция* — когда условия правила вышестоящего межсетевого экрана пересекаются с условиями правила нижестоящего межсетевого экрана и привилегии этих правил различны. Таким образом, на множестве пакетов, заданных пересечением условий указанных правил, возникнет одна из ситуаций описанных в двух предыдущих случаях;
- *избыточность* — когда вышестоящий межсетевой экран запрещает трафик, запрещенный нижестоящим межсетевым экраном, либо разрешает трафик, разрешенный нижестоящим межсетевым экраном. В этом случае фильтрация на нижестоящем межсетевом экране избыточна.

Противоречия в правилах защиты каналов связаны с некорректным заданием протоколов безопасности (IPSec, SSL/TLS и др.). Например, для IPSec проверяется условие, что при туннельном режиме IPSec туннели либо чередуются, либо вложены друг в друга.

Операционные правила представляют собой вызовы определенных функций (методов) по имени при возникновении определенных условий (например, наступлении заданной метки времени). Два и более операцион-

ных правила конфликтуют, если их условия могут выполняться одновременно, а методы, заданные в качестве действий, мешают выполнению друг друга или могут быть выполнены только в определенной последовательности.

Охарактеризуем **противоречия между категориями правил, реализующих политику безопасности**.

Не для всех категорий области действия правил пересекаются. Например, правила авторизации задаются только для пользователей, уже прошедших аутентификацию и не могут помешать действию правил аутентификации. В свою очередь, правила аутентификации не могут противоречить правилам авторизации, поскольку задаваемое в последних распределение доступа не зависит от результата и типа аутентификации.

Между категориями политики безопасности могут возникнуть следующие противоречия:

- аутентификация — фильтрация;
- аутентификация — операционные правила;
- авторизация — фильтрация;
- авторизация — операционные правила;
- фильтрация — защита каналов;
- фильтрация — операционные правила.

Представим *примеры типов противоречий* между различными категориями правил политики безопасности:

аутентификация — фильтрация — запрещающие правила фильтрации не позволяют соединиться с хостом, предоставляющим сервис;

аутентификация — операционные правила — действие операционного правила неосуществимо, поскольку пользователь системы или системный процесс, созданный для выполнения операционного правила, не может предоставить биометрических данных согласно правилу аутентификации;

авторизация — фильтрация — доступ к ресурсу разрешен пользователю, но соответствующий трафик отсекается межсетевым экраном;

авторизация — операционные правила — операционное действие не разрешено пользователю системы или системному процессу, созданному для выполнения операционного правила;

фильтрация — защита каналов — правила защиты каналов, специфицированные на ЯОП, содержат элементы фильтрации, такие как адреса и порты источника и получателя, поэтому аномалии затенения, обобщения, избыточности, корреляции в данном случае могут иметь место;

фильтрация — операционные правила — фильтр не позволяет пользователю системы или системному процессу, созданному для выполнения

операционного правила, получить доступ к ресурсу, над которым операционным правилом предписано совершить действие.

5. Архитектура системы верификации

Архитектура системы верификации политики безопасности, реализующей предлагаемый подход, является многомодульной (рис. 1).

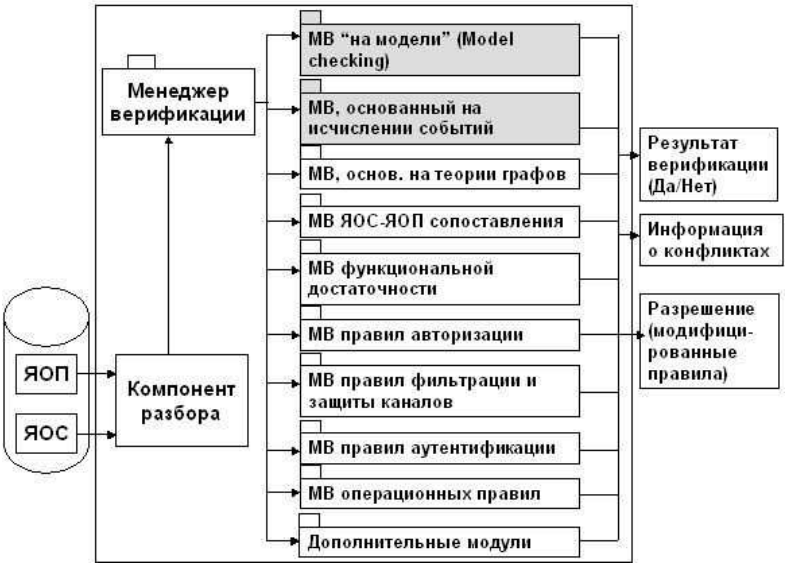


Рис. 1. Архитектура системы верификации

Основную работу по обнаружению и разрешению противоречий выполняют модули верификации (МВ). Менеджер верификации координирует работу этих моделей. Он запускает модули верификации для проверки непротиворечивости политики и собирает от них информацию о найденных конфликтах и способах их разрешения. В результате функционирования модулей верификации генерируются результат верификации, данные, идентифицирующие противоречие, и данные для модификации политики безопасности.

Модули верификации осуществляют проверку политики безопасности на основе различных математических методов.

Два *модуля верификации общего назначения* (на рис. 1 помечены серым цветом) реализуют единый подход к обнаружению и разрешению

всех противоречий, в том числе противоречий, возникающих между правилами различных категорий и противоречий применения политики к описанию системы. Один из модулей основан на *проверке на модели* (*Model checking*), второй использует *абдуктивный вывод* и *исчисление событий* (*Event Calculus*).

При обнаружении противоречий модули общего назначения работают менее эффективно, чем *специализированные модули* из-за более сложной формальной модели представления политики безопасности, описания системы и описания противоречий. Опишем кратко каждый из специализированных модулей.

При обнаружении противоречий модули общего назначения работают менее эффективно, чем специализированные модули из-за более сложной формальной модели представления политики безопасности, описания системы и описания противоречий. Опишем кратко каждый из специализированных модулей.

Модуль верификации, *основанный на теории графов*, предназначен для анализа достижимости компьютеров в сети. Для его реализации используется аппарат теории графов, в частности методы поиска минимального сечения графа.

Для обнаружения противоречий применимости политики к системе используется *модуль верификации сопоставления ЯОС-ЯОП*. Он проверяет наличие в ЯОС всех объектов, субъектов, описываемых в ЯОП, чтобы обеспечить возможность применения задаваемой политики к описываемой системе.

Модуль верификации функциональной достаточности проверяет по ЯОС наличие функциональных элементов для обеспечения выполнения правил политики, например, присутствие в системе межсетевого экрана для применения политик фильтрации.

Другие специализированные модули реализуют известные алгоритмы, которые разработаны для проверки правил конкретных категорий: авторизации, фильтрации и защиты каналов, аутентификации и операционных правил. Краткий перечень алгоритмов со ссылкой на источники рассмотрен во втором разделе.

6. Реализация системы верификации

На рис. 2 представлен пример главной формы пользовательского интерфейса системы верификации политики безопасности. Эта форма служит для управления процессом верификации. В ней предусмотрен выбор политики безопасности для верификации. Политика может быть просмотрена в текстовом редакторе.

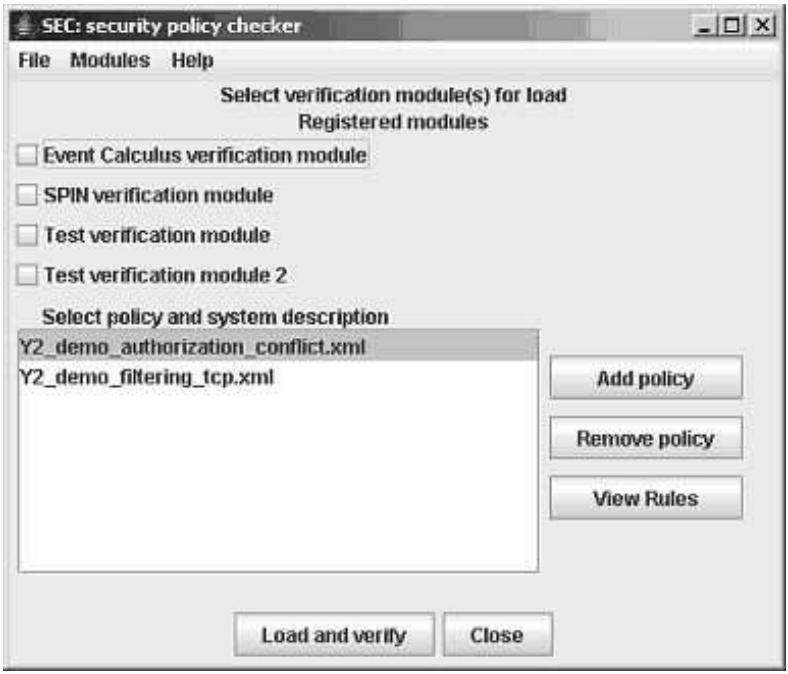


Рис. 2. Главная форма

Также с использованием этой формы могут быть подгружены необходимые для работы модули верификации. Список модулей по умолчанию задается в файле конфигурации.

После выбора верифицируемой политики и подходящих модулей можно запустить верификацию. По ходу работы модули генерируют журналы, содержащие информацию о результатах верификации, а также различную служебную информацию.

На рис. 3 представлена форма результатов верификации. Все обнаруженные в процессе верификации противоречия отображаются с использованием этой формы. По каждому противоречию выводится:

- имя модуля верификации, который обнаружил противоречие,
- тип противоречий,
- противоречивые правила и
- стратегии разрешения, если такие предусмотрены.

Для каждого противоречия можно выбрать стратегию разрешения и попытаться его разрешить.

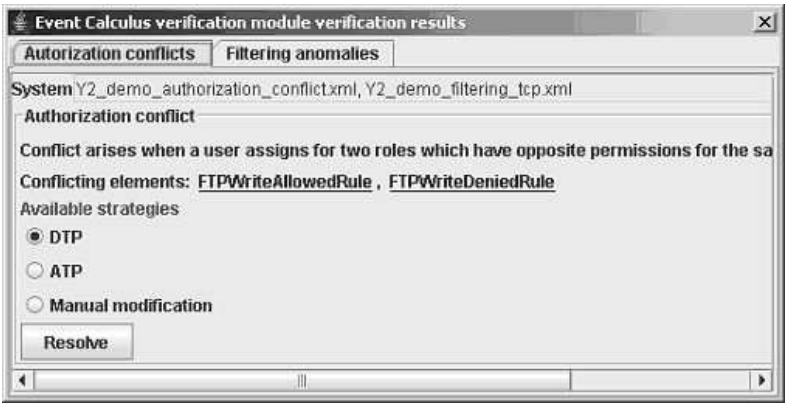


Рис. 3. Форма результатов верификации

Журналы работы различных модулей верификации содержат результат верификации и различную служебную информацию.

На рис. 4 показан примеры журналов работы модулей.

В начале журнала записывается информация о длительности процесса верификации. Затем выводится построенная верифицируемая модель на языке модуля.

На рис. 4 вверху показан журнал работы модуля, основанного на реализации абдуктивного вывода и исчисления событий (Event Calculus), а внизу — проверки на модели (Model Checking).

Для модуля Event Calculus описание представлено на языке Prolog, а для модуля Model Checking, реализованного на SPIN, — на языке Promela.

В конце лога отображаются результаты верификации — обнаружены ли противоречия, и какие правила в них задействованы.

Заключение

В настоящей работе рассмотрен предлагаемый авторами подход к построению многомодульной архитектуры *системы верификации политики безопасности*.

Представлены основные аспекты подхода, используемые языки описания политики безопасности и системы, классификация противоречий в политике безопасности, архитектура и реализация системы верификации политики безопасности.

Система верификации политики безопасности имеет многомодульную архитектуру. Основными модулями являются модули верификации

```
******************* Verification Time
*******************
875 milisec
******************* Generated axioms
*******************
initially_false(F) iff [[F=authorization_allowed(User,
write, server)], [F=authorization_denied(User, write,
server)]].
initiates(E,F,T) iff [[subject_role
(User,fTPWriteAllowedRole), E=request_authorization
(User, write, server), F=authorization_allowed(User,
write, server)], [subject_role
(User,fTPWriteDeniedRole), E=request_authorization
(User, write, server), F=authorization_denied(User,
write, server)]].
************************ Query
***************************
ciff('res/sec/ec/policies.alp', [holds_at
(authorization_allowed(User,Action,Target),T),
holds_at(authorization_denied(User,Action,Target),T)],
A).
************************ Answer
***************************
CONFLICT(S) FOUND
[subject_role(_107066,fTPWriteAllowedRole),
subject_role(_107066,fTPWriteDeniedRole), happens
(request_authorization(_107066,write,server),_17027),
happens(request_authorization
```

```
FTPWriteAllowedRole
                    conflicts.roles[1] =
FTPWriteDeniedRole
                    userRoles[0] = 1
                    userRoles[1] = 1
 31:    proc  1 (RoleAssigner) line  31 "model"
(state 5) <valid end state>
 31:    proc  0 (:init:) line  51 "model"
(state 7) <valid end state>
 31:    proc  - (:never:) line  68 "model"
(state 11) <valid end state>
3 processes created
***************************** VERIFICATION RESULT
*****************************
CONFLICT(S) FOUND
Rule-1: FTPWriteAllowedRule
Rule-2: FTPWriteDeniedRule
```

Рис. 4. Журналы работы модулей

и менеджер верификации. Модули верификации осуществляют проверку политики безопасности на основе различных математических методов. Менеджер верификации координирует работу этих моделей.

Система разработана на языке Java, с использованием JDK 1.5.0. При реализации абдуктивного вывода для исчисления событий использовался продукт CIFF 4.0, который распространяется в качестве библиотеки, использующей, в свою очередь вызывающей SICStus Prolog.

В качестве модуля, основанного на проверке на модели, был выбран SPIN 4.2.6. Остальные модули реализованы без использования дополнительного программного обеспечения.

Были проведены различные эксперименты по верификации различных категорий политики безопасности. Результаты этих экспериментов показали, что все модули успешно справляются с поставленными задачами выявления конфликтов.

МВ «на модели» хоть и требует больших временных и ресурсных затрат, но позволяет выявлять динамические конфликты, которые «пропускаются» другими модулями. Эксперименты показали также, что для обнаружения конфликтов конкретных категорий политики безопасности эффективнее использовать специализированные модули.

Дальнейшая работа связана с усложнением языка описания политики безопасности и расширением возможностей компонентов обнаружения и разрешения противоречий.

Литература

[1] *Lupu E.*, *Sloman M.* Conflicts in Policy-based Distributed Systems Management // IEEE Transactions on Software Engineering — Special Issue on Inconsistency Management. Nov. 1999. V. 25, № 6.

[2] UMBC eBiquity Project Rei: A Policy Specification Language. University of Maryland, Baltimore County, 2005.

[3] *Damianou N.*, *Dulay N. et al.* The Ponder Policy Specification Language // Workshop on Policies for Distributed Systems and Networks, Springer-Verlag, 2001.

[4] *Cholvy L.*, *Cuppens F.* Solving Normative Conflicts by Merging Roles // Proceedings of the fifth International Conference on Artificial Intelligence and Law, Washington, May 1995.

[5] *Dunlop N.*, *Indulska J.*, *Raymond K.* Methods for Conflict Resolution in Policy-Based Management Systems from EDOC, 2003.

[6] *Al-Shaer E.*, *Hamed H.*, *Boutaba R.*, *Hasan M.* Conflict classification and analysis of distributed firewall policies // IEEE Journal on Selected Areas in Communications. 2005. V. 23, № 10.

[7] *Hamed H.*, *Al-Shaer E.*, *Marrero W.* Modeling and verification of IPSec and VPN security policies // IEEE ICNP'05, 2005.

[8] *Bandara A.*, *Lupu E.*, *Russo A.* Using Event Calculus to Formalize Policy Specifications and Analysis // IEEE 4th International Workshop on Policies for Distributed Systems and Networks, June 2003.

[9] Common Information Model (CIM) Standards. `http://www.dmtf.org/standards/cim`.

Интеграция сигнатурного и поведенческого механизмов анализа данных мониторинга в системах обнаружения атак

В. В. Корнеев, В. В. Райх

В настоящей статье излагаются результаты исследований, позволяющих судить о степени применимости модифицированных нейронных сетей адаптивного резонанса ART2M для выявления аномальных сетевых сессий в трафике корпоративной сети в ситуации, когда в качестве примеров для обучения выступают результаты работы сигнатурного анализатора.

Введение

С момента своего появления средства мониторинга информационной безопасности претерпели и продолжают претерпевать концептуальные и технологические изменения, связанные как с повышением качества выполнения ими своих функций, так и с переосмыслением их места во всей совокупности защитных механизмов корпоративной вычислительной сети (КВС). В целом их эволюцию можно представить четырьмя этапами.

1. Первый этап. Создание и повсеместное внедрение антивирусных средств и сетевых средств защиты внешнего периметра (межсетевых экранов) — первых средств защиты, выполняющих свои функции по обнаружению и нейтрализации нарушений в реальном масштабе времени.

2. Текущий этап. Внедрение средств обнаружения атак и предотвращения вторжений, представляющих собой более интеллектуальные средства защиты, которые принято делить на группы, «привязанные» к моменту осуществления атак: средства анализа защищенности, средства обнаружения атак, средства перенаправления выявленных атак на ложные цели.

3. Начинающийся этап. Разработка и внедрение средств поддержки политики безопасности, включая ее формирование и контроль исполнения. Отличие данных средств от продуктов предыдущего этапа состоит

)Работа поддержана грантом РФФИ № 04-07-90010.

в том, что их настройка и функциональные возможности должны формулироваться не в технических терминах средств защиты (номеров портов, протоколов, имен файлов, процессов и других), как это происходит сейчас, а в терминах политики безопасности организации, оперирующих понятиями информационного ресурса, информационных потоков, служебных обязанностей персонала и подобных им.

4. Перспективный этап. Сращивание средств защиты информации от несанкционированного доступа с другими средствами обеспечения выполнения целевой функции КВС, такими, например, как системы поддержки отказоустойчивости, резервирования, балансировки нагрузки. Настройки данных средств должны будут формулироваться не просто в терминах положений политики безопасности, а в категориях поддержания заданного уровня качества предлагаемых КВС информационных сервисов.

Качество работы современных и перспективных систем защиты информации, во многом, определяется надежностью функционирования их датчиков и механизмов анализа данных. Надежность в данном случае характеризуется точностью и полнотой обнаружения подозрительных действий. В роли средств и систем, реализующих механизмы защиты, может выступать программное и аппаратное обеспечение самого различного класса. При этом особое внимание в настоящее время уделяется совершенствованию механизмов анализа данных различного рода системами обнаружения атак (IDS — Intrusion Detection System, IPS — Intrusion Prevention System), непосредственно выполняющих обработку первичных данных мониторинга — сетевого трафика и/или локальных событий на вычислительных узлах.

Одним из основных направлений повышения качества обнаружения атак IDS является дополнение повсеместно применяемого, однако не лишенного существенных недостатков, сигнатурного анализа данных различными реализациями поведенческих методов.

Одним из перспективных направлений внедрения поведенческих методов анализа данных мониторинга является применение нейросетевых средств, основанных на адаптивной кластеризации многомерных векторов признаков с автоматическим формированием обучающей выборки.

Целью настоящей статьи является изложение результатов очередного этапа исследований в области применения нейросетевых средств обнаружения аномалий, основанных на экспериментах по обработке реального трафика корпоративной сети.

Результаты ранее проведенных исследований

В проведенных ранее с участием авторов исследованиях [1, 2, 3, 4, 5] были получены следующие результаты.

Рассмотрены способы формирования профилей поведения компьютерной системы, представляющие собой решение задачи кластеризации многомерных векторов статистических признаков с использованием нейронных сетей [1]. Обученная нейросеть способна относить новые вектора к тому или другому классу за счет проверки на их вхождение в ранее выделенные кластеры. Таким образом, сама нейросеть становится профилем поведения защищаемой системы, который формируется автоматически в процессе ее обучения и может автоматически адаптироваться, если нейросеть допускает дообучение.

В рамках сравнительных исследований по выбору нейронных сетей, наиболее эффективно решающих задачу формирования профиля и последующего выявления аномального поведения [2], на основе интеграции алгоритмов обучения самоорганизующихся карт признаков Кохонена (SOM) и сетей теории адаптивного резонанса для бинарных и вещественных векторов (ART1 и ART2) [6, 7] был разработан модифицированный алгоритм обучения нейросетей теории адаптивного резонанса ART2M [3], показавший на тестовых выборках приемлемое быстродействие и простоту настройки параметров обучения (требуется выбрать только один параметр близости ρ).

Далее была предпринята попытка построить на базе созданного алгоритма нейросетевой анализатор, эквивалентный по точности сигнатурному [4]. Суть эксперимента заключалась в «очистке» сетевого трафика от пакетов, признанных сигнатурным анализатором (использовалась система обнаружения атак COA Snort) содержащими атаки, обучении нейросети на «чистом» трафике и последующей обработке обученной нейросетью исходного трафика. Полученные результаты показали невозможность построения работоспособной системы, основанной на такой модели функционирования. Причина в том, что изъятие «некорректных» пакетов из трафика вносит серьезные искажения в значения статистических показателей, использующихся в качестве входных данных нейросети. Кроме того, анализ статистических показателей трафика корпоративной сети в целом не дает представления о субъекте и объекте атаки, так как нарушение статистических свойств может обнаруживаться нейросетью на произвольном сетевом пакете, в том числе и не несущем непосредственно атакующее воздействие.

В связи с отмеченным выше обстоятельством были проведены аналогичные эксперименты, но на более низком уровне, допускающем, однако, сбор статистической информации [5]. Таким уровнем, по отношению к тра-

фику корпоративной сети в целом, был выбран уровень сетевых соединений (в частности, tcp-сессий), статистический анализ которых может дать представление как о субъекте и объекте атаки (в их качестве выступают инициатор и получатель соединения), так и о наличии или отсутствии самой атаки. Информация об этом может быть получена также с помощью сигнатурного анализатора на основе следующего правила: если хотя бы в одном пакете сессии обнаруживается сигнатура атаки, то вся сессия признается атакой или аномальным поведением.

В качестве исходных данных для экспериментов была использована база данных UCI KDD (`http://kdd.ics.uci.edu`), созданная исследовательской лабораторией Калифорнийского университета по заказу DARPA на основе анализа двухнедельного сетевого трафика центра ВВС США. Данная база с 1999 г. используется в качестве одного из эталонов для проверки действенности вновь разрабатываемых средств обнаружения компьютерных атак на основе поведенческих методов анализа данных. Эта база содержит статистические показатели около 5 млн. сетевых сессий, для каждой из которых указан тип обнаруженной в ней атаки, либо ее отсутствие.

По результатам экспериментов были сделаны следующие выводы.

Для получения удовлетворительных результатов при обучении нейросетей исходные статистические данные о сетевых соединениях должны подвергаться предварительной обработке по трем направлениям:

- структуризация данных за счет их разделения по признаку используемого протокола транспортного, а, по возможности, и прикладного уровня — дает снижение числа нейронов в обученной сети, а значит, — повышение ее быстродействия примерно на порядок;
- снижение размерности признакового пространства за счет исключения неинформативных показателей — также увеличивает быстродействие, как при обучении, так и при функционировании нейросети за счет снижения размерности обрабатываемых векторов на 10–60 %;
- приведение показателей к единому интервалу измерений [0, 1] за счет нормировки максимальным значением, что обеспечивает равное влияние различных показателей при их анализе нейросетью в составе входного вектора.

Полнота и точность распознавания нейросетью адаптивного резонанса ART2M аномальных сетевых соединений зависит от репрезентативности и достаточности объема обучающей выборки и действительно сессионного характера анализируемых сетевых взаимодействий. Как подтверждение, был зафиксирован низкий результат распознавания по протоколам icmp и udp, предполагающим взаимодействие в режиме запрос-ответ, и более

приемлемый результат по протоколам http и smtp, организующим более продолжительные сетевые соединения как с точки зрения объема передаваемой информации, так и с позиции количества сессий обмена данными.

Необходимо отметить, нейросеть, обученная на аномальных примерах, соответствующих сессиям с атаками, обладает лучшими характеристиками в разделении аномального и нормального поведения, по сравнению с нейросетью, обученной на нормальных примерах. В частности, такая нейросеть, обученная на репрезентативной выборке примеров для прикладных протоколов, реализующих обмен данными с установлением относительно продолжительных во времени сессий, таких как HTTP и SMTP, обеспечивает при эксплуатации значения ошибок первого рода порядка 10^{-2} и второго рода порядка 10^{-4} при быстродействии около 10^4 векторов/сек. (на типовом персональном компьютере), что соответствует средней загрузке сети FastEthernet.

Очередным шагом работ, описываемых далее, стало проведение тех же экспериментов, однако не на модельных данных из базы UCI KDD, а на реальном трафике корпоративной сети. Для этого были решены следующие задачи:

- разработан прототип интегрированной системы обнаружения атак, сочетающей сигнатурный и нейросетевой анализ данных;
- предложен перечень статистических показателей, которые могут характеризовать сетевые соединения по прикладным протоколам, использующим транспорт TCP;
- проведены эксперименты для получения количественных характеристик качества работы нейросетевого анализа данных в сравнении с сигнатурным.

Прототип интегрированной системы обнаружения атак

Разработанный прототип интегрированной системы обнаружения атак включает в свой состав в качестве сигнатурного анализатора СОА Snort, а также оригинальное программное обеспечение (ПО), реализующее нейросетевые механизмы анализа сетевого трафика. В совокупности данное ПО позволяет:

- формировать на основе содержания заголовков пакетов сетевого и транспортного уровней вектора статистических показателей сетевых сессий по заданным прикладным протоколам, идентифицируемым номерами портов TCP;

- направлять данные вектора на последующий нейросетевой анализ в сопровождении информации о наличии или отсутствии атак в пакетах сессии, получаемой от сигнатурного анализатора;
- обеспечивать автоматическое обучение нейросетей в соответствии с задаваемыми параметрами на основе информации о наличии/отсутствии атак в ходе сессии;
- обрабатывать после обучения нейросетей трафик в режиме реального времени и сохранять результаты обнаружения атак сигнатурным и нейросетевым методами в базе данных.

Для достижения приемлемой скорости обработки данных для каждого из протоколов и для входящих/исходящих в корпоративную сеть сессий обучается своя нейронная сеть. Такой подход оправдан, поскольку при этом возможно обеспечить меньшие размерность векторов и количество нейронов в обученной сети, что значительно влияет на быстродействие. При отсутствии такого предварительного разделения данных при обучении будет порождено большее число нейронов, на которые ляжет дополнительная нагрузка по учету не только специфики нормального и аномального поведения, но и прикладных протоколов в целом.

Технически интеграция оригинального ПО и СОА Snort была реализована с использованием встроенных возможностей данной СОА по расширению функциональности путем создания подключаемых модулей.

Архитектура СОА Snort предоставляет разработчику возможность использовать три типа подключаемых модулей: detection plugins (обнаруживающие модули), preprocessor plugins (препроцессорные модули), output plugins (модули вывода). Для решения задачи реализации взаимодействия Snort и ПО нейросетевого анализа созданы модули типа preprocessor plugins и output plugins.

Препроцессорный модуль получает каждый перехваченный пакет сетевого трафика до того, как этот пакет поступает в анализатор Snort (поиск в пакете сигнатур). Модуль этого типа используется в качестве поставщика информации. Он передает в приложение нейросетевого анализа через разделяемую память структуру, содержащую заголовки пакетов в формате библиотеки libpcap: Ethernet-заголовок, IP-заголовок, заголовок пакета транспортного уровня (tcp). На основе этих данных формируется вектор признаков, подлежащий кластеризации во время обучения нейросети или анализу во время ее эксплуатации.

Модуль вывода получает от других детектирующих модулей Snort сообщения об обнаруженных атаках. Его основная функция заключается в том, чтобы отобразить или сохранить эти сообщения в соответствующем формате. Модуль вывода используется также и в качестве поставщика ин-

формации об обнаруженных сигнатурным анализатором Snort атаках для реализации обучения нейросетевого анализатора.

Приложение нейросетевого анализа является самостоятельной программой, которая запускается до Snort, подготавливает необходимые структуры для взаимодействия с описанными выше подключаемыми модулями данной СОА и ожидает поступления от них данных.

Если приложение работает в режиме обучения, то вектора из очереди поступают на обработку в соответствии с алгоритмом обучения сети ART2M. При этом происходит автоматическое разделение на протоколы по номерам портов, а также по классу: нормальное или аномальное соединение — для каждого такого случая обучается своя нейросеть.

Если приложение работает в режиме обработки, то все вектора из очереди поступают на входы соответствующих (в зависимости от протокола) нейросетей. После этого они вместе с полученными результатами обработки передаются в модуль согласования, который при обнаружении аномалии выполняет запись сообщения об атаке в базу данных с идентификатором «аномальное поведение». Если данный вектор был помечен и сигнатурным анализатором, как аномальный, то в качестве кода атаки записывается значение, переданное подключаемым модулем вывода СОА Snort.

Формирование признакового пространства

В качестве основы для решения задачи формирования признакового пространства, описывающего сетевые сессии, была использована упоминавшаяся выше база данных UCI KDD, большинство информативных показателей которой были воспроизведены в оригинальном программном обеспечении, рассмотренном выше.

В нем также были использованы все выявленные ранее положения по подготовке исходных данных для анализа, в частности [5]:

- применение, по возможности, относительных значений;
- приведение значений показателей к единой шкале измерений;
- использование статистически независимых показателей.

Полученные таким образом результаты позволили сформировать следующий перечень статистических показателей (см. табл. 1).

Таким образом, из 42 показателей базы UCI KDD в разработанном ПО использовано 20 числовых показателей и еще 3 строковых (типы протокола транспортного и прикладного уровня, признак наличия атаки).

Отметим, что часть показателей базы UCI KDD не была реализована по причине их неактуальности. Например, с точки зрения рассматриваемых

Таблица 1. Реализованные показатели сетевых сессий и их связь с показателями базы UCI.KDD

№ пп	Описание	Аналогичный показатель базы UCI.KDD	Примечание
1	Продолжительность сессии в секундах	duration	Значение разделено на 10
2	Отношение количества байтов, переданных от клиента серверу, к количеству байтов, переданных от сервера к клиенту	src_bytes, dst_bytes	
3	Отношение количества команд, переданных в течение сеанса клиенту, к количеству команд, переданных в течение сеанса серверу	num_access_files	Под командой подразумевается наличие флага PUSH
4	Отношение числа «правильных» (т. е. с корректными значениями SN и ACK_SN) сегментов, полученных сервером, к общему числу сегментов, полученных сервером	wrong_fragment	
5	Отношение числа «правильных» (т. е. с корректными значениями SN и ACK_SN) сегментов, полученных клиентом, к общему числу сегментов, полученных клиентом	wrong_fragment	
6	Отношение количества байтов, переданных серверу и на которые было послано подтверждение приема, к общему количеству байтов, переданных серверу	wrong_fragment	
7	Отношение количества байтов, переданных клиенту и на которые было послано подтверждение приема, к общему количеству байтов, переданных клиенту	wrong_fragment	
8	Среднее количество «полезных» байтов, передававшихся в одном сегменте серверу	wrong_fragment	Значение разделено на 1024
9	Среднее количество «полезных» байтов, передававшихся в одном сегменте клиенту	wrong_fragment	Значение разделено на 1024
10	Количество соединений по этому же порту, открывшихся в сети за последние 2 сек.	srv_count	Значение разделено на 64
11	Отношение количества соединений по этому же порту, открывшихся на данном узле за последние 2 сек., к общему количеству соединений, открывшихся на данном узле за последние 2 сек.	same_srv_rate, diff_srv_rate	

12	Отношение количества соединений по этому же порту, открывшихся на других узлах за последние 2 сек., к количеству соединений по этому же порту, открывшихся в сети за последние 2 сек.	srv_diff_host_rate	
13	Количество соединений, открывшихся на данном узле за последние 2 сек.	count	Значение разделено на 16
14	Флаговый признак. Если сессия закрыта по флагу RST, то имеет значение 1. Иначе — 0	flag	
15	Флаговый признак. Если сессия закрыта по тайм-ауту 120 сек., то имеет значение 1. Иначе — 0	flag	
16	Отношение количества соединений по этому же порту, закрывшихся в сети за последние 2 сек. по этой же причине, к общему количеству соединений по этому же порту, закрывшихся в сети за последние 2 сек.	srv_rerror_rate	
17	Отношение количества соединений, закрывшихся на данном узле за последние 2 сек. по этой же причине, к общему количеству соединений, закрывшихся на данном узле за последние 2 сек.	rerror_rate	
18	Количество соединений, открытых данным узлом за последние 2 сек.	dst_host_count	Значение разделено на 16
19	Количество соединений по этому же порту открытых из данной сети в обратном направлении, за последние 2 сек.	dst_host_srv_count	Значение разделено на 64
20	Отношение количества соединений по этому же порту, открытых данным узлом за последние 2 сек., к общему количеству соединений, открытых данным узлом за последние 2 сек.	dst_host_same_srv_rate, dst_host_diff_srv_rate	
21	Отношение количества соединений по этому же порту, открытых другими узлами за последние 2 сек., к общему количеству соединений по этому же порту открытых из данной сети в обратном направлении, за последние 2 сек.	dst_host_srv_diff_host_rate	
22	Отношение количества соединений по этому же порту в обратном направлении, закрывшихся в сети за последние 2 сек. по этой же причине, к общему количеству соединений по этому же порту в обратном направлении, закрывшихся в сети за последние 2 сек.	dst_host_srv_rerror_rate	

23	Отношение количества соединений в обратном направлении, закрывшихся на данном узле за последние 2 сек. по этой же причине, к общему количеству соединений в обратном направлении, закрывшихся на данном узле за последние 2 сек.	dst_host_rerror_rate	

в исследовании прикладных протоколов (SMTP и HTTP) ряд показателей являются неприменимыми. Остальные исключенные показатели не допускают решения задачи нейросетевого анализа трафика в реальном времени. Они требуют детального анализа содержания сессии с позиций обработки данных прикладного протокола и настройки конкретного компьютера. Как следствие, значительно усложняется программное обеспечение, и такие случаи на практике являются предметом рассмотрения хостовых систем обнаружения атак (host-based IDS). В частности, не были, например, использованы следующие показатели:

is_hot_login — флаг, показывающий, что в ходе сессии на сервере был зарегистрирован пользователь, указанный в специальном списке;

is_guest_login — флаг, показывающий, что в ходе сессии на сервере пользователь зарегистрировался по гостевой учетной записи;

num_shells — количество командных интерпретаторов, порожденных в ходе сессии;

root_shell — флаг, показывающий, что в ходе сессии на сервере был запущен командный интерпретатор с полномочиями администратора;

su_attempted — флаг, показывающий, что в ходе сессии на сервере был запущен командный интерпретатор и предпринята попытка изменить его полномочия на полномочия администратора;

num_file_creations, num_access_files, num_outbound_cmds — показатели, касающиеся ftp-сессий;

logged_in — флаг, показывающий, что в ходе сессии на сервере был пользователь был зарегистрирован успешно;

num_failed_logins — количество неудачных попыток авторизации на сервере в ходе сессии.

Таким образом, предложенный перечень показателей можно считать полностью соответствующим составу показателей базы UCI KDD.

Для экспериментального доказательства данного положения было проведено два следующих эксперимента.

1. Обучение нейронных сетей адаптивного резонанса на аномальных и нормальных примерах из базы UCI KDD с использованием оригинального состава показателей, применявшихся ранее в экспериментах по установ-

лению самой возможности выполнения нейросетевой кластеризации аномальных и нормальных сессий [5].

2. Обучение нейронных сетей адаптивного резонанса на тех же аномальных и нормальных примерах из базы UCI KDD, но с использованием только указанного в табл. 1 перечня показателей, с последующим сопоставлением полученных результатов.

Для всех случаев при этом вычислялись:

- точность обнаружения атаки — как отношение числа аномальных сессий, обнаруженных нейросетью, к общему числу аномальных сессий, присутствовавших в выборке;
- ошибка первого рода (true negative) — как отношение числа аномальных сессий, ошибочно отнесенных сетью к нормальным, к общему числу сессий, отнесенных сетью к нормальным;
- ошибка второго рода (false positive) — как отношение числа нормальных сессий, ошибочно отнесенных сетью к аномальным, к общему числу сессий, отнесенных сетью к аномальным.

Полученные результаты приведены в табл. 2 и 3.

Таблица 2. Результаты обработки нейросетями данных из базы UCI.KDD с применением оригинального перечня показателей

Объект	**Кол-во обнаруженных нормальных векторов**	**Кол-во обнаруженных аномальных векторов**	**Из них аномальных векторов, определенных верно**	**Точность обнаружения атаки, %**	**Ошибка 1-го рода, %**	**Ошибка 2-го рода, %**
Протокол SMTP (параметр близости 0.85 для аномальных, 0.75 для нормальных)						
Реальные данные	95 371	1 183	1 183	100.0000	0.0000	0.0000
Сеть, обученная на аномальных примерах	95 445	1 109	1 109	93.7447	0.0775	0.0000
Сеть, обученная на нормальных примерах	95 156	1 398	1 172	99.0702	0.0116	16.1659
Протокол HTTP (параметр близости 0.78 для аномальных, 0.77 для нормальных)						
Реальные данные	619 045	5 092	5 092	100.0000	0.0000	0.0000
Сеть, обученная на аномальных примерах	618 913	5 224	5 016	98.5075	0.0123	3.9816
Сеть, обученная на нормальных примерах	620 521	3 616	2 913	57.2074	0.3512	19.4414

Таблица 3. Результаты обработки нейросетями данных из базы UCI.KDD с применением только совпадающих показателей

Объект	**Кол-во обнаруженных нормальных векторов**	**Кол-во обнаруженных аномальных векторов**	**Из них аномальных векторов, определенных верно**	**Точность обнаружения атаки, %**	**Ошибка 1-го рода, %**	**Ошибка 2-го рода, %**
Протокол SMTP (параметр близости 0.85 для аномальных, 0.75 для нормальных)						
Реальные данные	95 371	1 183	1 183	100.0000	0.0000	0.0000
Сеть, обученная на аномальных примерах	95 419	1 135	1 094	92.4768	0.0933	3.6123
Сеть, обученная на нормальных примерах	95 182	1 372	1 088	91.9696	0.0998	20.6997
Протокол HTTP (параметр близости 0.78 для аномальных, 0.77 для нормальных)						
Реальные данные	619 045	5 092	5 092	100.0000	0.0000	0.0000
Сеть, обученная на аномальных примерах	612 973	11 164	5 011	98.4093	0.0132	55.1147
Сеть, обученная на нормальных примерах	620 823	3 314	2 881	56.5789	0.3561	13.0658

Сопоставление значений в табл. 2 и 3 позволяет сделать вывод, что некоторое сокращение количества показателей, используемых в разработанном ПО нейросетевого анализа, обусловленное объективными причинами необходимости обеспечения обработки трафика в реальном времени, влияет на качество обнаружения атак как нейросетями, обученными на нормальных примерах, так и нейросетями, обученными на аномальных примерах.

Таким образом, представленный перечень показателей требует уточнения и, возможно, расширения для того, чтобы его можно было считать состоятельным и применимым к анализу сетевых соединений по протоколам HTTP и SMTP.

Литература

[1] *Райх В. В.* Применение нейронных сетей Кохонена для решения задач кластеризации в процессе мониторинга информационной безопасности // Математика и безопасность информационных технологий. Материалы конференции в МГУ 23–24 октября 2003 г. М.: МЦНМО, 2004. С. 321–327.

[2] *Райх В. В.* Исследование свойств нейронных сетей Кохонена и адаптивного резонанса применительно к задачам мониторинга информационной безопасности // Информационная безопасность. Материалы VI Международной научно-практической конференции, 1–7 июля 2004 г. Таганрог: изд-во ТРТУ, 2004. С. 193–195.

[3] *Корнеев В. В.*, *Райх В. В.* Нейросетевой алгоритм кластеризации на базе модифицированной сети адаптивного резонанса для вещественных векторов // Материалы Второй Всероссийской научно-технической конференции «Методы и средства обработки информации» (МСО-2005), 5–7 октября 2005 г., г. Москва.

[4] *Райх В. В.*, *Синица И. Н.*, *Шарашкин С. М.* Макет системы выявления атак на основе обнаружения аномалий сетевого трафика // Методы и средства обработки информации. Труды Второй Всероссийской научной конференции, 5–7 октября 2005 г. М.: издательский отдел факультета вычислительной математики и кибернетики МГУ им. М. В. Ломоносова, 2005. С. 175–181.

[5] *Корнеев В. В.*, *Райх В. В.* Применение модифицированных нейронных сетей адаптивного резонанса для выявления аномальных сетевых соединений // Математика и безопасность информационных технологий. Материалы конференции в МГУ, 2005 г. М.: МЦНМО, 2005.

[6] *Корнеев В. В.*, *Гареев А. Ф.*, *Васютин С. В.*, *Райх В. В.* Базы данных. Интеллектуальная обработка информации: 2-е изд. М.: Нолидж, 2001. 496 с.

[7] *Круглов В. В.*, *Борисов В. В.* Искусственные нейронные сети. Теория и практика. М.: Горячая линия-Телеком, 2001. 382 с., ил.

Часть III

СЕКЦИЯ «МАТЕМАТИЧЕСКИЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Метрические свойства некоторых классов функций

Б. А. Погорелов, М. А. Пудовкина

1. Введение

Часть методов криптографического анализа, в частности, линейного, сводится к аппроксимации нелинейных функций, используемых в криптографических алгоритмах, аффинными, поскольку системы линейных уравнений решаются за полиномиальное время. Известно, что функции, максимально далекие от аффинных, называемые бент-функциями, хуже всего поддаются аппроксимации. Однако, кроме класса аффинных функций, существуют другие классы функций, в которых легко решаются системы уравнений. К таким функциям относятся (см., например, [1]) мультиаффинные, биюнктивные, слабо положительные, слабо отрицательных функции, порождающие полиноминально решаемые классы систем булевых уравнений без ограничения на выбор неизвестных.

Пусть A — класс мультиаффинных, Bi — класс биюнктивных, WP — слабо положительных, WN — слабо отрицательных функций. Согласно работе [2] представляет интерес рассмотрение функций, которые принадлежат нескольким классам A, Bi, WP, WN. В этом случае можно рассчитывать на построение более быстрых алгоритмов решения систем булевых уравнений без ограничений на выбор неизвестных, чем в случае принадлежности функций только одному из классов.

Обозначим $M_1 = A \cap WP$, $M_2 = A \cap Bi$, $M_3 = WN \cap WP$, $M_4 = Bi \cap WP$, $M_5 = Bi \cap WN$. Отметим, что $M_1 = A \cap Bi \cap WP \cap WN$. В работе [2] описан вид функций, принадлежащих каждому из классов M_i, $i = \overline{1, 5}$.

Представляет интерес вопрос об аппроксимации произвольной функции функциями из этих классов. В качестве первого шага рассматриваются метрические свойства функций из каждого класса. В настоящей работе получены возможные значения расстояний между функциями из классов M_1, M_2, M_3 и бент-функциями из класса Майорана — МакФарланда.

Всюду ниже будем придерживаться следующих обозначений: V_n — множество всех двоичных n-мерных векторов, $S(X)$ — симметрическая группа

подстановок на множестве X; $F_n = \{f\colon V_n \to \{0, 1\}\}$; B_n — множество всех бент-функций из F_n ; $M_i^{(n)}$ — функции из класса M_i, существенно зависящие от n переменных; $M_{i,n}$ — функции из класса M_i, зависящие от n переменных; $\chi(\alpha, \beta)$ — метрика Хемминга; $\|\alpha\| = \chi(\alpha, \vec{0})$ — вес вектора $\alpha \in \in V_n$; G_f — граф функции $f \in F_n$; n_f — число компонент связности графа G_f; $G_f^{(i)} = (X_f^{(i)}, V_f^{(i)})$ — компонента связности графа $G_f = (X_f, V_f)$, $i = \overline{1, n_f}$; X_f — множество существенных переменных функции f; $n_f^{(0)}$ — число компонент связности графа G_f без петель; σ_j — j-я координатная функция подстановки $\sigma \in S(V_n)$; $D(M_i^{(n)}) = \{\chi(f_1, f_2) | f_1, f_2 \in M_i^{(n)}\}$, $i \in \{\overline{1, 5}\}$; $\langle \alpha, x \rangle$ — скалярное произведение, $\hat{\sigma}(n, d)$ — присоединенное число Стирлинга второго рода (число разбиений множества мощности n без единичных блоков на d блоков).

Если $f = hf$, где f, $h \in F_n$ — ненулевые функции, то будем использовать обозначение $h(x_1, \ldots, x_n) | f(x_1, \ldots, x_n)$.

2. Расстояния между функциями класса M_1

В работе [2] показано, что функция $f \in F_n$ вида

$$f(x_1, \ldots, x_n) = \left(\prod_{i=1}^{t_1} x_{s_i}^{\alpha_i}\right) \cdot \left(\prod_{i=t_1+1}^{t} (x_{s_{i_1}} + x_{s_{i_2}} + 1)\right)$$

принадлежит классу $M_{1,n}$, причем такое представление неоднозначно, и каждая функция из $M_{1,n}$ однозначно представима в виде

$$f^{(c)}(x_1, \ldots, x_n) = \prod_{i=1}^{t_1} x_{s_i}^{\alpha_i} \cdot \prod_{j=1}^{t_2} \prod_{a=1}^{q_j-1} (x_{s_a^{(j)}} + x_{s_{a+1}^{(j)}} + 1), \tag{1}$$

где $X_j = \{s_1^{(j)}, \ldots, s_{q_j}^{(j)}\} \subseteq \{\overline{1, n}\}$, $q_j = |X_j| \geqslant 2$, $j = \overline{1, t_2}$, $\{s_1, \ldots, s_{t_1}\} \cap \bigcup\limits_{j=1}^{t_2} X_j = = \emptyset$.

Там же показано, если $M_{1,n}$ существенно зависит от $k \in \{\overline{1, n}\}$ переменных, то $\|f\| = 2^{t_2+n-k}$, и

$$|M_{1,n}| = 1 + \sum_{r=0}^{n} \binom{n}{r} \sum_{i=0}^{r} \binom{r}{i} 2^i \hat{\sigma}(r - i),$$

где $\hat{\sigma}(r)$ — число разбиений множества мощности r без единичных блоков.

Представление функции в виде (1) назовем каноническим для класса M_1.

Каждой функции $f \in M_1^{(n)}$ в каноническом виде поставим в соответствие граф $G_f = (X_f,\ V_f)$, X_f — множество существенных переменных функции f, $(i,\ j) \in V_f$, $i \neq j$, тогда и только тогда, когда $(x_i + x_j + 1)|f(x_1,\ \ldots,\ x_n)$, и $(i,\ i) \in V_f$ тогда и только тогда, когда $x_i^{\alpha_i}|f(x_1,\ \ldots,\ x_n)$, $\alpha_i \in \{0,\ 1\}$. Упорядочим компоненты связности графа G_f таким образом, что первые $n_f^{(0)}$ компонент — компоненты связности графа G_f без петель. Пусть

$$\bar{X}_f = X_f \setminus \bigcup_{i=1}^{n_{f_1}^{(0)}} X_{f_1}^{(i)}, \qquad |\bar{X}_f| = n_f^{(1)}.$$

Раскрасим вершины графа G_f в белый и черный цвет таким образом, что i-я вершина окрашена в белый цвет, если $\beta_i = 0$ и в черный цвет — иначе. Пусть $\mu\colon \{0,\ 1\} \to \{\text{белый,черный}\}$, $\mu(0) =$‘белый’, $\mu(1) =$‘черный’.

Таким образом, каждому вектору $\beta = (\beta_1,\ \ldots,\ \beta_n) \in V_n$ однозначно соответствует раскраска $\tilde{\mu}(\beta)$ такая, что i-я вершина окрашена в $\mu(\beta_i)$ цвет. Назовем раскраску графа G_f правильной, если выполнены следующие два условия: 1) любая вершина $i \in X_f$ такая, что $(i,\ i) \in V_f$ и $x_i^{\alpha_i}|f(x_1,\ \ldots,\ x_n)$ раскрашена в цвет $\mu(\alpha_i + 1)$; 2) вершины, принадлежащие одной компоненте связности графа G_f, окрашены в одинаковый цвет.

Ясно, что правильно раскрасить компоненту графа G_f с петлей возможно единственным способом, а компоненту без петли — двумя способами. Кроме того, $f(\beta) = 1$, $\beta \in V_n$, тогда и только тогда, когда раскраска $\tilde{\mu}(\beta)$ правильная.

Приведем число функций из множества $M_{1,n}$ находящихся от нулевой функции на заданном расстоянии Хемминга.

Утверждение 1. *Число функций из $M_{1,n}$ веса 2^d, $d \in \{\overline{0,\ n-1}\}$, равно*

$$\sum_{k=n-d}^{n} \binom{n}{k} \sum_{i=0}^{k} \binom{k}{i} \hat{\sigma}(k-i,\ d+k-n).$$

Доказательство. Будем считать, что функция f задана в каноническом виде. Пусть k — число существенных переменных функции f, i — число единичных компонент графа G_f. Тогда

$\binom{n}{k}$ — число способов выбрать k существенных переменных функции f,

$\binom{k}{i}$ — число способов выбрать i единичных компонент графа G_f,

2^i — число способов раскрасить i единичных компонент графа,

$\hat{\sigma}(k-i,\ d+k-n) = \hat{\sigma}(k-i,\ n_f^{(0)})$ — число компонент графа G_f без петель. $\square$

Отметим, что наибольший вес функции $f \in M_{1,n}$, существенно зависящей от $k \in \{\overline{1, n}\}$ переменных, равен $2^{\lfloor k/2 \rfloor + n - k}$, а наибольший вес функции из $M_{1,n}$ равен 2^{n-1}.

Утверждение 2. 1. *Для любых* $h_1, h_2 \in \{\overline{0, n-1}\}$ *существуют функции* $f_1, f_2 \in M_{1,n}$ *такие, что*

$$\chi(f_1, f_2) = 2^{h_1} + 2^{h_2}.$$

2. *Пусть функция* $f \in M_{1,n}$ *существенно зависит от* k *переменных и* $|\bar{X}_f| = r$, $k \in \{\overline{1, n}\}$, $r \in \{\overline{1, k}\}$. *Тогда число функций из* $M_{1,n}$, *находящихся от функции* f *на расстояние* $2^{n_f^{(0)}+n-k} + 2^d$, $d \in \{\overline{0, n-1}\}$, *равно*

$$\sum_{t=n-d}^{n} \binom{n}{t} \sum_{b=1}^{t} \sum_{b_1=1}^{\min\{r,b\}} 2^{b-b_1} \binom{b}{b_1} \binom{r}{b_1} (2^{b_1} - 1) \hat{\sigma}(t-b, t+d-n).$$

Доказательство. 1. Справедливо равенство

$$\chi(f_1, f_2) = \|f_1\| + \|f_2\| - 2\,\|f_1 f_2\|\,.$$

Пусть

$$f_1(x_1, \ldots, x_n) = x_n^0 g_1(x_1, \ldots, x_{n-1}), \;\; f_2(x_1, \ldots, x_n) = x_n^1 g_2(x_1, \ldots, x_{n-1}).$$

Тогда $\|f_1 f_2\| = 0$. Значит для любых функций $g_i \in M_{1,n-1}$, $n_{g_i} = n_{g_i}^{(0)} = h_i \in \in \{\overline{0, n-1}\}$, $i = \overline{1, 2}$, выполняется равенство

$$\chi(f_1, f_2) = 2^{h_1} + 2^{h_2}.$$

2. Рассмотрим произвольную функцию $g \in M_{1,n}$. Будем считать, что функции f и g заданы в каноническом виде. Пусть k_g — число существенных переменных функции g, b — число единичных компонент графа G_g, $|\bar{X}_f \cap \bar{X}_g| = b_1$. Очевидно, что $\|fg\| = 0$, если существует $i \in \bar{X}_f \cap \bar{X}_g = = \{i_1, \ldots, i_{b_1}\}$ такое, что $x_i^{\alpha_i} | f$ и $x_i^{\alpha_i+1} | g$. Следовательно, $b_1 \in \{\overline{1, \min\{r, b\}}\}$, $b \in \{\overline{1, k_g}\}$.

Поскольку выполняется равенство $d = n_g^{(0)} + n - k_g$, то $k_g \in \{\overline{n-d, n}\}$ и $\binom{n}{k_g}$ — число способов выбрать k_g существенных переменных функции g, $\binom{b}{b_1}\binom{r}{b_1}$ — число способов выбрать b_1 единичных компонент таких, что $b_1 = |\bar{X}_f \cap \bar{X}_g|$, $(2^{b_1} - 1)$ — количество двоичных векторов $\beta = = (\beta_{i_1}, \ldots, \beta_{i_{b_1}})$ таких, что $(\beta_{i_1}, \ldots, \beta_{i_{b_1}}) \neq (\alpha_{i_1}, \ldots, \alpha_{i_{b_1}})$, т. е. существует хотя бы одно $i \in \bar{X}_f \cap \bar{X}_g = \{i_1, \ldots, i_{b_1}\}$, удовлетворяющее соотношениям: $x_i^{\alpha_i} | f$ и $x_i^{\alpha_i+1} | g$.

2^{b-b_1} — число способов раскрасить $b - b_1$ единичных компонент графа G_g, не принадлежащих множеству $\bar{X}_f \cap \bar{X}_g$.

$\hat{\sigma}(k_g - b,\ k_g + d - n) = \hat{\sigma}(k_g - b,\ n_g^{(0)})$ — число компонент без петель. $\square$

Для сравнения приведем аналогичные характеристики для класса аффинных функций. Известно, что расстояние между произвольными аффинными функциями из множества F_n равно 2^{n-1}, а число аффинных функций, находящихся на расстоянии 2^{n-1}, равно $2^{n+1} - 1$.

Утверждение 3. *Для любых* $h_1, h_2 \in \{\overline{0,\ \lfloor n/2 \rfloor}\}$ *и для любого* $h \in \{\overline{0,\ \min\{h_1,\ h_2\}}\}$ *существуют функции* $f_1, f_2 \in M_1^{(n)}$ *такие, что* $n_{f_1}^{(0)} = h_1$, $n_{f_2}^{(0)} = h_2$, $n_{f_1 f_2}^{(0)} = h$ *и*

$$\chi(f_1,\ f_2) = 2^{h_1} + 2^{h_2} - 2^{h+1}.$$

Следствие 1. *Минимальное расстояние между функциями из класса* $M_1^{(n)}$ *равно* 2, *а максимальное* — $\max\{2^{\lfloor n/2 \rfloor + 1} - 2,\ 2^{\lfloor (n-1)/2 \rfloor + 1}\}$.

3. Расстояния между функциями класса M_2

В работе [2] показано, что функция $f \in F_n$ вида

$$f(x_1,\ \ldots,\ x_n) = \prod_{i=1}^{t} (a_{i_1} x_{s_{i_1}} + a_{i_2} x_{s_{i_2}} + a_{i_0})$$

принадлежит классу $M_{2,n}$, причем такое представление неоднозначно и каждая функция $f \in M_{2,n}$ единственным образом представима в каноническом виде. Там же показано, если $f \in M_{2,n}$ существенно зависит от $k \in \{\overline{1,\ n}\}$ переменных, то $\|f\| = 2^{t_2 + n - k}$, и

$$|M_{2,n}| = 1 + \sum_{r=0}^{n} \binom{n}{r} \sum_{i=0}^{r} \binom{r}{i} 2^i \sum_{j=0}^{\lfloor (r-i)/2 \rfloor} 2^{r-i-j} \hat{\sigma}(r - i,\ j).$$

Функции $f \in M_2^{(n)}$ в каноническом виде поставим в соответствие граф $G_f = (X_f,\ V_f)$, $(i,\ j) \in V_f$, $i \neq j$, тогда и только тогда, когда

$$(x_i + x_j + \alpha_{ij}) | f(x_1,\ \ldots,\ x_n), \quad \alpha_{ij} \in \{0,\ 1\},$$

и $(i,\ i) \in V_f$ тогда и только тогда, когда $x_i^{\alpha_i} | f(x_1,\ \ldots,\ x_n)$. Нетрудно показать, что граф $G_f^{(i)}$ является двудольным при $i = \overline{1,\ n_f^{(0)}}$.

Метрические свойства функций из классов M_1 и M_2 близки между собой. Приведем число функций из множества $M_{2,n}$, находящихся от нулевой функции на заданном расстоянии.

Утверждение 4. *Число функций из $M_{2,n}$ веса 2^d, $d \in \{\overline{0,\, n-1}\}$, равно*

$$2^{n-d} \sum_{k=n-d}^{n} \binom{n}{k} \sum_{i=0}^{k} \binom{k}{i} \hat{\sigma}(k-i,\, d+k-n).$$

Доказательство. Число способов разбить множество X_j, $j \in \{\overline{1,\, n_f^{(0)}}\}$, на подмножества $X_j^{(1)}$, $X_j^{(2)}$, $X_j^{(1)} \cap X_j^{(2)} = \emptyset$, равно $2^{|X_j|-1}$.

Из утверждения 1 и равенства $\prod_{j=1}^{n_f^{(0)}} 2^{|X_j|-1} = 2^{k-i-n_f^{(0)}}$, получаем, что число функций веса 2^d с фиксированными существенными k переменными равно

$$\begin{aligned}
&\sum_{i=0}^{k} 2^i \binom{k}{i} \hat{\sigma}(k-i,\, n_f^{(0)}) \cdot 2^{k-i-n_f^{(0)}} \\
&= \sum_{i=0}^{k} 2^i \binom{k}{i} \hat{\sigma}(k-i,\, d+k-n) \cdot 2^{k-i-(d+k-n)} \\
&= 2^{n-d} \sum_{i=0}^{k} \binom{k}{i} \hat{\sigma}(k-i,\, d+k-n). \qquad \square
\end{aligned}$$

Следующее утверждение показывает, наборы расстояний между функциями в классах M_1 и M_2 равны, т. е. справедливо равенство $D(M_1^{(n)}) = D(M_2^{(n)})$.

Утверждение 5. 1. *Для любых h_1, $h_2 \in \{\overline{0,\, \lfloor (n-1)/2 \rfloor}\}$ и для любого $h \in \{\overline{0,\, \min\{h_1,\, h_2\}}\}$ существуют функции f_1, $f_2 \in M_2^{(n)}$ такие, что $n_{f_1}^{(0)} = h_1$, $n_{f_2}^{(0)} = h_2$, $n_{f_1 f_2}^{(0)} = h$ и*

$$\chi(f_1,\, f_2) = 2^{h_1} + 2^{h_2} - 2^{h+1}.$$

2. *Для любых h_1, $h_2 \in \{\overline{0,\, n-1}\}$ существуют функции f_1, $f_2 \in M_{2,n}$ такие, что*

$$\chi(f_1,\, f_2) = 2^{h_1} + 2^{h_2}.$$

3. *Пусть функция $f \in M_{2,n}$ существенно зависит от k переменных и $|\bar{X}_f| = r$, $k \in \{\overline{1,\, n}\}$, $r \in \{\overline{1,\, k}\}$. Тогда число функций из $M_{2,n}$, находящихся от функции f на расстояние $2^{n_f^{(0)}+n-k} + 2^d$, $d \in \{\overline{0,\, \lfloor n/2 \rfloor}\}$,*

равно

$$\sum_{t=n-d}^{n}\binom{n}{t}\sum_{b=1}^{t}\sum_{b_1=1}^{\min\{r,b\}}2^{n-d-b_1}\binom{b}{b_1}\binom{r}{b_1}(2^{b_1}-1)\hat{\sigma}(t-b,\,t+d-n).$$

Доказательство непосредственно следует из утверждений 2,3 и 4.

4. Расстояния между функциями класса M_3

В работе [2] показано, что функция $f\in F_n$ принадлежит классу $M_{3,n}$ тогда и только тогда, когда она представима в виде

$$f(x_1,\,\ldots,\,x_n)=\left(\prod_{i=1}^{t_1}x_{s_i}^{\alpha_i}\right)\cdot\left(\prod_{i=t_1+1}^{t}(x_{s_{i_1}}\vee\bar{x}_{s_{i_2}})\right).$$

Каждой функции $f\in M_{3,n}$ поставим в соответствие ориентированный граф $G_f=(X_f,\,V_f)$, $(i,\,j)\in V_f$, $i\neq j$, тогда и только тогда, когда $(x_i\vee\bar{x}_j)|f(x_1,\,\ldots,\,x_n)$, и $(i,\,i)\in V_f$ тогда и только тогда, когда $x_i^{\alpha_i}|f(x_1,\,\ldots,\,x_n)$. С помощью свойств орграфа G_f доказываются следующие утверждения.

Утверждение 6. *Для произвольного натурального числа $n\geqslant 1$ существуют функции из M_3, расстояние между которыми равно n.*

Утверждение 7. *Пусть*

$$k^{(r)}\geqslant 0,\ \delta_{i_r}^{(r)}\in\{0,\,1\},\ l_{i_r}^{(r)}\in\{\overline{1,\,n}\},\ j_{i_r}^{(r)}\in\{\overline{0,\,l_{i_r}^{(r)}-2}\},$$
$$\sum_{i=0}^{k^{(r)}}l_i^{(r)}<n,\ i_r=\overline{0,\,k^{(r)}},\ r=1,\,2.$$

Тогда существуют функции $f_1,\,f_2\in M_3^{(n)}$ такие, что

$$\|f_r\|=2^{l_0^{(r)}-1}\prod_{i=1}^{k^{(r)}}(2^{l_i^{(r)}-2}+2^{j_i^{(r)}}+\delta_i^{(r)})+\delta_0^{(r)},\ k^{(r)}\geqslant 1,$$
$$\|f_r\|=2^{l_0^{(r)}-1}+\delta_0^{(r)},\ k^{(r)}=0,$$

$r=1,\,2,$ *и*

$$\chi(f_1,\,f_2)=\sum_{r=1}^{2}\left(2^{l_0^{(r)}-1}\prod_{i=1}^{k^{(r)}}\left(2^{l_i^{(r)}-2}+2^{j_i^{(r)}}+\delta_i^{(r)}\right)+\delta_0^{(r)}\right).$$

5. Расстояние между бент-функциями из класса Майорана — МакФарланда

Всюду ниже $n = 2m$, $m \in \mathbb{N}$. Известно (см., например, [3]), что функция $b(x, y) = \langle x, \pi(y)\rangle + \psi(y)$ является бент-функцией для произвольной подстановки $\pi \in S(V_m)$ и функции $\psi \in F_m$. Обозначим через $B_n^{(1)}$ множество функций вида

$$b_{\pi,\psi}(x, y) = \langle x, \pi(y)\rangle + \psi(y),\ \pi \in S(V_m),\ \psi \in F_m$$

с учетом перестановки координат.

Пусть

$$v_f(g) = \sum_{x \in V_n} (-1)^{g(x)+f(x)} = 2^n - 2\chi(f, g), \quad J(\mu_1, \mu_2) = \{y \in V_m : \mu_1(y) = \mu_2(y)\}.$$

Отметим, если $\mu_1, \mu_2 \in S(V_m)$, то $|J(\mu_1, \mu_2)| = 2^m - \sigma(\mu_1, \mu_2)$, где

$$\sigma(\mu_1, \mu_2) = |\{x \in V_m : \mu_2^{-1}\mu_1(x) \neq x\}|$$

является хорошо известной метрикой на множестве всех подстановок $S(V_m)$. Пусть $V_n^{(0)}$, $V_n^{(1)}$ — векторы четного и нечетного веса из V_n, соответственно, $f^{(\alpha)}(x) = f(\alpha, x)$, $f\colon V_m \to V_m$.

Нетрудно показать, что если $f_i \in F_n$, $f_i(x, y) = \langle x, \mu_i(y)\rangle + \psi_i(y)$, $\mu_i\colon V_{n-t} \to V_t$, $\psi_i\colon V_{n-t} \to \{0, 1\}$, $t \in \{\overline{1, n-1}\}$, $i = 1, 2$, то справедливо равенство

$$v_{f_1}(f_2) = 2^t \sum_{y \in J(\mu_1,\mu_2)} (-1)^{\psi_1(y)+\psi_2(y)}.$$

Отсюда непосредственно следует следующее утверждение.

Утверждение 8. *Для любого $j \in \{\overline{-2^m, 2^m}\}$ существуют функции из класса Майорана — МакФарланда такие, что*

$$\chi(f_1, f_2) = 2^{n-1} - 2^{m-1}j.$$

Следствие 2. *Минимальное расстояние $d_{\min}(B_n^{(1)})$ между бент-функциями из $B_n^{(1)}$ удовлетворяет неравенству*

$$d_{\min}(B_n^{(1)}) \leqslant 2^{m-1}.$$

Выполняется следующее свойство.

Утверждение 9. *Пусть $i \in \{\overline{0, m}\}$, $\pi, \sigma \in S(V_m)$, $\psi_1, \psi_2 \in F_m$, и*

$$f_1(x, y) = \langle x, \pi(y)\rangle + \psi_1(y),$$
$$f_2(x, y) = \langle (x_1, \ldots, x_i, y_{i+1}, \ldots, y_m), \sigma(y_1, \ldots, y_i, x_{i+1}, \ldots, x_m)\rangle + \\ + \psi_2(y_1, \ldots, y_i, x_{i+1}, \ldots, x_m).$$

Тогда справедливо равенство

$$v_{f_1}(f_2) = 2^i \sum_{\alpha \in V_i} \sum_{(\beta,\gamma) \in J^{(i)}_{\pi,\sigma}(\alpha)} (-1)^{\|\beta\|_{\pi_j(\alpha,\beta)} + \|\gamma\|_{\sigma_j(\alpha,\gamma)} + \psi_1(\alpha,\gamma) + \psi_2(\alpha,\beta)},$$

где $J^{(i)}_{\pi,\sigma}(\alpha) = \{(\beta,\, \gamma) \in V_{m-i} \times V_{m-i} : \pi_j(\alpha,\, \gamma) = \sigma_j(\alpha,\, \beta),\ j = \overline{1,\, i}\}$.

Пусть $i \in \{\overline{0,\, m}\}$. Обозначим через $\tilde{B}^{(1,i)}_n(\pi,\, \sigma)$ множество пар функций $(f_1,\, f_2)$, где

$$\begin{aligned} f_1(x,\, y) &= \langle x,\, \pi(y)\rangle + \psi_1(y), \\ f_2(x,\, y) &= \langle (x_1,\, \ldots,\, x_i,\, y_{i+1},\, \ldots,\, y_m),\, \sigma(y_1,\, \ldots,\, y_i,\, x_{i+1},\, \ldots,\, x_m)\rangle + \\ &\quad + \psi_2(y_1,\, \ldots,\, y_i,\, x_{i+1},\, \ldots,\, x_m), \end{aligned}$$

$\pi,\, \sigma \in S(V_m)$, $\psi_1,\, \psi_2 \in F_m$, таких, что $\pi_j = \sigma_j$ и π_j не зависит от координат с номерами $\overline{i+1,\, m}$, $j = \overline{1,\, i}$. Приведем расстояние между функциями из множества $\tilde{B}^{(1,i)}_n(\pi,\, \sigma)$.

Утверждение 10. *Если* $i \in \{\overline{0,\, m}\}$, $\pi,\, \sigma \in S(V_m)$, $(f_1,\, f_2) \in \tilde{B}^{(1,i)}_n(\pi,\, \sigma)$, *то*

$$\chi(f_1,\, f_2) = 2^{2m-1} - 2^{i+1} l,$$

где $l = \sum_{j=1}^{2^i} l_{2j-1} l_{2j}$ *и* $l_j \in \{\overline{-2^{m-i-1},\, 2^{m-i-1}}\}$, $j = \overline{1,\, 2^{i+1}}$.

Литература

[1] *Горшков С. П.* Применение теории NP-полных задач для оценки сложности решения систем булевых уравнений. Обозрение прикладной и промышленной математики. Т. 2, вып. 3.

[2] *Горшков С. П.* О пересечениях классов мультиаффинных, биюнктивных, слабо положительных и слабо отрицательных булевых функций. Обозрение прикладной и промышленной математики, 1997. Т. 4, вып. 2.

[3] *Логачев О. А.*, *Сальников А. А.*, *Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

Неулучшаемая оценка нелинейности функции через значение алгебраической иммунности

М. С. Лобанов

В криптографии хорошо известны потоковые шифры. Изучению подобных схем шифрования и атакам на них посвящено множество работ. Надежность этих шифров во многом определяется свойствами булевых функций, которые используются в этих схемах шифрования в качестве нелинейных фильтров. Эти булевы функции должны удовлетворять целому набору криптографических критериев.

В последнее время в связи с появлением так называемой «алгебраической» атаки на потоковые шифры (см., например, [1, 5]), к булевым функциям, используемым в этих шифрах в качестве нелинейных фильтров, стало наряду с другими предъявляться требование обладания высокой алгебраической иммунностью. Еще одним из наиболее важных криптографических свойств булевых функций, особенно используемых в потоковых шифрах, является нелинейность.

В связи с этим очень интересен вопрос, как связаны нелинейность булевой функции и ее алгебраическая иммунность.

В [2] было доказано утверждение, позволяющее оценивать снизу нелинейность функции через значение ее алгебраической иммунности.

В настоящей работе мы получим более сильную нижнюю оценку нелинейности через значение алгебраической иммунности и построим функции, на которых эта оценка достигается при любых допустимых значениях параметров.

Известно, что булева функция единственным образом представляется полиномом.

Определение 1. Степенью булевой функции называется длина самого длинного слагаемого в ее полиноме (количество переменных в этом слагаемом).

Определение 2. Булева функция g над F_2^n называется аннигилятором булевой функции f над F_2^n, если $fg = 0$.

Очевидно, что аннигиляторы f образуют линейное подпространство в пространстве всех булевых функций от n переменных.

Определение 3. Алгебраической иммунностью $\mathrm{AI}(F)$ булевой функции f над F_2^n называется степень булевой функции g над F_2^n, где g не равная тождественно нулю функция с минимальной степенью, такая что $fg = 0$ или $(f+1)g = 0$.

Известно [1, 5], что для любой f над F_2^n выполнено $\mathrm{AI}(f) \leqslant \lceil \frac{n}{2} \rceil$.

Определение 4. Весом $\mathrm{wt}(x)$ набора x из F_2^n называется число единиц в x.

Определение 5. Расстояние между булевыми функциями f_1 и f_2 определяется как $d(f_1, f_2) = |\{x \in F_2^n \mid f_1(x) \neq f_2(x)\}|$.

Определение 6. Нелинейностью $\mathrm{nl}(f)$ булевой функции f над F_2^n называется $\min_{l:deg(l)\leqslant 1} d(f, l)$.

Определение 7. Для любого набора $u \in F_2^n$ значение

$$W_f(u) = \sum_{x \in F_2^n} (-1)^{f(x)+\langle u,x\rangle}$$

называется коэфициентом Уолша.

Нелинейность выражется через коэфициенты Уолша следующей формулой:

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in F_2^n} |W_f(u)|.$$

В [2] было доказано, что если $\mathrm{nl}(f) < \sum_{i=0}^{d} \binom{n}{i}$, то $\mathrm{AI}(f) \leqslant d+1$. Это эквивалентно нижней оценке нелинейности

$$\mathrm{nl}(f) \geqslant \sum_{i=0}^{\mathrm{AI}(f)-2} \binom{n}{i}.$$

Определение 8. Булева функция $f(x_1, \ldots, x_n)$ называется самодвойственной, если $f(x_1+1, x_2+1, \ldots, x_n+1) = f(x_1, \ldots, x_n) + 1$.

Можно заметить, что если f самодвойственная, то из того,что f не имеет ненулевого аннигилятора степени меньше k, следует, что $f+1$ тоже не имеет ненулевого аннигилятора степени меньше k. Поэтому минимальные степени ненулевых аннигиляторов функций f и $f+1$ совпадают. Таким образом, для нахождения алгебраической иммунности самодвойственной функции f достаточно ограничиться только аннигиляторами функции f.

Лемма 1. *Любой аннигилятор* $g(x_1, \ldots, x_n)$ *функции* $l(x_1, \ldots, x_n)$, $\deg(l) = 1$, *может быть представлен в виде*

$$g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)(l(x_1, \ldots, x_n) + 1),$$

где $\deg(f) = \deg(g) - 1$.

Доказательство. В силу аффинной эквивалентности можно считать, что $l = x_1 + 1$.

Рассмотрим запись $g(x_1, \dots, x_n)$ в виде полинома. В силу того, что аннигиляторы функции образуют линейное пространство, после вычеркивания всех мономов содержащих x_1, должна остаться функция $g_1(x_2, \dots, x_n)$, такая что $g_1 l = g_1(x_1 + 1) = 0$. Так как g_1 не зависит от x_1, то $g_1 = 0$. Следовательно, любой моном g содержит x_1, тогда

$$g(x_1, \dots, x_n) = x_1 f(x_1, \dots, x_n) = (l + 1)f,$$

где $\deg(f) = \deg(g) - 1$. □

Лемма 2. *Пусть $l(x_1, \dots, x_n)$ — булева функция*, $\deg(l) = 1$. *Тогда аннигиляторы функции l степени не больше t образуют линейное пространство размерности* $\sum\limits_{i=0}^{t-1} \binom{n-1}{i}$.

Доказательство. В силу аффинной эквивалентности можно считать, что $l = x_1 + 1$. Пусть $g(x_1, \dots, x_n)$ произвольный аннигилятор функции $l(x_1, \dots, x_n)$, такой что $\deg(g) \leqslant t$. Рассмотрим запись $g(x_1, \dots, x_n)$ в виде полинома. В силу того, что аннигиляторы функции образуют линейное пространство, после вычеркивания всех мономов содержащих x_1, должна остаться функция $g_1(x_2, \dots, x_n)$, такая что $g_1 l = g_1(x_1 + 1) = 0$. Так как g_1 не зависит от x_1, то $g_1 = 0$. Следовательно, любой моном g содержит x_1, тогда

$$g(x_1, \dots, x_n) = x_1 f(x_2, \dots, x_n),$$

где $\deg(f) \leqslant t - 1$.

При этом любая функция $g(x_1, \dots, x_n) = x_1 f(x_2, \dots, x_n)$, где $f(x_2, \dots, x_n)$ произвольная булева функция от $n - 1$ переменной степени не выше $t - 1$, является аннигилятором l степени не выше t. Из этого следует утверждение леммы. □

Замечание. Доказательство следующего утверждения можно найти в [4], но мы решили привести его в нашей работе ввиду его простоты.

Лемма 3. *Если f булева функция над F_2^n и* $\mathrm{AI}(f) > k$, *тогда*

$$\sum_{i=0}^{k} \binom{n}{i} \leqslant \mathrm{wt}(f) \leqslant \sum_{i=0}^{n-k-1} \binom{n}{i}.$$

Доказательство. Ищем аннигилятор функции f методом неопределенных коэффициентов:

$$g = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j + \dots + \sum_{1 \leqslant i_1 \leqslant \dots \leqslant i_k \leqslant n} a_{i_1 \dots i_k} x_{i_1} \dots x_{i_k}, \quad \deg(g) \leqslant k.$$

Функция g является аннигилятором f тогда и только тогда, когда $f(x) = 1$ влечет $g(x) = 0$. Тогда, для того чтобы $\mathrm{AI}(f) > k$, необходимо , чтобы получившаяся однородная система линейных уравнений на $a_0, a_1, a_2, \ldots$ имела бы только нулевое решение. Для этого необходимо, чтобы число неизвестных не превышало бы числа уравнений. Количество уравнений равно $\mathrm{wt}(f)$, а количество неизвестных $\sum\limits_{i=0}^{k} \binom{n}{i}$. Следовательно, левое неравенство доказано. Применяя такие же рассуждения к $f + 1$, получаем правое неравенство. □

Теорема 1. *Пусть $f(x_1, \ldots, x_n)$ булева функция над F_2^n и $\mathrm{AI}(f) = k$, тогда*

$$\mathrm{nl}(f) \geqslant 2^{n-1} - \sum_{i=k-1}^{n-k} \binom{n-1}{i} = 2\sum_{i=0}^{k-2} \binom{n-1}{i}. \tag{1}$$

Доказательство. Представим нелинейность функции f в виде $\mathrm{nl}(f) = 2^{n-1} - \frac{\alpha}{2}$, где $\alpha = \max_{u \in F_2^n} |W_f(u)|$.

Если $\max\limits_{u \in F_2^n} |W_f(u)|$ достигается на нулевом наборе, тогда или f, или $f + 1$ имеет вес $\frac{2^n - \alpha}{2}$. Тогда в соответствии с леммой 3 имеем

$$\frac{2^n - \alpha}{2} \geqslant \sum_{i=0}^{k-1} \binom{n}{i}.$$

Следовательно, $\alpha \leqslant \sum\limits_{i=k}^{n-k} \binom{n}{i} \leqslant 2 \sum\limits_{i=k-1}^{n-k} \binom{n-1}{i}$. Отсюда получаем соответствующую оценку на нелинейность.

Если $\max_{u \in F_2^n} |W_f(u)|$ не достигается на нулевом наборе, тогда существует функция $l(x_1, \ldots, x_n)$, $\deg(l) = 1$, такая что $d(f, l) = \frac{2^n - \alpha}{2}$. Функции f и l совпадают на $\frac{2^n + \alpha}{2}$ наборах.

Заметим, что

$$2^{n-1} - \frac{\alpha}{2} = d(f, l) = \mathrm{wt}((f+1)l) + \mathrm{wt}(f(l+1)).$$

Отсюда

$$\min\{\mathrm{wt}((f+1)l), \mathrm{wt}(f(l+1))\} \leqslant \frac{1}{2}\left(2^{n-1} - \frac{\alpha}{2}\right) = 2^{n-2} - \frac{\alpha}{4}.$$

Если $\mathrm{wt}(f(l+1)) < \mathrm{wt}((f+1)l)$, то определим $f_1 = f$, $l_1 = l + 1$, иначе определим $f_1 = f + 1$, $l_1 = l$.

Введем функцию $f_2 = f_1 l_1$. Тогда $\mathrm{wt}(f_2) \leqslant 2^{n-2} - \frac{\alpha}{4}$.

Ищем аннигиляторы g функции f_2 степени не выше $k-2$ методом неопределенных коэффициентов:

$$g = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j + \dots + \sum_{1 \leqslant i_1 \leqslant \dots \leqslant i_{k-2} \leqslant n} a_{i_1 \dots i_{k-2}} x_{i_1} \dots x_{i_{k-2}}.$$

Функция g является аннигилятором f тогда и только тогда, когда $f(x) = 1$ влечет $g(x) = 0$.

Следовательно, получаем однородную систему из не более чем $2^{n-2} - \frac{\alpha}{4}$ линейных уравнений на $\sum\limits_{i=0}^{k-2} \binom{n}{i}$ неизвестных. Пространство решений системы имеет размерность не менее $\sum\limits_{i=0}^{k-2} \binom{n}{i} - \left(2^{n-2} - \frac{\alpha}{4}\right)$.

В соответствии с леммой 2 размерность пространства аннигиляторов функции l_1 степени не выше $k-2$ равна $\sum\limits_{i=0}^{k-3} \binom{n-1}{i}$.

Если

$$\sum_{i=0}^{k-2} \binom{n}{i} - \left(2^{n-2} - \frac{\alpha}{4}\right) > \sum_{i=0}^{k-3} \binom{n-1}{i},$$

то найдется функция f_3, $\deg(f_3) \leqslant k-2$, такая что $f_2 f_3 = 0$, но $f_3 l_1 \neq 0$, тогда $f_3 l_1$ будет аннигилятором f_1, при этом $\deg(f_3 l_1) \leqslant k-1$, что противоречит $\mathrm{AI}(f) = k$.

Отсюда

$$\sum_{i=0}^{k-2} \binom{n}{i} - (2^{n-2} - \frac{\alpha}{4}) \leqslant \sum_{i=0}^{k-3} \binom{n-1}{i},$$

$$\frac{\alpha}{4} \leqslant 2^{n-2} - \frac{1}{2} \sum_{i=k-2}^{n-k+1} \binom{n-1}{i} + 2^{n-2} - \left(2^{n-1} - \frac{1}{2} \sum_{i=k-1}^{n-k+1} \binom{n}{i}\right),$$

$$\frac{\alpha}{4} \leqslant \frac{1}{2}\left(\sum_{i=k-1}^{n-k+1} \left(\binom{n-1}{i} + \binom{n-1}{i-1}\right) - \sum_{i=k-2}^{n-k+1} \binom{n-1}{i}\right) = \frac{1}{2} \sum_{i=k-1}^{n-k} \binom{n-1}{i}.$$

Следовательно, $\mathrm{nl}(f) \geqslant 2^{n-1} - \sum\limits_{i=k-1}^{n-k} \binom{n-1}{i}$. □

Следствие 1. *Если n нечетно и* $\mathrm{AI}(f(x_1, \dots, x_n)) = \left\lceil \frac{n}{2} \right\rceil$, *то*

$$\mathrm{nl}(f) \geqslant 2^{n-1} - \binom{n-1}{\frac{n-1}{2}}. \tag{2}$$

Заметим, что в [4] была построена функция от нечетного числа переменных n с алгебраической иммунностью $\left\lceil \frac{n}{2} \right\rceil$ и нелинейностью $\mathrm{nl}(f) = 2^{n-1} - \binom{n-1}{\frac{n-1}{2}}$. Из нашего следствия 1 видно, что эта функция достигает границы (2), т. е. среди всех функций с максимально возможной алгебраической иммунностью является функцией с наихудшей возможной нелинейностью. Подсчет ее нелинейности в статье довольно труден и занимает много места. Теперь же нижняя оценка нелинейности функции из [4] сразу следует из нашего следствия 1. Верхняя же оценка нелинейности функции из [4] будет следовать из нашей теоремы 2, потому что эта функция является частным случаем наших функций $f_{n,k}$, возникающих в доказательстве теоремы 2. Заметим также, что в [3] для построенной там функции f с нечетным числом переменных n и алгебраической иммунностью $\left\lceil \frac{n}{2} \right\rceil$ доказана нижняя оценка нелинейности $\mathrm{nl}(f) \geqslant 2^{n-1} - \binom{n-1}{\frac{n-1}{2}}$, которая, таким образом, совпадает с нашей оценкой из следствия 1 для всех функций с таким числом переменных и такой алгебраической иммунностью.

Следствие 2. *Если n четно и* $\mathrm{AI}(f(x_1, \ldots, x_n)) = \left\lceil \frac{n}{2} \right\rceil$, *то*

$$\mathrm{nl}(f) \geqslant 2^{n-1} - \binom{n}{\frac{n}{2}}.$$

Заметим, что в [4] оценка следствия 2 была доказана для очень узкого класса функций.

Теорема 2. *Оценка* (1) *из теоремы* 1 *неулучшаема для любого n и любого $k \leqslant \lceil \frac{n}{2} \rceil$. Более того, при любых допустимых параметрах существует уравновешенная функция, достигающая эту границу.*

Доказательство. Покажем, что оценка (1) из теоремы 1 неулучшаема, предъявив для любого n и любого $k \leqslant \left\lceil \frac{n}{2} \right\rceil$ функцию $f(x_1, \ldots, x_n)$, такую что $\mathrm{AI}(f) = k$ и $\mathrm{nl}(f) = 2^{n-1} - \sum\limits_{i=k-1}^{n-k} \binom{n-1}{i}$.

Определим функцию $f_{n,k}$ следующим образом:

$$f_{n,k}(x_1, \ldots, x_n) = \begin{cases} 0, & \text{если } \mathrm{wt}(x_1, \ldots, x_n) n-k; \\ x_1, & \text{если } k \leqslant \mathrm{wt}(x_1, \ldots, x_n) \leqslant n-k. \end{cases}$$

Теперь докажем, что для любого n и любого $k \leqslant \left\lceil \frac{n}{2} \right\rceil$ выполнено

$$\mathrm{AI}(f_{n,k}) = k, \quad \mathrm{nl}(f_{n,k}) = 2^{n-1} - \sum_{i=k-1}^{n-k} \binom{n-1}{i}.$$

Несложно заметить, что $f(x_1+1,\, x_2+1,\, \ldots,\, x_n+1) = f(x_1,\, \ldots,\, x_n)+1$, т. е. $f_{n,k}$ — самодвойственная. Следовательно, функция $f_{n,k}$ является уравновешенной функцией.

В силу самодвойственности $f_{n,k}$, чтобы доказать $\mathrm{AI}(f) \geqslant k$, достаточно доказать, что $f_{n,k}+1$ не имеет ненулевого аннигилятора степени меньше k.

Запишем возможный аннигилятор функции $f+1$ степени не выше $k-1$ с помощью неопределенных коэффициентов:

$$g = a_0 + \sum_{i=1}^{n} a_i x_i + \sum_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j + \cdots + \sum_{1 \leqslant i_1 \leqslant \ldots \leqslant i_{k-1} \leqslant n} a_{i_1 \ldots i_{k-1}} x_{i_1} \ldots x_{i_{k-1}}.$$

Функция g является аннигилятором $f_{n,k}+1$ тогда и только тогда, когда $f(x)+1=1$ влечет $g(x)=0$. Получаем систему линейных уравнений на коэффициенты функции g:

$$g(x_1,\, \ldots,\, x_n) = 0$$

для всех наборов x, таких что $\mathrm{wt}(x) \leqslant k-1$.

Так как $g(0,\, \ldots,\, 0)=0$, то $a_0=0$. Так как $g(x)=0$, если $\mathrm{wt}(x)=1$, то получаем, что $a_i = a_0 = 0$. Используя индукцию по весу наборов, мы получаем, что все коэффициенты g равны нулю, следовательно, $g \equiv 0$. Получаем, что $\mathrm{AI}(f_{n,k}) \geqslant k$.

Вычислим коэффициент Уолша функции $f_{n,k}$, соответствующий набору $(1,\, 0,\, \ldots,\, 0)$, используя самодвойственность $f_{n,k}$:

$$W_{f_{n,k}}(1,\, 0,\, \ldots,\, 0) = \sum_{(x_1,\ldots,x_n) \in F_2^n} (-1)^{f_{n,k}(x_1,\ldots,x_n)+x_1} =$$

$$= 2^n - 2\,\mathrm{wt}(f_{n,k}(x_1,\, \ldots,\, x_n) + x_1) =$$

$$= 2^n - 2(\mathrm{wt}(f_{n,k}(0,\, x_2,\, \ldots,\, x_n)) + \mathrm{wt}(f_{n,k}(1,\, x_2 \ldots,\, x_n)+1)) =$$

$$= 2^n - 4\,\mathrm{wt}(f_{n,k}(0,\, x_2,\, \ldots,\, x_n)) = 2^n - 4 \sum_{i=n-k+1}^{n-1} \binom{n-1}{i} = 2 \sum_{i=k-1}^{n-k} \binom{n-1}{i}.$$

Следовательно, $\mathrm{nl}(f_{n,k}) \leqslant 2^{n-1} - \sum\limits_{i=k-1}^{n-k} \binom{n-1}{i}$. Тогда из теоремы 1 следует, что $\mathrm{AI}(f_{n,k}) \leqslant k$, поэтому $\mathrm{AI}(f_{n,k}) = k$, следовательно,

$$\mathrm{nl}(f_{n,k}) \geqslant 2^{n-1} - \sum_{i=k-1}^{n-k} \binom{n-1}{i},$$

отсюда $\mathrm{nl}(f_{n,k}) = 2^{n-1} - \sum\limits_{i=k-1}^{n-k} \binom{n-1}{i}$. $\square$

Автор выражает глубокую благодарность Ю. В. Таранникову за постановку задачи, внимание к работе и ценные советы.

Литература

[1] *Courtois N.*, *Meier W.* Algebraic attacks on stream ciphers with linear feedback. Proc. EUROCRYPT 2003, v. 2656 in Lecture Notes in Computer Science, p. 345-359. Springer-Verlag, 2003.

[2] *Dalai D. K.*, *Gupta K. C.*, *Maitra S.* Results on algebraic immunity for cryptographically significant Boolean functions. Proc. Indocrypt 2004, Chennai, India, December 20–22, p. 92–106, v. 3348 in Lecture Notes in Computer Science, Springer-Verlag, 2004.

[3] *Dalai D. K.*, *Gupta K. C.*, *Maitra S.* Cryptographically significant Boolean functions: constraction and analysis in terms of algebraic immunity. Proc. FSE 2005. To be published in Lecture Notes in Computer Science, Springer-Verlag.

[4] *Dalai D. K.*, *Maitra S.*, *Sarkar S.* Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Cryptology ePrint archive (http://eprint.iacr.org/), Report 2005/229.

[5] *Meier W.*, *Pasalic E.*, *Carlet C.* Algebraic attacks and decomposition of Boolean functions. Proc. EUROCRYPT 2004, v. 3027 in Lecture Notes in Computer Science, p. 474–491. Springer-Verlag, 2004.

Гомоморфизмы регистров сдвига в линейные автоматы

В. И. Солодовников

Аннотация

Доклад посвящен описанию всех гомоморфизмов регистров сдвига над конечными полями с подстановочной по входной переменной функцией обратной связи в линейные автоматы.

Прежде всего, показывается, что гомоморфный образ регистра сдвига в линейном автомате всегда изоморфен линейному регистру сдвига. Тем самым, по ранее полученной автором теореме, вопрос о гомоморфизмах регистров сдвига в линейные автоматы сводится к вопросу о разложении функции (или представляющего ее многочлена) в так называемую сдвиг-композицию двух функций (многочленов), в котором левая функция — аффинная.

Далее устанавливается, что всякий многочлен однозначно представляется в виде суммы сдвиг-композиций линейных многочленов и одночленов с первой переменной. Этим линейным многочленам ставятся в соответствие многочлены от одной переменной и вопрос о разложении сводится к поиску общих делителей последних.

Наконец, указываются некоторые простые условия, достаточные для отсутствия нетривиальных внутренних гомоморфизмов регистра сдвига в линейные автоматы.

Гомоморфизмы являются неотъемлемой частью любой категории, в том числе и категории автоматов. Традиционный для теории автоматов интерес представляют автоматы, называемые регистрами сдвига. Это автоматы, вырабатывающие управляемые (то есть в общем случае зависящие от входа) усложненные (некоторой выходной функцией) рекуррентные последовательности. В [1] доказано, что всякий гомоморфизм двоичного регистра сдвига с линейной по входной переменной функцией обратной связи разлагается в композицию гомоморфизма на регистр и некоторого гомоморфизма, близкого к изоморфизму. При описании этого разложения основную роль играет некая бинарная некоммутативная операция на функциях (называемая здесь сдвиг-композицией). Она в некотором смысле распространяет операцию умножения многочленов от одной переменной на множество

всех функций. Вопрос о гомоморфизмах регистра сводится к вопросу о поиске общих правых делителей его функции обратной связи и выходной функции.

Доклад посвящен описанию всех гомоморфизмов регистров сдвига над конечными полями с подстановочной по входной переменной функцией обратной связи в линейные автоматы.

Используются следующие обозначения и терминология.

X — произвольное конечное множество, $F_{n+1}(X) = \{f \mid f\colon X^{n+1} \to X\}$ — множество всех X-значных функций от $n+1$ переменных, $n \geqslant 0$, $F(X) = \bigcup\limits_{n=0}^{\infty} F_{n+1}(X)$.

Функцию $f \in F_{n+1}()$ называют *подстановочной* (*биективной*) *по i-й переменной*, если при любой фиксации всех остальных переменных получаемое отображение $X \to X$ является биекцией. В случае подстановочности *по последней* (то есть $(n+1)$-й) переменной, через f^{-1} будем обозначать функцию, *обратную к функции f по последней переменной*, то есть $f^{-1} \in F_{n+1}(X)$ и $f^{-1}(x_1, \ldots, x_n, f(x_1, \ldots, x_{n+1})) = x_{n+1}$. В двоичном случае подстановочность по какой-либо переменной равносильна линейности по этой переменной.

$F^*_{n+1}(X)$ — множество всех подстановочных по последней переменной функций из $F_{n+1}(X)$, $F^*(X) = \bigcup\limits_{n=0}^{\infty} F^*_{n+1}(X)$.

$P = \mathrm{GF}(q)$ — конечное поле из q элементов, $P[x]$ — кольцо многочленов над P от одной переменной x, $d(\varphi)$ — степень многочлена φ.

$M(P)$ — множество всех *многочленов над P от переменных* $\{x_i \mid i \geqslant 1\}$ *с ограниченными степенями*, то есть формул вида

$$g = \sum_{\substack{0 \leqslant k,\\ 1 \leqslant i_1 \prec \ldots \prec i_k,\\ 1 \leqslant s_j \leqslant q-1}} a_{i_1,\ldots,i_k;s_1,\ldots,s_k} x_{i_1}^{s_1} \ldots x_{i_k}^{s_k},$$

где $a_{i_1,\ldots,i_k;s_1,\ldots,s_k} \in P$ называют коэффициентом при *одночлене* $x_{i_1}^{s_1} \ldots x_{i_k}^{s_k}$ степени $\sum\limits_{j=1}^{k} s_j$ и только конечное число коэффициентов отлично от нуля. Говорят, что одночлен *входит* в g, если коэффициент при нем ненулевой. Максимальная степень входящих в ненулевой многочлен g одночленов называется степенью g и обозначается через $d(g)$. одночлена назовем число

$$/x_{i_1}^{s_1} \ldots x_{i_k}^{s_k}/ = \sum_{j=1}^{k} s_j q^{i_j - 1}.$$

Каждый одночлен однозначно определяется своим номером. Хорошо известно, что любая функция из $F(P)$ однозначно представляется некоторым многочленом из $M(P)$. В случаях, когда число переменных функции определено, будем, при необходимости, отождествлять эту функцию с представляющим ее многочленом.

Автоматом с входным алфавитом X, множеством состояний S, выходным алфавитом Y, функцией переходов $\delta\colon S \times X \to S$ и функцией выходов $\lambda\colon S \times X \to Y$ называют пятерку объектов $A = (X, S, Y, \delta, \lambda)$. При этом подразумевается, что если автомат A находится в состоянии $s \in S$ и на его вход подается входной символ $x \in X$, то на его выходе появляется выходной символ $\lambda(s, x)$ и автомат переходит в состояние $\delta(s, x)$.

Для отображений ψ и φ через $\psi\varphi$ обозначается их композиция, при которой φ действует первым. Аналогично, для автоматов A и B через AB обозначается их последовательное соединение, при котором выход с автомата B подается на вход автомата A.

Гомоморфизмом автомата $A' = (X', S', Y', \delta', \lambda')$ в автомат $A = (X, S, Y, \delta, \lambda)$ называется тройка отображений (α, β, γ), $\alpha\colon X' \to X$, $\beta\colon S' \to S$, $\gamma\colon Y' \to Y$, удовлетворяющих условиям $\beta\delta' = \delta(\beta \times \alpha)$, $\gamma\lambda' = \lambda(\beta \times \alpha)$. Этот факт обозначают следующим образом: $(\alpha, \beta, \gamma)\colon A' \to A$. Если α и γ — тождественные вложения, то гомоморфизм называется *внутренним* и обозначается: $\beta\colon A' \to A$.

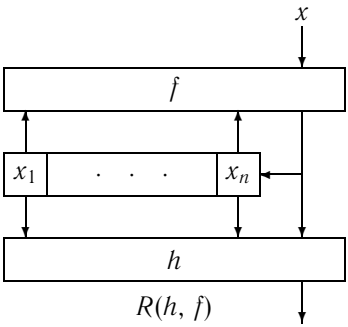
Любой гомоморфизм $(\alpha, \beta, \gamma)\colon A' \to A$ сводится к внутреннему гомоморфизму $\beta\colon \gamma A' \to A\alpha$, а в случае биективности α и к внутреннему гомоморфизму $\beta\colon \gamma A'\alpha^{-1} \to A$. Поэтому часто достаточно рассматривать только внутренние гомоморфизмы.

Гомоморфизм (α, β) автоматов без выхода назовем тривиальным, если $|\beta(S')| = 1$.

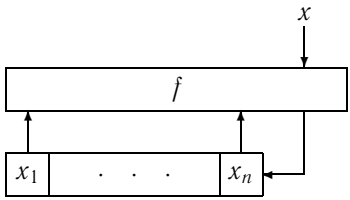
Регистром сдвига над множеством X длины n с функцией обратной связи f и выходной функцией h, где $f, h \in F_{n+1}(X)$, называется автомат $R(h, f) = (X, X^n, X, \rho, \mu)$, у которого функция переходов ρ и функция выходов μ определяются равенствами

$$\rho((x_1, \ldots, x_n), x) = (x_2, \ldots, x_n, f(x_1, \ldots, x_n, x)),$$
$$\mu((x_1, \ldots, x_n), x) = h(x_1, \ldots, x_n, f(x_1, \ldots, x_n, x))$$

для любых $x_1, \ldots, x_n, x \in X$. Регистр сдвига без выхода с функцией обратной связи f обозначается через $R(f)$. Эти автоматы изображаются следующим образом:



$R(h, f)$



$R(f)$

Для любых $f_i \in F_{n_i+1}(X)$, $i = 1, 2$ функция

$$f_2 \triangleleft f_1 \in F_{n_1+n_2+1}(X)$$

и отображение

$$\pi_{f_1,n_2} \colon X^{n_1+n_2} \to X^{n_2}$$

определяются равенствами

$$\begin{aligned} &f_2 \triangleleft f_1(x_1, \ldots, x_{n_1+n_2+1}) = \\ &\qquad = f_2(f_1(x_1, \ldots, x_{n_1+1}), f_1(x_2, \ldots, x_{n_1+2}), f_1(x_{n_2+1}, \ldots, x_{n_1+n_2+1})), \\ &\pi_{f_1,n_2}(x_1, \ldots, x_{n_1+n_2}) = \\ &\qquad = (f_1(x_1, \ldots, x_{n_1+1}), f_1(x_2, \ldots, x_{n_1+2}), f_1(x_{n_2}, \ldots, x_{n_1+n_2})) \end{aligned}$$

для любых $x_1, \ldots, x_{n_1+n_2+1} \in X$, так что

$$f_2 \triangleleft f_1 = f_2 \pi_{f_1,n_2+1}.$$

Операцию $\triangleleft$ назовем *сдвиг-композицией* функций.

Множество $F(X)$ относительно операции $\triangleleft$ является моноидом с единичным элементом $\boldsymbol{x}_1 \in F_1(X)$, а множество $F^*(X)$ — его подмоноидом. Операция $\triangleleft$ является продолжением на множество всех функций операции умножения многочленов в следующем смысле. Обозначим через $P[x]^*$ моноид (относительно умножения) всех ненулевых многочленов над полем P. Тогда отображение $w \colon P[x]^* \to F^*(P)$, где

$$w(c_0 + c_1 x + \ldots + c_n x^n) = c_0 x_1 + c_1 x_2 + \ldots c_n x_{n+1},$$

является инъективным гоморфизмом моноидов.

Следующая теорема сводит описание всех гомоморфизмов регистра на регистр с подстановочными по входной переменной функциями обратной связи к описанию разложений функций в сдвиг-композицию (см. [1]).

Теорема 1. *Пусть* $n, n_2 \geqslant 0$, $f \in F^*_{n+1}(X)$, $f_2 \in F^*_{n_2+1}(X)$, $h \in F_{n+1}(X)$, $h_2 \in F_{n_2+1}(X)$, $\beta\colon X^n \to X^{n_2}$. *Тогда следующие утверждения равносильны*:

1) $\beta\colon R(h, f^{-1}) \to R(h_2, f_2)$ — *внутренний гомоморфизм*;

2) $n \geqslant n_2$, $\beta = \pi_{f_1, n_2}$, $f = f_2 \lhd f_1$, $h = h_2 \lhd f_1$ *для некоторой функции* $f_1 \in F^*_{n_1+1}(X)$, *где* $n_1 = n - n_2$.

Далее для простоты будут рассматриваться только автоматы без выхода. Соответствующие результаты для автоматов с выходом легко получить воспользовавшись теоремой 1.

Всюду далее $X = P$ — конечное поле.

Линейным автоматом над P *длины* m *с одномерным входом без выхода* назовем автомат (P, P^m, δ), у которого функция переходов δ определяется равенством

$$\delta(s, x) = sQ + xb + b_0$$

для всех $s \in P^m$, $x \in P$, где Q — $m \times m$-матрица над P, $b, b_0 \in {}^m$.

Линейным регистром сдвига над P *длины* n *без выхода* называют регистр $R(f)$, у которого функция $f \in F_{n+1}(P)$ представляется в виде

$$f(x_1, \ldots, x_{n+1}) = a_0 + \sum_{i=1}^{n} a_i x_i + x_{n+1}.$$

Такие функции (многочлены) будем называть *унитарными* аффинными функциями (многочленами).

Подавтомат называют *внутренним*, если его входной алфавит не сокращен.

Теорема 2. *Для любого автомата* A, *являющегося внутренним подавтоматом линейного автомата над полем* P *с одномерным входом без выхода следующие утверждения равносильны*:

1) A *является гомоморфным образом некоторого регистра сдвига над* P *без выхода с подстановочной по последней* (*то есть входной*) *переменной функцией обратной связи*;

2) A *аффинно внутренне изоморфен некоторому линейному регистру сдвига над* P *без выхода*;

3) *любое состояние* A *достижимо из некоторого состояния* A, *не меняющегося при некотором входном знаке*.

Теорема 3. *Пусть* $n \geqslant 0$, $f \in F^*_{n+1}(P)$, α — *подстановка множества* P.

1. *Если* B — *линейный автомат над полем* P *с одномерным входом без выхода и* $(\alpha, \beta)\colon R(f^{-1}) \to B$ — *гомоморфизм, то существуют функции* $f_1 \in F^*_{n_1+1}(P)$, $f_2 \in F^*_{n_2+1}(P)$, *где* $n_1 + n_2 = n$, *и инъектив-*

ный внутренний аффинный гомоморфизм $\beta'\colon R(f_2^{-1}) \to B$ *такие, что* $f = \alpha^{-1} f_2 \lhd f_1$, f_2 *— унитарная аффинная функция и* $\beta = \beta' \pi_{f_1, n_2}$.

2. *Если* $f = \alpha^{-1} f_2 \lhd f_1$, *где* $f_1 \in F^*_{n_1+1}(P)$, $f_2 \in F^*_{n_2+1}(P)$, $n_1 + n_2 = n$, f_2 *— унитарная аффинная функция, то* $(\alpha, \pi_{f_1, n_2})\colon R(f^{-1}) \to R(f_2^{-1})$ *— гомоморфизм на линейный регистр сдвига.*

Теорема 3 сводит задачу об описании всех гомоморфизмов (α, β) регистра сдвига $R(f^{-1})$ в линейные автоматы (где α — подстановка) к задаче о нахождении всех разложений функции αf в сдвиг-композицию двух функций, в которых левая функция — аффинная. Оставшаяся часть доклада посвящена решению этой задачи.

Здесь целесообразно перейти с языка функций на язык представляющих их многочленов из $M(P)$.

Операцию $\lhd$ *на* $M(P)$ (*сдвиг-композицию многочленов*) определим следующим образом: $g_2 \lhd g_1$ — многочлен функции $f_2 \lhd f_1$, где g_i — многочлен функции f_i, $i = 1, 2$.

Множество $M(P)$ относительно операций $+$ и $\cdot$ является коммутативным кольцом, а относительно операции $\lhd$ — моноидом с единицей $\boldsymbol{x}_1$. Отображение $F(P) \to M(P)$, ставящее в соответствие каждой функции представляющий ее многочлен является сюръективным гомоморфизмом моноидов относительно операции $\lhd$.

Обозначим через $L(P)$ множество всех линейных многочленов из $M(P)$, то есть многочленов вида $a_1 x_1 + \ldots a_n x_n$. Оно является коммутативным кольцом с единицей $\boldsymbol{x}_1$ относительно операций $+$ и $\lhd$, изоморфным кольцу $P[x]$: изоморфизм $v\colon P[x] \to L(P)$ определяется равенством

$$v(c_0 + c_1 x + \ldots + c_n x^n) = c_0 x_1 + c_1 x_2 + \ldots + c_n x_{n+1}.$$

Множество $M(P)$ является абелевой группой относительно сложения. Определим умножение слева многочленов из кольца $P[x]$ на многочлены из $M(P)$ равенством

$$\varphi g = v(\varphi) \lhd g.$$

Тогда $M(P)$ — левый $P[x]$-модуль.

Пусть $M_0(P) = P \subset M(P)$, а $M_1(P)$ — множество всех многочленов из $M(P)$ с нулевым свободным членом, и пусть $E(P)$ — *множество всех одночленов с первой переменной*, то есть

$$E(P)\{x_1^{s_1} x_{i_2}^{s_2} \ldots x_{i_k}^{s_k} \mid 1 \leqslant k,\ 1 < i_2 < \ldots < i_k,\ 1 \leqslant s_j \leqslant q-1\} \subset M(P).$$

Теорема 4. $M(P) = M_0(P) + M_1(P)$ *— прямая сумма подмодулей* $P[x]$*-модуля* $M(P)$, *и* $M_1(P)$ *— свободный* $P[x]$*-модуль с базисом* $E(P)$.

Эта теорема означает следующее: *любой многочлен* $g \in M(P)$ *однозначно представляется в виде*

$$g = a_0 + \sum_{\substack{1 \leqslant k,\\ 1 \prec i_2 \prec \ldots \prec i_k,\\ 1 \leqslant s_j \leqslant q-1}} l_{i_2,\ldots,i_k;s_1,\ldots,s_k} \lhd x_1^{s_1} x_{i_2}^{s_2} \ldots x_{i_k}^{s_k}, \tag{1}$$

где $a_0 \in P$, $l_{i_2,\ldots,i_k;s_1,\ldots,s_k} \in L(P)$. Это представление назовем *разложением многочлена по одночленам с первой переменной*. Его легко получить, используя формулу

$$x_{i_1}^{s_1} x_{i_2}^{s_2} \ldots x_{i_k}^{s_k} = x_{i_1} \lhd x_1^{s_1} x_{i_2-i_1+1}^{s_2} \ldots x_{i_k-i_1+1}^{s_k} = x^{i_1-1}\left(x_1^{s_1} x_{i_2-i_1+1}^{s_2} \ldots x_{i_k-i_1+1}^{s_k}\right). \tag{2}$$

В качестве следствия из теоремы 4 сразу получаем следующую теорему.

Теорема 5 (об аффинных левых делителях). *Пусть* $g, g_1, g_2 \in M(P)$ *и разложения этих многочленов по одночленам с первой переменной имеют следующий вид*:

$$g = a_0 + \sum_{\substack{1 \leqslant k,\\ 1 \prec i_2 \prec \ldots \prec i_k,\\ 1 \leqslant s_j \leqslant q-1}} l_{i_2,\ldots,i_k;s_1,\ldots,s_k} \lhd x_1^{s_1} x_{i_2}^{s_2} \ldots x_{i_k}^{s_k},$$

$$g_1 = a_0' + \sum_{\substack{1 \leqslant k,\\ 1 \prec i_2 \prec \ldots \prec i_k,\\ 1 \leqslant s_j \leqslant q-1}} l'_{i_2,\ldots,i_k;s_1,\ldots,s_k} \lhd x_1^{s_1} x_{i_2}^{s_2} \ldots x_{i_k}^{s_k},$$

$$g_2 = a_0'' + l,$$

где $l \in L(P)$. *Тогда следующие утверждения равносильны*:

1) $g = g_2 \lhd g_1$;

2) $l_{i_2,\ldots,i_k;s_1,\ldots,s_k} = l \lhd l'_{i_2,\ldots,i_k;s_1,\ldots,s_k}$ *для всех* $1 \leqslant k$, $1 < i_2 < \ldots < i_k$, $1 \leqslant s_j \leqslant q-1$ *и* $a_0 = a_0'' + l(a_0', \ldots, a_0')$;

3) $v^{-1}(l_{i_2,\ldots,i_k;s_1,\ldots,s_k}) = v^{-1}(l)v^{-1}(l'_{i_2,\ldots,i_k;s_1,\ldots,s_k})$ *для всех* $1 \leqslant k$, $1 < i_2 < \ldots < i_k$, $1 \leqslant s_j \leqslant q-1$ *и* $a_0 = a_0'' + l(a_0', \ldots, a_0')$.

Утверждение 3 этой теоремы сводит задачу об описании всех *разложений* $g = g_2 \lhd g_1$ *с аффинным многочленом* g_2 *к задаче об описании всех общих делителей многочленов* $v^{-1}(l_{i_2,\ldots,i_k;s_1,\ldots,s_k}) \in P[x]$.

Если $g = g_2 \lhd g_1$, $g_2 = a + a_i x_i$, $1 \leqslant i$, a, $a_i \in P$, то g_2 назовем *тривиальным левым делителем* многочлена g.

Для любого ненулевого многочлена $g \in M(P)$ *через* $d'(g)$ *обозначим максимальное число переменных во входящих в* g *одночленах*. Для двоичного случая $d'(g) = d(g)$.

Следствие 1. *Пусть* $g \in M(P)$, $g(g) \geqslant 2$ *и выполнено хотя бы одно из следующих условий*:

1) *для некоторого* $s \geqslant 1$ *в* g *входит только один одночлен степени* s;

2) *для некоторого* $k_0 \geqslant 1$ *в* g *входит только один одночлен с числом переменных* k_0;

3) *для некоторого* r, *некратного* q, *в* g *входит только один одночлен с номером вида* $q^t r$;

4)

$$g = \sum_{\substack{0 \leqslant k, \\ 1 \leqslant i_1 \prec \ldots \prec i_k \leqslant n+1, \\ 1 \leqslant s_j \leqslant q-1}} a_{i_1,\ldots,i_k;s_1,\ldots,s_k} x_{i_1}^{s_1} \ldots x_{i_k}^{s_k},$$

$a_{n+1;1} \leqslant 0$, $d'(g) \leqslant 2$ *и многочлен* $\sum\limits_{i=1}^{n+1} a_{i;1} x^{i-1}$ *неприводим.*

Тогда g *не имеет нетривиальных аффинных левых делителей.*

Следствие 2. *Пусть* $f \in F^*_{n+1}(P)$, f *существенно зависит от* 1*-й переменной и для представляющего функцию* f^{-1} *многочлена* g *выполнено условие следствия* 3. *Тогда регистр* $R(f)$ *не имеет нетривиальных внутренних гомоморфизмов в линейные автоматы над полем* P *с одномерным входом без выхода.*

Для двоичного случая следствие 2 приобретает следующий более простой вид.

Следствие 3. *Пусть* $P = \mathrm{GF}(2)$, $f \in F^*_{n+1}(P)$, f *существенно зависит от* 1*-й переменной*,

$$g = \sum_{\substack{0 \leqslant k, \\ 1 \leqslant i_1 \prec \ldots \prec i_k \leqslant n+1}} a_{i_1,\ldots,i_k} x_{i_1} \ldots x_{i_k}$$

— представляющий функцию f *многочлен*, $d(g) \geqslant 2$ *и выполнено хотя бы одно из следующих условий*:

1) *для некоторого* $s \geqslant 1$ *в* g *входит только один одночлен степени* s;

2) *для некоторого нечетного* r *в* g *входит только один одночлен с номером вида* $2^t r$;

3) *многочлен* $\sum\limits_{i=1}^{n+1} a_i x^{i-1}$ *неприводим.*

Тогда регистр $R(f)$ *не имеет нетривиальных гомоморфизмов в линейные автоматы над полем* P *с одномерным входом без выхода.*

Пример (двоичный случай). Опишем все гомоморфизмы регистра $R(f)$ на линейные регистры для функции $f \in F^*_{n+1}(\mathrm{GF}(2))$, где $n = 8$ и f представляется многочленом

$$g = x_1 \oplus x_2 \oplus x_3 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_2x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_6 \oplus x_4x_7 \oplus x_5x_8.$$

1. По формуле (2) найдем разложение g по одночленам с первой переменной:

$$\begin{aligned} g = {} & (x_1 \oplus x_2 \oplus x_3 \oplus x_7 \oplus x_8 \oplus x_9) \triangleleft x_1 \\ & \oplus (x_2 \oplus x_3 \oplus x_4) \triangleleft x_1x_3 \oplus (x_3 \oplus x_4 \oplus x_5) \triangleleft x_1x_4. \end{aligned}$$

2.

$$\begin{aligned} v^{-1}(l_\emptyset) &= 1 \oplus x \oplus x^2 \oplus x^6 \oplus x^7 \oplus x^8 = (1 \oplus x \oplus x^2)(1 \oplus x^6), \\ v^{-1}(l_3) &= x \oplus x^2 \oplus x^3 = (1 \oplus x \oplus x^2)x, \\ v^{-1}(l_4) &= x^2 \oplus x^3 \oplus x^4 = (1 \oplus x \oplus x^2)x^2, \end{aligned}$$

и, следовательно, многочлен $1 \oplus x \oplus x^2$ — единственный нетривиальный общий делитель этих многочленов.

3. Для $a = 0, 1$ положим

$$\begin{aligned} g_{2,a} &= a \oplus x_1 \oplus x_2 \oplus x_3, \\ g_{1,a} &= a \oplus (x_1 \oplus x_7) \triangleleft x_1 \oplus x_2 \triangleleft x_1x_3 \oplus x_3 \triangleleft x_1x_4 \\ &= a \oplus x_1 \oplus x_7 \oplus x_2x_4 \oplus x_3x_6. \end{aligned}$$

Тогда по теореме 5

$$g = g_{2,a} \triangleleft g_{1,a}, \quad a = 0, 1$$

— все нетривиальные разложения с левым аффинным многочленом.

4. Для $a = 0, 1$ положим

$$\begin{aligned} f_{2,a} &\in F^*_3(\mathrm{GF}(2)), \quad f_{2,a} = g_{2,a}, \\ f_{1,a} &\in F^*_7(\mathrm{GF}(2)), \quad f_{1,a} = g_{1,a}. \end{aligned}$$

Тогда по теореме 3

$$(x \oplus a_0, \pi_{f_{1,a},2}) \colon R(f) \to R(f_{2,a} \oplus a_0), \quad a, a_0 = 0, 1$$

— все гомоморфизмы регистра $R(f)$ на линейные регистры ненулевой длины.

Литература

[1] *Солодовников В. И.* Гомоморфизмы двоичных регистров сдвига // Дискретная математика. 2005. Т. , № 1. С. 73–88.

Локальное аффинное обращение

О. А. Логачёв, Д. С. Назарова

Аннотация

В работе предложен новый класс методов криптоанализа, использующий теоретико-автоматные свойства фильтрующих генераторов. Приводятся примеры расчёта параметров локального обращения для некоторых классов фильтрующих функций.

Ключевые слова: потоковый шифр, булева функция, фильтрующий генератор, регистр сдвига, локальное аффинное обращение.

1. Введение

В последние годы обозначился существенный интерес к вопросам синтеза и анализа потоковых шифров. Проекты-конкурсы NESSIE (2000–2003 гг. [9]) и проходящий в настоящее время ECRYPT–eSTREAM (2004–2007 гг. [10]) показывают, что имеются определённые продвижения как в построении потоковых шифров, обосновании их свойств, так и в развитии методов криптографического анализа. Примером может служить активно развиваемый в настоящее время алгебраический метод, направленный на повышение эффективности решения полиномиальных уравнений над конечными полями. Указанный метод наряду с корреляционным методом активно используются при оценке стойкости шифров, построенных на основе фильтрующих генераторов. Вместе с тем, необходимо отметить, что имеющиеся в арсенале аналитика методы анализа фильтрующих генераторов основаны на использовании особенностей и свойств булевых функций, которые можно назвать «функциональными», т. е. характеризующими булеву функцию как отображение. Эти свойства (за исключением свойства сильной равновероятности булевой функции [3]) не затрагивают взаимодействие булевой функции с другими элементами фильтрующего генератора в процессе его функционирования. Другими словами отсутствует теоретико-автоматный подход при разработке методов анализа.

В настоящей работе предложен метод анализа фильтрующих генераторов, учитывающий в определённой степени особенности этих генераторов как конечных автоматов. Приводятся примеры расчёта оценок сложности

нахождения ключей фильтрующих генераторов для некоторых классов булевых функций.

2. Основные обозначения и определения

Пусть $\mathbb{F}_2$ — конечное поле из двух элементов, $V_n = \underbrace{\mathbb{F}_2 \times \ldots \times \mathbb{F}_2}_{\text{n раз}}$ — векторное пространство наборов-столбцов $\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right)^T$ длины n с компонентами из поля $\mathbb{F}_2$. Зафиксируем обозначения для векторов

$$\mathbf{0} = (0, 0, \ldots, 0)^T, \quad \mathbf{1} = (1, 1, \ldots, 1)^T,$$

а также для векторов канонического базиса V_n

$$\mathbf{e}_0 = (1, 0, \ldots, 0)^T, \quad \mathbf{e}_1 = (0, 1, \ldots, 0)^T, \quad \mathbf{e}_{n-1} = (0, 0, \ldots, 1)^T.$$

Булевой функцией от n переменных называется отображение из V_n в $\mathbb{F}_2$. Множество всех булевых функций от n переменных будем обозначать $\mathcal{F}_n$. Для записи значения булевой функции f на векторе $\mathbf{x} \in V_n$ будем использовать следующее выражение

$$f(\mathbf{x}) = f\left(x^{(0)}\mathbf{e}_0 \oplus x^{(1)}\mathbf{e}_1 \oplus \ldots \oplus x^{(n-1)}\mathbf{e}_{n-1}\right) = f\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right),$$

где «$\oplus$» — сложение по модулю 2 в $\mathbb{F}_2$ или V_n. Множество всех отображений из V_n в V_m (n,m — натуральные числа) будем обозначать $\mathcal{F}_{n,m}$. Для вектора $\mathbf{x} \in V_n$ через $(\mathbf{x})_{i,s} = \left(x^{(i)}, x^{(i+1)}, \ldots, x^{(i+s-1)}\right)^T$, $1 \leqslant i \leqslant n$, $1 \leqslant s \leqslant n - i$ будем называть i-ый фрагмент вектора вектора $\mathbf{x}$ длины s.

Через $\mathbb{N}$ обозначим множество натуральных чисел.

3. Общая модель локального аффинного обращения

Нам понадобятся для дальнейшего изложения два криптографических примитива. Первый — фильтрующий генератор (см. рис. 1), построенный с использованием регистра сдвига с линейной обратной связью длины n с полиномом обратных связей $\chi(\lambda) = \lambda^n \oplus \bigoplus_{i=0}^{n-1} \chi_i \lambda^i$ и фильтрующей булевой функцией $f \in \mathcal{F}_n$, обозначаемый далее $\mathrm{LFSR}(\chi, f)$. Второй — регистр сдвига длины n с функцией усложнения $f \in \mathcal{F}_n$ (см. рис. 2), обозначаемый далее $\mathrm{SR}(f)$.

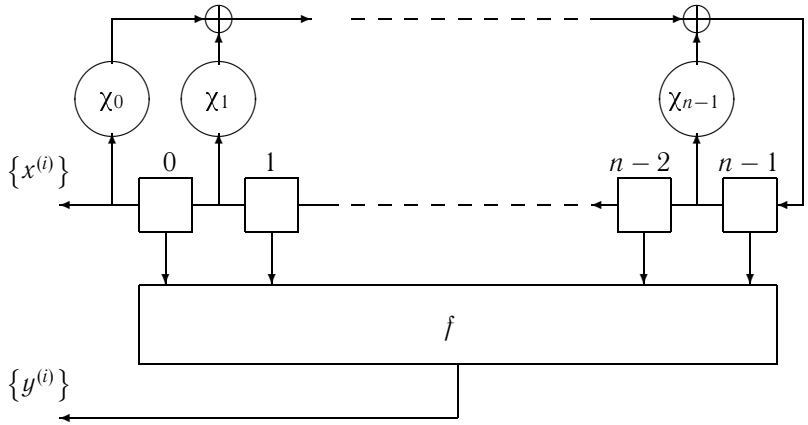


Рис. 1

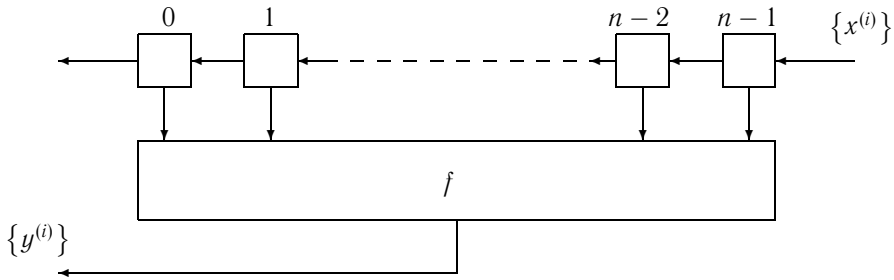


Рис. 2

Легко видеть, что с точки зрения функционирования $\mathrm{SR}(f)$ неотличим от фильтрующего генератора $\mathrm{LFSR}(\chi, f)$ в случае, если на $\mathrm{SR}(f)$ подаётся линейная рекуррентная последовательность над полем $\mathbb{F}_2$ порядка n с характеристическим многочленом $\chi(\lambda)$.

Для булевой функции f из $\mathcal{F}_n$ и натурального m определим отображение f_m^* из V_{m+n-1} в V_m, определяемое примитивом $\mathrm{SR}(f)$ вида

$$f_m^*(\mathbf{x}) = f_m^*\left(x^{(0)}, x^{(1)}, \ldots, x^{(m+n-2)}\right) = \\ = \left(f\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right), \ldots, f\left(x^{(m-1)}, x^{(m)}, \ldots, x^{(m+n-2)}\right)\right)^T, \quad (1)$$

для любого вектора $\mathbf{x} = \left(x^{(0)}, x^{(1)}, \ldots, x^{(m+n-2)}\right)^T \in V_{m+n-1}$.

Пусть A — $(k \times m)$-матрица над полем $\mathbb{F}_2$, $\operatorname{rank} A = k$, $1 \leqslant k \leqslant m$; B — $(l \times (m+n-1))$-матрица над полем $\mathbb{F}_2$, $\operatorname{rank} B = l$, $1 \leqslant l \leqslant m+n-1$.

Пусть $\mathbf{a} \in V_k$, $\mathbf{b} \in V_l$ и $\operatorname{rank}[A|\mathbf{a}] = k$, $\operatorname{rank}[B|\mathbf{b}] = l$. Будем обозначать через $\mathfrak{A} = (A, \mathbf{a})$ и $\mathfrak{B} = (B, \mathbf{b})$.

Определение 1. Пару $(\mathfrak{A}, \mathfrak{B})$ будем называть аффинным свойством, пару натуральных чисел $(m, m+n-1)$ — размером аффинного свойства, а пару натуральных чисел $\left(2^{m-k}, 2^{m+n-l-1}\right)$ — мощностью аффинного свойства. Для натуральных m и n будем обозначать через $\operatorname{Prop}(n, m)$ множество всех возможных аффинных свойств размера $(m, m+n-1)$.

Определение 2. Булева функция f из $\mathcal{F}_n$ обладает аффинным свойством $(\mathfrak{A}, \mathfrak{B}) \in \operatorname{Prop}(m, n)$, если для любых $\mathbf{x} \in V_{m+n-1}$, $\mathbf{y} \in V_m$ таких, что $\mathbf{y} = f_m^*(\mathbf{x})$, из выполнения соотношения $A\mathbf{y} \oplus \mathbf{a} = \mathbf{0}$ следует выполнение $B\mathbf{x} \oplus \mathbf{b} = \mathbf{0}$.

Необходимо отметить, что введённое в определении 2 аффинное свойство существенным образом отличается от всех введённых ранее криптографических свойств булевых функций за исключением сильной равновероятности ([3]), т. е. свойства функции быть без запрета. Такие известные криптографические свойства, как нелинейность, корреляционная иммунность и устойчивость, алгебраическая иммунность и т. п., являются функциональными свойствами, в то время как аффинное свойство является свойством конечного автомата $\operatorname{SR}(f)$, включающего в свой состав функцию выходов f, отображающую состояние автомата (вектор из V_n) в $\mathbb{F}_2$.

Рассмотрим теперь общее формальное описание метода восстановления начального состояния фильтрующего генератора $\operatorname{LFSR}(\chi, f)$ по его выходной последовательности (т. е. атаку на потоковый шифр по открытому и шифрованному текстам с угрозой вскрытия ключа).

Пусть для фильтрующего генератора $\operatorname{LFSR}(\chi, f)$ функция $f \in \mathcal{F}_n$ известна, многочлен $\chi(\lambda) = \lambda^n \oplus \bigoplus_{i=0}^{n-1} \chi_i \lambda^i$ известен и является примитивом (т. е. порождает линейную рекуррентную последовательность над полем $\mathbb{F}_2$ периода $2^n - 1$). Ключом генератора является начальное состояние регистра $\mathbf{x} = \left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right)^T \neq \mathbf{0}$, которое считается неизвестным. Известным также считается вектор $\mathbf{y} = \left(y^{(0)}, y^{(1)}, \ldots, y^{(N-1)}\right)^T$, где $y^{(i)} = f\left(L^i \mathbf{x}\right)$, $i = 0, 1, 2, \ldots, N-1$ и

$$L = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ \chi_0 & \chi_1 & \chi_2 & \cdots & \chi_{n-1} \end{bmatrix}.$$

Задача состоит в нахождении вектора $\mathbf{x} = \left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right)^T$ по вектору $\mathbf{y} = \left(y^{(0)}, y^{(1)}, \ldots, y^{(N-1)}\right)^T$ при известных параметрах $\mathrm{LFSR}(\chi, f)$, т. е. в решении уравнения

$$\mathbf{y} = f_N^*(\mathbf{x}^*) \tag{2}$$

относительно $\mathbf{x}^*$, где

$$\mathbf{x}^* = \left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}, x^{(n)}, \ldots, x^{(N+n-2)}\right)^T = \left(\mathbf{x}, x^{(n)}, \ldots, x^{(N+n-2)}\right)^T$$

— фрагмент линейной рекуррентной последовательности длины $N + n - 1$.

Пусть f обладает аффинным свойством $(\mathfrak{A}, \mathfrak{B}) \in \mathrm{Prop}(m, n)$ (см. опр. 2). Рассмотрим восстановление ключа генератора $\mathrm{LFSR}(\chi, f)$, основанное на локальном аффинном обращении. Под локальным аффинным обращением будем понимать процесс нахождения дополнительных линейных соотношений во фрагментах длины $m + n - 1$ линейной рекуррентной последовательности $\mathbf{x}^* = \left(x^{(0)}, x^{(1)}, \ldots, x^{(N+n-2)}\right)^T$ (см. (2)) при $n + m \ll \ll N$, $2^k \ll N$, используя аффинное свойство $(\mathfrak{A}, \mathfrak{B})$ фильтрующей функции f.

Пусть $(\mathbf{y})_{s,m}$, $s = 0, 1, \ldots, N - m$ — вектор-фрагмент длины m вектора $y \in V_N$, а $(\mathbf{x})_{s,m+n-1}$, $s = 0, 1, \ldots, N - m$ — вектор-фрагмент длины $m + n - 1$ вектора $\mathbf{x}^* \in V_{N+n-1}$. Просматриваем последовательно фрагменты вектора $\mathbf{y}$, проверяя выполнение условия $A(\mathbf{y})_{s,m} \oplus \mathbf{a} = \mathbf{0}$. Поскольку мощность множества решений системы линейных уравнений $A\mathbf{u} = \mathbf{a}$ равна 2^{m-k}, то вероятность попадания очередного фрагмента $(\mathbf{y})_{s,m}$ в это множество можно принять приблизительно равной 2^{-k}. Пользуясь тем, что $2^k \ll \ll N$, мы имеем в среднем значительное число фрагментов $(\mathbf{y})_{s,m}$, которые являются решениями системы линейных уравнений $A\mathbf{u} = \mathbf{a}$. Тогда соответствующие фрагменты $(\mathbf{x}^*)_{s,m+n-1}$ вектора $\mathbf{x}^*$ являются решениями системы линейных уравнений $B\mathbf{v} = \mathbf{b}$. Поскольку любая компонента $x^{(i)}$ вектора $\mathbf{x}^*$ является некоторой линейной функцией от $\mathbf{x} = \left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right)^T$, а именно

$$x^{(i)} = l_i\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right),$$

где

$$l_0\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right) = x^{(0)}, \ldots, l_{n-1}\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right) = x^{(n-1)}$$

и

$$l_i\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right) = l_0\left(L^i\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right)^T\right) \text{ при } i > n - 1,$$

то получаемые новые линейные соотношения в ряде случаев позволяют эффективно находить неизвестный вектор $\mathbf{x} = \left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right)^T$.

4. Примеры локального аффинного обращения

4.1. Функция голосования ([7], [8])

Пусть n — нечётное натуральное. Предположим, что в качестве фильтрующей функции f генератора $\mathrm{LFSR}(\chi, f)$ выбрана функция голосования от n переменных, т. е.

$$f(\mathbf{x}) = \begin{cases} 0 \text{ при } \mathrm{wt}(\mathbf{x}) \leqslant \dfrac{n-1}{2}, \\ 1 \text{ при } \mathrm{wt}(\mathbf{x}) \geqslant \dfrac{n+1}{2}. \end{cases}$$

Эта функция уравновешенная, обладает максимальной возможной алгебраической иммунностью $AI(f) = \left\lceil \dfrac{n}{2} \right\rceil = \dfrac{n+1}{2}$ (см. [7], [8]). Её нелинейность N_f равна $2^{n-1} - \binom{n-1}{\frac{n-1}{2}}$ (см. [7], [8]). Функция f также является симметрической и самодвойственной. Поскольку $W_f(\mathbf{e}_1) = W_f(\mathbf{e}_2) = \ldots = W_f(\mathbf{e}_n) = \binom{n-1}{\frac{n-1}{2}}$, то функция голосования не обладает свойством корреляционной иммунности.

Построим теперь некоторые возможные аффинные свойства, которым удовлетворяет функция голосования.

Лемма 1. *Пусть n — нечётное, $m = 2$, $k = l = 2$. Функция голосования от n переменных обладает аффинными свойствами* $(\mathfrak{A}_1, \mathfrak{B}_1)$, *где*

$$\mathfrak{A}_1 = (A_1, \mathbf{a}_1) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right),$$

$$\mathfrak{B}_1 = (B_1, \mathbf{b}_1) = \left(\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

и $(\mathfrak{A}_2, \mathfrak{B}_2)$, *где*

$$\mathfrak{A}_2 = (A_2, \mathbf{a}_2) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right),$$

$$\mathfrak{B}_2 = (B_2, \mathbf{b}_2) = \left(\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right)$$

Доказательство. Пусть некоторый фрагмент $(\mathbf{y})_{i,2}$ вектора $\mathbf{y}$ удовлетворяет условию $A_1(\mathbf{y})_{i,2} = \mathbf{a}_1$, т. е. $(\mathbf{y})_{i,2} = (0, 1)^T$. Тогда

$$f\left(x^{(i)}, \ldots, x^{(i+n-1)}\right) = 0, \quad f\left(x^{(i+1)}, \ldots, x^{(i+n)}\right) = 1$$

и, следовательно,

$$\mathrm{wt}\left((x^{(i)}, \ldots, x^{(i+n-1)})^T\right) = \frac{n-1}{2}, \quad \mathrm{wt}\left((x^{(i+1)}, \ldots, x^{(i+n)})^T\right) = \frac{n+1}{2}.$$

Это возможно лишь в случае, когда $x^{(i)} = 0$ и $x^{(i+n)} = 1$, т. е. выполнено соотношение $B_1(\mathbf{x})_{i,2} = \mathbf{b}_1$.

Аналогичными рассуждениями доказывается и второе утверждение леммы. □

Для подсчёта эффективности предлагаемого метода определения начального состояния фильтрующего генератора необходимо вычислить значения ряда параметров. В частности, необходимо оценить, сколь часто в выходной последовательности фильтрующего генератора происходит событие $\left\{y^{(i)} \neq y^{(i+1)}\right\}$, далее называемое знакопеременой.

В случае, когда фильтрующей функцией является функция голосования, удаётся точно подсчитать число знакоперемен на периоде выходной последовательности.

Теорема 1. *Пусть n — нечётное, f — функция голосования от n переменных и $\chi(\lambda) = \lambda^n \oplus \bigoplus_{i=0}^{n-1} \chi_i \lambda^i$ — примитивный многочлен над $\mathbb{F}_2$. Тогда число r_n знакоперемен выходного вектора*

$$\mathbf{y} = \left(y^{(0)}, y^{(1)}, \ldots, y^{(2^n-2)}\right)^T$$

фильтрующего генератора $\mathrm{LFSR}(\chi, f)$ *порядка* $2^n - 1$ *равно* $r_n = \binom{n-1}{\frac{n-1}{2}}$.

Доказательство. Пусть

$$V_{n,t} = \left\{\mathbf{x} \in V_n \mid \mathrm{wt}(\mathbf{x}) = t\right\}, \quad t = 0, 1, \ldots, n.$$

Рассмотрим разбиение этого множества $V_{n,t} = V_{n,t}^{(0)} \cup V_{n,t}^{(1)}$, где

$$V_{n,t}^{(\varepsilon)} = \left\{\mathbf{x} \in V_n \mid \mathrm{wt}(\mathbf{x}) = t, \ \ x^{(1)} = \varepsilon\right\}, \ \ \varepsilon = 0, 1, \ \ t \neq 0, n.$$

Легко видеть, что при $t \neq 0, n$ имеем $\#V_{n,t}^{(0)} = \binom{n-1}{t}$, $\#V_{n,t}^{(1)} = \binom{n-1}{t-1}$.

Знакоперемена вида $\left(y^{(i)}, y^{(i+1)}\right)^T = (0, 1)^T$ в выходном векторе $\mathbf{y}$ генератора $\mathrm{LFSR}(\chi, f)$ возможна тогда и только тогда, когда состояние в такте i генератора $(\mathbf{x})_{i,n} = \left(x^{(i)}, \ldots, x^{(i+n-1)}\right)^T \in V_{n,\frac{n-1}{2}}^{(0)}$, а состояние в такте $i+1$ генератора $(\mathbf{x})_{i+1,n} = \left(x^{(i+1)}, \ldots, x^{(i+n)}\right)^T \in V_{n,\frac{n+1}{2}}$. Знакоперемена вида $\left(y^{(i)}, y^{(i+1)}\right)^T = (1, 0)^T$ в выходном векторе $\mathbf{y}$ генератора $\mathrm{LFSR}(\chi, f)$

возможна тогда и только тогда, когда состояние в такте i генератора $(\mathbf{x})_{i,n} = \left(x^{(i)}, \ldots, x^{(i+n-1)}\right)^T \in V^{(1)}_{n,\frac{n+1}{2}}$, а состояние в такте $i+1$ генератора $(\mathbf{x})_{i+1,n} = \left(x^{(i+1)}, \ldots, x^{(i+n)}\right)^T \in V_{n,\frac{n-1}{2}}$. Заметим, что если $v \in V^{(0)}_{n,\frac{n-1}{2}}$, то $v \oplus 1 \in V^{(1)}_{n,\frac{n+1}{2}}$. Такие вектора будем называть противоположными.

Пусть состояния

$$(\mathbf{x})_{i,n} = \left(x^{(i)}, \ldots, x^{(i+n-1)}\right)^T \in V^{(0)}_{n,\frac{n-1}{2}}, \quad (\mathbf{x})_{j,n} = \left(x^{(j)}, \ldots, x^{(j+n-1)}\right)^T \in V^{(1)}_{n,\frac{n+1}{2}}$$

являются противоположными векторами, т. е. $(\mathbf{x})_{i,n} \oplus (\mathbf{x})_{j,n} = \mathbf{1}$. Поскольку для примитивного многочлена $\chi(\lambda)$ имеем $\chi_0 \oplus \chi_1 \oplus \ldots \oplus \chi_{n-1} = 0$, то для суммы битов, генерируемых в состояниях $(\mathbf{x})_{i,n}$ и $(\mathbf{x})_{j,n}$, справедливо соотношение

$$\begin{aligned} x^{(i+n)} \oplus x^{(j+n)} = \chi_0 x^{(i)} \oplus \chi_1 x^{(i+1)} \oplus \ldots \oplus \chi_{n-1} x^{(i+n-1)} \oplus \\ \oplus \chi_0 x^{(j)} \oplus \chi_1 x^{(j+1)} \oplus \ldots \oplus \chi_{n-1} x^{(j+n-1)} = \\ = \chi_0 x^{(i)} \oplus \chi_1 x^{(i+1)} \oplus \ldots \oplus \chi_{n-1} x^{(i+n-1)} \oplus \\ \oplus \chi_0 \left(x^{(i)} \oplus 1\right) \oplus \chi_1 \left(x^{(i+1)} \oplus 1\right) \oplus \ldots \oplus \chi_{n-1} \left(x^{(i+n-1)} \oplus 1\right) = \\ = \chi_0 \oplus \chi_1 \oplus \ldots \oplus \chi_{n-1} = 0. \end{aligned}$$

Следовательно, генерируемые биты в противоположных векторах (состояниях) совпадают. Предположим, что $x^{(i+n)} = x^{(j+n)} = 1$. Тогда $(\mathbf{x})_{i+1,n} \in V_{n,\frac{n+1}{2}}$, $(\mathbf{x})_{j+1,n} \in V_{n,\frac{n+1}{2}}$ (знакоперемена $(0, 1)^T$). Если $x^{(i+n)} = x^{(j+n)} = 0$, то $(\mathbf{x})_{i+1,n} \in V_{n,\frac{n-1}{2}}$ и $(\mathbf{x})_{j+1,n} \in V_{n,\frac{n-1}{2}}$ (знакоперемена $(1, 0)^T$). Для каждой пары противоположных векторов (состояний) существует единственная знакоперемена и таких пар ровно $\binom{n-1}{\frac{n-1}{2}}$. Поскольку в силу примитивности $\chi(\lambda)$ на периоде $\left(x^{(0)}, x^{(1)}, \ldots, x^{(2^n-2)}\right)^T$ все ненулевые векторы будут состояниями $\mathrm{LFSR}(\chi, f)$ в точности по одному разу, то число знакоперемен в выходном векторе $\mathbf{y} = \left(y^{(0)}, y^{(1)}, \ldots, y^{(2^n-2)}\right)^T$ будет в точности $\binom{n-1}{\frac{n-1}{2}}$. □

Предварительная часть вычислений в данном методе состоит в нахождении для N последовательных знаков линейной рекуррентной последовательности $\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}, \ldots, x^{(N-1)}\right)^T$ выражений в виде линейных

функций от $\mathbf{x} = \left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right)^T$, т. е.

$$
\begin{aligned}
&l_0(\mathbf{x}) = x^{(0)} = (\mathbf{e}_0, \mathbf{x}) = (\mathbf{C}_0, \mathbf{x}),\\
&l_1(\mathbf{x}) = x^{(1)} = (\mathbf{e}_1, \mathbf{x}) = (\mathbf{C}_1, \mathbf{x}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&l_{n-1}(\mathbf{x}) = x^{(n-1)} = (\mathbf{e}_{n-1}, \mathbf{x}) = (\mathbf{C}_{n-1}, \mathbf{x}),\\
&l_n(\mathbf{x}) = (\mathbf{e}_{n-1}, L\mathbf{x}) = (L^T\mathbf{e}_{n-1}, \mathbf{x}) = (\mathbf{C}_n, \mathbf{x}),\\
&l_{n+1}(\mathbf{x}) = (\mathbf{e}_{n-1}, L^2\mathbf{x}) = ((L^2)^T\mathbf{e}_{n-1}, \mathbf{x}) = ((L^T)^2\mathbf{e}_{n-1}, \mathbf{x}) = (\mathbf{C}_{n+1}, \mathbf{x}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&l_{n-1+j}(\mathbf{x}) = (\mathbf{e}_{n-1}, L^j\mathbf{x}) = ((L^j)^T\mathbf{e}_{n-1}, \mathbf{x}) = ((L^T)^j\mathbf{e}_{n-1}, \mathbf{x}) = (\mathbf{C}_{n-1+j}, \mathbf{x}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&l_{N-1}(\mathbf{x}) = (\mathbf{e}_{n-1}, L^{N-n}\mathbf{x}) = ((L^{N-n})^T\mathbf{e}_{n-1}, \mathbf{x}) = ((L^T)^{N-n}\mathbf{e}_{n-1}, \mathbf{x}) = (\mathbf{C}_{N-1}, \mathbf{x}).
\end{aligned}
$$

Для получения выражения s-го элемента линейной рекуррентной последовательности, $s > n$, необходимо умножить матрицу L^T на вектор из V_n. Так как сложность умножения матрицы на вектор не превосходит $O(n^2)$ операций, то сложность предварительного этапа не превосходит $O(Nn^2)$, $N = N(n)$. При этом N, необходимое для однозначного нахождения ключа x (в зависимости от n), будет определено ниже.

Заметим, что информация, полученная на предварительном этапе, может быть использована для нахождения различных ключей.

Для вероятности появления знакоперемены в выходном векторе $\mathbf{y}$ возьмём их среднее значение на цикле длины $2^n - 1$, т. е.

$$P\left\{y^{(i)} \neq y^{(i+1)}\right\} = \frac{\binom{n-1}{\frac{n-1}{2}}}{2^n - 1}.$$

Поскольку появление знакоперемены в выходном векторе даёт нам два линейных уравнения (см. лемму 1) относительно компонент вектора начального состояния генератора $\mathrm{LFSR}(\chi, f)$, то вероятность появления в каждом такте линейного уравнения относительно компонент начального вектора-состояния генератора $\mathrm{LFSR}(\chi, f)$ можно положить

$$p_n = \frac{2\binom{n-1}{\frac{n-1}{2}}}{2^n - 1}. \tag{3}$$

Воспользовавшись соотношением (см. [13])

$$\binom{2\nu}{\nu} \sim \frac{2^{2\nu}}{\sqrt{\pi\nu}}$$

получаем

$$p_n \sim \sqrt{\frac{2}{\pi(n-1)}}.$$

Для выходного вектора $\mathbf{y} = \left(y^{(0)}, y^{(1)}, \ldots, y^{(N-1)}\right)$ появятся в среднем

$$\tau = \tau_n(N) = \left[N \frac{2\binom{n-1}{\frac{n-1}{2}}}{2^n - 1} \right] = [p_n N]$$

линейных уравнений относительно компонент начального вектора-состояния генератора $\mathrm{LFSR}(\chi, f)$.

Полученная система уравнений заведомо совместна и в её множество решений входит искомое начальное состояние регистра — ключ. Пусть построенная система линейных уравнений имеет вид

$$B\mathbf{x} = \mathbf{b}, \tag{4}$$

где

$$B = \begin{bmatrix} b_{0\,0} & b_{0\,1} & \ldots & b_{0\,n-1} \\ b_{1\,0} & b_{1\,1} & \ldots & b_{1\,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{\tau-1\,0} & b_{\tau-1\,1} & \ldots & b_{\tau-1\,n-1} \end{bmatrix},$$

$$\mathbf{x} = \left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right)^T \in V_n, \ \ \mathbf{b} = \left(b^{(0)}, \ldots, b^{(n-1)}\right)^T \in V_n.$$

Для длины N выходного вектора $\mathbf{y}$, необходимой для однозначного определения начального состояния $\mathbf{x}$ (ключа) генератора $\mathrm{LFSR}(\chi, f)$ рассмотрим следующую математическую модель. Будем считать, что матрица коэффициентов левой части системы уравнений 4 является случайной матрицей с независимыми элементами. Пусть $A = \|a_{ij}\|$ — матрица размера $\tau \times n$, элементы которой независимы в совокупности и принимают значения 0 и 1 с равными вероятностями. Пусть $\rho_n(\tau)$ — ранг матрицы A.

Следующая теорема является основой дальнейших рассуждений.

Теорема 2 ([4]). *Пусть $s \geqslant 0$ и r — фиксированные целые числа, $r + s \geqslant 0$. Если $n \to \infty$ и $\tau = n + m$, то*

$$P\{\rho_n(\tau) = n - s\} \to 2^{-s(r+s)} \prod_{i=s+1}^{\infty} \left(1 - \frac{1}{2^i}\right) \prod_{i=1}^{r+s} \left(1 - \frac{1}{2^i}\right)^{-1},$$

где последнее произведение полагается равным единице при $r + s = 0$.

В [4] на основе этой теоремы показано, что ранг $\rho_n(\tau)$ обладает пороговым свойством: если $\tau/n \to \alpha$ и $0 \leqslant \alpha < 1$, то $P\{\rho_n(\tau) = \tau\} \to 1$, а если $\tau/n \to \alpha,\ \ \alpha > 1$, то $P\{\rho_n(\tau) = n\} \to 1$.

Так как τ — число линейных уравнений — равно, как показано выше, $\left[\dfrac{2\binom{n-1}{\frac{n-1}{2}}}{2^n - 1}N\right]$, т. е. является функцией от n и τ, то можно оценить число τ, достаточное для того, чтобы $\tau/n \to \alpha$, $\alpha > 1$ при $n \to \infty$. Воспользовавшись формулой Стирлинга ([13]), исследуем поведение τ/n при $n \to \infty$:

$$\lim_{n\to\infty} \tau/n = \lim_{n\to\infty} \frac{2\binom{n-1}{\frac{n-1}{2}}N}{(2^n-1)n} = \lim_{n\to\infty} \frac{2(n-1)!N}{\left(\frac{n-1}{2}\right)!\left(\frac{n-1}{2}\right)!n(2^n-1)} =$$

$$= \lim_{n\to\infty} \frac{2\sqrt{2\pi(n-1)}(n-1)^{n-1}e^{-(n-1)}N}{\left(\sqrt{2\pi\left(\frac{n-1}{2}\right)}\right)^2 \left(\left(\frac{n-1}{2}^{\frac{n-1}{2}}\right)\right)^2 \left(e^{-\frac{n-1}{2}}\right)^2 n(2^n-1)} =$$

$$= \lim_{n\to\infty} \frac{2\sqrt{2\pi(n-1)}N}{\pi(n-1)\left(\frac{1}{2}\right)^{n-1} n(2^n-1)} = \lim_{n\to\infty} \frac{\sqrt{2}2^n N}{\sqrt{\pi}\sqrt{n-1}(2^n-1)n} = \lim_{n\to\infty} \frac{\sqrt{2}}{\sqrt{\pi}}\frac{N}{n^{3/2}}.$$

Следовательно, при $N = O\left(n^{3/2}\right)$ можно добиться выполнения условия $\tau/n \to \alpha,\ \ \alpha > 1$. Таким образом, по выходному вектору фильтрующего генератора длины порядка $O\left(n^{3/2}\right)$ с вероятностью, близкой к единице, может быть построена система линейных уравнений, имеющая единственное решение, т. е. можно определить ключ фильтрующего генератора.

Оценим сложность определения ключа фильтрующего генератора с функцией голосования предложенным методом. Будем считать сложность в элементарных операциях сравнения, сложения и умножения элементов поля $\mathbb{F}_2$. Формально метод может быть разделён на три этапа:

а) первый — предварительный этап, который может быть выполнен независимо от наличия у криптоаналитика информации о выходном векторе генератора и его результаты могут использоваться при определении различных ключей. На этом этапе формируются уравнения, выражающие N последовательных элементов линейной рекуррентной последовательности через биты начального состояния (ключа) фильтрующего генератора. Для этого надо выполнить N раз операцию умножения матрицы размера $n \times n$ на n-мерный вектор. Так как сложность операции умножения квадратной матрицы n-го порядка на вектор равна $O\left(n^2\right)$ и $N = O\left(n^{3/2}\right)$, то сложность этапа предварительной работы составляет $O\left(n^{7/2}\right)$;

б) второй этап состоит в просмотре выходного вектора фильтрующего генератора, выделении тактов, соответствующих знакопеременам, и составления, путём выбора из соответствующих линейных уравнений, подготовленных на предварительном этапе, системы из $\tau = O(n)$ линейных уравнений для данного ключа. Сложность второго этапа составляет $O(N) = O\left(n^{3/2}\right)$;

в) третий этап состоит в решении методом Гаусса полученной линейной системы с n неизвестными, что потребует порядка $O\left(n^3\right)$ элементарных операций.

Таким образом, для фильтрующего генератора, использующего функцию голосования от n переменных (n — нечётно), неизвестный ключ может быть найден предложенным методом по выходному вектору длины $O\left(n^{3/2}\right)$ со сложностью

- $O\left(n^{7/2}\right)$ — предварительный этап;
- $O\left(n^{3/2}\right)$ — этап построения линейной системы;
- $O\left(n^3\right)$ — этап решения линейной системы

и с вероятностью, близкой к единице.

4.2. Симметрические функции ([11], [12])

Пусть n — произвольное натуральное число, $\mathfrak{S}_n$ — симметрическая группа степени n (группа подстановок элементов множества $I_n = \{1, 2, \ldots, n\}$).

Определение 3. Булева функция f из $\mathcal{F}_n$ называется симметрической, если для любой подстановки $\sigma \in \mathfrak{S}_n$ выполняется соотношение

$$f^\sigma\left(x^{(1)}, x^{(2)}, \ldots, x^{(n)}\right) = f\left(x^{(\sigma(1))}, x^{(\sigma(2))}, \ldots, x^{(\sigma(n))}\right) = \\ = f\left(x^{(1)}, x^{(2)}, \ldots, x^{(n)}\right).$$

Лемма 2. *Пусть $f \in \mathcal{F}_n$ — произвольная симметрическая функция, отличная от константы. Пусть $m = 2$, $k = 2$, $l = 1$. Функция f обладает аффинными свойствами $(\mathfrak{A}'_1, \mathfrak{B}'_1)$, где*

$$\mathfrak{A}'_1 = (A'_1, \mathbf{a}'_1) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right),$$
$$\mathfrak{B}'_1 = (B'_1, \mathbf{b}'_1) = ((1, 0, \ldots, 0, 1), (1))$$

и $(\mathfrak{A}'_2, \mathfrak{B}'_2)$, где

$$\mathfrak{A}'_2 = (A'_2, \mathbf{a}'_2) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right),$$
$$\mathfrak{B}'_2 = (B'_2, \mathbf{b}'_2) = ((1, 0, \ldots, 0, 1), (1))$$

Доказательство. Пусть некоторый фрагмент $(\mathbf{y})_{i,2}$ выходного вектора $\mathbf{y}$ удовлетворяет условию $A_1'(\mathbf{y})_{i,2} = \mathbf{a}_1'$, т. е. $(\mathbf{y})_{i,2} = (0,\ 1)^T$. Тогда

$$f\left(x^{(i)},\ \ldots,\ x^{(i+n-1)}\right) = 0, \quad f\left(x^{(i+1)},\ \ldots,\ x^{(i+n)}\right) = 1,$$

где $\left(x^{(i)},\ \ldots,\ x^{(i+n-1)}\right)^T \in V_{n,s}$, $\left(x^{(i+1)},\ \ldots,\ x^{(i+n)}\right)^T \in V_{n,t}$ и $|s-t| = 1$.

Справедлива следующая цепочка равенств:

$$|s-t| = \left|\mathrm{wt}\left(x^{(i)},\ \ldots,\ x^{(i+n-1)}\right) - \mathrm{wt}\left(x^{(i+1)},\ \ldots,\ x^{(i+n)}\right)\right| =$$
$$= \left|\sum_{j_1=i}^{i+n-1} x^{(j_1)} - \sum_{j_2=i+1}^{i+n} x^{(j_2)}\right| = \left|x^{(i)} - x^{(i+n)}\right| = 1.$$

Следовательно, $x^{(i)} \neq x^{(i+n)}$ или $x^{(i)} \oplus x^{(i+n)} = 1$ и выполнено соотношение $B_1'(\mathbf{x})_{i,2} = b_1'$.

Аналогичными рассуждениями доказывается и второе утверждение леммы. □

Предположим, что в качестве фильтрующей функции генератора $\mathrm{LFSR}(\chi,\ f)$ выбрана некоторая уравновешенная симметрическая функция f из $\mathcal{F}_n$.

Определение 4 ([11]). Пусть n — нечётное натуральное число. Симметрическая уравновешенная функция f из $\mathcal{F}_n$ называется тривиально уравновешенной, если выполняется соотношение

$$f(\mathbf{x} \oplus \mathbf{1}) = f(\mathbf{x}) \oplus 1$$

для любого $\mathbf{x} \in V_n$ (т. е. функция f является самодвойственной).

Лемма 3. *Пусть* $n = 2k+1$, $k \geqslant 0$, f — *симметрическая тривиально уравновешенная функция из* $\mathcal{F}_n$ *и* $\chi(\lambda) = \lambda^n \oplus \bigoplus_{i=0}^{n-1} \chi_i \lambda^i$ — *примитивный многочлен над* $\mathbb{F}_2$. *Тогда для числа* r_n *знакоперемен в выходном векторе* $\mathbf{y} = \left(y^{(0)},\ y^{(1)},\ \ldots,\ y^{(2^n-1)}\right)^T$ *фильтрующего генератора* $\mathrm{LFSR}(\chi,\ f)$ *периода* $2^n - 1$ *выполняется неравенство*

$$r_n \geqslant \binom{n-1}{\frac{n-1}{2}}.$$

Доказательство. Непосредственно следует из теоремы 1. □

Таким образом, можно считать, что вероятность появления знакоперемены в выходном векторе $\mathbf{y}$ удовлетворяет неравенству

$$P\left\{y^{(i)} \neq y^{(i+1)}\right\} \geqslant \frac{\binom{n-1}{\frac{n-1}{2}}}{2^n - 1}. \tag{5}$$

Поскольку в данном случае каждой знакоперемене соответствует одно линейное уравнение относительно компонент вектора — начального состояния генератора $\mathrm{LFSR}(\chi, f)$, то вероятность появления в каждом такте линейного уравнения относительно ключа удовлетворяет неравенству

$$p_n \geqslant \frac{\binom{n-1}{\frac{n-1}{2}}}{2^n - 1}. \tag{6}$$

Очевидно, что расчёты, аналогичные приведённым в разделе 4.1 приводят к полиномиальным (по n) оценкам необходимой для нахождения ключа длины N выходного генератора, сложности предварительного этапа и этапа построения линейной системы.

Весьма вероятной представляется следующая гипотеза: число знакоперемен в выходном векторе длины $2^n - 1$ генератора $\mathrm{LFSR}(\chi, f)$, где $\chi(\lambda)$ — примитивный многочлен степени n и f — уравновешенная симметрическая функция из $\mathcal{F}_n$, не менее, чем $\binom{n-1}{\frac{n-1}{2}}$.

4.3. Ротационно-симметрические функции ([14], [15], [16], [17])

Пусть n — натуральное и подстановка g из симметрической группы $\mathfrak{S}_n$ степени n имеет вид $g = (1, 2, \ldots, n)$.

Определение 5. Булева функция f из $\mathcal{F}_n$ называется ротационно-симметрической, если для любого вектора $\mathbf{x} = \left(x^{(1)}, x^{(2)}, \ldots, x^{(n)}\right) \in V_n$ и для любого k, $1 \leqslant k \leqslant n$ выполнено соотношение

$$f\left(g^k \mathbf{x}\right) = f^{g^k}\left(x^{(1)}, x^{(2)}, \ldots, x^{(n)}\right) = f\left(x^{(k+1)}, \ldots, x^{(n)}, x^{(1)}, \ldots, x^{(k)}\right) = \\ = f\left(x^{(1)}, x^{(2)}, \ldots, x^{(n)}\right).$$

Заметим, что любая симметрическая функция является также ротационно-симметрической. Обратное утверждение не верно.

Лемма 4. *Пусть $f \in \mathcal{F}_n$ — произвольная ротационно-симметрическая функция, отличная от константы. Тогда при $m = 2$, $k = 2$, $l = 2$ функция f обладает аффинными свойствами $(\mathfrak{A}'_1, \mathfrak{B}'_1)$, где*

$$\mathfrak{A}'_1 = (A'_1, \mathbf{a}'_1) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right),$$
$$\mathfrak{B}'_1 = (B'_1, \mathbf{b}'_1) = ((1, 0, \ldots, 0, 1), (1))$$

и $(\mathfrak{A}'_2, \mathfrak{B}'_2)$, где

$$\mathfrak{A}'_2 = (A'_2, \mathbf{a}'_2) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right),$$
$$\mathfrak{B}'_2 = (B'_2, \mathbf{b}'_2) = ((1, 0, \ldots, 0, 1), (1))$$

Доказательство. Аналогично доказательству леммы 2. □

В отличие от симметрических функций, имеющих постоянное значение на множествах $V_{n,k}$, $k = 0, 1, \ldots, n$, ротационно-симметрические функции имеют постоянное значение на множествах, называемых циклотомическими классами пространства V_n. Пусть вектор $\mathbf{x}$ из V_n. Циклотомический класс, соответствующий $\mathbf{x}$, определяется следующим образом:

$$\mathfrak{C}(\mathbf{x}) = \left\{ g^k \mathbf{x} \mid k = 0, 1, \ldots, n-1 \right\} \subset V_n.$$

С помощью леммы Бернсайда ([1],[24]) легко подсчитать число d_n циклотомических классов

$$d_n = \frac{1}{n} \sum_{k|n} \Phi(k) 2^{n/k},$$

где Φ — функция Эйлера. Мощность множества всех ротационно-симметричных функций в $\mathcal{F}_n$ очевидно равна 2^{d_n}.

Предложение 1. *Для произвольного вектора* $\mathbf{x}$ *из* V_n *справедливы соотношения для циклотомических классов*:

а) $\mathfrak{C}(\mathbf{x} \oplus \mathbf{1}) = \mathfrak{C}(\mathbf{x}) \oplus \mathbf{1}$;
б) $\#\mathfrak{C}(\mathbf{x} \oplus \mathbf{1}) = \#\mathfrak{C}(\mathbf{x})$.

Доказательство. Непосредственно следует из определения циклотомического класса. □

Лемма 5. *Пусть* $n = 2k+1$, $k \geqslant 0$, f — *ротационно-симметрическая тривиально уравновешенная функция из* $\mathcal{F}_n$ *и* $\chi(\lambda) = \lambda^n \oplus \bigoplus_{i=0}^{n-1} \chi_i \lambda^i$ — *примитивный многочлен над полем* $\mathbb{F}_2$. *Тогда для числа* r_n *знакоперемен в выходном векторе* $\mathbf{y} = \left(y^{(0)}, y^{(1)}, \ldots, y^{(2^n-2)}, y^{(0)}\right)$ *фильтрующего генератора* $\mathrm{LFSR}(\chi, f)$ *длины* 2^n *выполняется неравенство*

$$r_n \geqslant \binom{n-1}{\frac{n-1}{2}}.$$

Доказательство. Следует из теоремы 1. □

Таким образом, можно считать, что для вероятности появления знакоперемены в выходном векторе генератора $\mathrm{LFSR}(\chi, f)$ и для вероятности появления в каждом такте линейного уравнения относительно ключа выполнены неравенства (5) и (6) соответственно. Очевидно, что расчёты, аналогичные проведённым в разделе 4.1, приводят к полиномиальным (по n) оценкам необходимой для нахождения ключа длины N выходного вектора генератора, сложности предварительного этапа и этапа построения линейной системы.

4.4. Функции минимального преимущества

В ряде случаев локальное аффинное обращение может быть обусловлено достаточно специфичным внутренним свойством булевой функции. Рассмотрим следующий пример.

Пусть $n = 2p + 1$ — нечётное натуральное. Предположим, что в качестве фильтрующей функции генератора LFSR(χ, f) выбрана булева функция из $\mathcal{F}_n$, задаваемая соотношением

$$f(\mathbf{x}) = f(\mathbf{x}_1, \mathbf{x}_2) = \begin{cases} 1, \text{ если } \mathrm{wt}(\mathbf{x}_1) \geqslant \mathrm{wt}(\mathbf{x}_2) \\ 0, \text{ если } \mathrm{wt}(\mathbf{x}_1) < \mathrm{wt}(\mathbf{x}_2), \end{cases} \tag{7}$$

где $\mathbf{x}_1 = \left(x^{(1)}, x^{(2)}, \ldots, x^{(p)}\right)^T \in V_p$, $\mathbf{x}_2 = \left(x^{(p+1)}, x^{(p+2)}, \ldots, x^{(2p+1)}\right)^T \in V_{p+1}$.

Предложение 2. *Булева функция из $\mathcal{F}_n$, задаваемая соотношением* (7), *уравновешена.*

Доказательство. Соотношение (7) показывает, что

$$\mathrm{supp}(f) = \bigcup_{t=0}^{p} V_{p,t} \times \left[\bigcup_{r=0}^{t} V_{p+1,r}\right],$$

и, следовательно,

$$\mathrm{wt}(f) = \#\,\mathrm{supp}(f) = \sum_{t=0}^{p} \#\left(V_{p,t} \times \left[\bigcup_{r=0}^{t} V_{p+1,r}\right]\right) = \sum_{t=0}^{p} \binom{p}{t} \sum_{r=0}^{t} \binom{p+1}{r}. \tag{8}$$

Перегруппировав слагаемые в сумме (8), получим

$$\mathrm{wt}(f) = \sum_{i=0}^{p} \binom{p+1}{i}\binom{p}{i} + \sum_{j=0}^{p-1} \binom{p+1}{j}\binom{p}{j+1} +$$
$$+ \sum_{l=0}^{p-2} \binom{p+1}{l}\binom{p}{l+2} + \ldots + \sum_{d=0}^{1} \binom{p+1}{d}\binom{p}{d+p-1} + \binom{p+1}{0}\binom{p}{p}. \tag{9}$$

Воспользовавшись тождеством

$$\binom{p}{m} = \binom{p}{p-m},$$

а также основным рекуррентным соотношением для биномиальных коэффициентов ([5],[6])

$$\binom{n}{r} = \sum_{j=0}^{r} \binom{n-m}{j}\binom{m}{r-j},$$

получим

$$\mathrm{wt}(f) = \binom{2p+1}{p} + \binom{2p+1}{p-1} + \\ + \binom{2p+1}{p-2} + \ldots + \binom{2p+1}{1} + \binom{2p+1}{0} = 2^{2p} = 2^{n-1}. \qquad \square$$

Пусть входом регистра $\mathrm{SR}(f)$, где f определена соотношением (7), является вектор $\mathbf{x} = \left(x^{(0)}, x^{(1)}, \ldots, x^{(n-1)}\right)^T$, а выходом — вектор $\mathbf{y} = \left(y^{(0)}, y^{(1)}\right)^T$, т. е. $\mathbf{y} = f_2^*(\mathbf{x})$. Предположим, что $\mathbf{y} = (0, 1)^T$ — знакоперемена. Поскольку

$$f\left(x^{(0)}, \ldots, x^{(p-1)}, x^{(p)}, \ldots, x^{(n-1)}\right)^T = 0, \; f\left(x^{(1)}, \ldots, x^{(p)}, x^{(p+1)}, \ldots, x^{(n)}\right)^T = 1,$$

то

$$\begin{aligned} &\mathrm{wt}\left(x^{(0)}, \ldots, x^{(p-1)}\right) < \mathrm{wt}\left(x^{(p)}, \ldots, x^{(n-1)}\right), \\ &\mathrm{wt}\left(x^{(1)}, \ldots, x^{(p)}\right) \geqslant \mathrm{wt}\left(x^{(p+1)}, \ldots, x^{(n)}\right) \end{aligned} \tag{10}$$

Предположим, что $x^{(p)} = 0$, тогда справедлива следующая цепочка неравенств

$$\mathrm{wt}\left((x^{(1)}, \ldots, x^{(p)})^T\right) \leqslant \mathrm{wt}\left((x^{(0)}, \ldots, x^{(p-1)})^T\right) < \\ < \mathrm{wt}\left((x^{(p)}, \ldots, x^{(n-1)})^T\right) \leqslant \mathrm{wt}\left((x^{(p+1)}, \ldots, x^{(n)})^T\right).$$

Следовательно, не может быть выполнено второе из неравенств (10). Поэтому имеем $x^{(p)} = 1$.

Лемма 6. *Пусть* $n = 2p+1$, $m = 2$, $k = 2$, $l = 1$. *Функция минимального преимущества, задаваемая соотношением* (7), *обладает аффинным свойством* $(\mathfrak{A}, \mathfrak{B})$, *где*

$$\mathfrak{A} = (A, a) = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right),$$

$$\mathfrak{B} = (B, b) = ((0, \ldots, 0, 1, 0, \ldots, 0), (1)) = \left(\mathbf{e}_p \in V_{2p+1}, (1)\right).$$

Доказательство. Непосредственно следует из соотношений (10). $\square$

Возвращаясь к исходной задаче нахождения начального состояния генератора $\mathrm{LFSR}(\chi, f)$ по его выходной последовательности необходимо отметить следующее. Воспользовавшись средними величинами знакоперемен вида $(0, 1)^T$ в выходной последовательности, можно рассчитать сложность нахождения начального состояния $\mathrm{LFSR}(\chi, f)$, как это было сделано ранее для функции голосования, симметрических и ротационно-симметрических функций. Полученная оценка сложности будет иметь полиномиальный характер от n.

4.5. Конечные автоматы ([18], [19])

Вопросы восстановления информации о входных последовательностях (возможных) по известной выходной последовательности являются одними из основных в теории конечных автоматов ([20],[21],[22],[23]). В них очевиден и криптографический аспект. Конечно-автоматные модели регулярно используются в процессе криптоанализа потоковых шифров. Принципиальные возможности локально-аффинного обращения на теоретико-автоматном языке обсуждались в статье [2].

В принципиальном плане нас интересуют конечные автоматы, для которых существуют выходные последовательности конечной длины с однозначно восстанавливаемыми фрагментами (возможных) входных последовательностей, соответствующих данной выходной. Мы будем рассматривать примеры на основе конечного автомата $\mathrm{SR}(f)$, изображенного на рис. 2, что позволит нам не вводить язык теории автоматов и использовать лишь язык булевых функций.

Пусть $f \in \mathcal{F}_n$ и f линейно зависит от переменной $x^{(n-1)}$, т. е.

$$f\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-2)}, x^{(n-1)}\right) = f'\left(x^{(0)}, x^{(1)}, \ldots, x^{(n-2)}\right) \oplus x^{(n-1)},$$

где $f' \in \mathcal{F}_{n-1}$. Согласно результатам работы [3], эта функция является функцией без запрета, т. е. для любого $m \in \mathbb{N}$, $\mathbf{y} = \left(y^{(0)}, \ldots, y^{(m-1)}\right)^T \in V_m$ существует $\mathbf{x} = \left(x^{(0)}, \ldots, x^{(m+n-2)}\right)^T \in V_{m+n-1}$ такой, что

$$\mathbf{y} = f_m^*(\mathbf{x}).$$

Кроме того, из результатов работы [3] известно, что f является также сильно равновероятной функцией, т. е.

$$\#\left\{\left(f_m^*\right)^{-1}(\mathbf{y})\right\} = 2^{n-1}$$

для любого $\mathbf{y} \in V_m$. Таким образом, для любого выходного вектора $\mathbf{y} \in V_m$ регистра $\mathrm{SR}(f)$ все соответствующие $\mathbf{y}$ входные векторы можно представить в виде матрицы $M_{\mathbf{y}}$ размера $(n+m-1)$ вида

$$M_{\mathbf{y}} = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{2^{n-1}}] = \begin{bmatrix} x_1^{(0)} & x_2^{(0)} & \ldots & x_{2^{n-1}}^{(0)} \\ x_1^{(1)} & x_2^{(1)} & \ldots & x_{2^{n-1}}^{(1)} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{(m+n-2)} & x_2^{(m+n-2)} & \ldots & x_{2^{n-1}}^{(m+n-2)} \end{bmatrix} \tag{11}$$

и $\mathbf{y} = f_m^*(\mathbf{x}_i)$, $i = 1, 2, \ldots, 2^{n-1}$.

Рассмотрим класс булевых функций $D_n \subset \mathcal{F}_n$, удовлетворяющий условиям:

- Функции из D_n линейны по последней переменной;
- для любой функции $f \in D_n$ существует натуральное $m = m(f)$ и $\mathbf{y} \in \in V_m$ такие, что

$$\begin{aligned}
&x_1^{(m)} = x_2^{(m)} = \ldots = x_{2^{n-1}}^{(m)}\\
&x_1^{(m+1)} = x_2^{(m+1)} = \ldots = x_{2^{n-1}}^{(m+1)}\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&x_1^{(m+n-2)} = x_2^{(m+n-2)} = \ldots = x_{2^{n-1}}^{(m+n-2)},
\end{aligned}$$

т. е. у матрицы $M_{\mathbf{y}}^f$ любая из последних $n-1$ строк состоит из одинаковых элементов. Для любой функции f из семейства D_n линейность её по последней переменной обеспечивает однозначное восстановление для выходного вектора $\mathbf{w} = (\mathbf{a}, \mathbf{c})^T$, $\mathbf{a} \in V_m$, $\mathbf{c} \in V_k$ фрагмента входного вектора $\left(b_{(\mathbf{c})}^{(m+n-1)}, b_{(\mathbf{c})}^{(m+n)}, \ldots, b_{(\mathbf{c})}^{(m+n+k-2)}\right)^T$. Следовательно, булева функция обладает аффинным свойством $(\mathfrak{A}, \mathfrak{B}) \in \mathrm{Prop}(m, n)$, где $\mathfrak{A} = (A, \mathbf{a})$, $A = = E_m$ и $\mathfrak{B} = (B, \mathbf{b})$, $B = E_k$, $\mathbf{b} = (b^{(0)}, \ldots, b^{(k-1)}) = \left(b_{(\mathbf{c})}^{(0)}, \ldots, b_{(\mathbf{c})}^{(k-1)}\right)$. Заметим также, что k может быть сколь угодно большим.

На теоретико-автоматном языке (см. [2]) функции из класса D_n соответствуют конечным автоматам $\mathrm{SR}(f)$, для которых локально-обратный автомат под действием данного входного вектора $\mathbf{y}$ переходит из начального состояния в состояние, состоящее из одного вектора.

Пример 1. Пусть $n = 3$ и $f\left(x^{(0)}, x^{(1)}, x^{(2)}\right) = x^{(0)}x^{(1)} \oplus x^{(2)}$. Тогда любой выходной вектор $\mathbf{y} \in V_m$ при любом m имеет четыре соответствующих ему входных вектора $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4 \in V_{m+n-1}$ таких, что $f_m^*(\mathbf{x}_i) = \mathbf{y}$, $i = = 1, 2, 3, 4$. Пусть $\mathbf{a}_1 = (0, 1, 0, 1)^T \in V_4$. Тогда матрица $M_{\mathbf{a}_1}^f$ имеет вид

$$M_{\mathbf{a}_1}^f = \begin{bmatrix} 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 1\\ 1 & 1 & 1 & 0\\ 0 & 0 & 0 & 0\\ 1 & 1 & 1 & 1 \end{bmatrix},$$

где $(0, 0, 0, 0)$ — предпоследняя строка, $(1, 1, 1, 1)$ — последняя строка. Предположим, что

$$\mathbf{a} = (\mathbf{a}_1, \mathbf{a}_2)^T \in V_8, \quad \mathbf{a}_2 = \left(a^{(5)}, a^{(6)}, a^{(7)}, a^{(8)}\right), \quad A = E_8;$$
$$B = E_4, \quad \mathbf{b} = \left(b^{(1)}, b^{(2)}, b^{(3)}, b^{(4)}\right)^T \in V_4,$$

где

$$b^{(1)} = a^{(5)}, \quad b^{(2)} = a^{(5)} \oplus a^{(6)}, \quad b^{(3)} = a^{(6)} \oplus a^{(7)}, \quad b^{(4)} = a^{(5)} \oplus a^{(7)} \oplus a^{(8)}.$$

Тогда если фрагмент выходного вектора $(\mathbf{y})_{i,8} = \left(y^{(i)},\, y^{(i+1)},\, \ldots,\, y^{(i+7)}\right)^T$ регистра $\mathrm{SR}(f)$ удовлетворяет соотношению $A(\mathbf{y})_{i,8} = \mathbf{a}$, то фрагмент

$$(\mathbf{x})_{i+4,4} = \left(x^{(i+4)},\, x^{(i+5)},\, x^{(i+7)},\, x^{(i+8)}\right)^T$$

удовлетворяет соотношению $B(\mathbf{x})_{i+4,4} = \mathbf{b}$. Следовательно, данная функция f обладает аффинным свойством $(\mathfrak{A},\, \mathfrak{B}) = \left((A,\, \mathbf{a}),\, (B,\, \mathbf{b})\right)$ с указанными выше A, $\mathbf{a}$, B, $\mathbf{b}$. Легко видеть, что компоненты вектора $\mathbf{a}_2$ можно выбирать произвольным образом, а компоненты вектора $\mathbf{b}$ вычисляются по $\mathbf{a}_1$ и $\mathbf{a}_2$ однозначно. Кроме того, число компонент у вектора $\mathbf{a}_2$ может быть сколь угодно большим. Таким образом, функция $f\left(x^{(0)},\, x^{(1)},\, x^{(2)}\right) = x^{(0)}x^{(1)} \oplus x^{(2)}$ обладает целым семейством аффинных свойств.

5. Обсуждение результатов

Необходимо отметить некоторые особенности использованного в данной работе свойства. Полученные результаты показывают, что решающим свойством булевой функции (с точки зрения криптографической стойкости генератора) может оказаться не собственное её «функциональное» свойство, а свойство, отражающее взаимодействие булевой функции с различными элементами генератора псевдослучайных последовательностей в процессе его функционирования. В данном конкретном случае свойство локального аффинного обращения отражает взаимодействие регистра сдвига и булевой функции.

Таким образом, актуальным является исследование наряду с «функциональными» свойствами булевых функций также и конечно-автоматных свойств генераторов псевдослучайных чисел, содержащих в своём составе булевы функции. Очевидно, что такие исследования будут давать более адекватную оценку криптографических свойств генераторов псевдослучайных чисел.

Полученные результаты показывают также, что симметрические, ротационно-симметрические и «близкие» к ним (в определённом смысле) функции не являются приемлемыми для построения стойких фильтрующих генераторов. Термин «близкие» можно интерпретировать, как выполнение с высокой вероятностью свойства симметричности (ротационной симметричности) булевой функции. Это позволяет проводить соответствующие расчёты сложности определения ключей фильтрующего генератора, используя вероятностные рассуждения, несколько понижающие надёжность данного метода.

Литература

[1] О. А. Логачёв, А. А. Сальников, В. В. Ященко. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

[2] О. А. Логачёв, Г. В. Проскурин, В. В. Ященко. Локальное обращение конечного автомата с помощью автоматов. Дискретная математика, том 7, выпуск 2, 1995, с. 19–33.

[3] С. Н. Сумароков. Запреты двоичных функций и обратимость для одного класса кодирующих устройств. Обозрение прикладной и промышленной математики, № 1, 1994, с. 33–55.

[4] В. Ф. Колчин. Случайные графы. М.: ФИЗМАТЛИТ, 2004.

[5] Дж. Риордан. Введение в комбинаторный анализ. М.: ИЛ, 1963.

[6] Дж. Риордан. Комбинаторные тождества. М.: Наука, 1982.

[7] M. Lobanov. Tight bound between nonlinearity and algebraic immunity. Cryptology ePrint Archive, Report 2005/441, 2005.

[8] D. K. Dalai, S. Maitra, S. Sarcar. Basic Theory in Construction of Boolean Functions with Maximum Possible Anigilator Imminity. Cryptology ePrint Archive, Report 2005/229, 2005.

[9] NESSIE: New European schemes for signatures, integrity, and encryption. Information society technologies programme of the European commision (IST–1999–12324), `http://www.cryptonessie.org`.

[10] European Network of Exellence in Cryptography (ECRYPT), 2004–2007, `http://www.ecrypt.eu.org`.

[11] A. Canteaut, M. Videau. Symmetric Boolean functions. IEEE Transaction on Information Ttheory IT-51 (2005), no. 8, 2005, pp. 2791–2811.

[12] A. Braeken, B. Preneel. On the algebraic immunity of symmetric Boolean functions. Indocrypt 2005, LNCS 3348, Springer-Verlag, 2004, pp. 120–135.

[13] W. Feller. An Introduction to Probability Theory and Applications. Volume 1. John Wiley & Sons, New York, Chichester, Brisbane, Toronto, 1970.

[14] D. K. Dalai, S. Maitra, P. Stanica. Results on Rotation Symmetric Bent Functions. Cryptology ePrint Archive, Report 2005/118, 2005.

[15] P. Ke, Z. Chang, Q. Wen. Results on Rotation Symmetric Boolean Functions on Even Number Variable. Cryptology ePrint Archive, Report 2005/130, 2005.

[16] A. Maximov. Classes of Pleteaued Rotation Simmetric Boolean Functions under Transformation of Walsh Spectra. Cryptology ePrint Archive, Report 2004/354, 2004.

[17] S. Kavut, S. Maitra, S. Sarkar, M. D. Yucel. Enumeration of 9-variable Rotation Symmetric Boolean Functions having Nonlinearity > 240. Cryptology ePrint Archive, Report 2006/249, 2006.

[18] Б. А. Трахтенброт, Я. М. Барздинь. Конечные автоматы (поведение и синтез). «Наука», Москва, 1970.

[19] В. Б. Кудрявцев, С. В. Алешин, А. С. Подколзин. Введение в теорию автоматов. «Наука», Москва, 1985.

[20] D. A. Huffman. Canonical forms for information-lossless finite-state logical mashines. IRE Trans. Circuit Th., 6, Spec. Suppl., 1959, pp. 41–59.

[21] D. A. Huffvan. Notes on information-lossless finite-state automata. Nuovo cimento, 13, suppl. 2, 1959, pp. 397–405.

[22] Sh. Even. On information-lossless automata of finite order. IEEE Trans. Electronic Comput, 14, 1965, 4, pp. 561–569.

[23] А. А. Курмит. Автоматы без потери информации конечного порядка. «Зинатне», Рига, 1972.

[24] Applied Combinatorial Mathematics. Editor E. F. Beckenbach. John Wiley & Sons, INC, New York, Sydney, 1964.

Рекуррентные соотношения на выходную последовательность фильтрующего генератора и их обобщения

В. В. Баев

Рассматриваются фильтрующие генераторы (см. [1]) на основе двоичного регистра сдвига с линейной обратной связью. Такой генератор не подходит на роль псевдослучайного, если его выходная последовательность $\{b_i\}_{i\in\mathbb{N}}$ удовлетворяет рекуррентному соотношению малой длины T, т. е. существует такая функция g, что

$$\forall i \quad b_{i+T} = g(b_i, \ldots, b_{i+T-1}). \tag{1}$$

Введём необходимые обозначения.

- $\mathrm{GF}(2^n)$ — поле Галуа из 2^n элементов;
- $\mathbb{F}_2 := \mathrm{GF}(2)$ — поле из двух элементов;
- $V_n := \mathbb{F}_2^n$ — n-мерное векторное пространство над полем $\mathbb{F}_2$;
- $\mathcal{F}_n$ — множество всех булевых функций $V_n \to \mathbb{F}_2$;
- $\deg f$ — алгебраическая степень булевой функции $f \in \mathcal{F}_n$.

Пусть регистр сдвига над полем $\mathbb{F}_2$ имеет длину n. Пусть $f \in \mathcal{F}_n$ — фильтрующая функция. Линейное преобразование регистра на каждом такте обозначим $L : V_n \to V_n$.

В [6] показано, как можно эффективно находить начальное заполнение регистра, если удаётся найти тождества следующего вида:

$$\forall x \in V_n \quad h(x) = g(x, f(x), f(Lx), \ldots, f(L^T x)), \tag{2}$$

где $\deg h \leqslant d$ и $\deg g \leqslant e$ для достаточно малых d, e. Нетрудно видеть, что (2) является обобщением (1).

В данной работе получено выражение для линейной сложности выходной последовательности фильтрующего генератора через f и L (определение линейной сложности последовательности см. в [1]), найдены также полиномиальные алгоритмы поиска тождеств вида (2) и рекуррентных соотношений вида (1).

Если характеристический многочлен $\chi \in \mathbb{F}_2[x]$ регистра сдвига равен

$$\chi(x) = x^n - a_{n-1}x^{n-1} - \ldots - a_1 x - a_0, \tag{3}$$

то матрица L линейного преобразования регистра равна

$$L = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_0 & a_1 & a_2 & \cdots & a_{n-1} \end{pmatrix}$$

Теорема 1 ([4]). *Пусть характеристический многочлен* (3) *регистра сдвига неприводим. Пусть* $a \in \mathrm{GF}(2^n)$ *— корень* χ. *Тогда существует базис* $e_0, \ldots, e_{n-1}$ *линейного пространства* $\mathrm{GF}(2^n)$ *над полем* $\mathbb{F}_2$ *такой, что в этом базисе матрица* L *задаёт отображение* $x \mapsto a \cdot x$ *поля* $\mathrm{GF}(2^n)$ *в себя.*

Базис $e_0, \ldots, e_{n-1}$ задаёт отождествление V_n с полем $\mathrm{GF}(2^n)$. Поэтому можно считать, что фильтрующая функция f есть отображение $\mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$, принимающее значения в подполе $\mathbb{F}_2 \subset \mathrm{GF}(2^n)$. Поскольку преобразование регистра линейное, то при любом ненулевом начальном заполнении все последующие состояния регистра будут ненулевыми. Поэтому можно считать, что f определена на $\mathrm{GF}(2^n) \setminus \{0\}$. Функция $f : \mathrm{GF}(2^n) \setminus \{0\} \to \mathrm{GF}(2^n)$ представима единственным многочленом над полем $\mathrm{GF}(2^n)$ степени не более $2^n - 2$:

$$f(x) = \sum_{i=0}^{2^n-2} f_i \cdot x^i, \quad f_i \in \mathrm{GF}(2^n). \tag{4}$$

Обозначим $P_f := \{i | f_i \neq 0\}$. Тогда (4) можно переписать в эквивалентном виде

$$f(x) = \sum_{m \in P_f} f_m \cdot x^m, \quad f_m \in \mathrm{GF}(2^n) \setminus \{0\}. \tag{5}$$

Теорема 2. *Пусть характеристический многочлен* χ *регистра сдвига примитивен. Пусть при указанном выше отождествлении векторного пространства состояний регистра* V_n *с полем* $\mathrm{GF}(2^n)$ *фильтрующая функция* f *задаётся многочленом* (4). *Тогда линейная сложность выходной последовательности такого фильтрующего генератора равна* $|P_f|$.

Доказательство. Рассмотрим многочлен

$$M(x) := \sum_{i=0}^{|P_f|} \alpha_i x^i := \prod_{m \in P_f} (x - a^m). \tag{6}$$

a — примитивный элемент поля $\mathrm{GF}(2^n)$, поэтому все корни многочлена $M(x)$ имеют кратность 1. Функция f принимает значения в $\mathbb{F}_2$, поэтому P_f вместе с любым своим элементом $m \in P_f$ содержит весь циклотомический класс $[m]$. Следовательно, коэффициенты многочлена $M(x)$ принимают значения из поля $\mathbb{F}_2$. $\alpha_{|P_f|} = 1$.

Выпишем цепочку эквивалентных условий для следующего утверждения: выходная последовательность $\{b_i\}_{i\in\mathbb{N}}$ удовлетворяет линейному рекуррентному соотношению длины T с коэффициентами $\beta_0, \ldots, \beta_T$.

$$\forall i \quad \sum_{j=0}^{T} \beta_j \cdot b_{i+j} = 0 \iff$$

$$\forall i \quad \sum_{j=0}^{T} \beta_j \cdot f(a^{i+j} x_0) = 0. \tag{7}$$

Здесь x_0 — начальное значение регистра. Поскольку a — примитивный элемент поля $\mathrm{GF}(2^n)$, то $a^i x_0$ пробегает все ненулевые значения поля $\mathrm{GF}(2^n)$ при изменении i. Таким образом, (7) равносильно следующему равенству для многочленов из $\mathrm{GF}(2^n)[x]$ степени не более $2^n - 2$:

$$\sum_{j=0}^{T} \beta_j \cdot f(a^j x) = 0 \iff$$

$$\sum_{j=0}^{T} \beta_j \sum_{m\in P_f} f_m a^{jm} x^m = 0 \iff$$

$$\sum_{m\in P_f} f_m x^m \sum_{j=0}^{T} \beta_j \left(a^m\right)^j = 0 \iff$$

$$\forall m \in P_f \quad \sum_{j=0}^{T} \beta_j \left(a^m\right)^j = 0.$$

То есть для $\forall m \in P_f$ элемент $a^m \in \mathrm{GF}(2^n)$ является корнем многочлена $B(x) = \sum_{j=0}^{T} \beta_j x^j \in \mathbb{F}_2[x]$, причём все эти элементы a^m различны. Это равносильно тому, что многочлен $B(x)$ делится на $M(x)$.

Итого, самое короткое линейное рекуррентное соотношение задаётся многочленом $M(x)$, то есть линейная сложность выходной последовательности фильтрующего генератора равна $\deg M(x) = \left|P_f\right|$. □

Замечание 1. В [1] и [7] приведена универсальная линейная комбинация, которая задаёт линейную рекуррентную зависимость для выходной

последовательности фильтрующего генератора с функцией выхода f степени d. Коэффициенты этой комбинации являются коэффициентами многочлена

$$U(x) = \prod_{\substack{0 \leqslant m \leqslant 2^n - 1: \\ \mathrm{wt}(m) \leqslant d}} (x - a^m).$$

На этой линейной комбинации основывается верхняя оценка линейной сложности выходной последовательности, приведённая в [1]. А именно, линейная сложность не превосходит $\deg U(x) = \sum_{k=0}^{d} C_n^k$. Теорема 2 даёт точное значение линейной сложности, выраженное через примитивный характеристический многочлен χ регистра сдвига, его примитивный корень a и представление (5) для функции выхода генератора.

Теперь нас будут интересовать тождества вида (2). Однако мы будем считать, что x из поля $\mathrm{GF}(2^n)$:

$$\forall x \in \mathrm{GF}(2^n) \setminus \{0\} \quad h(x) = g(x, f(a^0 x), f(a^1 x), \ldots, f(a^T x)), \tag{8}$$

где $\forall m \in P_h$ $\mathrm{wt}(m) \leqslant d$, а функция $g : \mathrm{GF}(2^n) \times \mathbb{F}_2^{T+1} \to \mathbb{F}_2$ представима в виде

$$g(x, y_0, \ldots, y_T) = \sum_{\substack{u = (u_0, \ldots, u_T) \in \mathbb{F}_2^{T+1}: \\ \mathrm{wt}(u) \leqslant e}} g_u(x) \cdot y_0^{u_0} \cdot \ldots \cdot y_T^{u_T}, \tag{9}$$

где для $\forall u \in \mathbb{F}_2^{T+1} : \mathrm{wt}(u) \leqslant e$ и для $\forall m \in P_{g_u}$ выполнено $\mathrm{wt}(m) \leqslant s$.

Для фиксированных n, f, T, d, e, s множество всех таких пар функций (g, h) образует линейное пространство $R_{T,d,e,s}(f)$ над полем $\mathbb{F}_2$. Нам достаточно найти базис в этом пространстве.

Теорема 3. *Пусть характеристический многочлен* (3) *регистра сдвига примитивен. Пусть при указанном в теореме* 1 *отождествлении векторного пространства состояний регистра* V_n *с полем* $\mathrm{GF}(2^n)$ *фильтрующая функция* f *задаётся многочленом* (5). *Тогда для любых фиксированных констант* $d, e, s \in \{1, \ldots, n\}$ *существует полиномиальный* (*от* n, T, $|P_f|$) *алгоритм со следующими характеристиками*:

1. *Вход алгоритма*: *число* $n \in \mathbb{N}$ *и список элементов множества* $\{(i, f_i) | i \in P_f\}$ (*это множество задаёт функцию* f),

2. *Выход алгоритма*: $(g_1, h_1), \ldots, (g_N, h_N)$ – *список базисных элементов пространства* $R_{T,d,e,s}(f)$. *При этом каждая функция* h_i *задана набором коэффициентов представления* (5), *а каждая функция* g_i *задана списком элементов множества* $\{(u, g_u) | u \in \mathbb{F}_2^{T+1} : \mathrm{wt}(u) \leqslant e\}$. *В свою очередь каждая функция* g_u *из этого списка задана набором коэффициентов представления* (5).

Замечание 2. При получении тождеств (8) с помощью алгоритма из теоремы 3 и при использовании этих тождеств в быстрых алгебраических атаках [6] линейную комбинацию на «предвычислительном» шаге (precomputation step) можно получать так же, как это делалось в теореме 2 для функции f:

$$\forall x \in \mathrm{GF}(2^n) \setminus \{0\} \quad \sum_{i=0}^{S} \beta_i \cdot h(a^i x) = 0 \Longleftarrow$$

$$\sum_{i=0}^{S} \beta_i X^i = \prod_{m \in P_h} (X - a^m) \in \mathbb{F}_2[X].$$

Рекуррентные соотношения (1) на выходную последовательность фильтрующего генератора можно представить как частный случай тождеств (8):

$$\forall x \in \mathrm{GF}(2^n) \setminus \{0\} \quad f(a^T x) = \tilde{g}(f(a^0 x), f(a^1 x), \ldots, f(a^{T-1} x)). \tag{10}$$

Множество $R_{T,e}(f)$ функций $\tilde{g}$ степени $\leqslant e$, удовлетворяющих тождеству (10), (в случае, если $R_{T,e}(f)$ не пусто) соответствует аффинному подпространству в линейном пространстве $R_{T,0,e,0}(f)$. А именно, на пары $(g, h) \in R_{T,0,e,0}(f)$ нужно дополнительно наложить аффинные ограничения (поскольку $d = s = 0$, то h и все g_u из представления (9) — константы):

$$\begin{cases} h = 0, \\ \forall u \in \mathbb{F}_2^{T+1} : (2 \leqslant \mathrm{wt}(u) \leqslant e \text{ и } u_T = 1) \quad g_u = 0, \\ g_{(0,\ldots,0,1)} = 1. \end{cases} \tag{11}$$

При этом получим тождество

$$g(x, f(a^0 x), f(a^1 x), \ldots, f(a^T x)) = \\ = \tilde{g}(f(a^0 x), f(a^1 x), \ldots, f(a^{T-1} x)) + f(a^T x) = 0.$$

Теорема 4. *Алгоритм из теоремы* 3 *можно модифицировать в соответствии с ограничениями* (11) *так, что новый алгоритм будет полиномиальным, будет иметь тот же вход, а на выходе будет набор функций* $\tilde{g}_1, \ldots, \tilde{g}_M$, *порождающий аффинное пространство* $R_{T,e}(f)$. *Выход будет пустым в случае, если не существует функций* $\tilde{g}$ *степени* $\leqslant e$, *удовлетворяющих тождеству* (10).

Алгоритм из теоремы 3 можно использовать для построения быстрых алгебраических атак [6]. При этом нужно оценивать, что является более подходящим:

1) использовать линейную рекурренту (6), для представления (5) фильтрующей функции, или

2) найти одно из тождеств вида (8) для проведения быстрой алгебраической атаки, или

3) с помощью алгоритма из теоремы 4 найти рекурренту (10) для $T \ll \ll |P_f|$.

Пункты 2 и 3 могут быть предпочтительней, только когда $T \ll |P_f|$, или когда у нас в распоряжении имеется только T последовательных битов выходной последовательности. В пунктах 2 и 3 может не оказаться ни одного тождества. Если в пункте 3 получается хоть одна рекуррента длины T, то использовать пункт 2 уже бессмысленно, поскольку он предполагает дополнительные вычисления.

Литература

[1] Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черёмушкин А. В. *Основы криптографии*. М.: Гелиос АРВ, 2001.

[2] Баев В. В. *О некоторых алгоритмах построения аннигиляторов низкой степени для булевых функций*. Представлено к опубликованию в журнале «Дискретная математика». Т. 18, 2006.

[3] Баев В. В. *Некоторые нижние оценки на алгебраическую иммунность функций, заданных своими трэйс формами*. Труды VII Международной конференции «Дискретные модели в теории управляющих систем» (Покровское, 4–6 марта 2006 г.). М.: МАКС Пресс, 2006. с. 25–29.

[4] Лидл Р., Нидеррайтер Г. *Конечные поля*. В 2-х т. Пер. с англ. М.: Мир, 1988.

[5] Armknecht F. *Improving fast algebraic attacks*. Fast Software Encryption 2004, LNCS 3017, p. 65–82, Springer, 2004.

[6] Courtois N. *Fast algebraic attacks on stream ciphers with linear feedback*. Crypto 2003, LNCS 2729, p. 176–194. Springer, 2003.

[7] Hawkes P., Rose G. *Rewriting variables: the complexity of fast algebraic attacks on stream ciphers*. Crypto 2004, LNCS 3152, p. 390–406, Springer, 2004.

Структура пространства аннигиляторов для булевых функций с фиктивными переменными

В. В. Баев

При анализе криптографических свойств фильтрующих и комбинирующих генераторов, основанных на двоичных линейных регистрах сдвига, получили распространение алгебраические атаки [7] и быстрые алгебраические атаки [8], [5], [9]. Эти методы потребовали детального и разностороннего исследования пространств обнуляющих множителей низкой степени для булевых функций.

Введём необходимые обозначения:

- $\mathbb{F}_2$ — поле из двух элементов;
- $\mathcal{F}_n$ — множество всех булевых функций $\mathbb{F}_2^n \to \mathbb{F}_2$ от n переменных;
- $\deg f$ — алгебраическая степень булевой функции $f \in \mathcal{F}_n$.

Для функции $f \in \mathcal{F}_n$ будем рассматривать линейное пространство $A_d(f) := \{g \in \mathcal{F}_n | f \cdot g = 0,\ \deg g \leqslant d\}$. Элементы этого пространства будем называть аннигиляторами функции f.

В статьях [1], [2], [3], [6], [10] исследовались вопросы существования и методы эффективного поиска ненулевых аннигиляторов для заданных булевых функций.

Целью данной работы является описание пространства $A_d(f)$ для ненулевой функции $f \in \mathcal{F}_n$, у которой некоторые переменные фиктивны (несущественны).

Пусть для некоторого $k : k \leqslant n$ переменные x_i $(k \leqslant i \leqslant n)$ фиктивны для функции $f \in \mathcal{F}_n$. То есть

$$\forall (x_1, \ldots, x_{k-1}) \in \mathbb{F}_2^{k-1} \quad \forall (a_k, \ldots, a_n), (b_k, \ldots, b_n) \in \mathbb{F}_2^{n-k+1}$$

$$f(x_1, \ldots, x_{k-1}, a_k, \ldots, a_n) = f(x_1, \ldots, x_{k-1}, b_k, \ldots, b_n).$$

Для каждого $m \in \{k-1, \ldots, n\}$ рассмотрим функцию $f_m \in \mathcal{F}_m$, положив

$$f_m(x_1, \ldots, x_m) := f(x_1, \ldots, x_m, \underbrace{0, \ldots, 0}_{n-m}).$$

В частности, $f = f_n$.

Для функции $h \in \mathcal{F}_m$ обозначим пространство её аннигиляторов от m переменных

$$A_d^m(h) := \{g \in \mathcal{F}_m | \deg g \leqslant d,\ h \cdot g = 0\}.$$

Наша цель — выразить пространство $A_d^n(f)$ через пространства $A_i^{k-1}(f_{k-1})$, $i \in \{1, \dots, d\}$ (без фиктивных переменных $x_k, \dots, x_n$).

Будем действовать индуктивно: сперва выразим $A_d^n(f_n)$ через $A_d^{n-1}(f_{n-1})$ и $A_{d-1}^{n-1}(f_{n-1})$. Рассмотрим разложение функций f_n и $g \in \mathcal{F}_n$ по последней переменной:

$$\begin{aligned} f_n(x_1, \dots, x_n) &= f_{n-1}(x_1, \dots, x_{n-1}) + 0 \cdot x_n, \\ g(x_1, \dots, x_n) &= g_0(x_1, \dots, x_{n-1}) + g_1(x_1, \dots, x_{n-1}) \cdot x_n. \end{aligned}$$

В этих обозначениях имеем цепочку равносильных условий:

$$\begin{aligned} g \in A_d^n(f_n) &\iff \begin{cases} f_{n-1}g_0 = 0 \text{ и } \deg g_0 \leqslant d, \\ f_{n-1}g_1 = 0 \text{ и } \deg g_1 \leqslant d-1; \end{cases} \\ &\iff \begin{cases} g_0 \in A_d^{n-1}(f_{n-1}), \\ g_1 \in A_{d-1}^{n-1}(f_{n-1}). \end{cases} \end{aligned} \tag{1}$$

Далее мы по умолчанию будем подразумевать вложения $A_i^{n-1}(f_{n-1}) \subset \subset \mathcal{F}_{n-1} \subset \mathcal{F}_n$. Под произведением $A_i^{m-1}(f_{m-1}) \cdot x_m$ будем понимать множество произведений каждой функции из $A_i^{m-1}(f_{m-1})$ на «селекторную» функцию $[(x_1, \dots, x_m) \mapsto x_m]$. Формально можно записать так:

$$\begin{aligned} A_i^{m-1}(f_{m-1}) \cdot x_m := \{h \in \mathcal{F}_m | \exists g \in A_i^{m-1}(f_{m-1}) : \\ h(x_1, \dots, x_m) = g(x_1, \dots, x_{m-1}) \cdot x_m\}. \end{aligned}$$

Тогда из цепочки (1) получаем представление пространства $A_d^n(f_n)$ в виде прямой суммы векторных пространств:

$$A_d^n(f_n) = A_d^{n-1}(f_{n-1}) \oplus A_{d-1}^{n-1}(f_{n-1}) \cdot x_n. \tag{2}$$

Сумма прямая, поскольку

- $A_d^{n-1}(f_{n-1}) \subset \mathcal{F}_n$ содержит только функции, для которых переменная x_n фиктивна
- в то время, как для каждой ненулевой функции из $A_{d-1}^{n-1}(f_{n-1}) \cdot x_n$ переменная x_n существенна.

Далее аналогично разлагаем в прямую сумму пространства $A_d^{n-1}(f_{n-1})$ и $A_{d-1}^{n-1}(f_{n-1})$. И т.д., обобщая (2), для каждого $m \in \{k, \dots, n\}$ и каждого $i \in \{1, \dots, d\}$ используем разложение

$$A_i^m(f_m) = A_i^{m-1}(f_{m-1}) \oplus A_{i-1}^{m-1}(f_{m-1}) \cdot x_m. \tag{3}$$

Нижние индексы для буквы A в обозначении пространств аннигиляторов на каждом шаге разложения (3) могут только уменьшаться (от d до 0). Особым случаем является разложение $A_0^m(f_m)$, когда нельзя уменьшить нижний индекс. Но в этом случае (если f не тождественно равна нулю)

$$A_0^m(f_m) = \{0\}. \tag{4}$$

Соединяя представления (3) и (4), окончательно получаем

$$A_d^n(f) = \bigoplus_{\substack{u=(u_k,\dots,u_n)\in\mathbb{F}_2^{n-k+1}:\\ |u|<d}} A_{d-|u|}^{k-1}(f_{k-1}) \cdot \underbrace{x_k^{u_k} \cdot \ldots \cdot x_n^{u_n}}_{n-k+1}, \tag{5}$$

где $|u|$ — количество единиц в векторе $u \in \mathbb{F}_2^{n-k+1}$.

Итого, имея для ненулевой функции f_{k-1} пространства её аннигиляторов всех степеней от 1 до d, мы можем выразить пространство $A_d^n(f)$ с помощью представления (5), откуда можно делать выводы о размерности пространства $A_d^n(f)$ и его структуре.

Литература

[1] Баев В.В. *О сложности поиска аннигиляторов низкой степени для булевых функций*. Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. Интеллектуальный Центр МГУ. 2-3 ноября 2005 г. - М: МЦНМО, 2006. стр. 198-204.

[2] Баев В.В. *О некоторых алгоритмах построения аннигиляторов низкой степени для булевых функций*, журнал Дискретная Математика, том 18, выпуск 3, 2006. стр. 138-151.

[3] Баев В.В. *Некоторые нижние оценки на алгебраическую иммунность функций, заданных своими трэйс формами*. Дискретные модели в теории управляющих систем: VII Международная конференция, Покровское, 4-6 марта 2006 г.: Труды. - М.: МАКС Пресс, 2006. стр. 25-29.

[4] Ботев А.А. *Об алгебраической иммунности новых конструкций фильтров с высокой нелинейностью*, Дискретные модели в теории управляющих систем: VI Международная конференция: Москва, 7-11 декабря 2004 г. Труды. М.: Издательский отдел Факультета ВМиК МГУ им. М.В. Ломоносова, 2004. с. 227-230.

[5] Armknecht F. *Improving Fast Algebraic Attacks*, Fast Software Encryption 2004, LNCS 3017, pp. 65 - 82, Springer, 2004.

[6] Armknecht F. *On the Existence of low-degree Equations for Algebraic Attacks*, Cryptology ePrint Archive: Report 2004/185, http://eprint.iacr.org/2004/185

[7] Courtois N., Meier W. *Algebraic Attacks on Stream Ciphers with Linear Feedback*, Eurocrypt 2003, LNCS 2656, pp. 345-359, Springer, 2003.

[8] Courtois N. *Fast algebraic attacks on stream ciphers with linear feedback*, Crypto 2003, LNCS 2729, pp. 176–194. Springer, 2003.

[9] Hawkes P., Rose G. *Rewriting Variables: the Complexity of Fast Algebraic Attacks on Stream Ciphers*, Crypto 2004, LNCS 3152, pp. 390 - 406, Springer, 2004.

[10] Meier W., Pasalic E., Carlet C. *Algebraic Attacks and Decomposition of Boolean Functions*, Eurocrypt 2004, LNCS 3027, pp. 474-491, Springer, 2004.

Свойства кубических бент-функций специального вида

С. В. Агиевич

Пусть V_n — n-мерное векторное пространство над полем $\mathbb{F}_2$, $\mathcal{F}_n$ — множество всех функций $V_n \to \mathbb{F}_2$. Функцию $f \in \mathcal{F}_n$ от $\mathbf{x} = (x_1, \ldots, x_n)$ будем задавать многочленом Жегалкина с переменными x_i, $\deg f$ — степень данного многочлена. Аффинно эквивалентными назовем функции, получаемые друг из друга невырожденным аффинным преобразованием переменных и добавлением аффинной ($\deg \leqslant 1$) функции.

Пусть $\mathcal{B}_n \subset \mathcal{F}_n$ — множество всех бент-функций от n переменных. Бент-функции были введены Ротхаузом в работе [5] и впоследствии нашли применение в криптографии и теории кодирования. Известно, что аффинно эквивалентные функции являются (либо не являются) бент-функциями одновременно. В связи с этим интерес представляет следующая задача: для заданного n найти полную систему представителей классов аффинной эквивалентности $\mathcal{B}_n$.

Сложность аффинной классификации существенно зависит от степеней представителей классов эквивалентности. Классификация квадратичных ($\deg = 2$) функций проводится без труда с использованием теоремы Диксона (см., напр., [2]). Однако, классификация уже кубических ($\deg = 3$) бент-функций представляет значительные трудности.

Мы рассмотрели кубические функции $f \in \mathcal{B}_{n+2}$ следующего вида:

$$\begin{aligned} &f(u, v, \mathbf{x}) = uva(\mathbf{x}) + ub(\mathbf{x}) + vc(\mathbf{x}) + d(\mathbf{x}), \\ &\mathbf{x} \in V_n, \quad \deg a \leqslant 1, \quad \deg b, c, d \leqslant 2. \end{aligned} \tag{1}$$

Нами получены ограничения на функции a, b, c и d, которые могут быть использованы для определения канонических представителей классов аффинной эквивалентности.

Перейдем к результатам, прежде напомнив несколько определений. Функция $g \in \mathcal{F}_n$ — сбалансирована, если она принимает значения 0 и 1 одинаковое количество раз. Если g — квадратичная функция, то ее можно записать в матричной форме: $g(\mathbf{x}) = \mathbf{x}A\mathbf{x}^{\mathrm{T}} + \alpha$, где A — матрица порядка n, $\alpha \in \mathbb{F}_2$. При этом $B = A + A^{\mathrm{T}}$ называется симплектической матрицей g, а ранг B — рангом g.

Предложение 1. *Пусть бент-функция f имеет вид* (1), *где* $a = 0$. *Тогда f аффинно эквивалентна функции*

$$uv + ub^*(\mathbf{x}) + vc^*(\mathbf{x}) + d^*(\mathbf{x}), \quad \deg b^*,\ c^*,\ d^* \leqslant 2,$$

причем квадратичные части функций b и b^*, c и c^*, d и d^* совпадают.

Предложение 2. *Если f — бент-функция вида* (1) *и* $a = 1$, *то* $bc + d \in \mathcal{B}_n$.

Введем в расмотрение сужения f на $\mathbf{x}$:

$$\begin{aligned} f_1(\mathbf{x}) &= f(0,\ 0,\ \mathbf{x}) = d(\mathbf{x}),\\ f_2(\mathbf{x}) &= f(0,\ 1,\ \mathbf{x}) = c(\mathbf{x}) + d(\mathbf{x}),\\ f_3(\mathbf{x}) &= f(1,\ 0,\ \mathbf{x}) = b(\mathbf{x}) + d(\mathbf{x}),\\ f_4(\mathbf{x}) &= f(1,\ 1,\ \mathbf{x}) = a(\mathbf{x}) + b(\mathbf{x}) + c(\mathbf{x}) + d(\mathbf{x}). \end{aligned}$$

Предложение 3. *Если бент-функция f имеет вид* (1), *то справедлив один из случаев*:

A. *Сужения f_1, f_2, f_3, f_4 являются квадратичными функциями ранга n.*

B. *Сужения f_1, f_2, f_3, f_4 являются квадратичными функциями ранга $n - 2$.*

Предложение 4. *Пусть f — бент-функция вида* (1), *справедлив случай* 1 *и B_i — симплектические матрицы сужений f_i, $i = 1, 2, 3, 4$. Тогда $B_1^{-1} + B_2^{-1} + B_3^{-1} + B_4^{-1} = 0$.*

Предложение 5. *Пусть бент-функция f имеет вид* (1) *и справедлив случай* 2. *Тогда функции b, c, $b + c$, $a + b$, $a + c$, $a + b + c$ являются сбалансированными.*

При доказательстве данных результатов существенно использовалось представление бент-функций бент-прямоугольниками (подробнее см. [4]).

Наметим схему использования результатов для поиска канонических форм функций вида (1). Будем предполагать, что кубическая часть f задана и идет речь об уточнении функций a, b, c, d. По кубической части f мы можем определить квадратичные части функций b и c. Далее, если f не содержит мономов uvx_i, то $a = 0$ или $a = 1$. Перейти от $a = 0$ к $a = 1$ можно с помощью предложения 1. Предложение 5 позволяет ограничиться анализом только одного случая 1. С помощью предложения 4 можно уточнить функцию d, а с помощью предложения 2 — функции b и c. Кроме этого, предложение 2 позволяет проверить, может ли бент-функция иметь заданную кубическую часть.

Отметим, что в работе [1] был рассмотрен еще один случай, который подпадает как под ограничения 1, так и под ограничения 2:

A. По крайней мере одна из функций b, c или $b + c$ является аффинной.

В [1] были полностью описаны канонические формы функций, удовлетворяющих 1.

Для демонстрации полученных результатов построим полную систему представителей классов аффинной эквивалентности кубических бент-функций от 6 переменных. Впервые такую систему нашел Ротхауз в работе [5] с помощью компьютерных расчетов.

Пример. Пусть $f(u, v, \mathbf{x})$ — кубическая функция, $\mathbf{x} \in V_4$. Известно (см., напр., [3]), что аффинным преобразованием переменных кубическая часть f может быть приведена к одной из следующих пяти форм:

1	ux_1x_2
2	$u(x_1x_2 + x_3x_4)$
3	$ux_1x_2 + vx_3x_4$
4	$u(x_1x_2 + x_3x_4) + vx_1x_3$
5	$u(x_1x_2 + x_3x_4) + v(x_1x_2 + x_1x_3 + x_2x_4)$

Рассмотрим каждую из них по отдельности.

1, 2. Если кубическая часть f имеет вид ux_1x_2 или $u(x_1x_2 + x_3x_4)$, то справедлив случай 1 и, в соответствии с [1], f аффинно эквивалентна одной из функций:

1	$u(x_1x_2 + v) + x_1x_3 + x_2x_4$
2	$u(x_1x_2 + x_3x_4 + v) + x_1x_4 + x_3(x_2 + x_4)$

3. Пусть кубическая часть f имеет вид $ux_1x_2 + vx_3x_4$. Предположим, что $f \in \mathcal{B}_6$. С учетом предложения 1 можно считать, что f содержит моном uv. Следовательно, применимо предложение 2 и для определяющих f функций b, c и d выполняется: $bc + d \in \mathcal{B}_4$. Но $bc + d$ гарантированно содержит моном $x_1x_2x_3x_4$ и не может являться бент-функцией, поскольку $\mathcal{B}_4$ содержит только квадратичные функции. Полученное противоречие означает, что $f \notin \mathcal{B}_6$.

5. Аналогичным образом устанавливаем, что f с кубической частью $u(x_1x_2 + x_3x_4) + v(x_1x_2 + x_1x_3 + x_2x_4)$ не может являться бент-функцией.

4. Пусть кубическая часть f имеет вид $u(x_1x_2 + x_3x_4) + vx_1x_3$ и $f \in \mathcal{B}_6$. Соответствующая f функция b является квадратичной полноранговой и не может быть сбалансированной. Поэтому f не может удовлетворять ограничениям 2 и остается рассмотреть случай 1.

Пусть B_1 — симплектическая матрица соответствующей f функции d. Тогда, согласно предложению 4, матрицы

$$B_2 = B_1 + \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & & & \end{pmatrix}, \quad B_3 = B_1 + \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & & & \end{pmatrix},$$

$$B_4 = B_1 + \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & & & \end{pmatrix}$$

должны быть обратимы и $B_1^{-1} + B_2^{-1} + B_3^{-1} + B_4^{-1} = 0$. Рассматривая всевозможные матрицы B_1, удовлетворяющие данным ограничениям, находим допустимые функции d (с точностью до аффинных слагаемых):

$$x_1x_2 + x_1x_4 + x_2x_3, \quad x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3,$$
$$x_1x_4 + x_2x_3 + x_3x_4, \quad x_1x_3 + x_1x_4 + x_2x_3 + x_3x_4.$$

Одновременная перестановка переменных пар (x_1, x_3) и (x_2, x_4) переводит последние две функции в первые две. Кроме этого, замена x_4 на $x_4 + x_3$ переводит вторую функцию в первую. Важно, что указанные преобразования переменных не изменяют квадратичные части b и c. Таким образом, достаточно рассмотреть первую функцию

$$d(\mathbf{x}) = x_1x_2 + x_1x_4 + x_2x_3.$$

С помощью предложения 1 добъемся того, что f содержит моном uv, т. е. $a = 1$. Пусть l_b и l_c — аффинные части функций b и c соответственно. С помощью замен x_1 на $x_1 + 1$ и x_3 на $x_3 + 1$ мы можем исключить в l_c мономы x_1 и x_3. Затем с помощью замен x_2 на $x_2 + 1$ и x_4 на $x_4 + 1$ мы можем исключить в l_b мономы x_1 и x_3. Наконец, добавляя к f мономы u или v, мы можем исключить в l_b и l_c свободные члены.

Теперь, применяя предложение 2, мы требуем, чтобы функция

$$(x_1x_2 + x_3x_4 + l_b)(x_1x_3 + l_c) + d$$

являлась бент-функцией от 4 переменных. С учетом предыдущих ограничений на l_b и l_c это возможно только если $l_b = x_2 + x_4$ и $l_c = 0$.

Таким образом, f аффинно эквивалентна функции

4	$uv + u(x_1x_2 + x_3x_4 + x_2 + x_4) + vx_1x_3 + x_1x_2 + x_1x_4 + x_2x_3$

Литература

[1] *Агиевич С. В.* Об аффинной классификации кубических бент-функций. — Национальная академия наук Беларуси. Труды Института математики, 2006. Т. 14, № 1, с. 3–11.

[2] *Мак-Вильямс М. Дж.*, *Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

[3] *Черемушкин А. В.* Методы аффинной и линейной классификации двоичных функций. — В кн.: Труды по дискретной математике. Т. 4. М.: Физматлит, 2001, с. 273–314.

[4] *Agievich S.* On the representation of bent functions by bent rectangles. — In: Probabilistic Methods in Discrete Mathematics: Proceedings of the Fifth International Petrozavodsk Conference (Petrozavodsk, June 1–6, 2000). Utrecht, Boston: VSP, 2002, p. 121–135.

[5] *Rothaus O. S.* On bent functions. — J. Comb. Theory, 1979, Ser. A, v. 20, p. 300–305.

Статистическая атака на комбинирующий генератор гаммы с неравномерным движением в режиме реинициализации начального состояния

А. Н. Алексейчук, Р. В. Проскуровский,
Л. В. Скрыпник

1. Рассмотрим комбинирующий генератор гаммы (ГГ), состоящий из n двоичных линейных регистров сдвига (ЛРС) с примитивными многочленами обратной связи, степени которых равны соответственно $m_1, \ldots, m_n$, и уравновешенной комбинирующей булевой функции $f = f(z_1, \ldots, z_n)$ [1]. Предположим, что закон изменения состояний ЛРС является неравномерным и определяется последовательностью неотрицательных целочисленных векторов $\varepsilon(i) = (\varepsilon_1(i), \ldots, \varepsilon_n(i))$, $i = 0, 1, \ldots$, вырабатываемых (программным или случайным способом) некоторым дополнительным устройством — блоком управления движением данного ГГ. Для любых $j \in \overline{1, n}$, $i = 0, 1, \ldots$ величина сдвига j-го ЛРС в i-м такте равна $\varepsilon_j(i)$.

Обозначим $x_j^{(0)} = (x_j^{(0)}(0), \ldots, x_j^{(0)}(m_j - 1))$ начальное состояние (НС) j-го ЛРС, $x_j^{(0)}(0), x_j^{(0)}(1), \ldots$ — линейную рекуррентную последовательность, вырабатываемую j-м ЛРС в режиме равномерного движения по указанному НС, $j \in \overline{1, n}$. Положим

$$\delta_j(0) = 0, \ \delta_j(i) = \sum_{k=0}^{i-1} \varepsilon_j(k), \ i = 1, 2, \ldots, \ j \in \overline{1, n}. \tag{1}$$

Знак выходной последовательности генератора в i-м такте определяется по формуле

$$\gamma_i = f(x_1^{(0)}(\delta_1(i)), \ldots, x_n^{(0)}(\delta_n(i))), \ i = 0, 1, \ldots .$$

Предположим, что рассматриваемый ГГ функционирует в режиме реинициализации начального состояния [1, 2]. В этом случае по исходному НС $x^{(0)} = (x_1^{(0)}, \ldots, x_n^{(0)})$ генератора и последовательности двоичных векторов $c^{(1)}, \ldots, c^{(t)}$, называемых векторами инициализации, $c^{(l)} = (c_1^{(l)}, \ldots, c_n^{(l)})$,

$c_j^{(l)} = (c_j^{(l)}(0), \ldots, c_j^{(l)}(m_j - 1))$, $c_j^{(l)}(i) \in \{0, 1\}$, $j \in \overline{1, n}$, $i \in \overline{0, m_j - 1}$, $l \in \overline{1, t}$, формируются новые начальные состояния ГГ $x^{(l)} = (x_1^{(l)}, \ldots, x_n^{(l)})$, где $x_j^{(l)} = x_j^{(0)} \oplus c_j^{(l)}$, $j \in \overline{1, n}$, $l \in \overline{1, t}$, по которым вырабатывается t выходных последовательностей

$$\gamma_i^{(l)} = f(x_1^{(0)}(\delta_1^{(l)}(i)) \oplus c_1^{(l)}(\delta_1^{(l)}(i)), \ldots, x_n^{(0)}(\delta_n^{(l)}(i)) \oplus c_n^{(l)}(\delta_n^{(l)}(i))), \; i = 0, 1, \ldots, \tag{2}$$

$l \in \overline{1, t}$. (Здесь и далее символы $c_j^{(l)}(0)$, $c_j^{(l)}(1)$, ... обозначают знаки линейной рекурренты, вырабатываемой j-м ЛРС при равномерном движении по начальному состоянию $c_j^{(l)}$, $j \in \overline{1, n}$, $l \in \overline{1, t}$. Векторы $\delta^{(l)}(i) \stackrel{\text{def}}{=} (\delta_1^{(l)}(i), \ldots, \delta_n^{(l)}(i))$, $i = 0, 1, \ldots$, $l \in \overline{1, t}$ определяются в соотвествии с законом функционирования блока управления движением ГГ по формулам, аналогичным равенствам (1)).

Задача криптоанализа комбинирующего ГГ в режиме реинициализации начального состояния заключается в построении алгоритмов восстановления вектора $x^{(0)}$ по известным многочленам обратной связи ЛРС, функции f, отрезкам выходных последовательностей (2), векторам $c^{(1)}, \ldots, c^{(t)}$ и априорной информации о законе функционирования блока управления движением данного генератора гаммы.

2. Зафиксируем натуральное число i_0 и вектор $a = (a_1, \ldots, a_n) \in \mathbf{N}_0^n$.

Предлагаемая статистическая атака на комбинирующий ГГ с неравномерным движением имеет целью восстановление вектора

$$x^{(0)}(a) = (x_1^{(0)}(a_1), \ldots, x_n^{(0)}(a_n)) \tag{3}$$

по набору

$$\Gamma_{t,i_0} = \gamma_{i_0}^{(1)}, \gamma_{i_0}^{(2)}, \ldots, \gamma_{i_0}^{(t)} \tag{4}$$

знаков, выработанных генератором в момент времени i_0 при начальных состояниях $x^{(1)}, x^{(2)}, \ldots, x^{(t)}$ соответственно. Эта атака является базовой и, как показано ниже, позволяет (при определенных вероятностных допущениях) восстанавливать вектор (3) с бесконечно малой при $t \to \infty$ средней вероятностью ошибки. Проводя такую атаку многократно, при различных значениях a и i_0, можно, в принципе, восстановить достаточное количество знаков линейных рекуррент $x_j^{(0)}(0)$, $x_j^{(0)}(1)$, ... ($j \in \overline{1, n}$), по которым затем найти начальное состояние $x^{(0)}$ генератора, решая соответствующую систему булевых линейных уравнений с искаженной правой частью. Отметим, что в идейном плане описанная общая схема восстановления начального состояния комбинирующего ГГ с неравномерным движением близка к методу криптоанализа шифра A5/1, предложенному в [3].

3. Перейдем к изложению предлагаемой статистической процедуры восстановления вектора (3) по последовательности (4). Предварительно опишем вероятностную модель функционирования ГГ в режиме реинициализации начального состояния.

Предположим, что в выражении (2) при $i = i_0$ векторы $\delta^{(l)}(i_0)$, $l \in \overline{1, t}$, являются случайными элементами, распределенными на конечном множестве $\Delta \subseteq \mathbf{N}_0^n$ по известному закону

$$\mathbf{P}\{\delta^{(l)}(i_0) = u\} = p_\delta(u), \ u \in \Delta, \ l \in \overline{1, t}. \tag{5}$$

Предположим также, что $a = (a_1, \ldots, a_n) \in \Delta$.

Для любого $m \in \mathbf{N}$ обозначим V_m пространство двоичных векторов длины m над полем из двух элементов. Зафиксирум произвольное $L \in \mathbf{N}$ такое, что $\Delta \subseteq \{0, 1, \ldots, L-1\}^n$, и введем в рассмотрение множества

$$U_s = \{(y_j(i) : j \in \overline{1, n}, \ i \in \overline{0, L-1}) \in V_{nL} | (y_1(a_1), \ldots, y_n(a_n)) = s\}, \ s \in V_n. \tag{6}$$

Заметим, что, поскольку векторы $c^{(l)}$, $l \in \overline{1, t}$, и многочлены обратной связи ЛРС известны криптоаналитику, он может вычислить значение $c_j^{(l)}(i)$ для любых $j \in \overline{1, n}$, $l \in \overline{1, t}$, $i = 0, 1, \ldots$. В частности, для фиксированного выше вектора a криптоаналитик может найти двоичные векторы

$$g^{(l)}(a) = (c_1^{(l)}(a_1), \ldots, c_n^{(l)}(a_n)), \ l \in \overline{1, t}. \tag{7}$$

Сормулируем ряд дополнительных предположений относительно процесса функционирования рассматриваемого ГГ. А именно, предположим, что

(а) упорядоченный набор $(x_j^{(0)}(i) : j \in \overline{1, n}, \ i \in \overline{0, L-1})$ является реализацией случайного вектора $X = (X_j(i) : j \in \overline{1, n}, \ i \in \overline{0, L-1})$, распределеного по равномерному закону на множестве V_{nL};

(б) векторы (7) фиксированы (не случайны), и для любого $l \in \overline{1, t}$ упорядоченный набор $(c_j^{(l)}(i) : j \in \overline{1, n}, \ i \in \overline{0, L-1})$ является реализацией случайного вектора $Z^{(l)}$ с равномерным законом распределения на множестве $U_{g^{(l)}(a)}$ вида (6);

(в) случайные векторы X, $Z^{(l)}$, $\delta^{(l)}(i_0)$, $l \in \overline{1, t}$, независимы в совокупности.

При сделанных предположениях задачу восстановления вектора (3) можно сформулировать следующим образом: для данных a, i_0 требуется построить критерий различения по наблюдаемой последовательности (4) 2^n гипотез

$$H_s : X(a) \stackrel{\text{def}}{=} (X_1(a_1), \ldots, X_n(a_n)) = s, \ s \in V_n. \tag{8}$$

Заметим, что в силу предположения 2а априорные вероятности гипотез (8) одинаковы и равны 2^{-n}. Оптимальным критерием различения указанных гипотез является байесовский критерий [4], который, в рассматриваемом случае, заключается в принятии по реализации $\gamma_1, \ldots, \gamma_t$ случайной последовательности (4) гипотезы H_{s^*} такой, что вектор $s^* = s^*(\gamma_1, \ldots, \gamma_t) \in V_n$ является точкой максимума функции

$$\mathbf{P}_s\{\Gamma_{t,i_0} = \gamma_1, \ldots, \gamma_t\} = \mathbf{P}\left(\Gamma_{t,i_0} = \gamma_1, \ldots, \gamma_t | X(a) = s\right), \; s \in V_n.$$

Сформулируем теорему, устанавливающую явное выражение вероятности

$$\mathbf{P}_s\{\gamma_{i_0}^{(l)} = \gamma\} = \mathbf{P}\left(\gamma_{i_0}^{(l)} = \gamma | X(a) = s\right), \; \gamma \in \{0, \; 1\}, \; l \in \overline{1, \; t}, \; s \in V_n.$$

Обозначим

$$\rho_{f,a}(x) = 2^{-n} \sum_{y \in V_n \setminus \{0\}} (-1)^{xy} \hat{f}(y) \pi_\delta(a; \; y), \; x \in V_n, \tag{9}$$

где $\hat{f}(y) = \sum_{x \in V_n} (-1)^{f(x) \oplus xy}$ — преобразование Уолша—Адамара функции f,

$$\pi_\delta(a; \; y) = \sum_{u \in \Delta(a;y)} p_\delta(u), \; y \in V_n \setminus \{0\}, \tag{10}$$

$$\Delta(a; \; y) = \{u = (u_1, \ldots, u_n) \in \Delta \mid \forall \, j \in \overline{1, \; n} : (y_j = 1) \Rightarrow (u_j = a_j)\}.$$

Теорема 1. *Пусть $s \in V_n$ и при указанных выше предположениях 2а, 2б, 2в справедлива гипотеза H_s. Тогда члены случайной последовательности* (4) *независимы в совокупности, и для любого $l \in \overline{1, \; t}$ выполняется равенство*

$$\mathbf{P}_s\{\gamma_{i_0}^{(l)} = \gamma\} = \frac{1}{2}\left(1 + (-1)^\gamma \rho_{f,a}(s \oplus g^{(l)}(a))\right), \; \gamma \in \{0, \; 1\}. \tag{11}$$

Итак, опираясь на теорему 1, можно предложить следующую статистическую процедуру восстановления вектора (3) по наблюдаемой реализации $\gamma_1, \ldots, \gamma_t$ случайной последовательности (4):

1) вычислить значения (7) по известным векторам инициализации и многочленам обратной связи ЛРС комбинирующего ГГ;

2) для каждого $s \in V_n$ вычислить сумму

$$\sigma_s(\gamma_1, \ldots, \gamma_t) = \sum_{l=1}^{t} \ln \mathbf{P}_s\{\gamma_{i_0}^{(l)} = \gamma_l\},$$

используя формулы (9), (10), (11);

3) положить $x^{(0)}(a) = s^*$, где s^* — произвольный элемент множества V_n, удовлетворяющий условию $\sigma_{s^*}(\gamma_1, \ldots, \gamma_t) = \max_{s \in V_n}\{\sigma_s(\gamma_1, \ldots, \gamma_t)\}$.

4. Обозначим

$$\lambda_t = 2^{-n} \sum_{s \in V_n} \mathbf{P}\{s^*(\Gamma_{t,i_0}) \neq s\}$$

среднюю вероятность ошибочного восстановления вектора (3) с использованием описанной статистической процедуры. Положим

$$\rho(f, a) = \max_{x \in V_n} |\rho_{f,a}(x)|, \ \mu(f, a) = \min_{\substack{x,y \in V_n: \\ x \neq y}} |\rho_{f,a}(x) - \rho_{f,a}(y)|.$$

Теорема 2. *Пусть*

$$\rho(f, a) < 1. \tag{12}$$

Тогда для любого натурального t и произвольной последовательности двоичных векторов (7) *справедливо неравенство*

$$\lambda_t \leqslant (2^n - 1) \exp\left\{-\frac{t}{8}\mu(f, a)^2(1 - \rho(f, a)^2)^2\right\}.$$

В частности, если $\mu(f, a) > 0$, то при выполнении условия (12) $\lim_{t \to \infty} \lambda_t = 0$.

5. Описанную выше атаку на комбинирующий ГГ нетрудно модифицировать таким образом, чтобы уменьшить число проверяемых гипотез.

Пусть, например, $f(z_1, \ldots, z_n) = z_1 \oplus \ldots \oplus z_n$ (эта функция используется в конструкции ГГ шифра A5/1). Сохраняя введенные выше обозначения, положим

$$W_\nu = \{(y_j(i) : j \in \overline{1, n}, \ i \in \overline{0, L-1}) \in V_{nL} | y_1(a_1) \oplus \ldots \oplus y_n(a_n) = \nu\},$$
$$\nu \in \{0, \ 1\}, \tag{13}$$

$$h^{(l)}(a) = c_1^{(l)}(a_1) \oplus \ldots \oplus c_n^{(l)}(a_n), \ l \in \overline{1, t}. \tag{14}$$

Сформулируем следующее предположение:

(б′) значения (14) фиксированы (не случайны), и для любого $l \in \overline{1, t}$ упорядоченный набор $(c_j^{(l)}(i) : j \in \overline{1, n}, \ i \in \overline{0, L-1})$ является реализацией случайного вектора $Z^{(l)}$ с равномерным законом распределения на множестве $W_{h^{(l)}(a)}$ вида (13).

Обозначим $\tilde{\lambda}_t$ среднюю вероятность ошибки байесовского критерия для проверки по наблюдаемой последовательности (4) гипотез

$$H_0 : X_1(a_1) \oplus \ldots \oplus X_n(a_n) = 0, \ H_1 : X_1(a_1) \oplus \ldots \oplus X_n(a_n) = 1. \tag{15}$$

Теорема 3. *При выполнении предположений* 2*а*, 5, 2*в для любого натурального* t *справедливо неравенство*

$$\tilde{\lambda}_t \leqslant \exp\left\{-\frac{t}{2}p_\delta(a)^2\right\}.$$

Отметим, что для проверки гипотез (15) можно использовать также последовательный критерий А. Вальда [4]. Результаты моделирования статистической атаки на генератор гаммы шифра A5/1 с использованием последовательного критерия показывают, что для различения указанных гипотез с вероятностью 0,9 требуется, в среднем, в 4 раза меньше векторов инициализации по сравнению с критерием Неймана — Пирсона, который применяется в [3].

Литература

[1] Фомичев В. М. Дискретная математика и криптология. М.: ДИАЛОГ-МИФИ, 2003. 400 с.

[2] Armknecht F., Lano J., Preneel B. Extending the resynchronization attack. `http://eprint.iacr.org/2004/232`.

[3] Ekdahl P., Johansson T. Another attack on A5/1. IEEE Trans. on Inform. Theory. 2003. Vol. IT-49. № 1. P. 284–289.

[4] Боровков А. А. Математическая статистика. М.: Наука., 1984. 472 с.

Выявление зависимостей высокого порядка на основе модели (s, r)

Ю. С. Харин, А. И. Петлицкий

1. Введение

Важнейшей проблемой криптографической защиты информации является статистическое тестирование псевдослучайных последовательностей $x_t \in A = \{0, 1, \ldots, N-1\}$, $N > 1$, $t \in \mathbf{N}$ [1, 2]. Наиболее актуальной и трудной задачей статистического тестирования является выявление стохастических зависимостей высокого порядка $s \geqslant 32$ в выходных последовательностях криптографических генераторов. С целью снижения вычислительной сложности алгоритмов статистического тестирования для решения этой задачи необходимы «малопараметрические» модели стохастических зависимостей высокого порядка в случайных последовательностях. Среди таких моделей известны бинарная авторегрессия [3], модель Джекобса—Льюиса [4], MTD-модель Рафтери [5], цепь Маркова с переменным порядком [6]. В данном докладе для выявления стохастических зависимостей высокого порядка используется новая «малопараметрическая» модель — цепь Маркова s-го порядка с r частичными связями (s, r), предложенная в [7].

2. Модель (s, r) и ее свойства

Пусть x_t — однородная цепь Маркова s-го порядка на (Ω, F, P) с некоторой $(s+1)$-мерной матрицей вероятностей переходов $P = (p_{i_1, \ldots, i_{s+1}})$, $i_1, \ldots, i_{s+1} \in A$; $r \in \{1, \ldots, s\}$ — параметр, который назовем числом связей; $M_r^0 = (m_1^0, \ldots, m_r^0) \in \mathrm{M}$ — произвольный целочисленный r-вектор с упорядоченными компонентами $1 = m_1^0 < m_2^0 < \ldots < m_r^0 \leqslant s$, который назовем шаблоном связей; M — множество всевозможных таких векторов

)Результаты этого доклада получены при финансовой поддержке в рамках Государственной программы фундаментальных исследований Республики Беларусь «Математические модели».

с r компонентами, имеющее мощность $\mathrm{K} = |\mathrm{M}| = \mathrm{C}_{s-1}^{r-1}$; $Q^0 = (q^0_{j_1,\ldots,j_{r+1}})$, $j_1, \ldots, j_{r+1} \in A$, — некоторая $(r+1)$-мерная стохастическая матрица.

Цепь Маркова x_t называется [7] цепью Маркова s-го порядка с r частичными связями и обозначается (s, r), если ее вероятности одношаговых переходов имеют вид:

$$p_{i_1,\ldots,i_s,i_{s+1}} = q^0_{i_{m_1^0},\ldots,i_{m_r^0},i_{s+1}}, \ i_1, \ldots, i_{s+1} \in A. \tag{1}$$

Соотношение (1) означает, что вероятность перехода процесса в состояние i_{s+1} в момент времени $t > s$ зависит не от всех s предыдущих состояний процесса $i_1, \ldots, i_s$, а лишь от r избранных состояний $i_{m_1^0}, \ldots, i_{m_r^0}$. Таким образом, вместо $D = N^s(N-1)$ параметров модель (1) полностью определяется $d = N^r(N-1) + r - 1$ параметрами Q^0, M_r^0. Заметим, что если $s = r$, $M_r^0 = (1, \ldots, s)$, то $P = Q^0$ и (s, s) есть цепь Маркова s-го порядка [8].

Примем обозначения: $X_n = (x_1, \ldots, x_n) \in A^n$ — наблюдаемая реализация длительности $n > s$; $J_s = (j_1, \ldots, j_s) = (J_{s-1}, j_s) \in A^s$ — мультииндекс s-го порядка; $S_t(X_n; M_r) = (x_{t+m_1-1}, \ldots, x_{t+m_r-1}) \in A^r$ — функция $A^n \times \mathrm{M} \to A^r$, которую условимся называть селектором r-го порядка с параметрами $M_r \in \mathrm{M}$ и $t \in \{1, 2, \ldots, n-s+1\}$; $\mathbf{I}\{B\} \in \{0, 1\}$ — индикатор события B; $\Pi_{K_s} = \mathbf{P}\{X_s = K_s\}$ — начальное s-мерное распределение вероятностей (s, r);

$$\nu_{r+1}(J_{r+1}; M_r) = \sum_{t=1}^{n-s} \mathbf{I}\{S_t(X_n; M_{r+1}) = J_{r+1}\}$$

— частота $(r+1)$-граммы $J_{r+1} \in A^{r+1}$ для шаблона $M_{r+1} = \{M_r, s+1\}$, удовлетворяющая условию нормировки: $\sum\limits_{J_{r+1} \in A^{r+1}} \nu_{r+1}(J_{r+1}; M_r) \equiv n - s$. Условимся, что если вместо какого-то индекса стоит точка, то это означает суммирование по всем возможным значениям этого индекса: $\nu_{r+1}(J_r\cdot; M_r) = \sum\limits_{j_{r+1} \in A} \nu_{r+1}(J_{r+1}; M_r)$, $\nu_{r+1}(\cdot j_{r+1}; M_r) = \sum\limits_{J_r \in A^r} \nu_{r+1}(J_{r+1}; M_r)$.

Теорема 1. (s, r), *определяемая* (1), *эргодична тогда и только тогда, когда найдется целое число* $l \geqslant 0$ *такое, что*

$$\min_{J_s, J_s' \in A^s} \sum_{K_l \in A^l} \prod_{i=1}^{s+l} q^0_{S_i((J_s, K_l, J_s'); M^0_{r+1})} > 0.$$

Следствие 1. *Если* $\min_{J_{r+1}} q^0_{J_{r+1}} > 0$, *то* (s, r) *является эргодической.*

3. Идентификация модели (s, r)

Рассмотрим задачу построения оценок максимального правдоподобия (ОМП) $\hat{M}_r$ шаблона $M_r^0 \in \mathrm{M}$ и $\hat{Q}$ стохастической матрицы Q^0 по наблюдаемой реализации длительности $n > s$: $X_n = (x_1, \ldots, x_n) \in A^n$. На основе подстановочного принципа строится информационный функционал $\hat{I}_{r+1}(M_r)$, т. е. выборочная оценка количества информации по Шенному, содержащейся в r-грамме $S_t(X_n;\, M_r)$ о будущем символе $x_{t+1} \in A$:

$$\hat{I}_{r+1}(M_r) = \sum_{J_{r+1} \in A^{r+1}} \frac{\nu_{r+1}(J_{r+1};\, M_r)}{n-s} \ln \frac{(n-s)\nu_{r+1}(J_{r+1};\, M_r)}{\nu_{r+1}(J_r\cdot;\, M_r)\nu_{r+1}(\cdot j_{r+1};\, M_r)}.$$

Теорема 2. *ОМП* $\hat{M}_r$, $\hat{Q} = (\hat{q}_{J_{r+1}})$, $J_{r+1} \in A^{r+1}$, *параметров* M_r^0, Q^0 *определяются следующими соотношениями*:

$$\hat{M}_r = \arg\max_{M_r \in \mathrm{M}} \hat{I}_{r+1}(M_r),$$

$$\hat{q}_{J_{r+1}}(\hat{M}_r) = \begin{cases} \nu_{r+1}(J_{r+1};\, \hat{M}_r)/\nu_{r+1}(J_r\cdot;\, \hat{M}_r), \text{ если } \nu_{r+1}(J_r\cdot;\, \hat{M}_r) > 0, \\ 1/N, \text{ если } \nu_{r+1}(J_r\cdot;\, \hat{M}_r) \equiv 0. \end{cases} \tag{2}$$

Обозначим: $\Pi^*_{K_s}$, $K_s \in A^s$, — стационарное распределение вероятностей (s, r);

$$\mu_{r+1}(J_{r+1};\, M_r, M_r^0) = \mathbf{I}\{S_t(X_n;\, M_{r+1}) = J_{r+1}\} = \\ = \sum_{K_{s+1} \in A^{s+1}} \mathbf{I}\{S_1(K_{s+1};\, M_{r+1}) = J_{r+1}\} \Pi^*_{K_s} p_{K_{s+1}}, \quad J_{r+1} \in A^{r+1},$$

— распределение вероятностей $(r+1)$-граммы для шаблона $M_{r+1} = (M_r, s+1)$.

Теорема 3. *Если* (s, r), *задаваемая* (1), *стационарна и шаблон* $M_r^0 \in M$ *удовлетворяет условию идентифицируемости, то при* $n \to \infty$ *ОМП* $\hat{M}_r$, $\hat{Q}$, *определяемые* (2), *состоятельны*:

$$\hat{M}_r \xrightarrow{\mathrm{P}} M_r^0, \ \hat{Q} \xrightarrow{L_2} Q^0,$$

причем справедливо асимптотическое разложение для вариации оценки $\hat{Q}$:

$$\Delta_n^2(\hat{Q}) = \mathrm{E}\{\|\hat{Q} - Q^0\|^2\} = \sum_{J_{r+1} \in A^{r+1}} \frac{(1 - q^0_{J_{r+1}}) q^0_{J_{r+1}}}{(n-s)\mu_{r+1}(J_r\cdot;\, M_r^0, M_r^0)} + o(1/n).$$

Теорема 4. *Если* (s, r) *является стационарной, то при истинном шаблоне* $M_r = M_r^0$ *и* $n \to \infty$ *случайные величины*

$$\{q^*_{J_{r+1}} = \sqrt{n-s}(\hat{q}_{J_{r+1}}(M_r^0) - q^0_{J_{r+1}}) \mid J_{r+1} \in A^{r+1}\}$$

в совокупности распределены асимптотически нормально с нулевыми математическими ожиданиями и ковариациями:

$$\mathbf{cov}\{q^*_{J_{r+1}}, q^*_{J'_{r+1}}\} = \mathbf{I}\{J_r = J'_r\}\frac{(\mathbf{I}\{j_{r+1} = j'_{r+1}\} - q^0_{J_{r+1}})q^0_{J_{r+1}}}{\mu_{r+1}(J_r\cdot;\, M_r^0,\, M_r^0)}, \quad J_{r+1}, J'_{r+1} \in A^{r+1}.$$

Следствие 2. *В условиях теоремы* 4 *при* $n \to \infty$ *имеет место сходимость по распределению*:

$$\mathbf{P}\left\{\sum_{J_{r+1}:q^0_{J_{r+1}}>0} \nu_{r+1}(J_r\cdot;\, M_r^0)\frac{(\hat{q}_{J_{r+1}}(M_r^0) - q^0_{J_{r+1}})^2}{q^0_{J_{r+1}}} \leqslant z\right\} \to G_L(z),\ \ z \geqslant 0,$$

где $G_L(\cdot)$ — *функция* χ^2-*распределения с* $L = \sum\limits_{J_r \in A^r}(|D_{J_r}| - 1)$ *степенями свободы*, $D_{J_r} = \{j_{r+1} \in A : q^0_{J_{r+1}} > 0\}$.

Используя следствие 2 построен критерий статистической проверки гипотез H_0: $Q^0 = Q_0$ против альтернативы общего вида $H_1 = \bar{H}_0$, где $Q_0 = (q_{0J_{r+1}})$ — некоторая заданная стохастическая матрица. Решающее правило заданного асимптотического размера $\varepsilon \in (0, 1)$ имеет вид:

$$\text{принимается}\ \{H_0,\ \text{если}\ \rho \leqslant \Delta_\varepsilon;\ H_1,\ \text{если}\ \rho > \Delta_\varepsilon\},$$

где $\rho = \sum\limits_{J_{r+1}} \mathbf{I}\{q_{0J_{r+1}} > 0\}\nu_{r+1}(J_r\cdot;\, M_r^0)(\hat{q}_{J_{r+1}}(M_r^0) - q_{0J_{r+1}})^2/q_{0J_{r+1}}$, Δ_ε — квантиль уровня $1 - \varepsilon$ стандартного χ^2_L-распределения.

Для вычисления оценки $\hat{M}_r$ шаблона M_r^0 согласно (2) при известном истинном значении r^0 числа связей r предлагаются два алгоритма: $_1$ — алгоритм полного перебора значений целевой функции (2); $_2$ — алгоритм «наращивания шаблона», обеспечивающий сокращение перебора.

Алгоритм $_2$ «наращивания шаблона» заключается в последовательном вычислении шаблонов: $\hat{M}_{r_-}, \ldots, \hat{M}_{r^0}$, где $r_- \in \{1, \ldots, r^0\}$ — наименьший размер шаблона, задаваемый исходя из имеющихся вычислительных ресурсов. Этот подход аналогичен «алгоритму расширения пространства признаков» в задачах распознавания образов. Наибольшее быстродействие алгоритма $_2$, очевидно, достигается при $r_- = 1$.

В случае, когда r^0 известно с точностью до числового промежутка: $r_- \leqslant r^0 \leqslant r_+$, $1 \leqslant r_- < r_+ \leqslant s$, для совместного оценивания r^0, M_r^0 предлагается алгоритм $_3$ «сокращения шаблона». Вначале при $r = r_+$ алгоритмом

$_1$ вычисляется начальный шаблон $\hat{M}_{r_+}$ r_+-го порядка; затем осуществляется «сокращение» этого шаблона до r_--го порядка. Затем на основе $\{\hat{M}_r,\ \hat{I}_{r+1}(\hat{M}_r):\ r \in \{r_-, \ldots, r_+\}\}$ строится искомая оценка $\hat{M}_{\hat{r}}$, где оценки $\hat{s}$ и $\hat{r}$ удовлетворяют следующему соотношению:

$$h(\hat{s}, \hat{r}) = \min_{s_1 \leqslant \bar{s} \leqslant s_2,\ r_-(s) \leqslant \bar{r} \leqslant r_+(s)} h(\bar{s}, \bar{r}), \tag{3}$$

где $h(s, r) = -\sum\limits_{J_{r+1} \in A^{r+1}} \nu_{r+1}(J_{r+1};\ \hat{M}_r) \ln \hat{q}_{J_{r+1}}(\hat{M}_r) + \dfrac{N^r(N-1)}{2} \ln n.$

Теорема 5. *Если* (s, r), *задаваемая* (1), *стационарна и шаблон удовлетворяет условию идентифицируемости, то при* $n \to \infty$ *оценки* $\hat{s}$, $\hat{r}$, *определяемые* (3), *состоятельны.*

Для оценивания порядка s цепи Маркова с частичными связями могут быть применены методы из [9, 10] с использованием теорем 2, 3.

4. Численные результаты

Проведенный на Athlon XP 1600+ анализ быстродействия алгоритмов вычисления шаблона $\hat{M}_r$ дал следующие оценки затрат машинного времени (в секундах):

$$_1 - t^{(1)}_{\text{маш}} \approx 1.19 \cdot 10^{-7} \cdot g(r),$$
$$_2 - t^{(2)}_{\text{маш}} \approx 3.01 \cdot 10^{-7} \Big(g(r_-) + \sum_{i=r_-+1}^{r} (s - i + 1)(N^{i+1} + ni) \Big),$$
$$_3 - t^{(3)}_{\text{маш}} \approx 1.04 \cdot 10^{-7} \Big(g(r_+) + \sum_{i=r_-}^{r_+-1} i(N^{i+1} + ni) \Big),$$

где $g(z) = \mathrm{C}_{s-1}^{z-1} \cdot (N^{z+1} + nz)$. Формульные множители в этих выражениях найдены прямым подсчетом числа основных компьютерных операций каждого алгоритма, а числовые множители находились методом наименьших квадратов на основе выборки экспериментально зарегистрированных затрат машинного времени алгоритмов при различных сочетаниях N, s, r, n, r_-, r_+. По преимуществу в быстродействии алгоритмы упорядочены следующим образом: $_2$, $_1$, $_3$. Так, например, при $N = 2$, $r = 3$, $s = 128$, $n = 500$, $t^{(1)}_{\text{маш}} \approx 13.93$ с, $t^{(2)}_{\text{маш}} \approx 0.93$ с ($r_- = 1$), $t^{(3)}_{\text{маш}} \approx 676.78$ с ($r_- = 3$, $r_+ = 4$), что не противоречит полученным экспериментальным значениям затрат машинного времени: $\hat{t}^{(1)}_{\text{маш}} = 13.70$ с, $\hat{t}^{(2)}_{\text{маш}} = 1.01$ с, $\hat{t}^{(3)}_{\text{маш}} = 616.10$ с.

Авторы глубоко признательны А. М. Зубкову за уточнения постановок задач и критические замечания, способствовавшие улучшению результатов.

Литература

[1] Зубков А. М. Датчики псевдослучайных чисел и их применения // Сб.: Труды II Международной научной конференции «Математика и безопасность информационных технологий». М.: МГУ, 2003. С. 200–206.

[2] Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. Математические и компьютерные основы криптологии. Минск: Новое знание, 2003.

[3] Максимов В. Г. О цепях Маркова, связанных с двоичными регистрами сдвига со случайными элементами // Труды по дискретной математике. 1997. Т. 1. С. 221–226.

[4] Jacobs P. A., Lewis P. A. W. Discrete time series generated by mixtures I: correlational and runs properties // Journal of the Royal Stat. Soc. 1978, no. 1, p. 94–105.

[5] Raftery A. E. A model for high-order Markov chains // Journal of the Royal Stat. Soc. 1985, vol. 47, no. 3, p. 528–539.

[6] Buhlmann P., Wyner A. Variable length Markov chains // The Annals of Statistics. 1999, vol. 27, no. 2, p. 480–513.

[7] Харин Ю. С. Цепи Маркова с r-частичными связями и их статистическое оценивание // Доклады НАН Беларуси. 2004. Т. 48, no. 1. С. 40–44.

[8] Дуб Дж. Вероятностные процессы. М., 1956.

[9] Csiszar I., Shields P. C. The consistency of the BIC Markov order estimator // The Annals of Statistics. 2000, vol. 28, no. 6, p. 1601–1619.

[10] Tong H. Determination of the order of a Markov chain by Akaike's information criterion // Journal Applied Probability. 1975, 12, p. 488–497.

INAR-последовательности и их применение в задачах защиты информации

А. Н. Ярмола, Ю. С. Харин

1. Введение

Генераторы псевдослучайных последовательностей являются неотъемлемой частью поточных криптосистем [1]. Такие криптосистемы используются в системах защиты информации, применяемых в компьютерных сетях, мобильной радиотелефонной связи и электронной торговле. Поэтому актуальной является задача построения псевдослучайных последовательностей (ПСП), удовлетворяющих требованию статистической близости распределений вероятностей фрагментов последовательности к равномерному распределению. Выделяются три основных подхода к построению алгоритмов генерации ПСП [1]: 1) прямые методы построения элементарных ПСП, к которым относятся конгруэнтные генераторы, генераторы Фибоначчи, линейные рекуррентные последовательности (ЛРП) в конечном поле; 2) методы «улучшения» элементарных ПСП, которые заключаются в специальных функциональных преобразованиях этих последовательностей; 3) методы комбинирования алгоритмов генерации. «Улучшение» элементарных ПСП преследует три цели: получение последовательности с более близкими к равномерному распределению распределений вероятностей фрагментов; увеличение периода последовательности; увеличение криптостойкости последовательности. Одним из основных подходов к «улучшению» ПСП является комбинирование ЛРП [2], которое осуществляется с использованием следующих операций: сложение, умножение, прореживание.

В настоящем докладе предлагается модель дискретных временных рядов, построенная на основе модели INAR [3], которая применяется для построения генераторов псевдослучайных последовательностей.

)Работа поддержана ГПФИ (проект ММ-24).

2. Двоичная INAR-последовательность и ее свойства

Модель INAR(m) предложена Эльзаидом и Эль-Ошем [3] в качестве целочисленного аналога модели авторегрессии порядка m для решения задач анализа целочисленных временных рядов $z_t \in \mathbf{Z}_+ = \{0, 1, 2, \ldots\}$, $t = 1, 2, \ldots$:

$$z_t = \sum_{j=1}^{m} p_j \circ z_{t-j} + \eta_t, \quad t = m+1, m+2, \ldots, \tag{1}$$

где $\circ$ — оператор «биномиального прореживания» (binomial thinning): $p_j \circ z_{t-j} = \sum_{i=1}^{z_{t-j}} \xi_{t,i}^{(j)}$, $\{\xi_{t,i}^{(j)} : t = m+1, m+2, \ldots, \ i = 1, 2, \ldots, \ j = 1, \ldots, m\}$ — независимые в совокупности случайные величины Бернулли, $\mathbf{P}\{\xi_{t,i}^{(j)} = 1\} = 1 - \mathbf{P}\{\xi_{t,i}^{(j)} = 0\} = p_j$; $\{\eta_t\}$ — случайные величины, такие что η_t некоррелирована с $z_{t-1}, \ldots, z_{t-m}$, $t = m+1, m+2, \ldots$. С учетом этих обозначений модель (1) принимает вид:

$$z_t = \sum_{j=1}^{m} \sum_{i}^{z_{t-j}} \xi_{t,i}^{(j)} + \eta_t.$$

Используя эту идею модели , построим дискретный аналог модели INAR $x_t \in \mathcal{A}_N = \{0, 1, \ldots, N-1\}$ следующем виде:

$$x_t = \left(\sum_{i=1}^{m} \theta_i \sum_{j=0}^{x_{t-i}} \xi_{(t-1)N+j}^{(i)} \right) \bmod N, \quad t = m+1, m+2, \ldots, \tag{2}$$

где $\{\xi_t^{(i)} \in \{0, 1\}, \quad i = 0, \ldots, m\}$ — выходные последовательности некоторых простейших («элементарных») бинарных генераторов $G_1, \ldots, G_m$; в общем случае $\theta_j \in \mathcal{A}_N$, $\theta_m > 0$. Далее рассматривается специальный случай модели (2): $N = 2$, $\theta_j \in \mathcal{A}_2 = \{0, 1\}$, $j = 1, \ldots, m-1$, $\theta_m = 1$. Обозначим: $r = \sum_{j=1}^{m} \theta_j$ — вес Хэмминга вектора коэффициентов $\theta = (\theta_1, \ldots, \theta_m)'$; $1 \leqslant k_1 < \ldots < k_r \leqslant m \in$ — различные индексы, такие что $\theta_{k_j} = 1$, $j = 1, \ldots, r$, при этом $\theta_j = 0$ при всех других значениях j.

При исследовании вероятностных свойств последовательности (2) в качестве модели для выходных последовательностей $\{\xi_t^{(1)}\}, \ldots, \{\xi_t^{(m)}\}$ «элементарных» генераторов $G_1, \ldots, G_m$ будем использовать последовательности независимых одинаково распределенных случайных величин Бернулли; также будем полагать, что последовательности $\{\xi_t^{(1)}\}, \ldots, \{\xi_t^{(m)}\}$ — незави-

симы,

$$p_j = \frac{1}{2}(1+\varepsilon), \;\; j = 1, \ldots, m, \;\; |\varepsilon| < 1, \tag{3}$$

где $\varepsilon \in (-1;\, 1)$ — величина, характеризующая «степень несовершенства» генераторов $G_1, \ldots, G_m$ (если $\varepsilon = 0$, то $p_1 = \ldots = p_m = 1/2$ и все генераторы $G_1, \ldots, G_m$ порождают «чисто случайные» последовательности).

Исследуем распределение вероятностей последовательности x_t, порождаемой моделью (2), с помощью следующих функционалов, возникающих в задаче дискриминантного анализа цепей Маркова [5]: $\Delta = 2^{-m} \sum\limits_{i_0,\ldots,i_m \in \mathcal{A}_2} |p_{i_0,\ldots,i_m} - 0,5| \geqslant 0$ — среднее уклонение распределения вероятностей одношаговых переходов

$$p_{i_0,\ldots,i_m} = P\{x_t = i_m \mid x_{t-1} = i_{m-1}, \ldots, x_{t-m} = i_0\}$$

от равномерного распределения; $Z_m = \sum\limits_{i_1,\ldots,i_m \in \mathcal{A}_2} |\pi^*_{i_1,\ldots,i_m} - 2^{-m}| \geqslant 0$ — октаэдрическая норма уклонения стационарного m-мерного распределения $\Pi^* = (\pi^*_{i_1,\ldots,i_m})$, $i_1, \ldots, i_m \in \mathcal{A}_2$ от равномерного на $\mathcal{A}_2^m$ распределения. Чем меньше Δ, Z_m, тем выходная последовательность генератора (2) ближе к «чисто случайной последовательности».

Теорема 1. *Если выполнены условия* (3), *то двоичная последовательность* x_t, *определяемая* (2), *является эргодической цепью Маркова порядка* m, *причем*

$$p_{i_0,\ldots,i_m} = (1 + (-1)^{i_m}(-\varepsilon)^{S(i_0,\ldots,i_{m-1})})/2, \tag{4}$$

$$S(i_0, \ldots, i_{m-1}) = \sum_{j=1}^{m} \theta_j (i_{m-j} + 1), \;\; i_0, \ldots, i_m \in \mathcal{A}_2;$$

$$\Delta = |\varepsilon/2|^r (1 + 2|\varepsilon|)^r; \tag{5}$$

$Z_m \leqslant Z_+$, *и для верхней границы* Z_+ *справедливо асимптотическое* ($\varepsilon \to 0$) *разложение*:

$$Z_+ = (1-\varepsilon)(1+|\varepsilon|)^{r-1} \left|\frac{\varepsilon}{2}\right|^r \times$$
$$\times \left(1 + \sum_{j=1}^{m-1} \frac{4^{(r_j - j)}}{(1 + 1/|\varepsilon|)^{r_j}} \prod_{k=1}^{j} (1 + (-\varepsilon)^{\theta_{m-k}})\right) + \mathcal{O}(\varepsilon^{2r}), \tag{6}$$

где $r_j = \sum\limits_{k=1}^{j} \theta_{m-k}$, $j = 1, \ldots, m-1$.

Отметим, что для «элементарной» последовательности $\Delta = |\varepsilon|$, $Z_m = \mathcal{O}(|\varepsilon|)$, следовательно, в силу теоремы 1, несмотря на наличие в после-

довательности (2) стохастических зависимостей, данная последовательность (2) является менее предсказуемой, чем «элементарная» последовательность, и распределения вероятностей фрагментов последовательности (2) ближе к равномерному, чем распределения фрагментов такой же длины для «элементарного» генератора.

При исследовании свойств периодичности последовательности (2), будем полагать что выходные последовательности «элементарных» генераторов $G_1, \ldots, G_m$ — детерминированные периодические последовательности. При этом предположении x_t — также детерминированная периодическая последовательность. Обозначим T_j — период выходной последовательности генератора G_j $(j = 1, \ldots, m)$.

Теорема 2. *Если* $\min\{T_{k_1}, \ldots, T_{k_r}\} > 2$, *то для периода* T^* *двоичной последовательности* x_t, *определяемой* (2), *справедлива оценка сверху*:

$$T^* \leqslant T_{\max} = \operatorname{lcm}\left(\frac{T_{k_1}}{\gcd(T_{k_1}, 2)}, \ldots, \frac{T_{k_r}}{\gcd(T_{k_r}, 2)}\right); \tag{7}$$

причем, если $\{T_{k_j} : j = 1, \ldots, r\}$ — *нечетны и взаимно просты, то в* (7) *достигается верхняя граница.*

3. Применение в задачах защиты информации

Модель (2) может быть использована в качестве комбинирующей функции для построения генератора псевдослучайных последовательностей. Ключом в таком генераторе является составной вектор $(\theta, \eta_{k_1}, \ldots, \eta_{k_r})$, где η_j — ключ «элементарного» генератора G_j, $j = 1, \ldots, m$.

В силу результатов предыдущего раздела вероятностные свойства выходной последовательности будут лучше, чем вероятностные свойства выходных последовательностей комбинируемых «элементарных» генераторов. Период выходной последовательности также может быть существенно увеличен путем выбора «элементарных» генераторов.

Если «элементарные» генераторы являются линейными регистрами сдвига с обратной связью, то сложность нахождения ключа по наблюдаемой выходной последовательности есть $\mathcal{O}\left(\binom{r}{m} L^3\right)$, где L — суммарная длина всех регистров. Наибольшая сложность достигается при $r = [m/2]$: $\mathcal{O}\left(m^{-1/2} 2^m\right)$.

Литература

[1] Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. Математические и компьютерные основы криптологии. Минск: Новое знание, 2003.

[2] Варфоломеев А. А., Жуков А. Е., Пудовина М. А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. Учебное пособие. М.: ПАИМС, 2000. 272 с.

[3] Alzaid A. A. and Al-Osh M. An integer-valued pth-order autoregressive structure (INAR(p)) process // Journal of Applied Probability. 1990, 27, p. 314–324.

[4] Боровков А. А. Теория вероятностей. М.: Наука, 1986.

[5] Kharin Yu., Kostevich A. Discriminant analysis of stationary finite Markov chains // Math. Methods of Statistics. 2004, vol. 13, no. 1, p. 235–252.

Встраивание цифрового водяного знака в изображение с использованием комплексного преобразования Адамара

Е. В. Разинков, Р. Х. Латыпов

1. Введение

В этой статье мы предлагаем стегосистему цифровых водяных знаков, являющуюся качественной модификацией стегосистемы, предложенной Фалковски (Bogdan J. Falkowski) и Лим (Lip-San Lim) в [1]. Метод Фалковски и Лим встраивания цифровых водяных знаков (ЦВЗ) в изображение основан на мультиразрешающем и комплексном преобразованиях Адамара.

В соответствии с классификацией стегосистем, приведенной в [2], стегосистема, предложенная Фалковски и Лим, является закрытой. Закрытая стегосистема — это стегосистема, в которой для извлечения встроенного сообщения (в данном случае — цифрового водяного знака) требуется наличие у стегодетектора исходного сигнала. Стегосистемы закрытого типа имеют довольно узкую область возможного применения.

Краткое описание метода Фалковски и Лим:

1. К черно-белому изображению три раза применяется мультиразрешающее преобразование Адамара.
2. Низкочастотная область преобразования разбивается на матрицы 8×8.
3. К каждой из этих матриц применяется комплексное преобразование Адамара.
4. Цифровой водяной знак встраивается путем модификации аргументов некоторых комплексных элементов результирующих матриц.
5. К модифицированным матрицам применяется обратное комплексное преобразование Адамара.
6. Три раза применяется обратное мультиразрешающее преобразование Адамара.

В результате проведения численных экспериментов и анализа алгоритма, нами были выявлены следующие недостатки этого метода:

- Цифровой водяной знак недостаточно устойчив к искажениям изображения.
- Присутствие цифрового знака в изображении заметно при параметрах встраивания, позволяющих извлечь ЦВЗ с приемлемым количеством ошибок.
- Стегосистема ЦВЗ относится к закрытому типу.

Для того чтобы цифровой водяной знак был устойчив, он должен быть встроен в наиболее значимые компоненты изображения, незначительное изменение которых приводит к значительному искажению изображения. Для выделения таких компонент и используется мультиразрешающее преобразование Адамара, применяемое в соответствии с формулами [3]:

$$\begin{aligned}
L_{j+1}(u, v) &= \sum_x \sum_y L_j(x, y)\, h(x-2u)\, h(y-2v), \\
H_{j+1}(u, v) &= \sum_x \sum_y L_j(x, y)\, h(x-2u)\, g(y-2v), \\
V_{j+1}(u, v) &= \sum_x \sum_y L_j(x, y)\, g(x-2u)\, h(y-2v), \\
D_{j+1}(u, v) &= \sum_x \sum_y L_j(x, y)\, g(x-2u)\, g(y-2v),
\end{aligned} \tag{1}$$

где $h = (1, 1, 1, 1)$; $g = (1, -1, -1, 1)$; L — коэффициенты низкочастотной области преобразования.

Комплексное преобразование Адамара применяется путем последовательной замены строк и столбцов матрицы, подвергающейся преобразованию, на результат их умножения на комплексную матрицу Адамара [4].

При встраивании очередного бита ЦВЗ, в матрице, полученной в результате применения комплексного преобразования Адамара, случайно выбирается элемент, аргумент которого следует изменить. В зависимости от значения встраиваемого бита, аргумент комплексного числа следует увеличить или уменьшить на величину δ. При этом необходимо изменить еще один элемент матрицы в соответствии с формулой [1]:

$$\begin{aligned}
&\angle P(k_1, k_2) \to \angle P(k_1, k_2) + \delta \\
&\angle P(N_1 - k_1, N_2 - k_2) \to \angle P(N_1 - k_1, N_2 - k_2) - \delta
\end{aligned} \tag{2}$$

Положения всех модифицированных элементов и составляют секретный ключ, необходимый для извлечения и удаления ЦВЗ.

2. Предлагаемый метод

Приняв во внимание недостатки метода Фалковски и причины их появления, мы предлагаем модифицированный метод встраивания цифровых водяных знаков.

Для устранения необходимости наличия оригинального изображения для извлечения цифрового водяного знака мы предлагаем использовать следующий способ выбора величины δ: при встраивании каждого бита ЦВЗ значение δ выбирается так, чтобы определенный разряд аргумента комплексного числа после изменения на величину δ был четным или нечетным в зависимости от значения встраиваемого бита ЦВЗ. При извлечении ЦВЗ декодер сможет восстановить цифровой водяной знак без оригинального изображения, опираясь только на значения аргументов модифицированных комплексных элементов матриц, полученных в результате применения комплексного преобразования Адамара.

Если модуль комплексного числа достаточно мал, то небольшое изменение аргумента этого комплексного числа приведет к слишком незначительному изменению реальной и мнимой составляющих. Таким образом, если коэффициенты низкочастотной области мультиразрешающего преобразования Адамара будут близки к нулю, то их модификация в соответствии с методом Фалковски не приведет к нужному эффекту, и ЦВЗ будет встроен с погрешностью. Для устранения этой проблемы мы предлагаем решение, заключающееся в увеличении коэффициентов низкочастотной области мультиразрешающего преобразования Адамара на некоторую константу перед применением комплексного преобразования Адамара. После применения обратного комплексного преобразования Адамара, коэффициенты следует уменьшить на ту же константу. Такая модификация метода встраивания повышает устойчивость ЦВЗ, значительно уменьшает возможную погрешность, возникающую на этапе встраивания, позволяет эффективно выбирать величину δ вне зависимости от значения модулей изменяемых комплексных чисел.

Продемонстрируем преимущества предлагаемого метода. Цифровой водяной знак был встроен в изображение методом Фалковски и модифицированным методом. Изображения с ЦВЗ были уменьшены до 80 % от своего размера, а потом снова растянуты до прежних размеров. Из измененных таким образом изображений были извлечены цифровые водяные знаки.

Ниже приводятся оригинальное изображение и изображение со встроенным ЦВЗ.

Покажем теперь, что цифровой водяной знак, встроенный модифицированным методом, более устойчив к проведенному нами искажению.

Рис. 1. 1) Оригинальное изображение; 2) Изображение с ЦВЗ, встроенным с помощью модифицированного метода

Рис. 2. 1) Встраиваемый ЦВЗ, 2) Извлеченный ЦВЗ, встроенный оригинальным методом, 3) Извлеченный ЦВЗ, встроенный модифицированным методом

3. Заключение и результаты экспериментов

Предлагаемый нами метод показал хорошие результаты, как в отношении незаметности ЦВЗ, так и в отношении устойчивости ЦВЗ к искажениям изображения. Модифицированный метод освобожден от основных недостатков метода Фалковски. Основное его преимущество — для извлечения ЦВЗ, встроенного модифицированным методом, не требуется исходное изображение, что позволяет строить на основе этого метода полузакрытые и открытые стегосистемы, область возможного применения которых значительно шире, чем у закрытых стегосистем.

Эксперименты показывают, что цифровой водяной знак, встроенный предлагаемым нами методом:

- Незаметен или почти незаметен. Пиковое отношение сигнал/шум для изображения с ЦВЗ по отношению к оригинальному изображению составило в наших экспериментах 53,2 дБ.

- Сохраняется в изображении при уменьшении изображения вплоть до 53 % от первоначальных размеров.
- Сохраняется при повороте изображения на угол до 15 градусов.
- Устойчив к JPEG-компрессии с сохранением 25 % качества изображения.

Литература

[1] Bogdan J. Falkowski, Lip-San Lim «Image Watermarking Using the Complex Hadamard Transform». IEEE International Symposium on Circuits and Systems, May 28-31, 2000.

[2] Грибунин В.Г., Оков И.Н., Туринцев И.В. «Цифровая стеганография». М.: СОЛОН-Пресс, 2002.

[3] Fu Chang, Kung-Hao Liang, Tzu-Ming Tan, Wen-Liang Hwang «Binarization of Document Images Using Hadamard Multiresolution Analysis». ICDAR, 1999.

[4] Bogdan J. Falkowski, Susanto Rahardja «Complex Hadamard Transforms: Properties, Relations and Architecture». IEICE Trans. Fundamentals, Vol.E87-A, No.8 August 2004. P. 2077-2083.

Оценки ранга второй координатной последовательности линейной рекурренты максимального периода над собственным кольцом Галуа нечетной характеристики

В. Н. Цыпышев

1. Введение

Пусть $R = \mathrm{GR}(q^n, p^n)$ — кольцо Галуа [8, 9], $q = p^r$, p — простое число, u — линейная рекуррента полного периода над кольцом R с характеристическим многочленом Галуа $F(x)$ степени m [4].

Под *собственным* кольцом Галуа понимается кольцо Галуа, отличное от поля и от кольца вычетов.

Пусть $S = \mathrm{GR}(Q^n, p^n)$, $Q = q^m$ — кольцо разложения многочлена $F(x)$, θ — корень $F(x)$ в кольце S. Тогда [3] существует единственная константа $\xi \in S$ со свойством:

$$u(i) = \mathrm{Tr}_R^S(\xi\theta^i), \quad i \in \mathbb{N}_0, \tag{1}$$

где $\mathrm{Tr}_R^S(x) = \sum\limits_{\sigma \in \mathrm{Aut}(S/R)} x^\sigma$ — функция *след* из кольца S в кольцо R.

Известно, что произвольный элемент $s \in S$ однозначно представляется в виде

$$s = \sum_{i=0}^{n-1} \gamma_i(s) p^i, \quad \gamma_i(s) \in \Gamma(S), \quad i = \overline{0, n-1}, \tag{2}$$

где $\Gamma(S) = \{x \in S \mid x^Q = x\}$ — p-адическое координатное множество кольца S (система представителей Тейхмюллера). Множество $\Gamma(S)$ с операциями $\oplus$: $x \oplus y = (x + y)^{Q^n}$ и $\otimes$: $x \otimes y = xy$ является полем $\mathrm{GF}(Q)$. Поле $\Gamma(S)$ содержит в качестве подполя множество $\Gamma(R) = \{x \in R \mid x^q = x\}$ — p-адическое координатное множество кольца R, на котором аналогичным образом определяются операции сложения и умножения.

Известно [8, 9], что группа $\mathrm{Aut}(S/R)$ — циклическая, и порождается *автоморфизмом Фробениуса* ρ который на элементе $s \in S$ вида (2) дей-

ствует следующим образом:

$$\rho(s) = \sum_{i=0}^{n-1} \gamma_i(s)^q p^i. \tag{3}$$

Представление, аналогичное представлению (2), справедливо также для элементов кольца R. При этом последовательность $u(i)$, $i \in \mathbb{N}_0$, однозначно определяет *n p-адических координатных последовательностей* $u_l(i) = \gamma_l(u(i))$, $l = \overline{0, n-1}$, $i \in \mathbb{N}_0$, над полем $(\Gamma(R), \oplus, \cdot)$.

На практике для выработки псевдослучайных последовательностей на основе линейной рекурренты над кольцом Галуа широко может применяться способ, усложнения такой последовательности, состоящий в выборе одного или нескольких старших p-адических разрядов этой последовательности. В этой связи представляет интерес нахождение минимальных многочленов и либо точных значений рангов последовательностей $\gamma_l(u)$, $l = \overline{0, n-1}$, либо их нетривиальных оценок. В работе [7] были получены нижние и верхние оценки рангов координатных последовательностей линейных рекуррент максимального периода над примарными кольцами вычетов, а также минимальные многочлены координатных последовательностей некоторых классов таких линейных рекуррент. Кроме того, в работе [7] получены минимальные многочлены последовательностей u_l, $l = \overline{0, 1}$, над собственным кольцом Галуа.

В работе [2] были получены минимальный многочлен и ранг первой координатной последовательности линейной рекурренты u над собственным кольцом Галуа в произвольном координатном множестве. Далее, в работе [6] были найдены точные значения ранга второй координатной последовательности отмеченной линейной рекурренты над двоичным кольцом вычетов с минимальным многочленом Галуа степени, не меньшей пяти, в зависимости от координат начального вектора этой рекурренты.

Ниже мы найдем многочлены над полем $\Gamma(R)$ которые соответственно делят и делятся на минимальный многочлен второй координатной последовательности линейной рекурренты u в p-адическом координатном множестве при $p \geqslant 3$, и найдем, таким образом, оценки снизу и сверху для ранга этой последовательности.

2. Основные результаты

Пусть $M, w \in \mathbb{N}$. Обозначим через $\boldsymbol{I}(M, w)$ множество векторов $\vec{j} = (j_1, \ldots, j_M)$, $0 \leqslant j_l \leqslant p-1$, $l = \overline{1, M}$, обладающих свойством $\sum\limits_{l=1}^{M} j_l = w$,

и через $\left\{ {M \atop w} \right\}$ обозначим мощность множества $\boldsymbol{I}(M, w)$. Отметим, что $\left\{ {M \atop w} \right\}$ есть число заполнений M различных ящиков одинаковыми предметами, при условии, что в каждый ящик попадает не более $(p-1)$-го предмета. Справедливы равенства [5, с. 215]:

$$\left\{ {M \atop w} \right\} = \sum_{s=0}^{\min\{w,(M-w)/p\}} (-1)^s \binom{w}{s} \binom{M+w-ps-1}{M-1}, \tag{4}$$

если $0 \leqslant w \leqslant M(p-1)$, и

$$\left\{ {M \atop w} \right\} = 0 \tag{5}$$

в противном случае.

Всюду далее будем считать, что $N = \left\{ {m \atop p} \right\}$, и что все векторы $\vec{\jmath}^{(1)}, \ldots, \vec{\jmath}^{(N)}$ из множества $\boldsymbol{I}(m, p)$ упорядочены в лексикографическом порядке.

Теорема 1. *Пусть $R = \mathrm{GR}(q^n, p^n)$ — собственное кольцо Галуа, $q = p^r$, $p \geqslant 3$, $r \geqslant 2$, $F(x)$ — многочлен Галуа максимального периода степени m над кольцом R, ненулевая по модулю pR последовательность $u \in L_R(F)$ представлена с помощью функции след*:

$$u(i) = \mathrm{Tr}_R^S\left(\xi\theta^i\right), \tag{6}$$

где $S = \mathrm{GR}(q^{mn}, p^n)$ — кольцо разложения многочлена $F(x)$, θ — корень $F(x)$ в S, константа $\xi \in S$ однозначно определена. Пусть также $Q = q^m = p^t$, $t = rm$, $\theta_s = \gamma_s(\theta)$, $\xi_s = \gamma_s(\xi)$, $s = \overline{0, n-1}$. Тогда каждый элемент вида

$$\theta_0^{\sum_{l=0}^{m-1} p^{rm+rl-2}(\lambda_l + p\zeta_l)}, \quad \vec{\lambda} \in \boldsymbol{I}(m, p), \quad \vec{\zeta} \in \boldsymbol{I}(m, p-1), \tag{7}$$

является корнем многочлена $m_2(x)$ кратности p.

Теорема 2. *В условиях теоремы 1 выполнены неравенства*:

$$m(p+1) + p\left\{ {m \atop p} \right\}\left\{ {m \atop p-1} \right\} \leqslant \operatorname{rank} u_2 \leqslant m(p+1) + p\left\{ {m \atop p} \right\}\left\{ {m \atop p-1} \right\} +$$
$$+ (p-1)\sum_{s=2}^{p-1}\left\{ {m \atop ps} \right\}\left\{ {m \atop p-s} \right\} + p\left\{ {m \atop p} \right\} + \left\{ {m \atop p^2} \right\}.$$

Литература

[1] Куракин В. Л. Представления над кольцом $\mathbb{Z}/p^n$ линейной рекуррентной последовательности максимального периода над полем $\mathrm{GF}(p)$ // Дискрет. матем., 1992. Т. 4, вып. 4. С. 96–116.

[2] Куракин В. Л. Первая координатная последовательность линейной рекурренты максимального периода над кольцом Галуа // Дискрет. матем., 1994. Т. 6, вып. 2, с. 88–100.

[3] Нечаев А. А. Код Кердока в циклической форме // Дискрет. матем., 1989. Т. 1, вып. 4, с. 123–139.

[4] Нечаев А. А. Линейные рекуррентные последовательности над коммутативными кольцами // Дискрет. матем., 1991. Т. 3, вып. 4. С. 107–121.

[5] Сачков В. Н. Введение в комбинаторные методы дискретной математики. М.: Наука, 1982, 384 с.

[6] Helleseth T., Martinsen M. Binary sequences of period $2^m - 1$ with large linear complexity // Informatrion and Computation, 1999, **151**, p. 73–91.

[7] Kuzmin A. S., Nechaev A. A. Linear recurrent sequences over Galois rings // II Int. Conf. Dedic. Mem. A. L. Shirshov (Barnaul, Aug. 20–25, 1991). Contemporary Math., 1995, v. 184, p. 237–254.

[8] McDonald C. Finite rings with identity // New York: Marcel Dekker, 1974, 495 p.

[9] Radghavendran R. A class of finite rings // Compositio Math, 1970, v. 22, no. 1, p. 49–57.

[10] Zierler N., Mills W. Products of linear recurring sequences // J. of Algebra, 1973, v. 27, p. 147–157.

Схемы широковещательного шифрования, основанные на блоковых кодах

С. Н. Конюшок

1. Схема широковещательного шифрования (СШШ) [1, 2, 3] представляет собой криптографический протокол, с помощью которого центр распределения ключей (ЦРК) осуществляет передачу некоторой вспомогательной секретной информации абонентам сети связи так, что со временем абоненты, входящие в определенную привилегированную коалицию, могут восстановить общий секретный ключ, передающийся в зашифрованном виде из ЦРК по широковещательному каналу связи.

В [4] (и впоследствии, независимо в [5]) предложен общий подход к построению СШШ на основе покрытий множества V абонентов определенными подмножествами. Каждому такому подмножеству B ставится в соответствие секретный ключ, вырабатываемый в ЦРК. Затем каждому абоненту $x \in V$ по защищенному каналу связи передают набор секретных ключей, соответствующих подмножествам B, содержащим x. Наконец, для передачи общего секретного ключа некоторой привилегированной коалиции $P \subseteq V$ этот ключ зашифровывают на секретных ключах абонентов из P, соответствующих определенным подмножествам $B \subseteq P$, образующим покрытие множества P.

В [4] получены оценки параметров, характеризующих практическую эффективность СШШ, в которых подмножества B определяются как блоки уравновешенных неполных блок-схем с множеством элементов V.

Ниже предлагается метод построения СШШ на основе блоковых кодов. Получены оценки устойчивости и связности предложенных схем широковещательного шифрования. Установлено, что в достаточно широком классе кодов оптимальными по устойчивости (при фиксированном числе ключей, хранящихся у каждого абонента) и по числу ключей, хранящихся у каждого абонента (при фиксированной устойчивости) являются СШШ, основанные на кодах МДР.

2. Пусть F — конечное множество мощности $q \geqslant 2$, $G \subseteq F^n$ — код длины n над алфавитом F с минимальным расстоянием (Хэмминга) $d < n$, состоя-

щий из v кодовых слов ($(n, v, d)_q$-код). Пусть далее K — конечная абелева группа порядка $|K| > nq$.

Рассмотрим множества $B_{i,a} = \{(x_1, \ldots, x_n) \in G : x_i = a\}$, занумерованные упорядоченными парами (i, a), где $i \in \overline{1, n}$, $a \in F$. Обозначим $\tau_G = \max\{t \in \overline{0, v-1} | \forall\, C \subseteq V,\ |C| = t : \bigcup\{B_{i,a} : i \in \overline{1, n},\ a \in F,\ B_{i,a} \cap C = \emptyset\} = V \setminus C\}$.

Предлагаемая схема широковещательного шифрования D_G, основанная на коде G, представляет собой криптографический протокол, состоящий из двух этапов.

На первом этапе в ЦРК независимо, случайно и равновероятно генерируют элементы $u_{B_{i,a}} \in K$, $i \in \overline{1, n}$, $a \in F$ которые являются секретными ключами абонентов. Ключу $u_{B_{i,a}}$ присваивают открытый идентификатор (i, a). Затем каждому абоненту $x \in V$ по защищенному каналу связи передают набор секретных ключей

$$K_x = (u_{B_{i,a}} : x \in B_{i,a},\ i \in \overline{1, n},\ a \in F).$$

Пусть далее, на втором этапе, требуется передать из ЦРК абонентам, образующим некоторую привилегированную коалицию $P \subseteq V$ мощности $|P| \geqslant v - \tau_G$, случайный, равновероятный и не зависящий от $u_{B_{i,a}}$ ($i \in \overline{1, n}$, $a \in F$) групповой ключ $k_P \in K$ таким образом, чтобы ни один из абонентов, принадлежащих множеству $C = V \setminus P$, не получил никакой информации об этом ключе. С этой целью в ЦРК находят определенное покрытие $\{B_{i(1),a(1)}, \ldots, B_{i(m),a(m)}\}$ множества P блоками $B_{i,a}$, $i \in \overline{1, n}$, $a \in F$), не пересекающимися с C (согласно определению параметра τ_G неравенству $|P| \geqslant v - \tau_G$, такие покрытия существуют), и передают всем абонентам сети по широковещательному каналу связи многоадресное сообщение

$$b_P = ((i(1), a(1)), u_{B_{i(1),a(1)}} + k_P; \ldots; (i(m), a(m)), u_{B_{i(m),a(m)}} + k_P). \qquad (1)$$

Каждый абонент $x \in P$ может однозначно восстановить k_P по принятому сообщению (1), используя секретный ключ $u_{B_{i(l),a(l)}}$ из набора K_x, $l \in \overline{1, m}$. При этом в силу независимости и равновероятности ключей k_P, $u_{B_{i,a}}$, $i \in \overline{1, n}$, $a \in F$, абоненты, принадлежащие множеству C, не получат никакой апостериорной информации о ключе k_P.

Отметим, что введенный выше параметр τ_G называется устойчивостью схемы широковещательного шифрования D_G [2, 4].

Основными показателями эффективности СШШ D_G являются [2 – 5] максимальное число секретных ключей, хранящихся у абонентов, и t-связность схемы D_G, равная наименьшему числу зашифрований, которые в наихудшем случае необходимо выполнить в ЦРК для передачи абонентам произвольной привилегированной коалиции P мощности $v - t$ ($t \leqslant \tau_G$) секретного группового ключа.

Непосредственно из определения СШШ D_G следует равенство $n_G = n$, где n — длина кода G. При этом общее число ключей у абонентов СШШ D_G равно $b \leqslant nq$.

3. Для любого $l \in \mathbf{N}$ обозначим $\Gamma_q^{(l)}(v, n)$ класс $(n, v, d)_q$-кодов G, обладающих следующим свойством: для любых l столбцов таблицы размера $v \times n$, составленной из слов кода G, и произвольного вектора $\alpha \in F^l$ частота встречаемости α в указанных столбцах отлична от единицы.

Следующие утверждения устанавливают оценки устойчивости СШШ, основанных на блоковых кодах.

Теорема 1. *Пусть G — $(n, v, d)_q$-код, $G \in \Gamma_q^{(k-1)}(v, n)$, где $k \geqslant 2$. Тогда*

$$\left\lceil \frac{d}{n-d} \right\rceil \leqslant \tau_G \leqslant \left\lceil \frac{d}{k-1} \right\rceil. \tag{2}$$

Теорема 2. *Пусть G - ортогональная таблица силы 1 с параметрами $(n, v, d)_q$. Тогда*

$$\tau_G \leqslant \frac{v-1}{vq^{-1}-1}(1 + \ln(n-d)). \tag{3}$$

Отметим, что в ряде случаев граница (3) является более точной по сравнению с верхней оценкой (2). Рассмотрим, например, СШШ, соответствующую симплексному коду G с параметрами $n = (q^k - 1)(q-1)^{-1}$, $k \geqslant 2$, $d = q^{k-1}$ над полем $\mathrm{GF}(q)$ [6]. При фиксированном $k \geqslant 2$ и $q \to \infty$ оценка (3) имеет порядок $O(q(1 + (k-2)\ln q))$, что значительно меньше порядка оценки (2), равного $O(q^{k-1}(k-1)^{-1})$.

Из теоремы 1 и границы Синглтона [6], стр. 310, вытекает следующее утверждение.

Следствие 1. *Пусть для данных q, n и $k \geqslant 2$ существует $(n, q^k, d)_q$-код МДР G_0. Тогда СШШ D_{G_0} имеет наибольшую устойчивость $\tau_G = \left\lceil \frac{n-k+1}{k-1} \right\rceil$ среди всех кодовых СШШ D_G таких, что $G \in \Gamma_q^{(k-1)}(q^k, n)$.*

Кроме того, при выполнении хотя бы одного из условий (а) $k = 2$; (б) $n-1$ кратно $k-1$, $k \geqslant 3$; справедливо обратное утверждение: каждая СШШ D_G, имеющая наибольшую устойчивость среди всех схем широковещательного шифрования, основанных на кодах из класса $\Gamma_q^{(k-1)}(q^k, n)$, соответствует некоторому коду МДР.

Как показывает следующий результат, при достаточно общих условиях СШШ, основанные на кодах МДР, имеют не только максимальную устойчивость, но и наименьшее число ключей, хранящихся у каждого абонента (при фиксированной устойчивости).

Следствие 2. *Пусть G_0 - линейный код МДР длины n_0 и размерности k над полем* $\mathrm{GF}(q)$, *где* $n_0 = \tau_0(k-1)+1 \leqslant q+1$, $2 \leqslant k \leqslant n_0$, $\tau_0 \geqslant 1$. *Тогда для любого линейного $(n, q^k, d)_q$-кода G такого, что $\tau_G \geqslant \tau_0$ справедливо неравенство $n_G \geqslant n_{G_0}$.*

4. Следующие утверждения устанавливают оценки t-связности схем широковещательного шифрования, основанных на блоковых кодах.

Теорема 3. *Пусть G - $(n, q^k, d)_q$-код, $\chi_G(t)$ - t-связность СШШ D_G, где $0 \leqslant t < n(n-d)^{-1}$. Тогда, если $q \geqslant \dfrac{n}{n-d}$, то*

$$\chi_G(t) \leqslant \frac{nq - nt + (n-d)\binom{t}{2}}{n-(n-d)t}\left(1 + \ln\left(\frac{(q^k-t)(n-(n-d)t)}{nq-nt}\right)\right) + 1. \qquad (4)$$

В противном случае

$$\chi_G(t) \leqslant \frac{nq - nt + (n-d)\binom{t}{2}}{n-(n-d)t}(1 + (k-1)\ln q) + 1. \qquad (5)$$

Отметим, что границы (4), (5) опираются на градиентный алгоритм построения покрытия конечного множества его подмножествами [7], стр. 136. Предлагаемый ниже алгоритм формирования многоадресных сообщений, предназначенных привилегированным коалициям абонентов $P \subset V(|P| = q^k - t)$, приводит, в ряде случаев, к более точным оценкам t-связности СШШ D_G.

Алгоритм состоит из двух этапов.

На первом этапе для каждого $1 \leqslant i \leqslant n$ подсчитывается число

$$t_i = |\{u_{B_{i,a}} : B_{i,a} \not\subset P,\ a \in F\}|$$

различных секретных ключей вида $u_{B_{i,a}}$, каждый из которых принадлежит хотя бы одному абоненту коалиции $C = G \setminus P$. Затем полученный массив чисел сортируется по невозрастанию их значений.

На втором этапе алгоритма формируется покрытие множества P, состоящее из всех множеств $B_{i,a}$, которые не пересекаются с C и соответствуют значениям $a \in F$, $i \in \overline{1, m}$ где $m = t(n-d)+1$. Далее вычисляется искомое многоадресное сообщение

$$b_P = \left((i, a);\ k_P + u_{B_{i,a}} : B_{i,a} \subseteq P,\ a \in F,\ i \in \overline{1, m}\right).$$

Оценка мощности покрытия, получаемого с помощью приведенного алгоритма, приводит к следующему результату.

Теорема 4. *Для t-связности схемы широковещательного шифрования, построенной на основе произвольного $(n, q^k, d)_q$-кода G, справедливо неравенство*

$$\chi_G(t) \leqslant (t(n-d)+1)\left(q - t\left(\frac{n}{nt - d(t-1)}\right)\right),\ 0 \leqslant t < n(n-d)^{-1}.$$

Изложенные выше результаты показывают, что, хотя схемы широковещательного шифрования, основанные на блоковых кодах, уступают по своим характеристикам одной из лучших на сегодняшний день безусловно стойких СШШ (так называемой схеме CST [5]), они являются более эффективными по сравнению со схемами [4]. В частности, общее число секретных ключей в схеме широковещательного шифрования, соответствующей блоковому коду, может быть меньше числа абонентов сети, что принципиально невозможно для СШШ, основанных на блок-схемах.

Литература

[1] Berkovits S. How to broadcast a secret // Advances in Cryptology – EUROCRYPT'91. – №547. – Berlin: Springer-Verlag, 1992. – P. 536 – 541.

[2] Fiat A., Naor M. Broadcast encryption // Advances in Cryptology – CRYPTO'93. – №773. – Berlin: Springer-Verlag, 1994. – P. 480 – 491.

[3] Stinson D. R. On some methods for unconditionally secure key distribution and broadcast encryption // Designs, Codes and Cryptography. – 1997. – Vol. 12. – P. 215 – 243.

[4] Korjik V., Ivkov M., Merinovich Y., Barg A., van Tilborg H. A broadcast key distribution scheme based on block designs // Cryptography and Coding V. – №1025. – Berlin: Springer-Verlag, 1995. – P. 12 – 21.

[5] Naor D., Naor M., Lotspiech J. Revocation and tracing schemes for stateless receivers // Advances in Cryptology – CRYPTO'01. – №2139. – Berlin: Springer-Verlag, 2001. – P. 41 – 62.

[6] Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. – М.: Связь, 1979. – 743 с.

[7] Дискретная математика и математические вопросы кибернетики / Васильев Ю. Л., Ветухновский Ф. Я., Глаголев В. В. и др. – Т. 1. – М.: Наука, 1974. – 311 с.

Обобщенные марковские шифры: построение оценок практической стойкости к дифференциальным атакам

Л. В. Ковальчук

В данной работе будут описаны методы получения оценок практической стойкости немарковских блочных шифров к дифференциальному криптоанализу и приведены примеры оценок, полученных указанными методами. Также будут обобщены (в определенном смысле) результаты, опубликованные в [1, 2, 3, 4, 5, 6, 7, 8] (для марковских шифров) и в [10] (для некоторого класса немарковских шифров).

Практически во всех предшествующих работах, касающихся построения оценок стойкости шифра относительно дифференциального и линейного криптоанализа, рассматривались только марковские шифры (МШ). Основное свойство таких шифров состоит в том, что средняя (по ключам шифра) вероятность дифференциальной характеристики является произведением средних вероятностей раундовых дифференциалов.

Все известные результаты, характеризующие оценку стойкости таких шифров, используют или подразумевают этот факт. Однако указанное свойство не является, вообще говоря, справедливым для немарковских шифров, что приводит к невозможности применения для таких шифров классических методов получения оценок практической стойкости к дифференциальному криптоанализу.

В данной работе вводятся два новых определения: обобщённой дифференциальной характеристики шифра и обобщённого марковского шифра (ОМШ); описываются некоторые основные подклассы класса ОМШ. Новый класс ОМШ содержит, в частности, класс МШ, но не совпадает с ним. Данный класс интересен, в первую очередь, тем, что для ОМШ остаются справедливыми многие результаты, полученные в [1, 2, 3, 4, 5, 6, 7, 8] для МШ. Следует заметить, что методы получения этих результатов для ОМШ подобны методам получения соответствующих результатов для МШ, не смотря на то, что основное свойство МШ для них, вообще говоря, не выполняется. В частности, в работе будут построены (строго обоснованные) верхние оценки для средних вероятностей дифференциальных характеристик ОМШ и рассмотрены примеры применения этих оценок.

Пусть $\mathcal{T}$ — r-раундовый блочный шифр, G — произвольная группа, $f_{k_i} : G \to G$ — раундовая функция, $k_i \in V_n$, $V_n = \{0, 1\}^n$, $k = (k_1, \ldots, k_r)$. Обозначим $\mathcal{T}_k : G \to G$, $\mathcal{T}_k(x) = f_{k_r} \circ f_{k_{r-1}} \circ \ldots \circ f_{k_1}(x)$ и

$$M = (\mu_0, \ldots, \mu_r), \tag{1}$$

где $\mu_i(a, b) = a \circ_i b$, $i = \overline{0, r}$ произвольная групповая операция на G, $0_i \in G$ — нейтральный элемент (относительно групповой операции μ_i).

Определение 1. Обобщенной дифференциальной характеристикой (ОДХ) (связанной с последовательностью групповых операций M) назовем последовательность

$$(\Omega, M) = ((\omega_0, \mu_0), \ldots, (\omega_r, \mu_r)), \tag{2}$$

где $\omega_i \in G \setminus \{0_i\}$.

Определение 2. Средней (по ключам) вероятностью ОДХ (2) назовем величину

$$EDP(\Omega, M) = 2^{-nr} \sum_{k \in (V_n)^r} \frac{1}{|G|} \sum_{x_0 \in G} \prod_{i=1}^{r} \delta(f_{k_i}(x_{i-1} \circ_{i-1} \omega_{i-1}) \circ_i (f_{k_i}(x_i))^{-1}, \omega_i), \tag{3}$$

где $x_i = f_{k_i}(x_{i-1})$, $i = \overline{1, r}$.

Величина $EDP(\Omega, M)$ характеризует практическую стойкость шифра $\mathcal{T}$ к дифференциальному криптоанализу в общем случае. Для марковских шифров она совпадает с величиной $EDP(\Omega, M)$, введенной в [5].

Мы рассматриваем только такие (Ω, M), что $EDP(\Omega, M) \neq 0$.

Обозначим

$$d^f_{\mu_1,\mu_2}(x; \alpha, \beta) = 2^{-n} \sum_{k \in V_n} \delta\left(f_k(x \circ_1 \alpha) \circ_2 (f_k(x))^{-1}, \beta\right), \tag{4}$$

или $d^f(x; \alpha, \beta)$ (если μ_1, μ_2 фиксированы); и среднюю вероятность раундового дифференциала:

$$d^f_{\mu_1,\mu_2}(\alpha, \beta) = \frac{1}{|G|} \sum_{x \in G} d^f_{\mu_1,\mu_2}(x; \alpha, \beta), \tag{5}$$

или $d^f(\alpha, \beta)$, $x_i = f_{k_i}(x_{i-1})$, $i = \overline{1, r}$.

Как мы заметили выше, для марковских шифров $\mathcal{T}$ (где $\mu_1 = \mu_2 = \mu$ из (4), (5)) справедливы следующие соотношения:

$$d^{\hat{f}}(x;\, \alpha,\, \beta) = d^{\hat{f}}(0;\, \alpha,\, \beta) = d^{\hat{f}}(\alpha,\, \beta); \tag{6}$$

$$EDP(\Omega) = \prod_{i=1}^{r} d^{\hat{f}}(\omega_{i-1},\, \omega_i) = \prod_{i=1}^{r} d^{\hat{f}}(0;\, \omega_{i-1},\, \omega_i); \tag{7}$$

$$\max_{\Omega} EDP(\Omega) \leqslant \left(\max_{\substack{\alpha \in G \setminus \{0\}, \\ \beta \in G}} d^{\hat{f}}(0;\, \alpha,\, \beta) \right)^{r}. \tag{8}$$

Для немарковских шифров соотношения (6), (7), (8), вообще говоря, не выполняются; таким образом, для этих шифров нет методов построения оценок $EDP(\Omega)$.

Пусть μ_1, μ_2 — две групповые операции на G; M_x, $x \in G$ — множество матриц, связанных с шифром $\mathcal{T}$ (определенным выше) следующим образом:

$$M_x = \left(a^x_{\alpha\beta}\right)_{\alpha,\beta},\ a^x_{\alpha\beta} = d^{\hat{f}}_{\mu_1,\mu_2}(x;\, \alpha,\, \beta).$$

Заметим, что для марковских шифров (и только для них) $M_x = M_{x'}$ для всех x, $x' \in G$.

Пусть Π — множество подстановочных матриц ($|G| \times |G|$). Определим новый класс ОМШ, являющийся обобщением класса МШ. Свойства ОМШ позволяют использовать для построения верхних оценок средней вероятности ОДХ методы, подобные тем, которые используются для МШ.

Определение 3. Шифр $\mathcal{T}$ назовем обобщенным марковским шифром (относительно групповых операций μ_1, μ_2), если

$$\forall\, x,\, x' \in G\ \exists\, \pi,\, \pi' \in \Pi : \pi M_x = \pi' M_{x'}. \tag{9}$$

Шифр $\mathcal{T}$ является ОМШ относительно M (определенной в (1)), если он является ОМШ относительно μ_i, μ_{i+1} для всех $i \in \overline{0,\, r-1}$.

Теперь мы опишем основные подклассы ОМШ.

Теорема 1. *Шифр $\mathcal{T}$ с раундовой функцией*

$$f_{k_i} = \varphi(x \circ k_i^{(1)},\, k_i^{(2)}), \tag{10}$$

где $k_i = (k_i^{(1)},\, k_i^{(2)})$, $k_i^{(1)} \in V_m$, $k_i^{(2)} \in V_l$, $\varphi : V_m \to V_m$ — биекция, является ОМШ относительно любой M, определенной в (1).

Теорема 2. *Шифр Фейстеля $\mathcal{G}$ с раундовой функцией*

$$f_k(x) = f_k(u,\, v) = (v,\, u \oplus \varphi(v \bullet k)), \tag{11}$$

где k, u, $v \in V_n$, $x = (u,\, v)$, $\varphi : V_n \to V_n$ — биекция, $G = V_{2n}$, является ОМШ относительно операции XOR побитового сложения при любой коммутативной групповой операции μ на V_n, $\mu(a,\, b) = a \bullet b$.

Например, шифры IDEA, Rijndael являются ОМШ относительно любой M (определенной в (1)); шифр ГОСТ 28147-89 является ОМШ относительно операции XOR.

Приведём основные свойства ОМШ.

Теорема 3. *Для любого ОМШ (относительно M) выполняются следующие соотношения*:

$$\max_{\alpha\neq 0} d^f_{\mu_{i-1},\mu_i}(x;\ \alpha,\ \beta) = \max_{\alpha\neq 0} d^f_{\mu_{i-1},\mu_i}(0_{i-1};\ \alpha,\ \beta); \tag{12}$$

$$\max_{\alpha\neq 0} d^f_{\mu_{i-1},\mu_i}(\alpha,\ \beta) = \max_{\alpha\neq 0} d^f_{\mu_{i-1},\mu_i}(0_{i-1};\ \alpha,\ \beta); \tag{13}$$

$$EDP(\Omega,\ M) \leqslant \prod_{i=1}^{r} \max_{\omega\neq 0} d^f_{\mu_{i-1},\mu_i}(0_{i-1};\ \omega,\ \omega_i); \tag{14}$$

$$\max_{\Omega} EDP(\Omega,\ M) \leqslant \prod_{i=1}^{r} \max_{\alpha,\beta\neq 0} d^f_{\mu_{i-1},\mu_i}(0_{i-1};\ \alpha,\ \beta). \tag{15}$$

при всех $x,\ \beta \in G,\ i \in \overline{1,\ r}$

Заметим, что выполнение данных соотношений для МШ является следствием их основного свойства.

Следствие 1. *Для шифра ГОСТ* 28147-89 ([9]) *справедлива оценка* $\max_\Omega EDP(\Omega) \leqslant 2^{-56}$ *для подходящим образом выбранных s-блоков.* (*Эта оценка была получена с использованием минимального значения индекса ветвления u, возможно, может быть уменьшена.*)

Заметим, что если в ключевом сумматоре вместо сложения mod 2^{32} *использовать побитовое сложение, то можно гарантировать только оценку* $\max_\Omega EDP(\Omega) \leqslant 2^{-40}$.

Используя неравенства (12), (13), (14), (15), мы также можем построить верхнюю оценку для $EDP(\Omega,\ M)$, зависящую от индекса ветвления и некоторых параметров, связанных с s-блоками, для определенного класса ОМШ (если раундовая функция шифра содержит s-блоки). Результаты будут подобны результатам, полученным в [4, 5, 6] для МШ.

Литература

[1] Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. 1991. V. 4. № 1. P. 3–72.

[2] Lai X., Massey J. L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology — EUROCRYPT'91. Proceedings. Springer-Verlag, 1991. P. 17–38.

[3] Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology — EUROCRYPT'93. Proceedings. Springer-Verlag, 1994. P. 386–397.

[4] Kanda M. Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function // Selected Areas in Cryptography. (SAC 2000). Proceedings. Springer-Verlag, 2001. P. 324–338.

[5] Vaudenay S. On the security of CS-cipher // Fast Software Encryption (FSE'99). Proceedings. Springer-Verlag, 1999. P. 260–274.

[6] Knudsen L. R. Practically secure Feistel cipher // Fast Software Encryption (FSE'94). Proceedings. Springer Verlag, 1994. P. 211–221.

[7] Vaudenay S. Decorrelation: a theory for block cipher security // J. of Cryptology. 2003. V. 16. #4. P. 249–286.

[8] Kanda M., Takashima Y., Matsumoto T., Aoki K., Otha K. A strategy for constructing fast raund functions with practical security against differential differential and linear cryptanalysis // Selected Areas in Cryptography (SAC 1998). Proceedings. Springer Verlag, 1999. P. 264–279.

[9] ГОСТ 28147-89. Криптографическая защита систем обработки данных. Государственный комитет Стандартизации СССР, 1989.

[10] Alekseychuk A., Kovalchuk L. Upper bounds of maximum values of average differential and linear characteristic probabilities of Feistel cipher with adder modulo 2^m. // Theory of Stochastic Processes. 2006. T. 12(28). #1–2. P. 20–32.

О группе тактовых подстановок SA-криптосистем

А. С. Маслов

Пусть $\mathcal{B}$ — конечное множество, элементы которого будем называть блоками. Пусть $S(\mathcal{B})$ — симметрическая группа подстановок на $\mathcal{B}$, $F_\theta \in S(\mathcal{B})$ — преобразование зашифрования блоков из $\mathcal{B}$ на ключе $\theta \in \Theta$ и $\mathcal{F} = \{F_\theta \colon \theta \in \Theta\}$ — соответствующая блочная криптосистема. Как правило, преобразования F_θ имеют итерационную структуру:

$$F_\theta = \Sigma_{K_d} \cdots \Sigma_{K_1},$$

где $K_i = K_i(\theta) \in \mathcal{K}$ — тактовые ключи и $\Sigma_{K_i} \in S(\mathcal{B})$ — тактовые подстановки.

При анализе надежности блочных криптосистем используется теоретико-групповой подход. Одним из направлений этого подхода является исследование свойств группы $\langle F \rangle$, порожденной подстановками F_θ. Известно [1, 2], что если данная группа имеет малый порядок или импримитивна, то существуют криптоаналитические атаки, позволяющие отличить F_θ от случайной подстановки или даже определить значение секретного ключа θ за время, меньшее времени перебора всех элементов Θ.

Из-за зависимостей между K_i определение строения $\langle F \rangle$ зачастую затруднительно и вместо $\langle F \rangle$ рассматривают группу $\langle \Sigma \rangle$, порожденную подстановками Σ_K, $K \in \mathcal{K}$. В работах [3, 4, 5, 6] были найдены группы, порожденные тактовыми подстановками `DES`, `AES` (`Rijndael`), `Serpent`, `BelT` и др. Во всех случаях рассматриваемые подстановки порождали знакопеременную группу на соответствующем множестве блоков. Доказательства данных утверждений были основаны больше на интуиции исследователя, нежели на проверке каких-либо достаточно общих условий.

Такого рода достаточные условия были получены нами для так называемых *SA-криптосистем* (см., например, [7]). Данные системы были выбраны в качестве предмета исследования по двум причинам. С одной стороны, структура SA-криптосистем достаточно проста для теоретического анализа. С другой стороны, SA-криптосистемы достаточно широко распространены, например, `Rijndael` и `Serpent` — финалисты конкурса AES [8]; `Khazad`, `Anubis` — участники конкурса NESSIE [9].

Перейдем к результатам. Предварительно введем необходимые обозначения. Пусть V_l — l-мерное векторное пространство над полем $\mathbb{F}_2$, $A(V_l)$ —

знакопеременная группа подстановок на V_l, $\mathrm{GL}(V_l)$ — полная линейная группа пространства V_l, $V_l^* = V_l \setminus \{0\}$. Тактовые подстановки SA-криптосистемы строятся следующим образом:

1. Выбираются натуральные $m > 1$ и $n > 1$. Блоки $\mathcal{B} = V_{mn}$ разбиваются на n подблоков длины m.
2. Выбираются $s_1, \ldots, s_n \in S(V_m)$ (так называемые S-блоки).
3. Выбирается $a \in \mathrm{GL}(V_{mn})$.
4. Действие Σ_K определяется по правилу:

$$\Sigma_K(x_1, \ldots, x_n) = a(s_1(x_1 + k_1), \ldots, s_n(x_n + k_n)),$$
$$K = (k_1, \ldots, k_n), \quad x_i, k_i \in V_m.$$

По подстановкам s_i, $i = 1, \ldots, n$, построим группы $G(s_i) = \langle s_i^{k,k'}, k, k' \in \in V_m \rangle$, где

$$s_i^{k,k'}(x) = s_i^{-1}(k' + s_i(x + k)).$$

По преобразованию a построим орграф $\Gamma(a)$, в котором $\{1, \ldots, n\}$ — множество вершин, и вершины i, j соединены дугой (i, j) тогда и только тогда, когда в преобразовании

$$(y_1, \ldots, y_n) = a(x_1, \ldots, x_n), \quad x_i, y_i \in V_m,$$

y_j существенно зависит от x_i.

Нас интересовали два вопроса: в каком случае $\langle \Sigma \rangle$ является 2-транзитивной и в каком случае $\langle \Sigma \rangle = A(V_{mn})$. Полученные достаточные условия включают условие на линейное преобразование a и условие на подстановки s_i.

Условие 1. Орграф $\Gamma(a)$ является сильно связным и наибольший общий делитель длин всех его циклов равен 1.

Условие 2. Группы $G(s_i)$, $i = 1, \ldots, n$, 2-транзитивны.

Отметим, что нарушение условия 1 означает серьезные криптографические слабости у рассматриваемой криптосистемы и на практике не встречается. Так, отсутствие сильной связности в графе $\Gamma(a)$ означает, что некоторые координаты блока шифртекста преобразования F_θ зависят не от всех координат блока открытого текста. Кроме того, если длины циклов графа кратны некоторому $l > 1$, то у системы имеются запрещенные разностные соотношения [10], позволяющие отличить преобразование зашифрования F_θ от случайной подстановки.

Теорема 1. *Пусть выполнены условия* 1, 2 *и одно из следующих условий*:

а) *матрица A преобразования a является перестановочной*;

б) *$m \geqslant 3$ и матрица A имеет вид $A = B \otimes I$, где B — обратимая матрица порядка n, $\otimes$ — кронекерово произведение матриц, а I — единичная $m \times m$-матрица*;

в) $2^{mn} < (2^m - 1)^{n-1}(2^m + 2^{m-1} - 2)$;

то $\langle\Sigma\rangle$ является 2-транзитивной. Если дополнительно

г) $2^{mn} - 1$ *не является степенью простого числа*,

то $\langle\Sigma\rangle = A(V_{mn})$.

Условия 1, 2, 4в, 4г были проверены нами для криптосистем `AES`, `Khazad`, `Anubis` и `Square`. Во всех случаях тактовые подстановки порождали знакопеременную группу.

Следующий результат показывает, что условие 1 является также необходимым для 2-транзитивности $\langle\Sigma\rangle$.

Теорема 2. *Если группа подстановок $\langle\Sigma\rangle$ является 2-транзитивной, то выполнено условие 1.*

Кроме того, с ростом m почти для всех подстановок $s \in S(V_m)$ группы $G(s)$ оказываются 2-транзитивными.

Теорема 3. *Пусть подстановка s выбирается случайно и равновероятно из множества $S(V_m)$, тогда*

$$\mathsf{P}\{G(s)\ \text{2-транзитивна}\} = 1 - O\left(\exp(-c2^m)\right),$$

для некоторой абсолютной константы $c > 0$.

Следующая теорема позволяет свести задачу проверки 2-транзитивности группы $G(s_i)$ к проверке связности специального графа $\Phi(s_i)$, построенного по подстановке s_i. Для построения данного графа рассмотрим таблицу разностей подстановки s_i — матрицу

$$\Lambda_i = (\lambda_{\alpha\beta}), \quad \lambda_{\alpha\beta} = \sum_{x \in V_m} \mathbf{I}\{s_i(\alpha + x) = s_i(x) + \beta\}, \quad \alpha, \beta \in V_m^*,$$

где $\mathbf{I}\{E\}$ — индикатор наступления события E. Пусть $\Phi(s_i)$ — граф, определяемый матрицей смежности $M = \Lambda_i \Lambda_i^T = (m_{\alpha\beta})$: ребро (α, β), $\alpha, \beta \in V_m^*$, принадлежит графу $\Phi(s_i)$ тогда и только тогда, когда $m_{\alpha\beta} > 0$.

Теорема 4. *Для того, чтобы группа $G(s_i)$ являлась 2-транзитивной необходимо и достаточно, чтобы граф $\Phi(s_i)$ являлся связным.*

Литература

[1] *Kaliski B., Jr., Rivest R., Sherman A.* Is the Data Encryption Standard a Group? (Results of cycling experiments on DES) // J. of Cryptology, v. 1, p. 3–36, 1988.

[2] *Paterson K.* Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers // Advances in Cryptology, FSE'99 Proceedings, p. 201–214, 1999.

[3] *Wernsdorf R.* The one-round functions of DES generate the alternating group // Advances in Cryptology, EUROCRYPT'92 Proceedings, p. 99–112, 1993.

[4] *Wernsdorf R.* The round functions of RIJNDAEL generate the alternating group // Advances in Cryptology, FSE'2002 Proceedings, p. 143–148, 2002.

[5] *Wernsdorf R.* The Round Functions of SERPENT Generate the Alternating Group // Submitted to NIST as an AES comment, May 2000. Available at `http://csrc.nist.gov/encryption/aes/round2/comments/ 20000512-rwernsdorf.pdf`.

[6] *Величко М. В.*, *Осиновская А. А.*, *Супруненко И. Д.* Группа тактовых подстановок криптосистемы BelT // Национальная Академия наук Беларуси. Труды Института математики (в печати).

[7] *Biryukov A.*, *Shamir A.* Structural cryptanalysis of SASAS // Advances in Cryptology, EUROCRYPT'2001 Proceedings, p. 394–405, 2001.

[8] Advanced Encryption Standard (AES) Development Effort // Available at `http://csrc.nist.gov/encryption/aes/index2.html`, 2001.

[9] NESSIE: new European schemes for signatures, integrity and encryption // Available at `http://www.cryptonessie.org`, 1999.

[10] *Biham E.*, *Birykov A.*, *Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials // Advances in Cryptology — EUROCRYPT'99 Proceedings, p. 12–23, 1999.

Стеганография: выделение инварианта для процесса печати и сканирования

Н. В. Кошкина, О. Ю. Никитина

Рассмотрена проблема выделения инварианта для процесса печати и сканирования, возникающая при решении одной из задач комнпьютерной стеганографии (а именно, защиты иннфорнмации, сохраненной на буманжнных носителях). В результате анализа отдельных подпроцессов печати и сканирования выделены критические компоненты, вызывающие наибольшие искажения. Установлены коэффициенты дискретного преобразования Фурье, которые являются наиболее стойкими к нелинейным искажениям, цветовому шуму и умеренной обрезке и соответственно могут быть использованы для внедрения дополнительной информации.

1. Введение

В сегодняшнем мире — мире сверхсложных информационных технологий и огромного количества информации, существующей в цифровом виде, остро, как никогда прежде, стоит задача поиска и извлечения для процесса печати и сканирования.

Коммерческая доступность перцепционно качественного преобразования аналоговой информации в цифровую форму и наоборот приводит к необходимости поиска новых средств противодействия подделке важных документов: паспортов, водительских прав, удостоверений личности, справок, договоров, пластиковых карточек и другого. По этой же причине сегодня востребованы эффективные методы защиты авторских изображений, ежедневно публикуемых в СМИ.

Среди исследователей наблюдается растущий интерес к проблеме выделения инварианта для процесса печати и сканирования [1], [2], [3]. Однако, в силу сложности характера проблемы прогресс не очень существенен.

Эффективных универсальных решений проблемы не существует, однако при определенных ограничениях можно построить аналитическую мо-

)Работа выполнена при поддержке молодёжного гранта Национальной академии наук Украины № ВМ 140.07 от 22.06.2005.

дель и выделить критические компоненты, вызывающие наибольшее искажения в процессе печати и сканирования. Мы разбили печать и сканирование на отдельные подпроцессы, каждый из которых вносит свой вклад в итоговое искажение изображения и проанализировали полученные подпроцессы.

2. Основные этапы при которых вносятся искажения при печати и сканировании

При печати искажения вносятся в результате выполнения следующих подпроцессов:

1. Преобразование размера исходного изображения к внутренним размерам образа для текущего разрешения печати.
2. Применение цветового профиля принтера.
3. Полутоновое растрирование.
4. Увеличение размеров растровых точек.
5. Нестабильность печатных форм.

При сканировании можно выделить следующие подпроцессы:

1. Шум матрицы сканера и интерполяция сканера.
2. Гамма-коррекция сканера.
3. Преобразование в цифровую форму.
4. Геометрические преобразования.

Степень, с которой каждый из этих подпроцессов влияет на изображение, зависит от специфики устройств и параметров их настойки. Анализ выделенных подпроцессов показал, что возможные искажения изображения в процессе печати и сканирования можно поделить на три группы: нелинейные искажения, цветовой шум и геометрические преобразования.

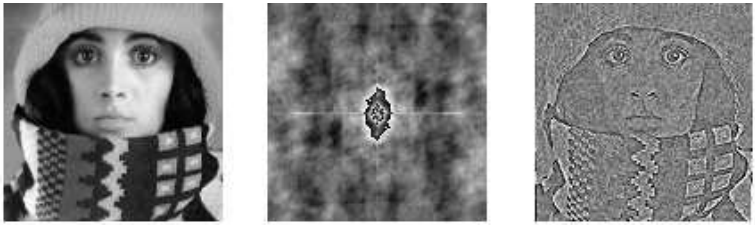
3. Выбор области для поиска и извлечения инварианта

Так как стойкость стеганографических систем защиты существенно возрастает при внедрении скрываемых данных в частотную область защищаемых объектов, мы выполнили анализ влияния нелинейных искажений, цветового шума и геометрических преобразований на коэффициенты дискретного преобразования Фурье (ДПФ) [4].

Исходное изображение $f(k, m)$ можно представить в виде амплитудного и фазового спектров. Амплитудный спектр или модуль вычисля-

ется как $|F(r, d)| = \sqrt{\mathrm{Re}^2(F) + \mathrm{Im}^2(F)}$, а фазовый спектр $\arg F[(r, d)] = -\arctan \frac{\mathrm{Im}(F)}{\mathrm{Re}(F)}$, где $\mathrm{Re}(F)$ — действительная часть спектра, а $\mathrm{Im}(F)$ — его мнимая часть. Фазы спектра более чувствительны к искажениям, нежели амплитуды, поскольку несут в себе большее количество информации об изображении.

Этот факт проиллюстрирован на рис. 1: фрагмент 1(a) содержит исходное изображение; фрагмент1(b) — изображение, для которого выполнили ДПФ, потом отбросили фазы, положив $\arg F[(r, d)] = 0$, и выполнили обратное ДПФ; фрагмент1(c) — изображение, для которого выполнили ДПФ, потом отбросили амплитуды, положив $|F(r, d)| = 1$, и выполнили обратное ДПФ. Кроме того, известно, что одно из возникающих в процессе печати и сканирования искажений, а именно обрезка, приводит к сдвигу фаз [1] и информационным потерям за этот счет. Учитывая оба вышеприведённых факта, в данной работе мы более детально изучаем влияние искажений на амплитудный спектр изображения.



a) b) c)

Рис. 1

4. Выделение инварианта к нелинейным искажениям, цветовому шуму и умеренной обрезке

Выделение инварианта к перечисленным искажениям может базироваться на следующих фактах:

1. Низко и среднечастотные коэффициенты амплитуд сохраняются намного лучше, нежели высокочастотные. Прослеживается тенденция: чем ниже частота, тем меньше вносимое в нее при печати и сканировании искажение.
2. В низко и среднечастотной полосах спектра во время печати и сканирования увеличиваются коэффициенты с низкими амплитудами,

коэффициенты с высокими амплитудами практически сохраняются. Данный факт соблюдается для различных изображений, разных технологий печати и разрешений изображения, принтера и сканера.

3. Если не изменять гамма-коррекцию в течении печати и сканирования, а использовать ее стандартное значение, то коэффициенты с высокими амплитудами увеличиваются примерно на единицу. Грубо говоря, если процесс печати и сканирования аппроксимировать как линейный фильтр (для достаточно больших коэффициентов и достаточно низких частот), то после применения стандартной гамма-коррекции имеем фиксированное изменение на $+1$ численного значения указанных амплитуд (полученное эксперементально).
4. Модификации на уровне последнего младшего разряда численных значений высоких амплитуд в низкочастотной полосе при обратном ДПФ рассеиваются по всему изображению и не вызывают его существенного перцепционного искажения.

Таким образом, низкочастотные коэффициенты спектра с высокими амплитудами наиболее инварианты к нелинейным искажениям, цветовому шуму и умеренной обрезке и обладают некоторой избыточностью, которую можно использовать для внедрения дополнительной информации.

Литература

[1] C.-Y. Lin, S.-F. Chang. Distortion Modeling and Invariant Extraction for Digital Image Print-and-Scan Process. Intl. Symp. on Multimedia Information Processing, Taipei, December 1999.

[2] S. V. Voloshynovskiy, O. Koval, F. Deguillaume, T. Pun. Visual communications with side information via distributed printing channels: extended multimedia and security perspectives. In Proceedings of SPIE: Security, Steganography, and Watermarking of Multimedia Contents VI, p. 428–445, San Jose, CA, USA, January 2004.

[3] K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran. Modeling the print-scan process for resilient data hiding. In Proceedings of SPIE: Security, Steganography, and Watermarking of Multimedia Contents VII, v. 5681, p. 418–429, March 2005.

[4] В. К. Задирака, С. С. Мельникова. Цифровая обработка сигналов. Киев: Наукова думка, 1983. 294 с.

Особенности форматов MPEG с точки зрения их использования для сокрытия информации в видеопоследовательности

А. В. Зырянов

В последнее время, благодаря росту вычислительной мощности компьютерной техники и увеличению пропускной способности каналов связи, цифровое видео получило широкое распространение. Большую роль в этом процессе сыграло появление стандарта кодирования MPEG. Наиболее распространенными версиями стандарта являются MPEG-2 (1994 год), согласно которой кодируется видеопоток DVD, и MPEG-4 (1998 год), обеспечивающий возможность передачи и просмотра видео со скоростью 64 Кбит/с.

В докладе рассматриваются некоторые аспекты использования в видеопотоках группы форматов MPEG известных методов сокрытия информации, обычно применяемых к статическим изображениям.

Очевидно, что наилучший контейнер для сокрытия информации это тот, передача которого является типичным событием и не вызывает подозрений. Поэтому до последнего времени наиболее распространенными и наиболее хорошо исследованными типами контейнеров являлись графические изображения различных форматов, в частности, формата JPEG. Об этом свидетельствует большое количество опубликованных алгоритмов сокрытия данных внутри неподвижных изображений, например в [1, 2, 7].

Благодаря распространению цифрового видео появилась возможность использовать контейнеры данного типа для передачи информации. Несмотря на глубокие исследования в области вставки цифровых водяных знаков (ЦВЗ) [3], фактически отсутствуют публикации, освещающие вопросы скрытой передачи информации внутри видеопотока.

Целью данного доклада является освещение ключевых отличий способа кодирования видео MPEG от кодирования статических изображений JPEG. Так, в отличие от статических изображений, в видео применяют более сложные алгоритмы кодирования, основной задачей которых является уменьшение как пространственной, так и временной избыточности последовательности кадров. Исходя из этого, существует ряд препятствий для

создания эффективных методов сокрытия информации, отвечающих требованиям к объемам передаваемых сообщений и скрытности канала связи.

Основными отличиями видео от статических изображений являются:

1. Наличие временной избыточности. Она заключается в том, что обычно изменения между соседними кадрами незначительны, и по этой причине нет смысла кодировать каждый кадр по отдельности.
2. Жесткие требования к кодирующему и декодирующему устройствам. Процедуры сжатия и восстановления должны выполняться в реальном времени и обеспечивать установленные стандартом ограничения по скорости передачи.
3. Из ограничения по скорости передачи следует, что, по сравнению со стандартом JPEG, применяются более совершенные методы уменьшения пространственной избыточности, а также может использоваться более грубая таблица квантования. Коэффициенты таблицы квантования зависят от так называемого «шага квантования», значение которого выбирается в зависимости от объема получаемого видеопотока.
4. Алгоритмы кодирования видео должны быть устойчивы к ошибкам в канале связи и ошибкам декодирования. Для этих целей существуют рекомендации стандартов [4, 5] по выбору интервала между ключевыми кадрами и кадрами, предсказанными по ним. Так, в пункте 3.2 рекомендации [6] указано, что макроблок не может использоваться в качестве основы для предсказания более чем 132 раза.

В связи с вышеуказанными особенностями, возникает ряд трудностей, с которыми можно столкнуться при разработке стеганографических систем на основе видеопотока группы стандартов MPEG:

1. Ограничения по размеру выходного потока. В связи с нарушением статистической структуры контейнера, средняя длина кодового слова увеличивается. Это может привести к увеличению размера контейнера на 5–10 %.
2. Накопление ошибки предсказания в последующих кадрах, что негативно сказывается на восприятии видео.
3. Сложность реализации алгоритмов, осуществляющих сокрытие информации в реальном времени и без повторного сжатия с потерями.

Для демонстрации вышеуказанных трудностей для контейнеров MPEG-2 и MPEG-4 были применены стандартные алгоритмы сокрытия информации в статических изображениях, описанные, например, в [1, 7]. В частности, был использован известный метод сокрытия в наименьшем значащем

бите (или сокращенно LSB), использующий коэффициенты ДКП кадров видео.

В стеганографических системах важную роль играет восприятие человеком отличий чистого контейнера и контейнера с информацией. Чем меньше происходит изменений при использовании алгоритмов сокрытия информации, тем надежнее построенная система. Применительно к видео и графическим изображениям, особое внимание необходимо уделять визуальным искажениям, происходящим в контейнере.

Для количественной оценки этих изменений можно применить метод оценки соотношения сигнал/шум. Если обозначить $I_{i,j}$ — элементы исходного контейнера, $O_{i,j}$ — элементы контейнера с информацией, M и N — размеры кадра по горизонтали и вертикали соответственно, то метрика PSNR задается следующим соотношением [7]:

$$\mu_{PSNR} = MN \frac{\max_{i,j}(I_{i,j})^2}{\sum\limits_{i,j}(I_{i,j} - O_{i,j})^2}. \qquad (1)$$

График зависимости коэффициента PSNR от номера кадра в потоке (см. рис. 1) имеет характерный ступенчатый вид, что свидетельствует

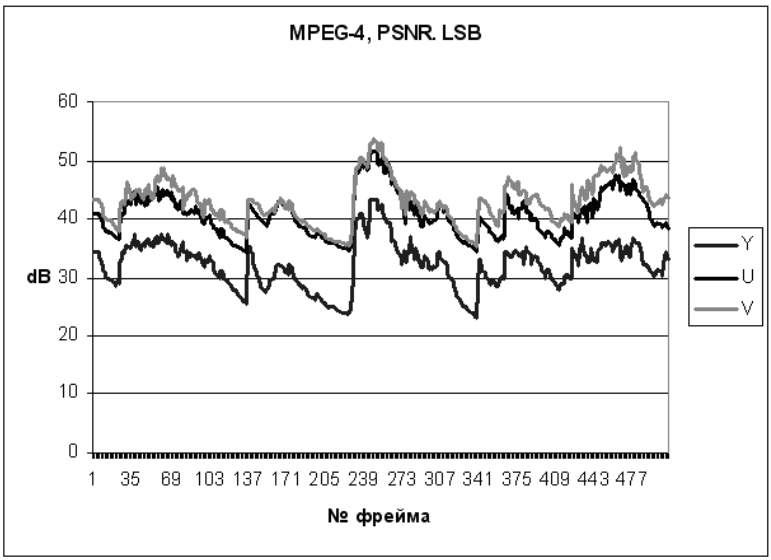


Рис. 1. Изменение соотношения сигнал/шум при сравнении чистого контейнера и контейнера со скрытой информацией

о негативном эффекте накопления ошибки предсказания движения. Этот эффект проявляется в том, что визуальные отличия чистого контейнера и контейнера с информацией увеличиваются при переходе от одного B-или P-кадра к другому.

Таким образом, продемонстрировано, что при переносе принципов сокрытия информации со статических изображений на видеопоследовательности возникает ряд особенностей, связанных со способами кодирования цифрового видео. Эти особенности необходимо учитывать при разработке устойчивых к атакам стеганографических алгоритмов.

Литература

[1] *В. Г. Грибунин*, *И. Н. Оков*, *И. В. Туринцев*. Цифровая стеганография. М.: СОЛОН-Пресс, 2002.

[2] *A. Westfeld*. High Capacity Despite Better Steganalysis (F5 — A Steganographic Algorithm). Information Hiding. 4th International Workshop. Lect. Notes in Computer Science, v. 2137. Springer-Verlag, 2001, p. 289–302.

[3] *J.-S. Pan*, *H.-C. Huang*, *L. C. Jain*. Intelligent Watermarking Techniques. World Scientific, 2004.

[4] Стандарт MPEG-2 ISO/IEC 13818-2.

[5] Стандарт MPEG-4 ISO/IEC 14496-2.

[6] Рекомендация IEEE 1180 «Considerations of Specifying IDCT Mismatch Errors», п. 2.3, 1990.

[7] *А. В. Аграновский*, *П. Н. Девянин*, *Р. А. Хади*, *А. В. Черемушкин*. Основы компьютерной стеганографии. М.: Радио и связь, 2003.

Часть IV

СЕКЦИЯ «МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»

Объекты критически важных инфраструктур: анализ защищенности и риски успешной реализации компьютерных атак

А. А. Климовский, М. В. Большаков,
Ф. М. Пучков

Введение

Одной из важных задач государства в обеспечении национальной безопасности является защита критически важных инфраструктур и их элементов от возможных деструктивных воздействий как со стороны человека, так и со стороны окружающей среды. Такие критически важные элементы представляют собой набор взаимосвязанных физических объектов, природных, технологических и человеческих ресурсов, поддерживающих важные для государства функции, направленные на удовлетворение базовых потребностей общества в социальной, материальной, политической, духовной и информационной сферах его жизнедеятельности. Отдельные объекты, составляющие критические сегменты инфраструктуры, характеризуются тем, что их работоспособность напрямую или косвенным образом, в течение относительно небольшого интервала времени, влияет на состояние национальной безопасности государства. Потеря функциональности подобных объектов может привести к крупномасштабным авариям, техногенным катастрофам, утрате здоровья или гибели людей. В контексте настоящего исследования будем согласно данному выше определению именовать такие объекты критически важными объектами (КВО) [1]. По указанной выше причине очень важен перманентный контроль и всесторонний анализ защищенности подобных объектов на всех этапах их жизненного цикла. Особый контроль при этом необходим за информационной [2] системой управления КВО, поскольку она играет определяющую роль в процессе функционирования объектов подобного типа. В соответствии с при-

[1] Более точное определение КВО приводится в [1].

[2] Более того, — информационно-вычислительной и телекоммуникационной составляющей такой системы.

нятым соглашением для краткости систему управления КВО будем обозначать КВОИ (Критически Важный Объект Информационный) [1, 2].

При проведении подобного анализа защищенности, как отмечено в [1], необходимо учитывать положение анализируемого объекта в дереве критических инфраструктур и их сегментов, а также механизмы взаимодействия и его связи с другими объектами. Указанного можно добиться путем категоризации — введения такого понятия как «уровень значимости» (CL) объекта или подсистемы, последующим проектированием и построением системы обеспечения безопасности и анализа защищенности КВО в соответствии с этим уровнем. «Уровень значимости» (категория критичности) КВО при этом будет выражаться целым неотрицательным числом. Указанное соответствие может выглядеть следующим образом:

- значениям $CL \leqslant 1$ соответствует базовый (минимальный) уровень значимости (для защиты объектов с таким «уровнем значимости» имеет смысл ограничиться базовым набором требований безопасности);
- значению $CL = 2$ соответствует средний уровень значимости;
- значению $CL = 3$ соответствует высокий уровень значимости;
- значениям $CL \geqslant 4$ соответствует максимальный уровень значимости.

Детали такого подхода изложены в [1]. Ниже будет предложена, с использованием результатов такой категоризации, классификация методов анализа защищенности компьютерных систем управления КВО, которую можно использовать в качестве основы для построения общей методики анализа защищенности информационных технологий, используемых в таких системах, и также оценки рисков неблагоприятных событий, а именно, — реализации деструктивных воздействий на подобные объекты.

1. Методы анализа защищенности информационных технологий в системах управления критически важными объектами

Анализ защищенности представляет собой особый вид аудита — постоянную или периодическую оценку состояния КВОИ на предмет возможных деструктивных воздействий, посредством использования уязвимостей, «узких» мест реализации программно-аппаратной структуры. Приведем краткую характеристику существующих методов анализа защищенности.

Программное обеспечение может содержать ошибки и программные закладки, которые обнаруживаются уже в процессе эксплуатации системы. Процесс изменения конфигурации может быть очень сложным и вклю-

чать в себя координированное взаимодействие нескольких администраторов различных подсистем КВОИ, что нередко может приводить к появлению дополнительных уязвимостей. На выявление вышеперечисленных уязвимостей направлены сканеры безопасности, призванные проверять наличие известных программных и аппаратных уязвимостей и наиболее типичных ошибок конфигурации программного обеспечения и оборудования.

Функциональность другого вида анализаторов защищенности направлена на мониторинг заданных критических параметров системы, отражающих состояния критически важного для штатного режима функционирования КВОИ ресурса. К числу таких параметров, например, могут быть отнесены загруженность каналов передачи данных, наличие достаточного объема оперативной и постоянной памяти, загрузка процессоров. Используя подобные данные можно спрогнозировать вероятность успешного исполнения своих функций КВОИ на некоторый промежуток времени, выявить «узкие» места в программно-аппаратной структуре, предположить место и вероятную причину сбоя.

Будем придерживаться следующей классификации методов анализа защищенности информационных технологий в зависимости от способа их применения:

- динамический анализ;
- статический анализ, включая
  - анализ на соответствие российским и международным стандартам;
  - экспертный анализ.

В настоящей работе более детально представлена методика проведения *экспертного анализа*, который, в отличие от других, позволяет получить «картину» рисков неблагоприятных событий в целом, для отдельного киберобъекта, как носителя информационных технологий, а также адекватную оценку степени (уровня) его защищенности. Кроме того, приведены способы интеграции указанного подхода с другими методами оценки защищенности (динамическими и анализом на соответствие стандартам).

1.1. Динамический анализ

Динамический анализ защищенности информационных технологий в системах управления критически важными объектами с необходимостью должен применяться в режиме реального времени на этапе эксплуатации объекта. Такой подход включает в себя:

- активный аудит[3)] событий на КВОИ, направленный на обнаружение деструктивных информационных воздействий и выработку мер оперативного реагирования [3];
- мониторинг работоспособности состояния основных аппаратно-программных средств, поддерживающих функциональность системы, их анализ и выработку мер оперативного реагирования;
- применение средств проверки наличие доступных потенциальному нарушителю уязвимостей — сканеры безопасности.

С учетом большого количества событий, подлежащих обработке в таком режиме, динамический анализ, как правило, выполняется автоматически (или полуавтоматически).

Динамический анализ, являясь важной составляющей системы мер по обеспечению безопасности информационных технологий в традиционных объектах защиты, может быть эффективно использован в системе анализа защищенности и оценки рисков, связанных с информационной безопасностью критически важных объектов. База событий активного аудита и мониторинга состояния системы, накопленная за определенный промежуток времени, может быть использована для уточнения вероятностной и структурной модели анализируемого объекта при проведении повторной процедуры экспертного анализа защищенности КВОИ (более подробно в подразделе 2.2).

Выделим некоторые типы данных, распознавание которых и соответствующая им статистика могут существенно влиять на структуру и параметры модели КВОИ, используемой при экспертной оценке защищенности объекта.

- Дата, время и результат события (успешное/неуспешное) с целью выявления степени интенсивности и эффективности кибератак и уточнения соответствующих «весовых коэффициентов», использующихся при анализе рисков неблагоприятных событий (см. подраздел 2.2);
- Действия, предпринимаемые автоматически при обнаружении нарушений с целью накопления статистических данных с целью более точного определения степени эффективности указанных действий и уточнения соответствующих «весовых коэффициентов», адекватных мерам защиты и функциям безопасности киберобъекта (см. подраздел 2.2);

[3)] Активный аудит — оперативный контроль за состоянием объекта на предмет наличия деструктивных информационных воздействий, анализ и выработка мер оперативного реагирования (более подробно см. [4]).

- Тип события, идентификаторы субъектов, участвующих в событии с целью распознавания кибератак на такие объекты, как операционная система, сетевое оборудование и другие. Подобные характеристики позволяют существенно упростить построение структурной модели КВОИ.

1.2. Анализ на соответствие российским и международным стандартам

Одной из важных составляющих мероприятий по анализу защищенности КВОИ от возможных кибератак является оценка соответствия объекта положениям законодательных актов и требованиям нормативно-регламентирующей базы в сфере информационной безопасности. Подобные положения и требования представлены в таких документах, как федеральные законы, указы Президента, постановления Правительства РФ, руководящие документы и рекомендации, как регулирующих органов государственной власти, так и международных организаций. В качестве критериев оценки уровня защищенности КВОИ при проведении аудита на основе упомянутых подходов, которые принято именовать критериальными, используются требования международных стандартов и отечественной нормативной базы в области информационной безопасности, включая:

- руководящие документы ФСТЭК (ранее — Гостехкомиссии РФ);
- международные стандарты, такие как ISO/IEC 17799, ISO/IEC 15408, BSI/IT Baseline Protection Manual и COBIT;
- отраслевые стандарты, определяющие требования, специфицированные для банковских, телекоммуникационных и систем другого прикладного назначения.

Отметим, что для проведения анализа на соответствие подобным стандартам используются следующие методы:

- составление и применение «вопросников» с последующей обработкой полученных результатов вручную или автоматически;
- тестирование и верификация программно-технических средств защиты информации.

Поскольку в большинстве случаев подобные методы позволяют проводить анализ на соответствие некоторой общей системе требований, они зачастую не учитывают особенности анализируемого объекта и, как следствие, не позволяют оценивать возможность проведения кибератак и прямо судить о степени защищенности информационной системы в целом. В этой связи, с целью получения окончательной экспертной оценки защищенности КВОИ, результаты подобных оценок целесообразно использовать для по-

строения адекватной модели КВОИ. Результаты ранее проведенного анализа могут быть использованы как факторы, позволяющие более точно описать угрозы информационной безопасности объекта.

2. Экспертный анализ

Под «экспертным анализом» будем понимать трудноформализуемую часть анализа, выполняемую специально обученной группой экспертов, либо автоматизированной (в автоматическом / полуавтоматическом режиме) экспертной системой. Для крупных распределенных объектов, какими, как правило, являются объекты критически важных сегментов национальной инфраструктуры, представляется целесообразным построение, обучение на презентативной выборке и использование специальной экспертной системы, интегрированной с системой анализа рисков неблагоприятных событий. Такую экспертную систему можно применять на всех этапах жизненного цикла КВОИ, как информационной системы. Важным отличием экспертного анализа от динамических методов анализа является тот факт, что в процессе работы экспертной системы (группы экспертов) модель анализируемого объекта остается неизменной.

В связи с отсутствием четкой постановки задачи на проведение экспертного анализа объектов, подобных рассматриваемым в настоящей работы, готовых и апробированных программно-технических решений ее не существует. По этой причине целесообразна разработка новой, оригинальной методики анализа защищенности комплексов, подобных КВОИ, с использованием в ее составе разработанных ранее отдельных элементов, которые необходимы для эффективной реализации методики.

В данном разделе описаны основные принципы реализации такой методологии, позволяющей для отдельного КВОИ выявлять его архитектурные уязвимости и оценивать общий уровень защищенности. Метод заключается в проведении определенных действий на следующих трех последовательных этапах:

- этап I — создание модели проектируемого КВОИ, построение структуры в соответствии с таксономией и разработка правил вывода (в модели) — угроз безопасности КВОИ;
- этап II — анализ возможных сценариев развития кибератак на КВОИ и оценка вероятности возникновения этих сценариев (в рамках модели);
- этап III — получение окончательной интегральной оценки рисков неблагоприятных событий (потери функциональности) в связи с деструктивными воздействиями на данный КВОИ.

Важной составляющей предлагаемой методики является создание средств описания модели проектируемого КВОИ. Отметим, что такая модель должна эффективно учитывать следующие характеристики КВОИ:

1) «степень критичности» и ценность активов киберобъекта;
2) угрозы киберобъекту со стороны потенциальных нарушителей;
3) функции безопасности киберобъекта [4)];
4) предположения безопасности, задающие определенную «модель нарушителя» и определяющие степень эффективности функций безопасности в противодействии угрозам киберобъекту;
5) архитектуру/внутреннее строение киберобъекта.

В качестве основы указанной модели была разработана и использована *таксономия киберобъектов*, представляющая собой древовидную структуру сущностей — *элементов таксономии*. Таксономия киберобъектов выполняет роль онтологии для предлагаемой экспертной системы. Каждому элементу таксономии соответствует определенный киберобъект, а именно, — отдельная составляющая (компонент) КВОИ, также некоторый его тип. Типы позволяют группировать киберобъекты с одинаковыми (похожими) свойствами и функциональностью. Киберобъекты, соответствующие листовым вершинам дерева, будем называть *атомарными*. Каждый киберобъекты имеет набор *атрибутов*, часть характеристик которых включают следующую информацию:

- идентификатор типа и экземпляра киберобъекта;
- «уровень значимости» киберобъекта по отношению к КВОИ;
- ценность активов киберобъекта (в числовом выражении);
- функциональность киберобъекта и его подвиды;
- угрозы присущие данному киберобъекту и перечень предусловий, необходимых для возможности их реализации (такие, например, как наличие у злоумышленника локального доступа к киберобъекту и подобные им);
- функции безопасности киберобъекта;
- предположения безопасности киберобъекта;
- внутренняя структура (или содержимое) киберобъекта;
- «множество доступов» киберобъекта (как субъекта информационной системы) к другим объектам.

2.1. Таксономия киберобъектов

Изложение таксономии киберобъектов разделено на несколько пунктов с тем, чтобы в каждом из них описывались атрибуты и свойства только

[4)] требование по мерам обеспечения безопасности для данного объекта.

одного элемента. В каждом отдельном пункте при этом могут быть ссылки на другие пункты в соответствии с иерархией элементов таксономии.

К числу киберобъектов и их подвидов, некоторые из которых более детально представлены далее в таксономии, могут относиться следующие:

- КВОИ;
- подсистема;
- регламент КВОИ;
- компонент;
- помещение;
- рабочая станция, включая
  - — сервер;
  - — рабочее место;
- сетевое оборудование;
- специфическое оборудование (банкоматы, промышленные установки и прочее оборудование);
- операционная система, в том числе
  - — семейство Windows (Windows 95/98/NT/2000/XP/2003);
  - — семейство Linux (kernel-2.0.x, kernel-2.2.x, kernel-2.4.x, kernel-2.6.x);
  - — семейство Free BSD (версии 1.x, 2.x, 3.x, 4.x, 5.x);
  - — семейство MAC OS X (версии 10.0, 10.1, 10.2, 10.3, 10.4);
  - — семейство Solaris (версии 7, 8, 9, 10);
- программное обеспечение, включая
  - — веб сервер;
  - — СУБД, в том числе
    - ∗ Oracle;
    - ∗ IBM DB2;
    - ∗ MySQL;
  - — ПО для мониторинга состояния функциональности основных программно-аппаратных средств и аудита киберобъекта на предмет обнаружения деструктивных информационных воздействий и оперативного реагирования;
  - — ПО для поддержки совместной работы пользователей в локальных сетях, включая
    - ∗ сервисы аутентификации;
    - ∗ средства передачи сообщений;

  * файловые сервера;

- данные, имея в виду
  - — электронные документы организации;
  - — программное обеспечение (исполняемые модули, библиотеки, исходные коды);
  - — конфигурационные файлы, поддерживающие корректную работу сервисов безопасности (параметры безопасности);
  - — конфигурационные файлы, обеспечивающие корректную работу остальных сервисов.

Следует сразу же подчеркнуть, что представленный перечень киберобъектов и их подвидов не является «жестким» и может изменяться также как и следующий далее набор характеризующих их атрибутов. В настоящей работе излагается общая идея подхода к формированию модели, которая может быть положена в основу системы экспертного анализа защищенности КВОИ. Для каждого отдельного объекта такая модель должна формироваться с учетом его особенностей и условий окружения, включая постановку задачи. Формирование и модификация подобного перечня может проводиться на основе документов, в которых более детально рассмотрены типовые условия применения методики (с учетом решаемой задачи), и международных стандартов [6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 18, 19].

Для лучшего понимания приведем в качестве примера описание двух киберобъектов разного уровня иерархии: киберобъект «КВОИ» и киберобъект «оборудование».

2.1.1. Киберобъект «КВОИ». Методика идентификации критически важных объектов и автоматизированных систем управления ими детально изложена в [1]. К атрибутам, идентифицирующим КВОИ при таком подходе могут относиться следующие.

Атрибут «уровень значимости киберобъекта» (CL):

- $CL = 0$ или $CL = 1$ — соответствует базовому уровню защищенности киберобъекта;
- $CL = 2$ — соответствует среднему уровню защищенности киберобъекта;
- $CL = 3$ — соответствует высокому уровню защищенности киберобъекта;
- $CL = 4$ — соответствует максимальному уровню защищенности киберобъекта.

Атрибут «угрозы, присущие данному киберобъекту»:

- угроза нарушения штатных электронных регламентов взаимодействия отдельных компонентов киберобъекта между собой и с внешними информационными системами;
- полная потеря функциональности (отсутствие доступа к активам основных сервисов киберобъекта);
- угроза нарушения целостности информационных активов киберобъекта (например, электронных документов);
- угроза нарушения конфиденциальности информационных активов киберобъекта по отношению к внешним подсистемам;
- угроза нарушения конфиденциальности информационных активов киберобъекта по отношению к внутренним подсистемам.

Атрибут «функции безопасности киберобъекта»:

- динамический контроль за корректностью выполнения электронных регламентов;
- статический анализ на наличие уязвимостей в программных реализациях электронных регламентов КВОИ;
- мониторинг состояния доступных сервисов киберобъекта, предусмотренных штатным режимом работы киберобъекта;
- физическая и логическая защита каналов связи между подсистемами киберобъекта;
- обеспечение корректного объединения (интеграция) политик информационной безопасности различных подсистем в составе киберобъекта.

Киберобъект «КВОИ» состоит из набора объектов типа «подсистема».

2.1.2. Киберобъект «оборудование». Элемент таксономии «оборудование» имеет следующие атрибуты.

- «уровень значимости» (CL), включая
  - — $CL = 0$ или $CL = 1$ — соответствует базовому уровню защищенности;
  - — $CL = 2$ — соответствует среднему уровню защищенности;
  - — $CL = 3$ — соответствует высокому уровню защищенности;
  - — $CL = 4$ — соответствует максимальному уровню защищенности;
- подвиды киберобъекта, в том числе
  - — рабочая станция, представляющая собой
    - * сервер (пользователи не имеют физического доступа к соответствующему оборудованию);

  * рабочее место (пользователи имеют физический доступ к соответствующему оборудованию);

— сетевое оборудование (маршрутизаторы, коммутаторы, сетевые кабели);
— специфическое (банкоматы, промышленные установки и прочее оборудование);

- конфигурация;
- параметры;
- угрозы, присущие данному киберобъекту;
- предположения безопасности данного киберобъекта;
- требования по обеспечению безопасности данного киберобъекта.

Укажем возможные значения некоторых атрибутов.
Атрибут «угрозы, присущие данному киберобъекту»:

- отказ, выход из строя;
- внедрение закладок в аппаратное обеспечение (более подробно см., например, [15]);
- компрометация устройства (T.Compromise[5]) — злоумышленник может получить частичный или полный контроль над устройством с возможностью изменять правила коммутации, иметь доступ к передаваемым данным;
- несанкционированное управление устройством (T.UnauthMgmt) — злоумышленник может получить несанкционированный доступ к функциям управления устройством (более подробно см., например, в [16]);
- сбой в работе (T.Fail) — в результате частичного отказа устройства или сбоя питания могут нарушиться функции безопасности;
- злонамеренные действия персонала (T.HostileAdmin) — авторизованный сотрудник, имеющий возможность управления устройством, может самовольно изменить конфигурацию или записи аудита;
- ошибочные действия персонала (T.AdminError) — авторизованный сотрудник может по ошибке неверно сконфигурировать устройства, нарушив политику безопасности.

Атрибут «предположения по мерам безопасности данного киберобъекта»:

- A.Physical — физический доступ к устройству имеют только авторизованные сотрудники;

[5] Далее, имея ввиду, что если рассматриваемый атрибут описан в [19], в скобках приводится соответствующий ему идентификатор из этой статьи.

- A.Expert (для среднего, высокого и максимального уровней защищенности) — злоумышленник является экспертом в области компьютерных технологий, хорошо знакомый с алгоритмами и протоколами, используемыми устройством;
- A.ExternalStorage — имеется защищенное хранилище, подключенное к управляющей сети, пригодное для хранения записей аудита и конфигурации;
- A.TrainedAdmin — персонал знаком со всей документацией по устройству и придерживается рекомендаций по установке и настройке;
- A.GoodAdmin — среди персонала, авторизованного для управления устройством, нет злоумышленников;
- A.ProtectedMgmt — для управления и мониторинга устройства используется физически отдельные линии связи.

Атрибут «требования по обеспечению безопасности данного киберобъекта»:

- P.AuditAdmin — при любой модификации конфигурации устройства должна быть сгенерирована и помещена во внешнее защищенное хранилище запись аудита, содержащая время изменения, идентификатор сотрудника, дополнительные сведения о модификации;
- P.SecureDefault — все настройки по умолчанию должны быть в наиболее безопасном состоянии;
- P.Guidance — должны присутствовать руководства по безопасной установке, настройке, сопровождению устройства;
- P.StandardsBased (для среднего, высокого и максимального уровней защищенности) — все используемые функции и протоколы должны быть открытыми стандартами и быть реализованы также в устройствах других производителей;
- P.OpenDesign (для среднего, высокого и максимального уровней защищенности) — общая структурная схема и используемые алгоритмы должны быть неограниченно доступны для изучения с привлечением независимых экспертов;
- P.OpenCode (для максимального уровня защищенности) — все функциональные схемы устройства и полные исходные коды встроенного программного обеспечения должны быть неограниченно доступны для изучения с привлечением независимых экспертов.

2.2. Схема алгоритма анализа защищенности КВОИ

Рассмотрим в общем виде схему алгоритма, согласно которому должна функционировать проектируемая экспертная система автоматизированного

анализа защищенности объектов КВОИ и оценки рисков неблагоприятных событий для таких объектов.

Прежде, чем перейти к описанию схемы алгоритма, введем несколько определений. *Деструктивным информационным воздействием или кибератакой на КВОИ* будем называть последовательность действий, называемых *шагами атаки*, предпринимаемых для реализации действий, направленных на нарушение правил функционирования КВОИ, установленных политикой безопасности КВОИ, которые призваны поддерживать штатные режимы работы КВОИ. Шаги атаки будем отождествлять с реализациями угроз киберобъектам таксономии.

Введем следующее обозначение: $av_1, \ldots, av_n$ — список всех возможных значений атрибутов всех киберобъектов таксономии.

Состоянием КВОИ будем называть вектор $(\alpha_1, \ldots, \alpha_n)$, где

$$\alpha_i = \begin{cases} 1, & \text{если значение соответствующего атрибута равно } av_i; \\ 0 & \text{иначе.} \end{cases}$$

Функционированию указанной экспертной системы должно предшествовать формирование таблицы, содержащей информацию о зависимостях действий, предпринимаемых в ходе реализаций угроз киберобъекту, от функций, направленных на обеспечение безопасности киберобъекта, предположений по мерам обеспечения безопасности и, возможно, некоторых других атрибутов, часть из которых представлена выше. В рассматриваемой модели указанные зависимости определяются *множеством весов* W различных атрибутов, показывающих «степень влияния» значения атрибута киберобъекта на возможность реализации киберугрозы. Указанная таблица может иметь следующую структуру:

	av_1	av_2	...	av_{n-1}	av_n
...					
тип КО и тип угрозы (t)	w_1^t	w_2^t	...	w_{n-1}^t	w_n^t
...					

В таблице используются следующие обозначения:

- КО — киберобъект таксономии;
- $av_1, \ldots, av_n$ — список всех возможных значений атрибутов;
- $w_i^t \in W$ — «вес» соответствующего значения атрибута киберобъекта по отношению к угрозе t.

Указанная таблица будет представлять собой динамическую модель поведения КВОИ.

Алгоритм анализа защищенности объектов КВОИ основан на построении *размеченной системы переходов* (рис. 1), состояния которой отвечают состояниям КВОИ, а переходы — шагам потенциальных кибератак.

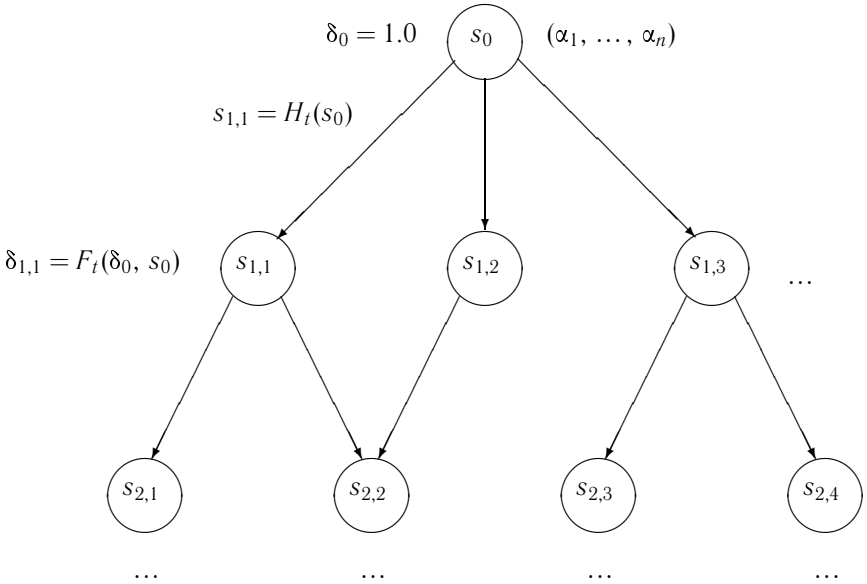


Рис. 1. Схема вычислений для системы переходов

Будем считать, что для каждой киберугрозы t имеется пара функций:

- $F_t\colon [0, 1] \times \{0, 1\}^n \to [0, 1]$ (функция задает вероятность реализации киберугрозы в данном состоянии КВОИ);
- $H_t\colon \{0, 1\}^n \to \{0, 1\}^n$ (функция задает правило перехода КВОИ в следующее состояние по текущему его состоянию).

Кроме того, будем считать, что определена функция $Dmg\colon \{0, 1\}^n \to \mathbb{R}$, которая по данному состоянию определяет величину ущерба, наносимого КВОИ, в случае, если указанное состояние будет достигнуто.

В качестве примера функций F_t, H_t, Dmg можно использовать следующую содержательную модель.

- Каждый атрибут влияет на вероятность реализации угрозы КВОИ независимо от значений других атрибутов. В этом случае $W = \mathbb{R}^+$ и $F_t(r, \alpha_1, \ldots, \alpha_n) = r \cdot \prod_{i:\ \alpha_i = 1} w_i^t$.

- Реализация каждой угрозы предоставляет один новый доступ злоумышленника к ресурсам КВОИ (например, доступ к хосту или владение паролем одного из сотрудников). Тогда $H_t(\alpha_1, \ldots, \alpha_n) = (\alpha_1 \vee e_1, \ldots, \alpha_n \vee e_n)$. В данном случае реализация угрозы t предоставляет один новый доступ злоумышленника к ресурсам КВОИ, характеризующийся вектором $e \in \{0, 1\}^n$.
- Размер ущерба КВОИ характеризуется определенными значениями атрибутов, такими как, например, получение злоумышленником доступа к конфиденциальной информации. Тогда

$$Dmg(\alpha_1, \ldots, \alpha_n) = \begin{cases} N \text{ единиц ущерба}, & \text{если } \alpha_i = e_i = 1 \\ & \text{для некоторого } i; \\ 0 & \text{в противном случае.} \end{cases}$$

В данном случае ущерб КВОИ характеризуется значениями атрибутов, соответствующими ненулевым позициям вектора $e \in \{0, 1\}^n$.

Первым этапом методики является построение модели КВОИ. Построение модели заключается в представлении исходного киберобъекта в виде иерархии элементов таксономии и задания значений всех атрибутов (задание структурной модели КВОИ). Данный этап выполняется вручную или полуавтоматически. Результатом выполнения работы на этапе I будет являться вектор $s_0 \in \{0, 1\}^n$, показывающий начальное состояние КВОИ в системе переходов (рис. 1).

На втором этапе для каждого необработанного состояния $s = (\alpha_1, \ldots, \alpha_n)$ с условием $Dmg(s) \leqslant \Delta$ (где Δ — верхний порог величины ущерба, при котором он еще не считается существенным для функционирования КВОИ) и вероятности состояния δ, для каждой угрозы t вычисляется значение $\delta_t = F_t(\delta, s)$. Если окажется, что $\delta_t \geqslant \sigma$ (где σ — нижний порог для значения вероятности состояния КВОИ, при котором оно еще считается достижимым), то в текущей системе переходов порождается новое состояние КВОИ, определяемое вектором $H_t(s)$ и значением вероятности δ_t (рис. 1). Если состояние $H_t(s)$ в системе переходов уже существует, то новое состояние не порождается, а лишь пересчитывается вероятность его возникновения.

Указанная последовательность шагов повторяется до тех пор, пока возможно порождение новых состояний КВОИ.

При завершении второго этапа система переходов будет представлять собой размеченный, ориентированный граф, в котором простые пути, ведущие из начальной вершины, отвечают возможным сценариям развития атаки.

На третьем этапе строится картина рисков неблагоприятных для исходного КВОИ событий. С этой целью для каждого полученного сценария атаки вида $s_0 \to s_1 \to \ldots \to s_k$ вычисляется величина этого риска по формуле:

$$R = Dmg(s_k) \cdot \delta_k,$$

где δ_k — вероятность состояния s_k. В качестве окончательного результата выдается:

- либо интегральная оценка защищенности КВОИ, получаемая при сложении значений рисков по всем сценариям развития кибератак;
- либо перечень возможных сценариев развития кибератак с указанием вычисленных значений рисков.

2.3. К вопросу анализа защищенности для предприятий нефтегазового комплекса

В данном подразделе в кратком изложении будут представлены некоторые аспекты возможного применения предлагаемой методики для предприятий нефтегазовой отрасли.

При анализе защищенности и оценке рисков предприятий нефтегазового комплекса необходимо кроме информационных аспектов (изложенных ранее) учитывать другие аспекты неинформационного характера. В ходе такого анализа должны быть учтены законодательные акты, положения регламентирующих документов в области обеспечения безопасности жизни и здоровья людей, охраны окружающей среды. Такими в частности являются акты и документы, касающиеся:

- промышленной безопасности;
- транспортировки опасных грузов;
- ведении строительных работ;
- охраны окружающей среды;
- разработки полезных ископаемых.

(названия и некоторый перечень таких законодательных актов приведены в [1]).

Главной задачей анализа защищенности предприятий является снижение рисков деструктивных воздействий на них, которые могут возникнуть как результат природных явлений, различных технических сбоев, ошибок персонала предприятия, преступной деятельности. Таким образом, необходимо учесть все факторы риска для данного предприятия (человеческий фактор, организационный фактор, природно-экологический, информационный).

При рассмотрении информационной составляющей таких КВО можно выделить следующие дополнительные киберобъекты:

- контроллер (обработчик сигналов), включая подвиды:
  - RTU (удаленный терминал);
  - PLC (программируемый логический контроллер);
- сенсор — служит для получения информации о состоянии технологического процесса;
- управляющее оборудование — осуществляет контроль за рабочими компонентами.

С учетом внесенных дополнений становится возможным выделить типовую структуру КВОИ нефтегазового комплекса (прототип модели в соответствии с таксономией).

Первым шагом применения методики анализа защищенности для КВО нефтегазового комплекса (а не только его информационной составляющей) является выделения и анализ угроз, характерных для рассматриваемой области. Разделим все угрозы на три следующие основные группы:

- угрозы, возникающие из-за стихийных явлений;
- угрозы, возникающие из-за ошибок персонала или сбоев оборудования предприятия;
- угрозы, возникающие из-за преступных действий.

Рассмотрим каждую из этих групп угроз. К угрозам, возникающим из-за стихийных явлений, можно отнести:

- паводки;
- ураганы;
- град;
- землетрясения;
- пожары природного характера;
- смещение масс (лавины, сели, оползни, разжижение почвы).

Угрозами, возникающими из-за ошибок персонала или оборудования предприятия, являются:

- неконтролируемое распространение химически опасных веществ;
- пожары техногенного характера;
- взрывы;
- прочие производственные аварии.

Под угрозами, возникающими из-за преступных действий, будем понимать следующие:

- умышленная ошибка в обслуживании оборудования;
- превышение служебных полномочий, нарушение должностных инструкций.

Следующим шагом является создание формальных моделей угроз. Фактически на этом шаге происходит выделение условий, при которых возможно осуществление угрозы, определение взаимного влияния угроз (причин и последствий). Важно отметить, что для определения потенциально уязвимых элементов предприятия, также необходимо провести соответствие выделенных угроз и объектов комплекса:

- производственные, добывающие и обрабатывающие установки;
- инфотелекоммуникационное оборудование;
- линии снабжения;
- производственные и служебные помещения.

После построения формальных моделей угроз появляются объективные условия и основания для создания модели анализируемого предприятия и выявления (на ее основе) возможных деструктивных воздействий, получение значений рисков неблагоприятных ситуаций.

Заключение

В данной публикации рассмотрены некоторые вопросы анализа защищенности КВОИ. Приведено обоснование актуальности такого рода анализа, описание возможных методов его проведения. Показано, что для сложных архитектурно, как правило, распределенных на гетерогенной сетевой среде критически важных объектов, эффективным, а зачастую, и единственно возможным является подход к анализу их защищенности на основе экспертного анализа. Такой анализ и оценка уровня защищенности объекта выполняется с помощью построения математической модели анализируемого КВОИ в соответствии с разработанной таксономией киберобъектов (составляющих частей КВОИ), методология применения которой представлена в настоящей работе.

Описанная выше процедура позволяет получить полную (в рамках построенной модели) картину рисков неблагоприятных ситуаций для подконтрольного (анализируемого) критически важного объекта, связанных с его информационной безопасностью. Ее подробный (строгий) анализ позволяет экспертам выработать обоснованные предложения по формированию или изменению политики безопасности КВОИ, включению новых требований по безопасности для отдельных составляющих КВОИ или к изменению внутренней структуры самого объекта. Такие действия объективно

приводят к изменению модели КВОИ. По этой причине необходимо, начиная с первого этапа, повторить всю описанную выше процедуру анализа рисков. Данный итерационный процесс продолжается до тех пор, пока значения рисков неблагоприятных событий для моделируемого объекта превышают предельно допустимые границы.

Существенным фактором, позитивно выделяющим подход на основе экспертного анализа из числа других является то, что он позволяет проводить эффективный анализ и оценку защищенности КВОИ как на этапах проектирования и разработки, так и на этапах эксплуатации и модернизации КВОИ. При этом следует отметить, что методология этого подхода учитывает не только архитектурно-технологические особенности объекта, но и механизмы (регламенты) функционирования объекта и его составляющих, взаимодействие с другими объектами. Как уже отмечалось ранее, это обстоятельство является крайне важным, поскольку специфика задачи обеспечения национальной безопасности и структура национальной информационно-телекоммуникационной инфраструктуры на сегодняшний день таковы, что нельзя рассматривать ни один ее объект изолированно. При анализе защищенности объекта необходимо учитывать большое число факторов, характеризующих взаимодействие данного объекта с другими элементами инфраструктуры.

Предлагаемая методика позволяет анализировать возможные деструктивные информационные воздействия (кибератаки) на КВОИ, оценивать степень опасности реализации таких воздействий, выявлять возможные слабые места в системе защиты, вырабатывать адекватные предложения по улучшению политики безопасности и осуществлять управление рисками неблагоприятных для КВОИ и КВО событий.

Отметим что предлагаемая методика является расширяемой и, кроме оценки рисков неблагоприятных ситуаций для КВОИ, она позволяет также анализировать риск деструктивных воздействий непосредственно на КВО (с помощью расширения таксономии киберобъектов и построения дополнительных угроз). Возможность подобного расширения для предприятий нефтегазовой отрасли кратко проиллюстрирована в данной статье.

К достоинствам предлагаемой методики можно отнести способность к эффективной интеграции с другими методами анализа и широкие возможности автоматизации многих ее этапов, что позволит применять методику для детального анализа больших и сложных систем управления объектами критически важных инфраструктур РФ.

Литература

[1] *Васенин В. А.* Научные проблемы противодействия кибертерроризму. Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. (Интеллектуальный Центр МГУ, 2–3 ноября 2005 г.) М.: МЦНМО, 2006 г. С. 49–63.

[2] *Васенин В. А.*, *Галатенко А. В.* Компьютерный терроризм и проблемы информационной безопасности в Интернете // Высокотехнологичный терроризм. Материалы российско-американского семинара. (Москва, 4–6 июня 2001 г.) Российская академия наук в сотрудничестве с Национальными академиями США. С. 211–224.

[3] *Васенин В. А.* Проблемы математического, алгоритмического и программного обеспечения компьютерной безопасности в Интернет. Материалы конференции МаБИТ-2003. (Москва, 2003.) С. 111–142.

[4] *Васенин В. А.*, *Галатенко А. В.*, *Корнеев В. В.*, *Макаров А. А.* Математическое и программное обеспечение активного аудита больших распределенных систем, Материалы конференции МаБИТ-2004. (Москва, 2004.) С. 99–117.

[5] *Климовский А. А.* К анализу подходов классификации компьютерных атак. Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. (Интеллектуальный Центр МГУ, 2–3 ноября 2005 г.) М.: МЦНМО, 2006 г. С. 368–390.

[6] *Krsul I. V.* Software vulnerability analysis. PhD thesis, Purdue University, 1998.

[7] *Bishop M.*, *Bailey D.* A critical analysis of vulnerability taxonomies. University of California, Davis, September 1996.

[8] *Vijayaraghavan G.*, *Kaner C.* Bug Taxonomies. STAR EAST 2003, Orlando, FL, May-2003.

[9] *Neumann P.*, *Parker D.* A summary of computer misuse techniques // 12th National Computer Security Conference, 1989.

[10] *Temmingh R.* Breaking into computer networks from the Internet, 2001.

[11] *Mirkovic J*, *Reiher P.* A taxonomy of DDoS Attack and DDoS defense mechanisms. 2002.

[12] Expression of Needs and Identification of Security Objectives (EBIOS), SGDN/DCSSI, `http://www.ssi.gouv.fr/en/confidence/methods.html`.

[13] International standard ISO/IEC 15408, ISO/IEC 15408-1,2,3:1999(E), `http://www.iso.ch/`.

[14] *Neumann P. G.* Computer-Related Risks. ACM Press/Addison Wesley, 1995.

[15] *Грушо А. А.*, *Тимонина Е. Е.* Роль скрытых каналов при построении защиты в распределенных компьютерных системах. Материалы конференции МаБИТ-2003 (Москва, 2003). С. 276–283.

[16] *Галатенко А. В.*, *Наумов А. А.*, *Слепухин А. Ф.* Реализация системы управления доступом к информации в виде встраеваемых модулей аутентификации, Материалы конференции МаБИТ-2003, Москва, 2003. С. 237–240.

[17] Основы информационной безопасности: курс лекций: учебное пособие / Издание третье / Галатенко В. А. Под редакцией академика РАН В. Б. Бетелина / — М.: ИНТУИТ.РУ Интернет-университет Информационных Технологий, 2006.

[18] *Васенин В. А.*, *Большаков М. В.*, *Савкин В. Б.* К вопросу обеспечения информационной безопасности в Федеральном центре управления информационно-технологическими ресурсами. Международная конференция Проблемы функционирования информационных сетей: Материалы конференции (Новосибирск, 31 июля – 3 августа 2006) — ЗАО РИЦ Прайс Курьер, Новосибирск, 2006. С. 59–66.

[19] *Савкин В. Б.* Профили защиты элементов критически важных объектов и меры по поддержанию доверия. Материалы Второй международной научной конференции по проблемам безопасности и противодействия терроризму (в данном сборнике).

Профили защиты элементов критически важных объектов и меры по поддержанию доверия

В. Б. Савкин

1. Введение

В данной работе рассматривается вопрос составления требований безопасности к системам управления критически важными объектами (КВО) целиком, а также к отдельным их компонентам. Предлагаемая методика разработки пакетов требований основывается на том факте, что среди используемых в составе КВО средств вычислительной техники (СВТ) немалую долю составляют классы (типы) средств, имеющие общие уязвимости. Для таких классов целесообразно разработать общие средства и рекомендовать общие методы их защиты. Такие методы естественно формулировать в виде требований безопасности, а наборы требований — оформлять в виде профилей защиты. Структура и содержание профиля защиты задаётся в Руководящих документах Гостехкомиссии РФ (ФСТЭК РФ), в частности, в Положении по разработке профилей защиты и заданий по безопасности. Представленные ниже предложения составлены с учётом требований, перечисленных в этих документах.

2. Общая методика разработки профилей защиты

Для каждого класса СВТ следует предусмотреть несколько уровней защищённости от типовых угроз, в зависимости от важности КВО, информационная система управления которым рассматривается, а также от роли в ней защищаемого элемента. Таким образом, должна быть получена «линейка» — упорядоченный набор профилей для каждого класса СВТ, позиционируемого для применения в КВО.

Предлагаемая методика получения необходимых требований безопасности состоит из следующих шагов.

1. *Классификация элементов компьютерных* (*информационно-вычислительных*) *систем управления КВО*. Выделяются классы типовых элементов, используемых при создании крупных, практически значимых распределённых информационно-вычислительных комплексов. Для каждого класса грубо (в первом приближении) описываются его функции безопасности.

2. *Создание методики определения уровня критичности*[1] *элемента информационно-телекоммуникационной системы управления КВО* на основе его идентификаторов и структуры. Критичность отдельного элемента зависит во-первых, от критичности содержащего его объекта или его структурной единицы (в случае, если последняя может быть отдельно идентифицирована и категоризирована), и во-вторых, от важности данного элемента для объекта или его структурной единицы. На основе идентификаторов КВО можно судить о критичности объекта или структурной единицы. Структура объекта при этом определяет роль элемента, а следовательно его важность и необходимый уровень его защищённости.

Таким образом, двухуровневая схема определения критичности элемента охватывает как характеристики КВО, так и его архитектурную иерархию.

3. *Определение типовых условий окружения*, а именно угроз безопасности[2], требований политики безопасности и предположений об окружении применительно к конкретному элементу.

Список угроз безопасности получается декомпозицией общих угроз объекту на угрозы его отдельным элементам. Защита от этих угроз возлагается на средства и механизмы, встроенные в собственно элемент. Предположения об окружении выводятся из структуры объекта с учётом уровня его критичности и отражают угрозы, от которых должны защищать элементы КВО, соседние с рассматриваемым по архитектурной иерархии. Типовые требования политики безопасности формулируются на основе структуры объекта с помощью общих, концептуальных подходов к обеспечению безопасности, с использованием экспертной оценки и анализа мирового опыта. Требования политики задают меры безопасности, которые долж-

[1] Критичность здесь и далее понимается в смысле уровня ущерба (потерь материально-технического, политического, социального характера или других, которые возникают в случае деградации (частичной или полной) отдельных элементов или системы управления КВО в целом, произошедшей вследствие деструктивного информационного воздействия на систему управления).

[2] Здесь и далее в настоящей работе речь идёт об информационной безопасности, а точнее, о безопасности информационных технологий, используемых в составе информационно-вычислительно-телекоммуникационных системам управления критически важными объектами, которая далее для краткости именуется просто «безопасностью».

ны быть заданы на верхнем по отношению к рассматриваемому элементу уровню иерархии.

4. *Определение базовых и максимальных требований к элементу.* Когда известны угрозы и предположения, можно приступить к перечислению требований безопасности к элементу, описывающих механизмы и мероприятия по защите. Требования формулируются на основе экспертной оценки с учётом мировой практики и последних научных и технологических достижений в данной области. За базовый уровень требований можно взять уровень функциональности и доверия, достигнутый в типовых продуктах данного назначения, имеющихся на мировом рынке. Максимальный уровень следует положить таким, какого можно добиться на практике за разумный с позиции заказчика срок, взяв за основу наивысшие достижения и воспользовавшись наилучшей из известных методологией. Для каждого конкретного элемента степень его критичности будет показывать уровень требований на отрезке между базовым и максимальным.

5. *Оформление требований в виде ряда профилей защиты.* Между базовым и максимальным уровнем необходимо предусмотреть 1–2 промежуточных, с таким расчётом, чтобы соседние уровни легко дифференцировались по степени защищённости. Перечисленные таким образом угрозы, предположения и требования оформляются согласно соответствующим специальным нормативным документам.

Предлагаемая методика позволяет, используя ряд формальных и полуформальных моделей, а так же заключения экспертов, получить набор профилей защиты для каждого из типовых элементов, входящих в состав системы управления КВО. Предложения методики основаны на стандарте ГОСТ Р ИСО/МЭК 15408-1,2,3-2002 и на Руководящих документах ФСТЭК РФ.

3. Классификация основных элементов компьютерных систем управления КВО

Исходя из анализа традиционных решений, используемых при построении информационных систем, можно выделить следующие типовые классы средств вычислительной техники (аппаратных и программных компонентов), присутствующих в большинстве КВО.

Для каждого из таких классов далее приведены механизмы безопасности, которые должны присутствовать для защиты целостности и конфиденциальности от перечисленных выше угроз. Предложенная классификация будет также использоваться в дальнейшем при описании методов защиты от других угроз.

1. *Сервер или рабочая станция* включает в себя:

- вычислительный модуль (содержит один или несколько процессоров и оперативную память);
- устройство локального хранения данных (диски, дисковый массив);
- сетевой интерфейс (обычно используется технология ethernet);
- универсальную операционную систему, поддерживающую исполнение прикладных программ произвольного назначение, предоставляющую им возможность использования перечесленных выше и, возможно, ряда других, требуемых приложением, аппаратных ресурсов и разграничивающую доступ к этим ресурсам;
- локальную консоль с возможностью подключения сменных носителей информации (с необходимой физической защитой).

Операционные системы (ОС) для сервера или рабочей станции можно поделить на следующие подклассы согласно их роли в обеспечении безопасности объекта:

1) ОС с базовыми механизмами защиты, имеющая традиционные для коммерческих (представленных на мировом рынке) систем функции безопасности на основе дискреционной модели логического разграничения доступа;

2) ОС с дополнительными механизмами разграничения доступа, используемыми для поддержки безопасного исполнения различных сервисов;

3) ОС с механизмами мандатного разграничения доступа, поддерживающими многоуровневую модель.

При разработке типовых требований безопасности (профилей защиты) целесообразно рассматривать эти подклассы отдельно.

2. *Оборудование для организации локальной вычислительной сети* содержит, как правило, следующие элементы:

1) коммутаторы: наиболее распространены коммутаторы ethernet с поддержкой виртуальных сетей по стандарту IEEE 802.1q;

2) маршрутизаторы IP с поддержкой интерфейсов ethernet и возможностью подключения к глобальным сетям (WAN — Wide Area Network).

Следует отметить, что функции коммутатора и маршрутизатора могут быть совмещены в одном устройстве.

Для устройств этого класса характерно наличие фильтров сетевого трафика (иногда разбитых на несколько уровней), предназначенных для разграничения доступа внутри распределённой системы.

3. *Оборудование для организации защищенных каналов* — шлюзы виртуальных частных сетей (VPN — Virtual Private Network) — могут использоваться для защиты конфиденциальности и целостности данных при их передаче как по внутренним каналам системы управления, так и для обмена с внешними сетями.

4. *Межсетевые экраны* (с поддержкой физических и виртуальных сетей) используются для более тонкого разграничения доступа между подсистемами объекта. Функции межсетевого экрана могут присутствовать в маршрутизаторе.

Межсетевые экраны используются для защиты периметра и для внутреннего разграничения доступа. Кроме того, они могут быть эффективно интегрированы с системой активного аудита и обнаружения вторжений.

5. *Программное обеспечение поддержки исполнения высокоуровневых задач*, таких, как сценариев, регламентов, бизнес-процессов, может включать в себя следующие элементы:

- среду исполнения сценариев или интерпретатор бизнес-процессов;
- программное обеспечение промежуточного слоя (middleware);
- программное обеспечение, предназначенное для интеграции данных (осуществляющее преобразование между различными форматами и схемами данных);
- шлюзы или адаптеры для связи с другими информационными системами или между подсистемами (преобразования идентификационных и аутентификационных данных для входящих и исходящих информационных запросов);
- анализаторы сценариев или бизнес-процессов (проверка свойств, связанных с их безопасностью).

Средства поддержки электронных административных регламентов являются ключевыми для обеспечения безопасности межведомственного обмена в составе систем управления государственными информационными ресурсами, осуществляя контроль всех доступов как к внешним, так и к внутренним ресурсам.

6. *Веб-серверы* являются распространённым классом программных компонентов для создания пользовательского интерфейса, и обычно включают в себя функции аутентификации пользователей и разграничения их доступа к ресурсам веб-сайта.

7. *Сервер баз данных*, как правило, включает в себя собственные механизмы аутентификации пользователей, разграничения и протоколирования доступа.

8. *Программное обеспечение для мониторинга и аудита* можно разделить на следующие две группы:

1) устанавливаемое на серверах (так называемые сенсоры или агенты), среди которых стандартизованные требования можно предъявлять к тем из них, которые предоставляют доступ по стандартным протоколам и предназначены для интеграции с различными системами мониторинга или активного аудита;
2) устанавливаемое на выделенных узлах (входящих в контур управления объектом и составляющих подсистему мониторинга и активного аудита.

Назначение данного класса программного обеспечения состоит в сборе, хранении и анализе данных аудита и мониторинга, а именно — протоколов и результатов замеров. Необходимы как средства ручного анализа протоколов, так и автоматического (система активного аудита).

9. *Программное обеспечение для поддержки совместной работы пользователей в локальных сетях*, среди которого можно выделить распространённые подклассы:

1) сервисы аутентификации пользователей;
2) средства передачи сообщений (электронная почта, мгновенные сообщения и др.);
3) файловые сервера для рабочей группы.

Программное обеспечение данного класса включает в себя функции аутентификации пользователей и разграничения доступа к ресурсам локальной сети.

4. Определение типовых условий окружения

В данном разделе описывается очередной шаг, предусмотренный методикой разработки профилей защиты для элементов компьютерных систем управления КВО. Действия, выполняемые на данном шаге, определяются стандартом ГОСТ Р ИСО/МЭК 15408, и далее предлагается интерпретация этого стандарта в применении к рассматриваемому в настоящей работе классу информационно-телекоммуникационных систем.

4.1. Общие угрозы безопасности системы управления КВО

Общие угрозы безопасности, рассмотренные ниже, получены путём анализа мирового опыта (отражённого, в частности, в стандарте

ISO 17799 [3]), дополненного результатами работ по идентификации КВО. В список угроз включаются прежде всего традиционные угрозы.

Угрозы целостности и конфиденциальности:

- утечка обрабатываемой информации;
- нарушение целостности (подмены, удаления) информации;
- захват контроля над системой управления КВО или её частью злоумышленниками.

Угрозы доступности:

- частичное нарушение процесса нормального функционирования системы;
- полная потеря управления КВО.

В дополнение к общепринятым угрозам безопасности (целостности, конфиденциальности и доступности) будем также рассматривать и дополнительный тип угроз, связанный со статусом управляемых объектов (КВО):

- угрозы потери доверия к системе.

Полноценное выполнение КВО своих функций в выполнении задач хозяйственного комплекса и экономики страны существенно зависит от доверия, которым этот объект пользуется в глазах потенциальных пользователей. В случае потери доверия к КВО происходит объективное его неприятие значительным числом пользователей, на которых он рассчитан, что не может не вызвать эффективную потерю его функциональности как объекта, поддерживающего запланированные государственные функции. Таким образом, необходима поддержка надлежащего уровня доверия к реализации и функционированию КВО.

В качестве еще одной в дополнение к общепринятым для КВО следует рассматривать

- угрозу зависимости от поставщика средств вычислительной техники (СВТ).

Объективное отставание отечественной IT-индустрии по элементной базе, по ряду других, в том числе программных средств, поддерживающих, например, системные и телекоммуникационные функции, не дает права исключать возможность попадания подобных критически важных объектов в зависимость от поставщиков СВТ, которые неподконтрольны органам государственной власти. Указанное обстоятельство требует такого подхода к плану развития архитектурно-технологического каркаса системы

управления КВО, который бы предусматривал действия, направленные на решение этой проблемы.

Исходя из сформулированных общих угроз можно с помощью декомпозиции вывести условия окружения для отдельных элементов:

- *угрозы* получаются ограничением и детализацией общих угроз на конкретный элемент;
- *требования политики* предназначены, по большей части, для противодействия угрозам, направленным на структуру объекта;
- *предположения об окружении* характеризуют, насколько данным угрозам способны противодействовать другие элементы.

5. Определения целей безопасности элемента

Согласно Положению по разработке профилей защиты и заданий по безопасности Гостехкомиссии России [1], цели безопасности (security objectives) отражают намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации при условиях, определяемых установленными ранее предположениях об окружении. Посредством целей безопасности следует показать, что должно быть сделано для обеспечения надлежащего уровня защищённости изделия информационных технологий.

На основании изложенного выше можно заключить, что определение целей безопасности является промежуточным этапом при формулировании требований безопасности. Цели безопасности выводятся из ранее полученных условий окружения таким образом, чтобы для каждого такого условия существовала цель, отражающая необходимость защиты от соответствующей угрозы или следования соответствующему правилу политики. Цели могут относиться к собственно СВТ, тогда они в дальнейшем переходят в требования безопасности, а могут относиться к окружению, в этом случае достижение целей должно осуществляться правильным использованием изделия. Для подтверждения правильности вывода следует приводить таблицу соответствия условий и целей, являющейся важной составной частью обоснования выбора целей.

6. Определения требований безопасности элемента

Требования безопасности являются самой важной составляющей профиля защиты, так как именно они определяют свойства описываемого объекта с точки зрения его защищённости. Возможные требования подразде-

ляются на функциональные требования безопасности и требования доверия. Стандарт ГОСТ Р ИСО/МЭК 15408 содержит каталог требований безопасности, содержащий иерархически упорядоченный список требований вместе с информацией об их зависимостях, способах выбора и уточнения. Данный каталог не является полным, а содержит те требования, которые были признаны разумными и полезными советом экспертов, участвовавших в разработке «Общих Критериев», поэтому при разработке профилей защиты, наряду с требованиями из каталога, могут также понадобиться и дополнительные требования, разработанные авторами профиля. Кроме собственно списка требований безопасности, профиль должен содержать обоснование, показывающее корректность перехода от целей безопасности к требованиям и полноту покрытия целей.

Корректное определение требований безопасности и формулирование обоснований — трудоёмкая процедура, требующая для своего успешного проведения участия коллегии экспертов и временных затрат от нескольких месяцев до нескольких лет в зависимости от сложности объекта. Принимая во внимание это обстоятельство, а также тот факт, что полный результат подобной работы достаточно объёмен, в настоящей публикации не приведено полного примера определения требований безопасности. Предложения по продолжению работы на этом направлении приведены в следующем разделе.

7. Обеспечение доверия к безопасности элементов элементов компьютерных систем управления КВО

Для критически важных с точки зрения национальной безопасности объектов совершенно необходимыми являются меры по достижению и поддержанию доверия к безопасности управляющих ими информационно-вычислительных комплексов, которые выражаются в повышенных («жёстких») требованиях как к отдельным используемым в составе этих комплексов СВТ, так и к архитектуре подсистем, комплектуемых ими. С учётом того обстоятельства, что работы по созданию такого комплекта доверенных СВТ находятся в начальной стадии, в данном разделе меры по обеспечению и поддержки доверия к безопасности элементов предлагаются в виде плана поэтапного формулирования, достижения и дальнейшего уточнения требований безопасности к СВТ, увязанных с работами по созданию и дальнейшему развитию полигона-макета КВО. План включает в себя следующие этапы:

1) создание начального варианта макета;

2) разработка пакета профилей защиты, то есть формирование требований безопасности к СВТ;

3) создание и ввод в эксплуатацию первой очереди компьютерной системы управления КВО, построенной на основе архитектуры и инструментальных средств, протестированных на полигоне;

4) накопление и использования опыта ее эксплуатации.

Предложенные меры составлены в расчете на то, что первая очередь системы управления КВО будет основана на существующих компонентах. Это означает, что будет использована зарубежная аппаратура (компьютеры и сетевое оборудование, основанная на импортных интегральных схемах), современное системное и прикладное программное обеспечение общего назначения (в основном, с открытыми исходными текстами), коммерческие СУБД. Только это может позволить осуществить своевременный запуск первой очереди такого объекта силами небольшого коллектива (оценки проводились из расчета запуска до 2010 г. коллективом не более 100 разработчиков).

7.1. Меры, принятые на этапе создания макета КВО

В качестве макета КВО для отработки решений по обеспечению информационной безопасности его компьютерной системы управления рассматривается прототип федерального информационно-технологического центра (ФИЦ), предназначенного для реализации межведомственного взаимодействия в такой национально значимой системе, которую принято называть «электронное правительство».

Общая архитектура макета была разработана с учетом требований безопасности, на основе предварительно сформулированной модели угроз. Проведена классификация компонентов макета, для каждого типа определены его функции безопасности в контексте данного полигона, выделены типичные элементы, не являющиеся специфичными для данного объекта. Таким образом, произведена неформальная декомпозиция типовых функций безопасности информационно-телекоммуникационной системы управления данным КВО на отдельные элементы. Проведена работа по описанию методики создания профилей защиты для типовых элементов как ФИЦ, так и подобных распределённых информационно-телекоммуникационных систем.

7.2. Меры по разработке профилей защиты

Проведенная работа по определению задач отдельных компонентов Федерального информационного центра (ФИЦ) по обеспечению его информационной безопасности должна быть продолжена и результат её может выражаться в виде пакета профилей защиты, описывающих все требова-

ния безопасности всех типовых СВТ, которые могут быть использованы в составе КВО.

Основной задачей здесь будет являться формулировка всех функциональных требований к каждому из выделенных ранее типовых классов СВТ.

В плане требований доверия для отдельных компонентов ФИЦ, как объекта, относящегося к категории критически важных, предлагается ориентироваться на ОУД 2–3 для базовой защиты, и на ОУД 5–6 для максимальной. Необходимо также выполнять требования третьего класса защищенности СВТ согласно РД Гостехкомиссии России для среднего уровня защиты, и второго класса — для максимальной защиты. Соответствующим классом защищенности можно руководствоваться при выборе стойкости защитных механизмов, что относится к функциональным требованиям. Данная рекомендация сделана, исходя из предположений о том, что

- некоторая информация, обрабатываемая в ФИЦ, может быть отнесена к государственной тайне;
- программные средства, разрабатываемые в рамках проекта по созданию объекта, основанного на представленных на полигоне решениях, будут, в основном, получены доработкой существующего программного обеспечения с открытым кодом, либо произведены отечественными компаниями, с которыми будет установлено сотрудничество.

Проекты профилей должны быть изучены независимыми экспертами в области оценки безопасности информационных технологий с целью нахождения недостатков и их исправления. Можно порекомендовать размещение проектов профилей в публичном доступе и налаживание сбора мнений компетентных экспертов, интересующихся проблемой защиты информационно-телекоммуникационных систем такого класса. Основное внимание следует обратить на полноту списка условий окружения и целей безопасности, поскольку она обосновывается лишь экспертной оценкой, а не какими-либо моделями.

После разработки профилей должен последовать этап их сертификации и регистрации согласно требованиям действующих нормативных документов.

7.3. Запуск первой очереди объекта

Для запуска первой очереди необходимо провести выбор компонентов, которые, наряду с наличием необходимой функциональности и возможности уложиться в выбранный архитектурно-технологический каркас, удовлетворяют требованиям разработанных профилей защиты, либо могут удовлетворить им после доработки. Очевидно, поиск или разработка таких

компонентов может вестись одновременно с разработкой соответствующих профилей защиты. Выбранные таким образом компоненты следует сертифицировать на соответствие профилям и необходимому уровню доверия.

В случае использования компонентов зарубежной разработки необходимо принять меры по уменьшению зависимости от производителя, в том числе следующие:

- выбор нескольких компонент различных производителей, удовлетворяющих требованиям;
- создание плана периодических проверок взаимозаменяемости компонентов.

Программные средства-компоненты системы управления КВО должны быть проверены на предмет отсутствия недекларированных возможностей. Проверять готовые программные модули с открытыми исходными текстами по полному списку требований к уровням 2 и 1 контроля отсутствия недекларированных возможностей может быть нецелесообразно ввиду отсутствия необходимой документации и большого объёма кода. Однако, в предположении о высокой квалификации и ответственности разработчиков и отсутствии программных закладок, полезным будет автоматический анализ кода на наличие распространённых ошибок, приводящих к уязвимостям. Кроме того, необходимо вести работы по независимому аудиту имеющейся в мире базы свободно распространяемого системного ПО (ядра ОС и основные утилиты). Перечисленные меры, дополненные реализацией новых механизмов безопасности в плане средств разграничения доступа, модульной аутентификации и других подобных механизмов, должны привести к созданию защищённого дистрибутива ОС, удовлетворяющего требованиям высоких уровней контроля отсутствия недекларированных возможностей, и высоких оценочных уровней доверия по ГОСТ Р ИСО/МЭК 15408.

Кроме сертификации компонентов, необходимо принять парадигму поддержки доверия, как описано в стандарте. По выполнению этих действий можно вводить первую очередь ФИЦ в эксплуатацию.

7.4. Начало эксплуатации объекта и использование полученного опыта

По мере приобретения опыта эксплуатации первой очереди ФИЦ можно предположить целесообразность выполнения следующих действий.

- В рамках данного КВО могут быть выделены особо доверенные контуры компьютерной системы управления объектом, и по отношению к ним разработаны повышенные требования доверия. По мере развития объекта и повышения его значения в масштабе государства,

соответствующие компоненты могут быть заменены до более доверенных. Например, программное общего назначения или стандартное импортное сетевое оборудование могут быть заменены на специально разработанные более защищенные изделия, вплоть до разработки таких контуров целиком на отечественной доверенной базе.
- Парадигма поддержки доверия может быть уточнена.
- Могут быть созданы подразделения ФИЦ для специальных задач, с уточнёнными требованиями безопасности.

Авторы считают, что в интересах обеспечения надёжного и безопасного функционирования важных для государства и общества объектов, а также для успешного продолжения работ по созданию общегосударственной системы «электронного правительства», исследования в области решения поставленных в настоящей работе задач должны быть продолжены. Выполнение этого условия позволит вывести методы защищённости критически важных объектов от деструктивных информационных воздействий, которые будут находиться в распоряжении соответствующих государственных органов, на передовой мировой уровень, учитывая при этом особенности, характерные для соответствующего этапа развития России.

Литература

[1] Руководящий документ. Безопасность информационных технолог ий. Положение по разработке профилей защиты и заданий по безопасности. — Гостехкомиссия России, 2003 г.

[2] В. А. Васенин. Научные проблемы противодействия кибертерроризму. // Математика и безопасность информационных технологий. Материалы конференции в МГУ 2–3 ноября 2005 г., М.: МЦНМО, 2006. С. 49–63.

[3] ISO/IEC 17799:2000 — Information technology — Code of practice for information security management — First edition, 01.12.2000.

[4] Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. — Гостехкомиссия России, 2003 г.

Система мониторинга поведения транспортного протокола на уровне ядра операционной системы

В. А. Пономарев, О. Ю. Богоявленская,
Ю. А. Богоявленский

Введение

Протокол Transmission Control Protocol (TCP) [1, 2] играет ключевую роль в управлении трафиком Интернет, контролируя двунаправленные соединения точка-точка. Алгоритмы протокола определяют качественные и количественные характеристики потоков данных большинства приложений Интернет. Именно поэтому поведение реализаций протокола TCP оказывает определяющее влияние на безопасность, устойчивость, надежность и производительность современных сетей. Исследование указанных свойств TCP является весьма актуальным и требует совершенных инструментальных средств мониторинга.

Существующие общеизвестные средства мониторинга поведения TCP [3, 4] позволяют решать широкий спектр задач, но не предназначены для выявления фактов применения несанкционированных информационных воздействий, так как не предоставляют локализованные в ядре ОС данные о динамике состояний и значений переменных, отражающих поведение соединений TCP. Таким образом, задача разработки системы, предоставляющей такие данные, является актуальной.

С точки зрения безопасности такая система будет исчерпывающим решением, позволяющим интегрировать в ОС все возможные функции защиты на уровне TCP. С точки зрения моделирования поведения TCP такая система будет предоставлять исследователю широкий набор данных, которые необходимы для построения и проверки адекватности моделей.

В статье описан прототип системы GetTCP, представляющей собой расширение реализации TCP ядра ОС Linux. Система использует файловую систему relayfs [5] для передачи из ядра в пространство пользователя (с последующей записью в файл) полной информации об изменении

во времени состояний и значений переменных существующих TCP-соединений.

GetTCP работает без потерь, в реальном масштабе времени. Система практически не влияет как на временны́е характеристики TCP, так и на работу других сетевых компонент ядра. Предусмотрена возможность применения GetTCP в многопроцессорных системах.

Статья структурирована следующим образом. В разделе 1 описана архитектура системы, в разделе 2 — ее реализация. Эксперимент по определению реактивности GetTCP представлен в разделе 3. Раздел 4 содержит описание некоторых возможностей применения системы для решения задач безопасности.

1. Основные архитектурные решения

Служебные структуры данных и переменные TCP/IP доступны только в ядре ОС Linux, где, следовательно, и должна действовать часть системы.

С другой стороны, данные нужно хранить в файлах. Надежно и с минимальным влиянием на временны́е характеристики ядра эту функцию следует реализовывать на пользовательском уровне. Причины, по которым нежелательно осуществлять запись в файл напрямую из ядра ОС (снижение надежности, потенциальные проблемы с обеспечением безопасности, отсутствие стандартного программного интерфейса и, как следствие, необходимость использования «трюков» при программировании), описаны в [6].

Архитектура системы представлена на рис. 1. Блок K работает в адресном пространстве ядра, получая данные, которые необходимо записывать, при отправке каждого сегмента TCP. Блок U работает в пользовательском адресном пространстве и записывает полученные данные в файл F. Для уменьшения объема он записывается в двоичном формате, поэтому необходим блок T для преобразования файла к виду, удобному для дальнейшего анализа.

2. Реализация

Описанная выше архитектура была реализована с использованием ядра операционной системы Linux версии 2.6.16 (дистрибутив OpenSUSE 10.1).

Очевидна необходимость передачи данных от блока K к блоку U с минимальными накладными расходами. Для этого целесообразно использовать работающую в оперативной памяти специальную файловую систему relayfs, которая предназначена для эффективной передачи больших объе-

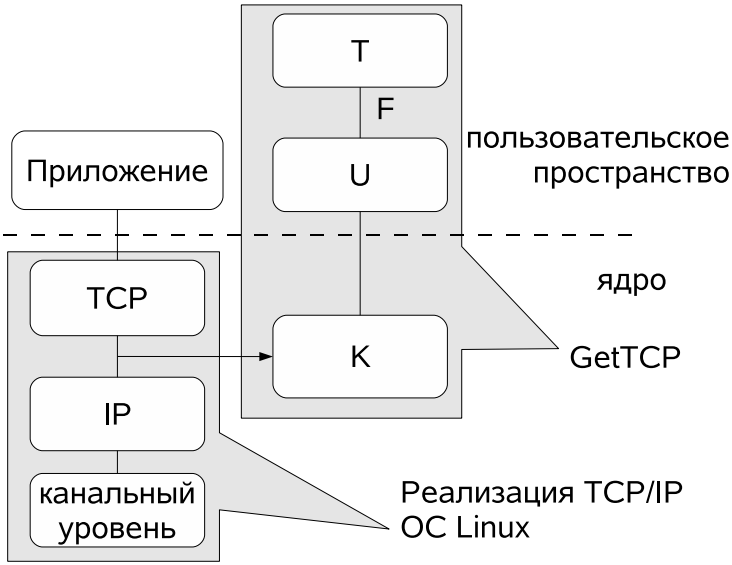


Рис. 1. Архитектура системы GetTCP

мов данных из адресного пространства ядра в пользовательское адресное пространство.

Блок *K* был реализован как загружаемый модуль ядра gettcp_kernel, непосредственно выполняющий функции мониторинга путем взаимодействия с подсистемой TCP/IP ядра. Блок *U* записи данных в файл *F* был реализован как исполняемый файл gettcp_save.

В исходный файл подсистемы TCP ядра, содержащий код отправки TCP-сегмента, были добавлены вызовы функций GetTCP, а также код, обеспечивающий запись состояния TCP, в котором произошла передача (возможно, повторная) сегмента данных и код, обеспечивающий работоспособность ядра при незагруженном модуле gettcp_kernel.

При загрузке этого модуля создается канал передачи данных relayfs, определенный для модуля gettcp_kernel как кольцевой буфер, состоящий из нескольких под-буферов, в которые записываются поступающие данные. В программе gettcp_save этот канал, согласно архитектуре relayfs, представлен как каталог файловой системы, содержащий файл управления модулем gettcp_kernel, файл характеристик реактивности системы и набор файлов данных мониторинга (по три на каждый процессор), предназначенных для дальнейшей записи в долговременную память.

Эти три файла содержат передаваемые данные и счетчики заполненных gettcp_kernel и прочитанных gettcp_save под-буферов, которые обеспечивают управление кольцевым буфером по стандартной схеме. Таким образом, осуществляется контроль потока данных от модуля gettcp_kernel к программе gettcp_save. При переполнении кольцевого буфера передача данных со стороны ядра приостанавливается и формируется информация о количестве потерянных данных о сегментах TCP. Отмеченная ситуация может быть исключена путем подбора параметров GetTCP.

Программа gettcp_save создает для каждого процессора поток (thread), ожидающий появления новых данных, и записывающий их в в файл по мере появления. При этом поток активируется только при заполнении очередного под-буфера, а все остальное время проводит в состоянии ожидания. При активации поток читает данные, появившиеся с момента предыдущей активации, записывает их в файл и обновляет счетчик обработанных под-буферов.

Для доступа к данным, передаваемым через relayfs, программа gettcp_save использует ввод-вывод, основанный на отображения файла в память. При этом кольцевой буфер с помощью соответствующего системного вызова отображается в пользовательское адресное пространство. Дальнейший доступ к данным осуществляется как к обычному массиву, что существенно уменьшает накладные расходы за счет исключения файловых операций.

Таким образом, реактивность системы GetTCP обеспечивается за счет:

- использования расположенной в оперативной памяти файловой системы relayfs;
- реализации программы gettcp_save с помощью потоков, активирующихся только при заполнении очередного под-буфера;
- организации доступа к файлам данных как к массивам.

3. Эксперимент по определению реактивности

В ходе работы модуль gettcp_kernel системы GetTCP постоянно вычисляет время, которое необходимо для сохранения порции данных об одном сегменте TCP в буфере для последующей передачи на пользовательский уровень. Для этой цели используется регистр TSC, доступный в процессоре Pentium (и в следующих за ним моделях процессоров), и содержащий счетчик, увеличивающийся на единицу с каждым тактом процессора. Применение регистра TSC позволяет добиться высокой точности измерения

времени (при тактовой частоте процессора $3 \cdot 10^9$ Гц разрешение равно $\frac{1}{3} \cdot 10^{-9}$ с).

Измеренная величина задержки, внесенной GetTCP в передачу сегмента данных с уровня TCP на уровень IP, а также известный размер сегмента, используются для построения гистограммы распределения величины задержки и размера сегмента. Гистограмма затем может быть прочитана из пользовательской программы.

Для оценки задержки, вносимой GetTCP в передачу сегмента, был проведен эксперимент, в ходе которого с помощью утилиты для измерения производительности на транспортном уровне Iperf [7] передавался максимально возможный объем данных за фиксированный интервал времени (10 секунд). Такая передача проводилась для различных максимальных длин сегментов (от 100 до 1500 байт с шагом 50 байт).

Измерения проводились на следующей аппаратно-программной платформе: две ПЭВМ на основе процессора Celeron с тактовой частотой 3 ГГц; оперативная память объемом 512 Мб; интегрированная сетевая карта SiS900 10/100 Мбит/с; локальная сеть Ethernet 100 Мбит/с; ОС Linux, ядро 2.6.16 (дистрибутив OpenSUSE 10.1).

Полученные результаты представлены в таблице 1 и на гистограмме (рис. 2) распределения задержек, вносимых GetTCP в передачу сегмента TCP (ось ординат в логарифмическом масштабе). Для большинства сегментов (94.02 %) эта задержка не превышает 0.32483 мкс.

Таблица 1. Задержки, вносимые GetTCP в передачу сегмента TCP

Интервал, мкс	Количество сегментов, %
(0, 0.32483]	94.02
(0.32483, 0.64966]	3.44
(0.64966, 0.97448]	1.19
(0.97448, 1.2993]	0.43
(1.2993, 1.6241]	0.11
(1.6241, 1.9490]	0.03
(1.9490, 2.2738]	0.01
(2.2738, 2.5986]	0.01
(2.5986, 2.9234]	0.33
(2.9234, 3.2483]	0.18
(3.2483, 3.5731]	0.04
(3.5731, 3.8979]	0.02
(3.8979, 4.2228]	0.01
(4.2228, 4.5476]	0.02
> 4.5476	< 0.1

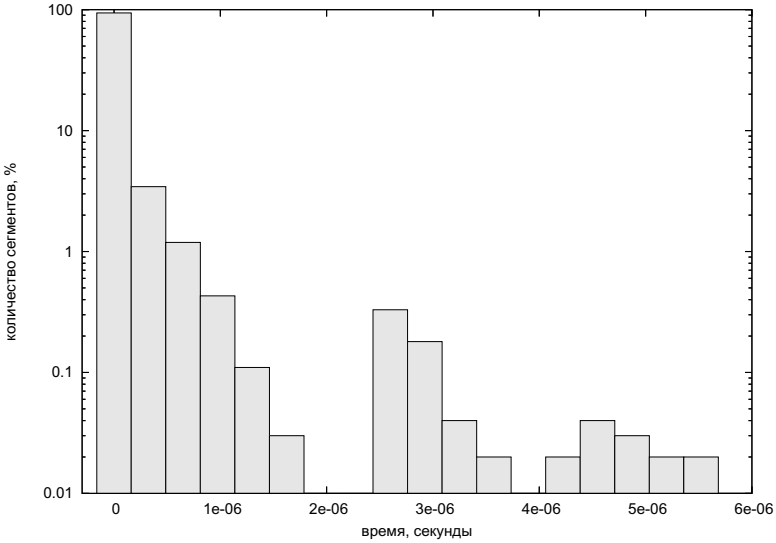


Рис. 2. Гистограмма распределения задержек, вносимых GetTCP в передачу сегмента TCP

4. Применение системы для решения задач безопасности

Особенность системы GetTCP состоит в том, что кроме обычной информации, доступной на пользовательском уровне (заголовки сегментов TCP, дейтаграмм IP и другой), становятся доступными значения внутренних переменных ядра ОС Linux, использующиеся при работе алгоритмов TCP, такие как текущий размер окна или время кругового оборота (round-trip time, RTT). Отмеченное обстоятельство позволяет использовать GetTCP в ситуациях, когда несанкционированное информационное воздействие сложно (или невозможно) обнаружить, используя данные, доступные на пользовательском уровне.

При этом возможно построение системы, сочетающей как доступ к внутренним данным ядра ОС, так и достаточно сложные алгоритмы, выполняющиеся в пользовательском пространстве, которые нецелесообразно реализовывать в ядре ОС.

В качестве примера несанкционированного информационного воздействия можно привести описанную в [8] DoS-атаку. Такая атака использу-

ет особенности алгоритма предотвращения насыщения в TCP, и приводит к катастрофическому падению пропускной способности TCP-соединения. Особенностью этой DoS-атаки является сравнительно небольшая интенсивность вредоносного трафика. Отметим, что это затрудняет ее обнаружение в отличие, например, от атак, заключающихся в перегрузке маршрутизаторов или каналов передачи данных большими объемами трафика.

Суть атаки [8] заключается в том, что с помощью трафика с определенными временны́ми характеристиками (всплески заданной длительности через определенные интервалы времени) достигается переход TCP-алгоритма подверженной деструктивному воздействию системы в состояние ожидания повторной передачи (retransmission timeout, RTO).

Доступ к внутренним переменным алгоритма TCP позволяет определить, чем было вызвано падение пропускной способности соединения и принять необходимые меры (например, каким-либо образом изменить минимальный интервал ожидания при повторной передаче, minRTO, исключив тем самым совпадение периодов вредоносного трафика и попыток повторной передачи алгоритма TCP системы, подверженной атаке).

Другой класс атак на транспортном уровне — отправка сегментов с поддельным адресом отправителя и информацией, приводящей, например, к разрыву TCP-соединения (или к невозможности установить TCP-соединение). В качестве примера можно привести атаку [9]. Набор утилит, входящий в комплект dsniff, использует технологию перехвата данных, описанную, например, в [10]. Утилита tcpkill, входящая в состав dsniff, позволяет разрывать указанное соединение путем отправки поддельных сегментов с установленным флагом RST.

Такие атаки можно распознавать по различным отличительным особенностям последовательности обмена сегментами. Например, активность программы tcpkill приводит к получению системой, подверженной атаке, нескольких сегментов TCP с установленным флагом RST в ответ на один сегмент с запросом на установление соединения, тогда как в нормальных условиях этот ответ должен содержать только один сегмент с флагом RST.

5. Заключение

В статье представлен прототип системы GetTCP, позволяющий выполнять полный мониторинг поведения TCP-соединений на уровне ядра ОС Linux. При реализации прототипа использован ряд системных механизмов, обеспечивающих очень малое влияние процесса мониторинга на временны́е характеристики алгоритмов TCP ядра.

На рис. 3 показан график изменения размера окна TCP, полученный с помощью системы GetTCP.

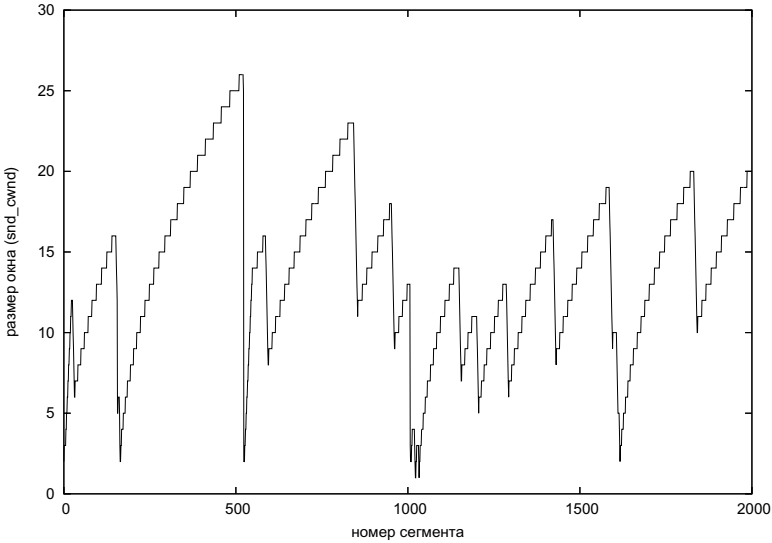


Рис. 3. График изменения размера окна TCP

Предлагаемый подход является перспективным для построения программных систем обнаружения несанкционированных информационных воздействий. Систему GetTCP можно рассматривать как базовое инструментальное системное средство для разработки интегрированных в операционную систему функций защиты транспортного уровня.

Литература

[1] Postel J. Transmission Control Protocol. STD7, RFC793, September 1981.
[2] Allman M., Paxon V., Stevens W. TCP Congestion Control, RFC2581.
[3] tcpdump. `http://www.tcpdump.org`.
[4] tcptrace. `http://masaka.cs.ohiou.edu/software/tcptrace`.
[5] High-Speed Data Relay Filesystem (relayfs). `http://www.opersys.com/relayfs`.
[6] Driving Me Nuts — Things You Never Should Do in the Kernel. `http://www.linuxjournal.com/article/8110`.
[7] The TCP/UDP Bandwidth Measurement Tool (iperf). `http://dast.nlanr.net/Projects/Iperf`.

[8] Kuzmanovic A., Knightly E. W. Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants). ACM SIGCOMM 2003, `http://www.sigcomm.org/sigcomm2003/papers/p75-kuzmanovic.pdf`.

[9] dsniff. `http://www.monkey.org/~dugsong/dsniff`.

[10] Sipes S. Intrusion Detection FAQ: Why your switched network isn't secure. September 10, 2000. `http://www.sans.org/resources/idfaq/switched_network.php`

Реализация сервисов безопасности с помощью неинтерактивных встраиваемых модулей

А. В. Галатенко

Аннотация

В работе «Реализация системы управления доступом к информации в виде встраиваемых модулей аутентификации», результаты которой докладывались на конференции МаБИТ-03, предлагался подход к реализации сервисов безопасности с помощью встраиваемых неинтерактивных модулей аутентификации (Pluggable Non Interactive Authentication Modules, PNIAM). В настоящей работе рассматривается развитие, которое система PNIAM получила в последнее время, прежде всего с целью адаптации PNIAM для нужд систем с повышенными требованиями к безопасности.

1. Введение

Необходимость вынесения сервисов безопасности за рамки приложений и их относительно независимой реализации следует как из общих принципов модульности программного обеспечения, так и из соображений сохранения высокого уровня защищенности информационных систем.

В области информационной безопасности имеют место две противоположные тенденции:

- снижение уровня защищенности, обеспечиваемого существующими реализациями, как в силу выявления уязвимостей и появления новых методов атак, так и вследствие повышения быстродействия компьютеров и расширения возможностей применения метода «грубой силы»;
- появление новых реализаций сервисов безопасности, обладающих повышенной защищенностью.

Чтобы поддерживать защищенность ИС на высоком уровне, необходимо переходить на новые реализации сервисов безопасности или, по крайней мере, модифицировать старые. Это можно сделать экономически и тех-

нически целесообразным образом, только если многочисленные, сложные приложения отделены от сервисов и могут оставаться неизменными.

Ряд сервисов, например, сервис идентификации/аутентификации, целесообразно реализовать централизованно в рамках локальной или корпоративной сети, чтобы, для удобства пользователей, поддержать концепцию единого входа в распределенную систему. Отдельные приложения по мере необходимости удаленно вызывают подобные сервисы, выступая, если это требуется, в роли связующего звена между ними и пользователями или прикладными сущностями. Очевидно, централизованные сервисы должны быть свободны от специфики приложений, а приложения, свою очередь, — от знания специфики сервисов; взаимодействие между ними происходит на основе стандартизованных интерфейсов и/или протоколов.

Как уже отмечалось выше, уровень защищенности, обеспечиваемый некоторой реализацией сервиса безопасности, со временем имеет тенденцию к снижению. Выявляются дефекты реализации, порой обнаруживаются просчеты алгоритмического плана, за счет повышения быстродействия электронных компонентов становятся применимыми методы грубой силы. Соответственно, для поддержания уровня защищенности требуется постоянное усовершенствование реализаций сервисов безопасности или даже их смена. Сделать это экономически целесообразным образом можно лишь в том случае, когда нет необходимости в перекомпиляции (и, тем более, модификации) прикладного ПО.

Универсальные приложения могут использоваться в разных организациях с различными требованиями к информационной безопасности. Набор используемых сервисов безопасности и их реализаций также может варьироваться. Более того, иногда требуется применение нескольких реализаций одного сервиса. Например, элемент функциональных требований «Общих критериев» [6] FIA_UAU.5 предписывает использовать сочетание механизмов аутентификации. Выполнить подобные требования при сохранении стабильности приложений можно только в том случае, когда обеспечена возможность динамической или, по крайней мере, конфигурируемой смены набора реализаций сервисов безопасности.

Примером реализации описанной выше идеологии служат встраиваемые модули аутентификации (Pluggable Authemtication Modules, PAM, [9], [8]). Однако проведенный в [4] анализ выявил в системе PAM целый ряд существенных недостатков, которые были устранены в системе PNIAM.

2. Управляющая библиотека PNIAM

Первоначально управляющая библиотека PNIAM предоставляла приложениям четыре вида функций:

- функции аутентификации (pniam_authenticate);
- функции авторизации (pniam_authorize);
- функции протоколирования (пара pniam_account_start и pniam_account_end);
- функции смены аутентификационных токенов (pniam_change).

Однако в системах с повышенными требованиями к безопасности возникает необходимость в функции пятого типа — выставлении привилегий субъектов (таких как мандатные метки, роли, интегральные квоты ресурсов, доступные системные вызовы, флаги протоколирования и т.п.). Использование привилегий, не входящих в состав стандартных дистрибутивов, диктуется требованиями политики безопасности. Для устранения отмеченного недостатка в состав управляющей библиотеки была добавлена функция инициализации привилегий pniam_setcred. Говоря содержательно, выставление привилегий производится в два этапа: сначала модули собирают всю необходимую информацию, затем производится собственно выставление. Такая реализация обеспечивает выполнение выставления привилегий в заданном администратором порядке (что существенно, так как выставление привилегий некоммутативно).

Еще один недостаток предыдущей версии управляющей библиотеки PNIAM, существенный с точки зрения систем с повышенными требованиями к защищенности — фрагментарность протоколирования результатов и ошибок. Для устранения отмеченного недостатка была реализована динамически подгружаемая функция pniam_log, производящая протоколирование. Описанная реализация позволяет легко менять используемые средства протоколирования, обеспечивая заданную надежность доставки сообщений в регистрационные журналы. Детализация протоколирования задается с помощью конфигурационного файла log_conf в конфигурационной директории PNIAM.

3. Дополнительные PNIAM-модули

Решались следующие задачи:

1) создание набора модулей для инициализации привилегий пользователей;

2) создание набора модулей для перевода аутентификации на отечественные криптографические стандарты;

3) создание набора модулей для выбора стойких запоминаемых паролей.

В рамках решения первой задачи были созданы модули для выставления идентификаторов пользователей и групп, мандатных меток и ролей ([3]), флагов протоколирования ([1]), интегральных квот ресурсов ([2]), домашней директории, временной директории и корня файловой системы.

В рамках решения второй задачи были созданы модули аутентификации и смены аутентификационных токенов на основе ГОСТ Р 34.11-94 [7]. Созданные модули поддерживают хранение паролей в совокупности passwd и shadow файлов директории passwd.d, а также позволяют работать как с непосредственно вводимыми паролями, так и паролями на основе мнемоник (см. ниже).

В рамках решения третьей задачи реализовано два способа генерации мнемоник: с помощью ключевых фраз и с помощью последовательности изображений. Оба способа ориентированы на запоминание случайной последовательности символов заданной длины из алфавита с заданной мощностью. Отсеивание слабых паролей можно производить с помощью созданных модулей pniam_scheck (проверка достаточности числа различных символов) и pniam_cracklib (проверка стойкости к словарным атакам).

Литература

[1] Ахманов С.А., «Протоколирование и фильтрация системных вызовов в ядре ОС Linux» — материалы конференции «Математика и безопасность информационных технологий» (МаБИТ-03), Москва, 2003, стр. 240–253.

[2] Ахманов С.А., Надежкин Д.А., Раевский Д.А., «Дополнительные механизмы обеспечения безопасности в ядре ОС Linux: фильтр системных вызовов, протоколирование системных вызовов, квотирование ресурсов на уровне пользователя» — Международная научная конференция «Суперкомпьютерные системы и их применение» (SSA'2004), Минск, 2004, стр. 266–271.

[3] Галатенко А.В., «Реализация многоуровневой политики безопасности в ОС Linux» — Информационная безопасность. Инструментальные средства программирования. Микропроцессорные архитектуры. Москва, НИИСИ РАН, 2003г., с. 107–125.

[4] Галатенко А.В., «Реализация сервисов безопасности на основе встраиваемых модулей» — Информационная безопасность. Инструментальные средства программирования. Микропроцессорные архитектуры. Москва, НИИСИ РАН, 2003г., с. 91–106.

[5] Галатенко А.В., Наумов А.А., Слепухин А.Ф., «Реализация системы управления доступом к информации в виде встраиваемых модулей аутентификации» — материалы конференции «Математика и безопасность информационных технологий» (МаБИТ-03), Москва, 2003, стр. 237–239.

[6] ГОСТ Р ИСО/МЭК 15408–2–2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ин-

формационных технологий. Часть 2. Функциональные требования безопасности. — М.: ИПК Издательство стандартов, 2002.

[7] ГОСТ Р 34.11-94 «Криптографическая защита информации. Функция хэширования» — Госстандарт России, Москва, 1994.

[8] Материалы по встраиваемым модулям аутентификации, `http://kernel.org/pub/linux/libs/pam/`

[9] Morgan A. Pluggable Authentication Modules (PAM). — Internet Draft: draft-morgan-pam-08.txt, Dec 8, 2001

Контроль доступа к информационным ресурсам в многозвенных информационных системах

Д. П. Зегжда, А. В. Коротич

Аннотация

В статье рассматривается подход к организации контроля доступа к ресурсам информационных систем, построенных по многозвенной архитектуре. Предложенный подход предусматривает внедрения шлюза доступа, обеспечивающего контроль доступа и управление полномочиями пользователей в терминах бизнес-логики приложения. Подход предусматривает формализацию политики безопасности системы, и позволяет отделить реализацию средств контроля доступа от реализации бизнес-логики.

1. Введение

В настоящее время существует несколько подходов к построению информационных систем, каждый из которых обладает уникальными особенностями организации информационных потоков. Несмотря на кажущееся отсутствие общих свойств у информационных систем, построенных с использованием различных архитектурно-технологических подходов, в основе любой из них лежит одна из двух наиболее популярных архитектур, а именно, — клиент-серверные и многозвенные системы (см. [1]). Причем клиент-серверная архитектура на самом деле является частным случаем многозвенной архитектуры. Схема информационной системы, построенной в соответствии с многозвенной архитектурой, показана на рис. 1. В контексте настоящей работы такая система рассматривается в качестве типовой.

В типовую информационную систему, имеющую многозвенную архитектуру, входят следующие компоненты.

- Автоматизированные рабочие места (АРМ) пользователей. В соответствии с получившей широкое распространение идеологией «тонкого клиента» на АРМ пользователей для доступа к ресурсам и сервисам информационной системы используется Web броузер (например, Internet Explorer), работающий с протоколами прикладного

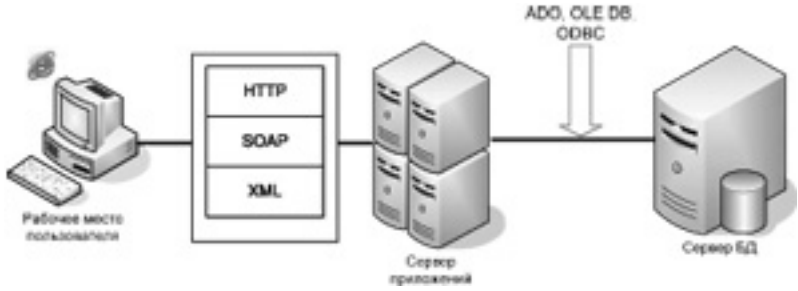


Рис. 1. Схема типовой многозвенной информационной системы

уровня, позволяющими обмениваться запросами сложной структуры(см. [2, 3]), к числу которых относятся SOAP, HTTP, XML.

- Сервер приложений. Это компонент информационной системы, реализующий логику обработки данных в системе и обслуживающий запросы пользователей. Для обращения к базам данных (БД) сервер приложений может использовать любые стандартные технологии доступа. В качестве протокола взаимодействия с клиентами используется протокол SOAP с инкапсуляцией параметров вызова в XML-контейнере.
- Сервер БД. Представляет собой структурированное хранилище данных информационной системы. Сервер не несет функциональной нагрузки, связанной с обработкой данных. Как правило, доступ к серверу БД физически возможен только с сервера приложений. В качестве сервера БД может быть использована любая современная БД.

Многозвенные системы характеризуются наличием большого числа компонент, реализующих контроль и управление доступом на разных уровнях организации информационных ресурсов системы. В качестве таких уровней можно рассматривать следующие.

1. Уровень хранения. Уровень информационных ресурсов БД, таких как таблицы, записи, поля записей, отношения между ними. Средства контроля доступа основаны на назначении прав доступа к указанным сущностям.
2. Уровень приложения. Уровень информационных ресурсов, доступных через сервер приложений, представляющих собой сервисы (функции), предоставляемые приложениям пользователя. Средства контроля доступа позволяют ограничивать набор функций, доступных пользователю, и контролировать допустимые диапазоны значений их параметров.

3. Уровень представления. Уровень семантически значимых информационных ресурсов, отображаемых пользовательским приложением. Средства контроля доступа на этом уровне реализуются непосредственно в составе пользовательского приложения, выводящего на экран только ту информацию, которая должны быть доступна пользователю. Для приложений с повышенными требованиями к их защищенности такой подход непригоден, поскольку легко может быть обойден нарушителем, знакомым с основами программирования.

Несмотря на то, что каждый из перечисленных компонентов, входящих в состав информационных систем, предоставляет развитые средства разграничения доступом, задача контроля и управления доступом к ресурсам информационной системы в целом до сих пор является актуальной. Это объясняется тем, что в многозвенных системах информационный ресурс — это высокоуровневое понятие, не отображаемое однозначно в защищаемые каждым из компонентов разграничения доступа сущности (сетевые порты, определенные на уровне сети, файлы, определенные на уровне ОС, таблицы, определенные на уровне БД). Информационный ресурс — составная сущность, являющаяся совокупностью различных видов взаимосвязанных ресурсов и обладающая семантикой реального понятия автоматизируемого бизнес-процесса (документооборот, бухгалтерский учет и подобные им). Доступ к информационным ресурсам современных систем диктуется обязанностями участников бизнес-процесса и не укладывается в рамки дискреционной и даже ролевой модели разграничения доступа, являющейся основным инструментом управления доступом на каждом из уровней. С точки зрения практической применимости, наиболее востребованными являются средства разграничения доступом, позволяющие реализовать такую политику разграничения доступом, которая будет соответствовать реальным правилам бизнес-процесса и будет учитывать семантику работы системы (см. [4]). В статье описывается подход к созданию средств контроля и управления доступом к информационным ресурсам многозвенных систем в соответствие с политикой безопасности, заданной в терминах предметной области информационных систем.

2. Условия и возможные методы решения задачи

При решении поставленной задачи необходимо выполнить ряд условий, которые позволили бы расширить область применения предлагаемого подхода и обеспечить его преимущество перед существующими подходами. В отличие от существующих подходов, разрабатываемый подход должен обладать следующими свойствами:

- возможность контроля доступа в терминах предметной области информационной системы;
- независимая от прикладной части системы реализация средств защиты;
- инвариантность средств защиты по отношению к защищаемым типам ресурсов;
- сохранение совместимости с существующим программным обеспечением информационных систем.

Анализ существующих подходов показывает, что в зависимости от архитектуры программной системы возможны следующие варианты разработки средств контроля доступа:

- в составе прикладного программного обеспечения;
- на базе сервера приложений;
- на базе сервера БД.

С одной стороны, чем выше уровень абстракции информационного ресурса, доступ к которому контролируется, тем выше сложность реализации средств контроля доступа, поскольку они должны формировать эту абстракцию из низкоуровневых информационных ресурсов, в соответствии с правилами, определенными в системе. С другой стороны, чем выше уровень абстракции, тем более приближенными к предметной области являются сущности и правила контроля доступа. Например, документ в системе электронного документооборота на уровне ресурсов базы данных может быть представлен как набор полей нескольких таблиц. Контролировать доступ к таблицам можно с помощью средств контроля доступа, встроенных в БД. Сложность реализации таких средств относительно невелика. Однако, вынуждая администратора безопасности управлять доступом к документам на уровне прав доступа к полям таблиц, разработчики системы повышают риск влияния человеческого фактора, приводящего к некорректному управлению доступом. Фактически администратор системы в данном случае должен самостоятельно сопоставлять реальные правила бизнес-процесса с физическими сущностями серверов ресурсов. Успешное решение поставленной задачи заключается в нахождении баланса между уровнем абстракции сущностей контроля доступа и сложностью реализации средств защиты. Ввиду чрезмерной сложности компонент информационной системы, интеграция средств разграничения доступа непосредственно в состав программного обеспечения компонент информационной системы не представляется возможным. Таким образом, задача сводится к разработке внешних по отношению к компонентам информационной системы средств контроля доступа, способных интерпретировать

взаимодействия сущностей системы в терминах предметной области и сопоставлять их с правилами обеспечения безопасности автоматизируемого процесса. Практическим воплощением данного подхода должен являться комплекс внешних средств контроля доступа, располагаемых на специализированном звене защиты (шлюзе доступа). При этом одним из главных условий применения подхода является сохранение совместимости или минимальная переделка существующего программного обеспечения (ПО) информационных систем.

3. Предлагаемое решение

Предлагаемый подход заключается во внедрении между клиентами и сервером приложений шлюза-посредника (рис. 2), выступающего в роли фильтра запросов клиентов системы и реализующего политику безопасности на уровне информационных ресурсов. Шлюз перехватывает все запросы пользователей и определяет их соответствие заданной политике безопасности. Для этого шлюз анализирует обращения к функциям сервера приложений, определяет параметры запросов, влияющие на принятие решения о предоставлении доступа, и передает их в функцию контроля доступа. Кроме самих параметров запроса, проверяемого на соответствие политики безопасности, основным параметром процедуры контроля доступа являются атрибуты безопасности объектов, доступ к которым будет осуществлен в процессе выполнения вызываемой клиентом функции (см. [5]). Поскольку шлюз доступа не обладает информацией о том, к каким объектам системы в ходе выполнения запрошенной клиентом операции будет произведен доступ, то определение объектов доступа и их атрибутов безопасности, должно быть реализовано на сервере приложений. Таким образом, разработчики прикладного ПО должны предусмотреть сервис получения атрибутов безопасности и предоставить его в распоряжение шлюза контроля доступа. Важен тот факт, что для того, чтобы успешно взаимодействовать со шлюзом, разработчикам сервера приложений не требуется переписывать функционал всей системы. Им достаточно добавить к нему дополнительный сервис, возвращающий атрибуты безопасности указанных объектов. Получив атрибуты безопасности объектов, к которым осуществляется доступ, функция контроля доступа шлюза применяет к ним правила политики безопасности. Если запрос клиента удовлетворяет заданным логическим условиям политики безопасности, то он передается без изменений серверу приложений. Иначе шлюз отвергает запрос и возвращает клиенту ошибку отказа в доступе.

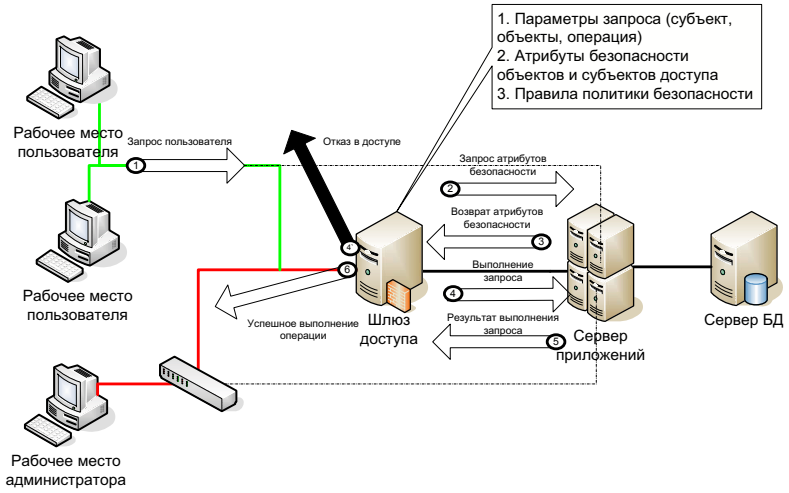


Рис. 2. Схема внедрения шлюза контроля доступа

Внедрение шлюза контроля доступа может осуществляться как в ходе разработки информационной системы, так и в уже готовую, функционирующую систему. В первом случае разработчик сервера приложений должен предусмотреть необходимую поддержку шлюза контроля доступа в соответствии с методикой его внедрения. Во втором случае необходимо, чтобы разработчик сервера приложений осуществил его доработку и расширил его возможности функциями получения атрибутов безопасности объектов контроля доступа. В любом случае последовательность действий по внедрению шлюза контроля доступа будет выглядеть следующим образом.

1. На этапе проектирования информационной системы должны быть определены объекты контроля доступа в виде семантически значимых информационных ресурсов, обработку которых осуществляет система, и для которых существуют требования по разграничению доступа. Должен быть определен набор ролей, использующихся в информационной системе, и полномочия по доступу к объектам для каждой роли. Полномочия ролей должны быть сформулированы в виде правил политики безопасности с использованием автоматизированных CASE средств.
2. На этапе разработки (или доработки) сервера приложений должны быть реализованы функции получения атрибутов безопасности объектов контроля доступа в соответствии с предложенными спецификациями.

3. На этапе интеграции информационной системы шлюз должен быть установлен «в разрыв» сетевого соединения между клиентами и сервером приложений, и в него должно быть загружено формализованное описание политики безопасности информационной системы.
4. На этапе эксплуатации системы управление доступом осуществляется путем назначения пользователям информационной системы ролей, предусмотренных политикой безопасности.

4. Формальная модель контроля доступа к ресурсам ИС

Чтобы показать, что предлагаемый подход является оптимальным с точки зрения баланса между уровнем абстракции сущностей контроля доступа и сложностью реализации средств защиты, построим модель контроля доступа к ресурсам ИС, позволяющую оценить сложность контроля доступа для различных методов. Сложность метода контроля доступа определяется сложностью функции принятия решения о доступе (см. [6]). Введем следующие множества, декартово произведение которых образует область определения функции принятия решения о доступе (функции контроля доступа):

- S — множество субъектов ИС;
- O — множество объектов доступа ИС;
- A — множество операций над объектами ИС.

Тогда функция контроля доступа задается следующим образом:

$$\mathrm{Access}(S,\ O,\ A) \rightarrow \mathrm{true},\ \mathrm{false},$$

где true означает, что запрашиваемый субъектом из множества S вид доступа из множества A к ресурсу из множества O является соответствующим политике безопасности, а false — противоречащим ей.

Определим функции контроля доступа для ресурсов различных уровней:

- $\mathrm{Access}_{db}(S_{db},\ O_{db},\ A_{db})$ — для ресурсов БД (уровень 1, самый низкий);
- $\mathrm{Access}_{app}(S_{app},\ O_{app},\ A_{app})$ — для ресурсов сервера приложений (уровень 2);
- $\mathrm{Access}_{inf}(S_{inf},\ O_{inf},\ A_{inf})$ — для ресурсов информационной системы (уровень 3, самый высокий).

Выбранные уровни ресурсов иерархически упорядочены. Ресурсы более высокого уровня представляют собой совокупность ресурсов нижнего уровня. Объекты сервера приложений могут быть представлены как совокупность объектов БД:

$$o_{app_m} \times a_{app_l} \to \sum_{i,j}^{N} o_{db_{mi}} \times a_{db_{lj}}.$$

Функция контроля доступа к ресурсам сервера приложений раскладывается на функции контроля доступа к ресурсам сервера БД:

$$\begin{aligned}\mathrm{Access}_{app}(s_n,\, o_m,\, a_l) &= \mathrm{Access}_{db}\left(s_n,\, \sum_{i,j}^{N} o_{db_{mi}} \times a_{db_{lj}}\right) = \\ &= \sum_{i,j}^{N} \mathrm{Access}_{db}(s_n,\, o_{db_{mi}},\, a_{db_{lj}}).\end{aligned}$$

Аналогичным образом функция контроля доступа к ресурсам информационной системы раскладывается на функции контроля доступа к ресурсам сервера БД:

$$\begin{aligned}\mathrm{Access}_{inf}(s_n,\, o_p,\, a_q) &= \mathrm{Access}_{app}\left(s_n,\, \sum_{k,o}^{N} o_{app_{pk}} \times a_{app_{qo}}\right) = \\ &= \sum_{k,o}^{N} \mathrm{Access}_{app}\left(s_n,\, o_{app_{pk}},\, a_{app_{qo}}\right) = \\ &= \sum_{k,o}^{N} \sum_{i,j}^{M} \mathrm{Access}_{db}\left(s_n,\, o_{db_{pki}},\, a_{db_{qoj}}\right).\end{aligned}$$

Определим сложность функции контроля доступа как мощность пространства ее входных и выходных аргументов. В приведенном виде, каждая из функций задается на множестве субъектов, объектов и типов доступа к ресурсам базы данных. Чем выше уровень ресурса, к которому осуществляется контроль доступа, тем больше аргументов принимает функция контроля доступа. Таким образом, сложность $S(x)$ функции управления доступом для каждого из случаев можно оценивать размерностью пространства ее входных аргументов, а именно:

- $S(\mathrm{Access}_{inf})$ — 3-мерное пространство;
- $S(\mathrm{Access}_{app})$ — 5-мерное пространство;
- $S(\mathrm{Access}_{db})$ — 7-мерное пространство.

Полученная оценка сложности функции контроля доступа показывает, что контроль требований политики безопасности, предъявляемых к доступу к семантически значимым информационным ресурсам системы, не может быть эффективно реализован на уровнях сервера баз данных и сервера приложений. Поскольку требования политики безопасности могут быть сформулированы только на уровне семантически значимых информационных ресурсов информационной системы (см. [7]), то проекция этих требований на инструменты контроля доступа к объектам низших уровней приводит к существенному возрастанию сложности правил контроля доступа. На практике это приводит к возникновению противоречий, когда для одного и того же множества входных аргументов функция контроля доступа возвращает оба выходных значения. Таким образом, контроль доступа к ресурсам информационной системы в терминах прикладной области является наиболее адекватным способом защиты доступа в современных информационных системах.

5. Выводы

Таким образом, предлагаемый подход позволяет осуществлять контроль и управление доступом в информационных системах с использованием семантики представленных в них информационных ресурсов. Поскольку сами требования безопасности, предъявляемые к информационной системе, задаются в терминах ее прикладной области, то с помощью разработанного подхода становится возможным реализовать эти требования и, в тоже время, значительно упростить управление доступом в ходе их эксплуатации. Основными преимуществами решения являются:

- обеспечение независимости средств контроля и управления доступом от прикладной информационной системы;
- управление доступом в терминах прикладной области;
- сохранение совместимости с существующим программным обеспечением;
- централизация управления доступом к ресурсам информационной системы.

Предлагаемое решение может быть использовано для организации защиты как существующих, так и разрабатываемых информационных систем, строящихся по многозвенной архитектуре. Важным достоинством предлагаемого решения является его инвариантность по отношению к видам информационных ресурсов (см. [8]). С одинаковым успехом данное решение можно применить для организации контроля доступа к информационным

ресурсам самых различных типов, таким как файлы, web-страницы, формы, мультимедиа данные.

Литература

[1] John H. Heimann. Securing Three-Tier Systems with Oracle 8i.

[2] Don Box, David Ehnebuske, Gopal Kakivaya, Andrew Layman, Noah Mendelsohn, Henrik Nielsen, Satish Thatte, Dave Winer. Simple Object Access Protocol (SOAP) 1.1. W3C Note, 8 May 2000.

[3] XML Protocol (XMLP) Requirements. W3C Working Group Note, 28 July 2003.

[4] Ravi S. Sandhu, Edward J. Coyne. Role-based Access control models. IEEE Computer, Number 29, 1996.

[5] Eric Yuan, Jin Tong. Attributed Based Access Control (ABAC) for Web Service. IEEE International Conference on Web Services (ICWS'05), July 2005.

[6] Li Gong, Xiaolei Qian. The Complexity and Composability of Secure Interoperation. 1994 IEEE Symposium on Security and Privacy, May 1994.

[7] M.-Y. Hu, S. Demurjian, T. C. Ting. User-Role Based Security Profiles for an Object-Oriented Design Model. Database Security, VI: Status and Prospects (C. Landwehr and S. Jajodia, eds), North-Holland, 1993.

[8] Ivan Zuzak, Sinisa Srbljic, Ivan Benc. Building Distributed Access Control System Using Service-Oriented Programming Model. International conference on Networking and Services (ICNS'06), July 2006.

Проактивный подход к мониторингу выполнения политики безопасности компьютерных сетей

В. С. Богданов, И. В. Котенко

1. Введение

В настоящее время широко распространенным подходом к управлению безопасностью компьютерных сетей является подход, основанный на использовании политики безопасности. Политика безопасности описывает множество правил функционирования системы, в том числе правил обеспечения конфиденциальности, целостности и доступности ресурсов системы.

На этапе эксплуатации компьютерной системы перед администраторами сети стоит *задача проверки соответствия политики безопасности*, *сформулированной на этапе проектирования*, *ее реализации в реальной системе*, а также задача анализа адекватности этой политики целям обеспечения защиты информационных ресурсов компьютерной системы от текущих угроз безопасности [1].

Настоящая работа посвящена решению первой задачи. Подход, предлагаемый в данной работе, схож с подходом, который используется при активном анализе уязвимостей. При таком анализе исследователь пытается имитировать действия злоумышленника для компрометации различных ресурсов, а затем устраняет обнаруженные уязвимости.

Предлагаемая *система проактивного мониторинга* (*СПМ*) выполнения политики безопасности действует подобным образом. Она использует все доступные знания о системе и политике для автоматической генерации действий пользователя, которые способны опровергнуть или подтвердить выполнение политики. СПМ выполняет данные действия и фиксирует их результаты.

)Работа выполняется при финансовой поддержке РФФИ, программы фундаментальных исследований ОИТВС РАН (контракт № 3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза POSITIF (контракт IST-2002-002314) и RE-TRUST (контракт № 021186-2).

Данная статья построена следующим образом. *Во втором разделе* представлены основные особенности решаемой задачи проверки выполнения политики безопасности. *Третий раздел* посвящен описанию базовых этапов, алгоритмов и особенностей проверки политики безопасности. Реализация предлагаемой системы проактивного мониторинга и проведенные эксперименты рассмотрены в *четвертом разделе*. В *пятом разделе* содержатся выводы и направления будущих исследований.

2. Задача проверки выполнения политики безопасности

Политика безопасности компьютерной сети обычно формулируется на нескольких уровнях детализации [2]: от самого высокого до самого низкого. Для решения поставленной задачи наиболее интересны первый и последний уровень политики безопасности. Политика безопасности высокого уровня описывается руководящими документами и кроме аспектов, относящихся к информационным технологиям, описывает организационные и технические аспекты безопасности. Политика низкого уровня является детализацией политики высокого уровня и представляет собой детальное описание конфигурации информационных и технических средств, а также разрешенных (запрещенных) действий по их использованию.

Можно выделить две основные задачи анализа политики безопасности:

1) проверка выполнения низкоуровневой политики безопасности в компьютерной сети;
2) проверка соответствия высокоуровневой и низкоуровневой политик безопасности.

В данной работе решается первая задача. Для ее решения используется метод сравнения с эталоном [3]. Суть метода в том, что поведение тестируемой системы сравнивается с поведением эталонной системы. В качестве эталона используется формальная модель политики безопасности в реальной компьютерной сети, построенная на основе спецификации правил политики безопасности на некотором языке спецификации.

Выделяется несколько различных категорий правил политики безопасности:

- правила аутентификации — задают методы аутентификации субъектов;
- правила авторизации — определяют права доступа субъектов к объектам;

- правила фильтрации — фиксируют ограничения, накладываемые на сетевой трафик;
- правила защиты канала — определяют методы защиты сетевого трафика.

Для реализации политики безопасности применяются три основных механизма [2]:

1) механизмы разграничения сетевого трафика, основанные на использовании брандмауэров;
2) механизмы защиты сетевого трафика, основанные на применении VPN-средств и (или) специализированных устройств шифрования;
3) механизмы аутентификации и авторизации сетевых сервисов.

В числе функций, которые реализованы в современном брандмауэре, средстве реализации VPN и (или) специализированном устройстве шифрования, могут присутствовать: фильтрация трафика, перенаправление трафика, трансляция сетевых адресов, шифрование пакетов и т.п. Эти действия, так или иначе, являются действиями по обработке пакетов. Для формализации этих действий в работе используются *конечные автоматы*.

Для описания механизмов аутентификации и разграничения доступа применяется *модель матрицы доступов*.

3. Этапы, алгоритмы и особенности проверки политики безопасности

Используемые модели разграничения сетевого трафика, аутентификации и разграничения доступа позволяют разработать автоматическую проактивную систему проверки выполнения политики безопасности в компьютерной сети.

Предполагается, что данная система получает на вход информацию о конфигурации компьютерной сети и низкоуровневые правила политики безопасности. На основе этой информации система строит модель компьютерной сети, которая содержит модели брандмауэров, устройств VPN и сетевых сервисов, а также связи между ними. Затем система использует модели для генерации тестовых воздействий, применяет их к компьютерной сети, получает и анализирует отклики сети. На основе откликов делается заключение о правильности или нарушении выполнения политики безопасности, формируется перечень этих нарушений и детальные данные о них.

Опишем *основные этапы работы такой системы и алгоритмы*, которые могут быть в ней использованы.

Первым этапом проверки выполнения политики безопасности является этап создания модели компьютерной сети и политики. Необходимо получить формализованную информацию о конфигурации сети и политике безопасности и преобразовать их во внутреннее представление и построить модель компьютерной сети и политики.

Вторым этапом является этап генерации совокупности тестовых воздействий, для проверки выполнения политики безопасности.

Каждое тестовое воздействие предназначено для проверки реакции одного из двух элементов модели: брандмауэра или рабочей станции (сервера).

Для брандмауэра и устройств VPN таким воздействием может быть последовательность пакетов, которая будет послана ему по сети с определенного узла. Для рабочей станции таким воздействием может быть операция чтения или записи над файлом выполненная определенным пользователем.

Третий этап — оптимизация последовательности применения тестовых воздействий. После того, как будут сгенерированы совокупности тестовых воздействий, необходимо их оптимизировать.

Оптимизация может затрагивать следующие аспекты:

- удаление избыточных тестовых воздействий;
- нахождение оптимальной последовательности тестовых воздействий;
- нахождение последовательностей тестовых воздействий, которые можно выполнять параллельно.

Эти задачи тесно взаимосвязаны, хотя и формулируются различным образом.

Первая задача состоит в нахождении и удалении таких тестовых воздействий, результат которых можно предсказать, выполнив другие тестовые воздействия. Таким образом, применение избыточных тестовых воздействий становится излишним.

Вторая задача заключается в нахождении такой последовательности применения тестовых воздействий, которая позволит выявлять нарушения политики безопасности за меньшее число шагов.

Третья задача состоит в нахождении последовательностей тестовых воздействий, которые можно выполнять параллельно.

Четвертый этап — это выполнение тестовых воздействий на тестируемой сети и получение откликов сети на эти воздействия.

И, наконец, **пятый**, заключительный **этап** — это анализ откликов на тестовые воздействия и генерация отчетов о выявленных нарушениях политики безопасности.

Рассмотрим подробнее *алгоритмы*, *предназначенные для проверки выполнения политики безопасности*.

Используемая модель *брандмауэра или устройства VPN* представляет собой конечный автомат. Для тестирования автомата необходимо чтобы тестовые воздействия исчерпывали бы все возможные входные воздействия во всех состояниях автомата.

Эта задача может быть решена с помощью следующего алгоритма:

1. Перебрать все состояния конечного автомата:

    1.1. Найти кратчайший путь от начального состояния автомата к текущему состоянию;

    1.2. Перебрать все входные воздействия:

        1.2.1. Создать новое тестовое воздействие;

        1.2.2. Добавить все входные воздействия для пути, найденного в пункте 1.1, к текущему тестовому воздействию;

        1.2.3. Добавить текущее входное воздействие из пункта 1.2 к текущему тестовому воздействию;

        1.2.4. Выдать текущее тестовое воздействие.

Полученный набор тестовых воздействий будет исчерпывающим тестовым набором для данного автомата.

Для *исчерпывающей проверки выполнения правил авторизации сетевого сервиса* необходимо проверить наличие соответствующих прав доступа для всех пар субъект-объект.

Генерация тестовых воздействий для сетевого сервиса может быть описана следующим алгоритмом:

1. Перебрать все субъекты;

    1.1. Перебрать все объекты;

        1.1.1. Перебрать все права доступа;

            1.1.1.1. Создать новое тестовое воздействие;

            1.1.1.2. Добавить к тестовому воздействию аутентификацию в качестве субъекта;

            1.1.1.3. Добавить к тестовому воздействию проверку наличия права для объекта.

Полученный набор тестовых воздействий будет исчерпывающим тестовым набором для данной матрицы доступов.

Существует несколько важных *аспектов* (*особенностей*) *проведения проверок политики безопасности на реальной сети*.

Рассмотрим три таких аспекта:

- выполнение «опасных операций»;
- конфликты с работающими пользователями и реализуемыми процессами обработки информации;
- необходимость иметь базу данных аутентификации.

В процессе выполнения проверки политики на реальной сети может возникнуть *необходимость выполнения «опасных операций»*. Под опасными операциями мы понимаем операции, которые могут привести к нарушению целостности компьютерной системы и содержащейся в ней информации. Например, для файловой системы такими операциями будут удаление или изменение файла. Необходимо предусмотреть резервное копирование данных при выполнении опасных операций или совсем исключить их из процесса тестирования.

Другим аспектом выполнения проверок на реальной сети является *возможность возникновения конфликтов с работой других пользователей и реализуемыми процессами обработки информации*. Такие конфликты могут возникать в результате выполнения практически любых операций, как опасных, так и безопасных с точки зрения целостности информации. Например, может быть запрещен доступ на чтение к файлу, который нужен для редактирования некоторому пользователю. Для устранения таких конфликтов необходимо предусмотреть регламентное время для проведения тестирования, либо учитывать причины возникновения конфликтов при анализе результатов тестирования.

Последним рассматриваемым аспектом является *необходимость иметь в наличии базу данных, которая содержит данные аутентификации* для всех пользователей системы. Эта необходимость вызвана тем, что перед проверкой наличия права субъекта на выполнение операции над объектом необходимо аутентифицироваться в системе как проверяемый субъект. Необходимость создания такой базы данных сужает сферу применения данной системы.

4. Реализация системы проактивного мониторинга

На основе указанных обобщенных алгоритмов были разработаны детальные алгоритмы проактивного мониторинга выполнения политики безопасности [4].

На языке Java с использованием JDK 1.5.0 выполнена *реализация прототипа системы проактивного мониторинга* (СПМ), состоящего из четырех основных компонентов [4]: конфигуратора, сканеров, сборщика информации и пользовательского интерфейса.

Обобщенная архитектура СПМ изображена на рис. 1. СПМ состоит из четырех основных компонентов: конфигуратора, сканера, сборщика информации и пользовательского интерфейса.

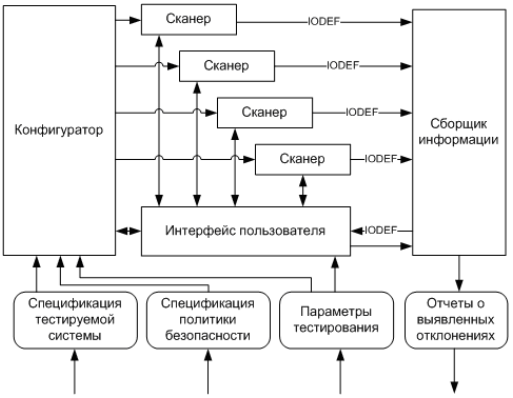


Рис. 1. Обобщенная архитектура системы

Конфигуратор — это компонент, который предназначен для планирования и формирования комплекса сценариев для проведения мониторинга политик. Он получает на вход спецификацию тестируемой системы и спецификацию проверяемых политик безопасности. На основе этих данных конфигуратор формирует сценарии для сканеров, находящихся в системе. Сценарии достаточно просты для выполнения сканерами без проведения дополнительного планирования. Данный подход имеет следующие достоинства:

- становится возможным планировать проверки, проводимые совместно несколькими сканерами;
- самая трудоемкая часть работы выполняется одним компонентом централизованно,
- сканеры представляют собой «легкие» компоненты с простой логикой исполнения;
- уменьшается поток информации, передающейся по сети, так как основная работа с базой данных действий пользователя совершается одним компонентом (конфигуратором), а не несколькими.

Сканер — компонент, проверяющий определенную конфигуратором часть правил политики безопасности в заданном фрагменте тестируемой системы. Задание сканеру передается конфигуратором в виде сценария.

Выполняя данный сценарий, сканер проводит проверку политики. Результаты проверки сканер отсылает сборщику информации.

Сборщик информации получает отчеты о результатах проведенных проверок от сканеров, анализирует полученную информацию и формирует сводные отчеты, которые выдаются пользователю (или «старшей системе»).

Интерфейс пользователя позволяет пользователю управлять работой всех компонентов системы, задавать входные данные конфигуратору, просматривать отчеты сборщика информации.

Для упрощения конфигурирования и передачи информации между компонентами конфигуратор, сборщик информации и интерфейс пользователя объединены в одном исполняемом модуле.

Для достижения наилучших результатов, как минимум, один сканер должен присутствовать в каждом сегменте сети. Помимо этого необходимы сканер, установленный на рабочей станции, сканер, находящейся за пределами сети, и сканер на рабочей станции, которая подключается к анализируемой сети с помощью модема. Если используется беспроводная сеть, нужен также сканер, находящийся на хосте беспроводной сети

Информация от сканера к сборщику информации и от сборщика информации к интерфейсу пользователя передается в формате IODEF [5]. Вся остальная информация внутри системы передается во внутреннем формате, основанном на XML.

В процессе исследований предлагаемого подхода были выполнены различные эксперименты по ее использованию. Для проведения *экспериментов* использовалась модель тестовой сети, состоящей из трех сегментов: внешней сети, внутренней сети и демилитаризованной зоны (ДМЗ). В ДМЗ был сконфигурирован FTP сервер, реализующий правила авторизации для доступа к разделяемым документам. Между сегментами сети расположены брандмауэры, реализующие правила фильтрации межсегментного трафика. В правила авторизации и фильтрации намеренно вносились ошибки, которые система успешно обнаруживала.

Основной экран интерфейса пользователя СПМ показан на рис. 2. Панель закладок на основном экране интерфейса пользователя позволяет просматривать информацию, касающуюся текущей загруженной конфигурации сети, текущей загруженной политики безопасности, состояния сканеров, а также отчет о выявленных отклонениях от политики безопасности.

На рис. 3 показаны результаты работы системы в тестовой сети. Вкладка Report отображает отчеты о выявленных отклонениях от политики безопасности. С помощью вкладки Log можно просмотреть полный лог действий системы.

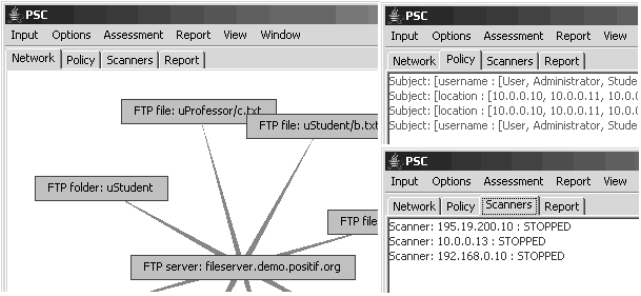


Рис. 2. Основной экран интерфейса пользователя

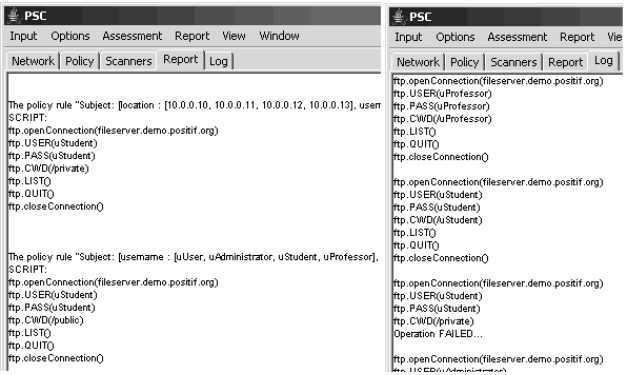


Рис. 3. Результаты работы системы

5. Заключение

В работе предложен подход к проактивному мониторингу выполнения политики безопасности в компьютерной сети на основе сравнения поведения компьютерной сети с математической моделью.

Рассмотрен подход к моделированию основных механизмов реализации политики безопасности в сети: брандмауэров, устройств VPN и различных сетевых сервисов. Определены особенности и недостатки проактивного подхода и методы их устранения.

Указанный подход был воплощен в программном прототипе системы проактивного мониторинга (СПМ) выполнения политики безопасности.

Направлениями дальнейших исследований является разработка методов оптимизации тестовых воздействий, совершенствование предложенных

моделей и методик проактивного мониторинга и проведение экспериментальной оценки предложенных решений.

Литература

[1] Котенко И. В., Юсупов Р. М. Перспективные направления исследований в области компьютерной безопасности // Защита информации. Инсайд. 2006. № 2.

[2] Бармен С. Разработка правил информационной безопасности. М.: Вильямс, 2002.

[3] Beizer B. Software testing techniques. Boston: International Thomson Computer Press, 1990.

[4] Богданов В. С., Котенко И. В. Архитектура, модели и методики функционирования системы проактивного мониторинга выполнения политики безопасности // Труды СПИИРАН. Выпуск 3. Том 2. СПб.: Наука, 2006.

[5] IODEF/IDMEF Solutions, 2004. `http://www.ecsirt.net/service/products.html`.

Автоматизированная система обработки информации в интересах обеспечения безопасности критически важных объектов

С. А. Афонин, А. С. Козицын, А. С. Титов

1. Задачи автоматизированного информационного поиска в интересах обеспечения безопасности критически важных объектов

Одним из важных направлений обеспечения информационной безопасности объектов критически важных для государства инфраструктур [1] является перманентный сбор и анализ информации, имеющей отношение к способам и средствам как реализации деструктивных информационных воздействий против таких объектов, так и мер, методов и средств организации противодействия. К информации такого сорта относятся, например, данные о потенциальных угрозах системам управления критическими объектами, действия преступных и террористических групп, планирующих и выполняющих компьютерные атаки, об уязвимостях в системах, которые при этом используются. Такая информация циркулирует в сетях, включая корпоративные сети и Интернет. Она аккумулируется в различных хранилищах данных, которые формируются как в административном, так и в инициативном порядке. Анализ этой информации представлял ранее, и, тем более, представляет в настоящее время безусловный интерес. Обработка такой информации осуществляется как аналитиками государственных ведомств, так и специалистами служб безопасности критически важных объектов. Она требует высокой квалификации и не может быть выполнена в полностью автоматическом режиме. Вместе с тем, использование специализированных поисковых информационных систем позволяет значительно снизить рутинную нагрузку на человека по сбору, предварительной обработке и группировке информации, и дает возможность аналитику сосредоточиться на решении основных задач анализа, построении и проверке гипотез. К основным услугам, которые должны предоставлять поисковые системы, используемые в данной области, следует отнести:

- поиск информации;
- информационный мониторинг;
- персонифицированный поиск;
- классификация информации;
- оценку путей распространения событий и информации;
- оценку географического распределения информации;
- выявление скрытых характеристик информации.

Поиск информации является одной из наиболее часто встречающихся задач. В процессе поиска система должна выбрать из всего имеющего объема информации наиболее интересные для аналитика данные и представить их в удобном для дальнейшего анализа виде. При осуществлении поиска система анализирует поисковый запрос, заданный человеком, проводит фильтрацию всей имеющейся информации и выдает подборку материалов, соответствующих запросу. Для удобства пользователя язык запросов должен быть максимально прост и выразителен, представление результатов должно быть интуитивно понятным, а качество результатов достаточным для работы аналитика. Стандартными средствами повышения качества поиска являются методы контекстного поиска, методы тематического поиска, методы нечеткого поиска, методы выделения фактов, а методами представления результатов поиска являются ранжирование, аннотирование, кластеризация и визуализация информации.

Информационный мониторинг позволяет пользователю получать с выбранной им периодичностью новую информацию из доступных ему информационных источников (включая Интернет) по темам, которые представляют для него интерес, а также группировать полученную информацию по степени новизны отдельных ее составляющих.

Персонифицированный поиск позволяет предоставлять каждому пользователю результаты, наиболее четко соответствующие информационным потребностям пользователя. Для осуществления персонифицированного поиска и построения профиля пользователя, описывающего его типичные информационные потребности могут использоваться персональные каталоги, в которые пользователь отбирает интересные для него документы, информация о навигации пользователя, а также информация о типичных запросах. Вся эта информация собирается в автоматическом режиме и не требует от пользователя каких-либо профессиональных знаний по настройке поисковых систем.

Классификация информации является мощным инструментом повышения релевантности результатов поиска при контекстном поиске. В большинстве случаев пользователя интересуют ключевые слова в определенной тематике. Например слово «вирус» интересует специалиста по безопасно-

сти только в компьютерной, но не в медицинской тематике. Однако, представляется затруднительным задать несколько ключевых слов, которые бы позволили выделить все тексты по компьютерной тематике, поскольку специальные статьи могут не содержать таких слов как «компьютер». В этом случае полезно предоставить пользователю возможность указать в поисковом запросе интересующую его тематику, а поисковая система на основе внутренней информации автоматически определит рубрику каждого найденного по ключевым словам документа и предоставит пользователю только интересующие его результаты. Классификаторы могут быть разных типов: тематические, эмоциональные, стилистические, целевые, по авторству. В большинстве существующих систем классификация документов осуществляется в ручном режиме, что не позволяет обрабатывать большие потоки информации. Кроме того, как правило, в поисковых системах используется только один классификатор — тематический. В связи с этим, в таких системах невозможно исполнять запросы на пересечение различных классификаторов контента, например, невозможно найти все тексты определенной тематики с определенным отношением автора к обсуждаемой теме (пересечение тематического и эмоционального классификатора).

Оценка путей распространения и географического распределения событий и информации производится на основе автоматического выделения из анализируемых текстов дат и привязок к географическим объектам и на основе поискового запроса позволяет определить, какие географические объекты и в какое время упоминались в связи с интересующей пользователя информацией. Отображение информации должно осуществляться в виде таблиц или анимационных карт и статических карт с выделением связанных фактов для каждой исследуемой области

Выделение скрытых характеристик базируется на выделении фактов и корреляционном анализе и помогает оценить статистические особенности характера информации, а также изменение характера информации. Такие методы позволяют выявлять:

- резкое изменение отношения в определенном регионе к тем или иным обсуждаемым политических вопросам;
- выделяющееся на среднем фоне преобладание агрессивных позиций отдельного средства массовой информации при обсуждении определенных вопросов;
- частое «случайное» упоминание имен в связи с определенной тематикой;
- резкое увеличение обсуждения в публикациях и форумах, связанных с безопасностью какой-либо компоненты программного комплекса.

2. Функциональные возможности системы информационного поиска

При описании необходимых функциональных возможностей автоматизированной системы информационного обеспечения следует ориентироваться в первую очередь на ее использование в современном электронном информационном пространстве (информационные ведомственные порталы, порталы в сети Интернет, СМИ, специализированные форумы и другие источники).

Основными характеристиками этого информационного пространства являются [2]: большой объем информации, непрерывное изменение информации, нечеткая структура данных. Для работы в этом информационном пространстве система информационного обеспечения должна предоставлять возможности обработки информации с использованием современных высокопроизводительных средств параллельной интеллектуальной обработки данных [3], и на основании результатов предварительной обработки предоставлять возможность поиска в информационном пространстве согласно информационной потребности пользователя. Информационная потребность пользователя может выражаться:

- запросом, сформулированным с использованием языка запросов;
- запросом, сформулированным в свободной форме на естественном языке;
- подготовленной пользователем подборкой документов;
- заданием области поиска и частоты сбора информации.

Результатом работы поисковой системы должна являться подборка документов, удовлетворяющих информационной потребности пользователя согласно заданным формальным критериям смыслового соответствия для каждого из перечисленных выше способов ее выражения. Данная подборка может содержать либо все версии документов, полученных при сборе информации в соответствии с явными пользовательскими указаниями, либо только текущие версии документов, во всех иных случаях.

Полученная подборка документов должна быть упорядочена с учетом таких факторов, как:

- степень соответствия документа запросу;
- степень важности или популярности источника документа;
- актуальность вновь поступающей информации для пользователя.

Результат работы системы должен представляться пользователю в компактной форме. С этой целью для каждого из документов должны ав-

томатически формироваться рефераты, а схожие документы в результатах могут объединяться в тематические группы.

Для решения поставленных задач автоматизированная система информационного обеспечения должна обладать следующей функциональностью:

- полнотекстовый поиск;
- тематический поиск информации (тематическая фильтрация входящего информационного потока) по общим темам и по темам, заданным пользователем [4] и специализированная классификация;
- выделение фактов (собственных имен, дат, чисел);
- выделение новых тем в информационном потоке;
- визуализация результатов поиска;
- поиск с использованием структуры документов [5];
- определение актуальности сообщений;
- выделение структуры текста;

Для решения типичных задач, ежедневно решаемыми аналитиками и работниками служб безопасности, помимо осуществления простого поиска, необходимо проведение перманентного *мониторинга* [12] информационных ресурсов по определенным запросам пользователя.

Задачи *мониторинга* можно разделить на следующие классы:

- поиск новой информации по фиксированному запросу;
- определение степени изменения заданного ресурса;
- поиск новых ресурсов по заданной тематике;
- выявление новых тематических направлений в заданной теме.

Поиск новой информации по фиксированному запросу. В случае, когда в должностные обязанности аналитика входит непрерывное отслеживание новых материалов по заданной тематике, аналитик может задать обычный поисковый запрос при помощи указания ключевых слов и рубрик и поставить его на мониторинг. С заданной периодичностью система будет предоставлять пользователю подборку новых документов, найденных в открытых источниках и соответствующих запросу пользователя. В качестве примера использования данной функциональности может служить запрос сотрудника безопасности критически важного объекта на поиск информации о новых найденных уязвимостях в используемых на объекте программных продуктах.

Поиск новых ресурсов по заданной тематике. Данный вид поиска используется, когда пользователя интересуют не отдельные документы, а ресурсы (сайты, порталы, базы данных) по определенной тематике. Источником информации для поиска ссылок на новые ресурсы могут быть

как web-документы (форумы, домашние страницы пользователей, обычные документы), так и сообщения, передаваемые по спискам рассылки электронной почты в заданной предметной области.

Определение степени изменения заданного ресурса. Эту функцию можно рассматривать как систему мониторинга выбранной совокупности ресурсов. Пользователь сообщает список адресов интересующих его ресурсов. Система автоматически производит периодический контроль состояния ресурса и в случае обнаружения изменений информирует об этом пользователя.

Выявление новых тематических направлений в заданной теме. Методы математического анализа текстов позволяют отслеживать момент возникновения нового тематического направления.

Использование подобных автоматизированных систем значительно упрощает задачу мониторинга информационного пространства в целях выявления информации, затрагивающей вопросы террористической деятельности и потенциальных угроз, и позволяет сократить время реагирования, значительно повышая тем самым уровень безопасности критически важных объектов.

В настоящий момент для реализации приведенной выше функциональности информационной системы сбора информации о потенциальных террористических угрозах и уязвимостях разработаны и опробованы модели и алгоритмы для реализации полнотекстового, тематического и специализированного поиска, выделения фактов, поиска новой информации по фиксированному запросу и поиска новых ресурсов по заданной тематике.

3. Основные алгоритмы системы информационного поиска

Построение эффективны средств поиска и анализа требует использования наукоемких алгоритмов. Ниже рассмотрены основные алгоритмы, использующиеся в системе обработки информации в интересах обеспечения безопасности критически важных объектов.

3.1. Тематический поиск информации и специализированная классификация

Тематический поиск информации осуществляется на основе предварительной тематической классификации информации с использованием методов автоматической классификации. Наибольшее распространение для обработки больших объемов данных получили вероятностные и нейросетевые методы классификации из-за большой производительности. Однако,

у каждого из этих методов имеются определенные недостатки. Нейросетевые методы требуют сложного обучения, а вероятностные методы плохо работают при выборе из большого количества вариантов. Одним из возможных решений является использование разработанного авторами модифицированного вероятностного метода с использованием деревьев рубрик. Основная идея метода состоит в предварительной автоматической гравитационной кластеризации [6] рубрик на этапе обучения системы.

При обучении системы на вход модулю обучения подается массив обучающих текстов, по которым в соответствие каждой рубрике ставится массив статистических величин, называемых статистическим портретом рубрики. Каждый статистический портрет представляется точкой в многомерном пространстве с единичной массой,и на основе алгоритма гравитационной кластеризации автоматически строится дерево рубрик (рис. 1). Следует отметить, что качество рубрикации с использованием такого автоматически построенного дерева рубрик, как правило, лучше, чем с использованием дерева, построенного человеком на основе его представления о смысловых взаимосвязях рубрик.

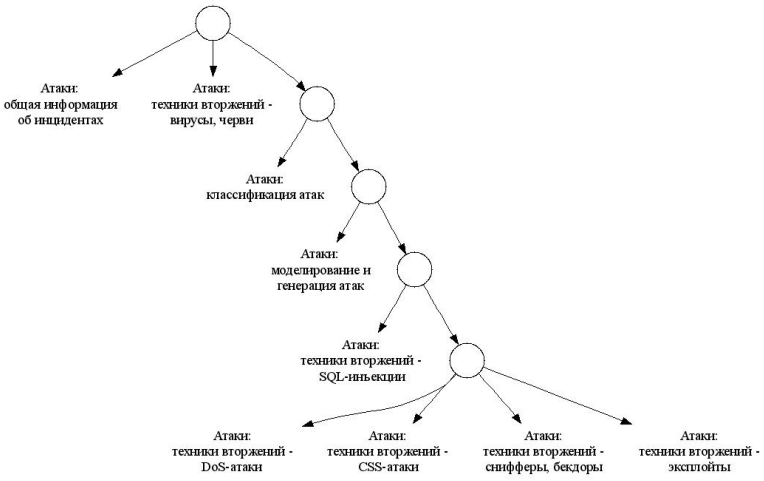


Рис. 1. Пример дерева рубрик для тематики «Компьютерные атаки»

После построения дерева в процессе рубрикации вероятностный алгоритм производит спуск по дереву рубрик производя на каждом шаге процедуру выбора из небольшого количества вариантов на основе заданных обучающих выборок текстов.

Проведенные испытания показывают, что использование дерева повышает точность определения рубрики при большом количестве рубрик с 60–65 % до 87–92 %.

В реализуемой системе предусматривается возможность поиска по нескольким пересекающимся тематическим рубрикаторам с возможностью пересечения рубрик. Данная функция предоставляет обширные возможности по уточнению предмета поиска, например, аналитик может задать в качестве области поиска пересечение рубрик разных типов: «Финансы», «Терроризм», «Нефть», «Ирак». Кроме того, в системе предусмотрена классификация по эмоциональным, целевым, стилистическим и авторским классификаторам осуществляемая на основе той же математической модели, что и тематическая классификация. Основной сложностью при настройке на специальные классификаторы и обучении системы является подбор адекватных обучающих выборок. Если для тематического классификатора обучающие тексты могут быть подобраны неквалифицированными людьми, поскольку тема текста является, как правило, интуитивно понятной, то для составления остальных классификаторов (в том числе эмоционального, представляющего наибольший практический интерес) требуются эксперты в области личностной и социальной психологии. Наличие эмоционального классификатора позволяет задавать системы запросы вида «Федеральные войска», «Негативное отношение» для выявления эмоционального фона в прессе при освещении интересующих аналитика тематик.

3.2. Поиск ресурсов

Задача поиска информационных ресурсов по заданной пользователем тематике может быть разделена на следующие этапы:

- составление списка ссылок на новые ресурсы, потенциально относящиеся к тематике пользователя;
- выделение границ информационных ресурсов;
- классификация ресурсов.

Составление списка ссылок на новые ресурсы производится путем сканирования заданных пользователем источников (списков рассылки, Интернет ресурсов) и выделения всех исходящих ссылок на новые ресурсы.

Задача определения корневой страницы и границы ресурса может решаться как эвристическими методами (например, разделением документов на ресурсы в соответствии со структурой адресов URL), так и путем анализа структуры перекрестных ссылок. Последний метод представляется более универсальным, так как он не зависит от конкретной схемы размещения документов ресурса на сервере, в частности, от системы управления содер-

жанием сайта. Этот метод основан на предположении, что автор ресурса будет использовать навигационные ссылки, позволяющие быстро переходить к документам более высокого уровня, а корневые страницы разделов (или всего ресурса в целом) позволяют пользователю быстро найти интересующую его информацию. При этих предположениях корневые страницы разделов должны иметь относительно большое число входящих ссылок, а документы раздела будут расположены на относительно небольшом расстоянии от соответствующих корневых страниц. Каждому документу можно сопоставить его вес (или меру качества) как источника информации и вес как каталога. Вес документа как источника информации полагается равным сумме весов каталогов, которые ссылаются на этот документ. Вес документа как каталога, напротив, определяется как сумма весов источников, на которые он ссылается. Сформулированные выше предположения о структуре и семантике перекрестных ссылок ресурса позволяют предположить, что корневые страницы ресурсов должны иметь высокое значение веса как источники информации. Задача построения множества потенциальных корневых страниц ресурса решается следующим образом.

Пусть задан граф G перекрестных ссылок между всеми документами сервера, на котором расположен заданный документ d. Вершинам этого графа соответствуют документы, а ребрам — ссылки между ними. Такой граф можно построить методом обхода интернет-документов, начиная со станицы d. В случае если заданная страница d не содержит исходящих ссылок, то в качестве стартовой страницы можно выбрать одну из станиц с усеченным адресом. Матрицу инцидентности A графа G будет иметь вид:

$$A_{ij} = \begin{cases} 1, & \text{документ } i \text{ ссылается на документ } j; \\ 0, & \text{документ не } i \text{ ссылается на документ } j. \end{cases}$$

Определяются вектор-столбец s весов документов как источников, и h — как каталогов, удовлетворяющих равенству $s = Ah$ и $h = A^T s$. Веса источников и каталогов могут быть вычислены путем построения главного собственного вектора матриц AA^T и $A^T A$. Существенно, что матрица инцидентности A для большинства ресурсов будет разреженной, и к ней применимы специальные алгоритмы линейной алгебры.

Для классификации заданного информационного ресурса (совокупности взаимосвязанных гипертекстовых документов) предлагается следующий трехступенчатый процесс:

- выделение «существенных» страниц ресурса;
- классификация отдельных страниц;
- вычисление веса ресурсов.

Выделение существенных страниц ресурса достигается за счет анализа структуры графа, соответствующего ресурсу. Этот анализ проводится исходя из следующих предположений.

- Если документ содержит значимую для данного ресурса информацию, то соответствующая ему вершина графа должна иметь высокую входящую степень.
- Если вершина имеет высокую исходящую степень, то соответствующий документ содержит «общую» (для данного ресурса) информацию.

Для определения существенных документов ресурса производится вычисление весовых коэффициентов, соответствующих алгоритму Клейнберга и разделение полученного множества весов на два кластера методом k-средних (одномерная кластеризация). Существенными документами считаются корневая страница ресурса и документы, вошедшие в полученные кластеры (с максимальными значениями весовых коэффициентов). Весовые коэффициенты могут также учитывать и такой параметр, как расстояние документа о корневой страницы документа.

После выделения значимых документов ресурса производится их классификация, в результате которой для каждого документа D вычисляется степень его соответствия рубрикам C_i, которая обозначается как $P(C_i|D)$.

Степень соответствия всего ресурса S категории C_i оценивается по формуле

$$P(C_i \mid S) \approx \sum_{j=1}^{|S|} P(C_i \mid D_j) W(D_j),$$

где $W(D_j)$ обозначает вычисленный ранее вес документа.

Проведенные авторами эксперименты показывают, что данный алгоритм позволяет находить корневые страницы удовлетворяющих запросу ресурсов, даже если эти корневые страницы вообще не содержат ключевых слов.

3.3. Выделение фактов

Текстовые документы открытых информационных источников содержат упоминания различных имен собственных: фамилий, названий организаций, торговых марок, названий населенных пунктов и других географических названий. Эта информация может использоваться как для построения более точных алгоритмов классификации, так и для интеллектуального анализа документов, например, для автоматического поиска закономерностей в упоминаниях перечисленных объектов. При первом упоминании какого-либо объекта в тексте на естественном языке обычно указывается

и некоторая дополнительная информация об объекте. Так, например, при первом упоминании фамилии можно ожидать, что будет указана должность или какая-либо другая социальная характеристика человека. Задача извлечения фактов из текстовых документов состоит в составлении списка упоминаемых в тексте объектов, включая их дополнительную информацию.

Предполагается, что исходные документы удовлетворяют всем правилам грамматики русского языка. Источником таких документов могут служить, например, публикации в средствах массовой информации. Обработка документов производится по следующей схеме. На первом этапе обработки исходного документа необходимо провести его графематический анализ — разделение текста на отдельные лексемы, выделение лексем, написанных с заглавной буквы, определение сокращений и аналогичных характеристик. Этот этап носит технический характер и подробно не рассматривается. Лексемы, написанные с заглавной буквы, образуют множество потенциальных вхождений имен собственных. На втором этапе строится список предполагаемых имен собственных, включая их дополнительные описания (например, описанием МиГ-21 может быть слово «истребитель»). Один и тот же фрагмент текста может считаться упоминанием разных объектов. На третьем этапе производится анализ построенного списка имен, который позволяет разрешить неоднозначности, полученные на предыдущем этапе, удалить ошибочно определенные вхождения и объединить различные упоминания одного и того же объекта.

Поиск фамилий может производиться в трех вариантах:

- поиск фамилии и имени (и отчества) в случае, когда все элементы встречаются в словаре имен;
- поиск фамилии использует словарь имен, но допускает употребление фамилий, не включенных в словарь;
- поиск, когда имя и фамилия не встречаются в словаре.

При поиске названий организаций под названием организации понимается либо последовательность лексем в кавычках (например, компания «Вымпелком», гранатомет «Муха»), либо именная группа, содержащая слово, написанное с заглавной буквы (например, «вчера на Воскресенском заводе железобетонных изделий произошел ...»). Разделить название собственно организаций и названия других объектов можно только используя семантическую информацию, поэтому название «организация» является условным. При поиске названий организаций, не заключенных в кавычки, может возникнуть смысловая неоднозначность. Так, например, фраза «Воскресенский завод железобетонных изделий не производит» содержит упоминание объекта «Воскресенский завод», в то время как во фразе «Воскресенский завод железобетонных изделий закрыт» упомина-

ется завод железобетонных изделий. Алгоритм поиска в данном случае должен выдавать оба варианта, а выбор конкретного объекта должен производиться на следующем этапе. Если в тексте встречается введенная ранее в явной форме аббревиатура, то ее следует расшифровывать полным названием, указанным ранее, независимо от того, имеет ли она какие-либо другие трактовки. Если аббревиатура не была введена в явной форме, но ранее встречалось название организации, которая может сворачиваться в такую аббревиатуру, то это название следует считать ее расшифровкой. Алгоритм проверки соответствия аббревиатуры и полного названия организации проверяет возможные комбинации первых букв слов названия. Аббревиатуры, которым не соответствуют введенные в тексте организации, должны быть «общеизвестными» и встречаться без явной расшифровки в значительном количестве документов.

Поиск названий населенных пунктов проводится на основании справочника, включающего названия основных географических объектов на территории Российской Федерации и других стран. Для каждого населенного пункта эта база данных содержит указание на его масштаб и ссылку на его административную принадлежность (район, область). Предполагается, что крупные населенные пункты могут употребляться без каких-либо уточняющих оборотов, в то время как упоминания мелких населенных пунктов должны сопровождаться дополнительными ссылками на другие географические названия (деревня Холмы Смоленской области).

Выделение названий населенных пунктов, в сочетании с определением временной привязки документа, позволяет выявлять пространственно-временную картину распространения того или иного явления. Оно может быть обнаружено системой автоматической обработки текстов. Примером такого применения является оценка интенсивности упоминаний в региональных средствах массовой информации событий, связанных с торговлей оружием. Сообщения о торговле оружием могут быть выделены из общего информационного потока средствами системы тематической фильтрации, а для отобранного множества документов может быть проведен анализ по названиям населенных пунктов, что позволит определить географическую принадлежность сообщения. Для зарубежных географических названий существуют свободно распространяемые англоязычные базы данных географических объектов. Для каждого объекта указывается его имя (на языке оригинала в английской транскрипции) и географические координаты, что позволяет применять описанные методы, основанные на близости объектов.

На основе метода выделения фактов были разработаны и опробованы алгоритмы оценки путей распространения и географического распределения информации с отображением на карту России и прилегающих к ней

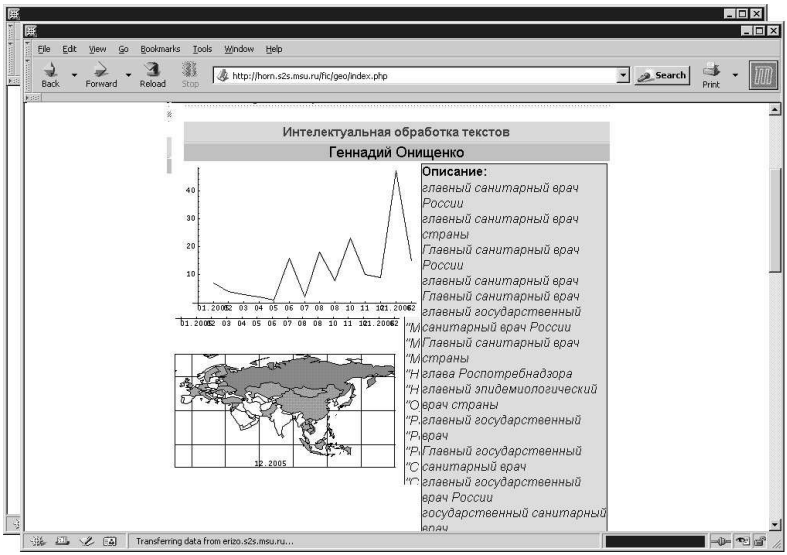


Рис. 2. Анимационная карта распространения информации

странам. Эксперимент проводился на запросах «птичий грипп»(на подборке новостей за несколько лет) и «соль» (на подборке новостей за неделю после «солевого» кризиса). Построенные карты с динамическим цветовым отображением новостей (рис. 2) наглядно показывали основные тенденции развития и распространения информации по заданным запросам.

4. Перспективные направления развития

В целях дальнейшего развития системы обработки информации в интересах обеспечения безопасности критически важных объектов и для улучшения качества предоставляемых системой информационных услуг планируется, прежде всего, разработать и включить в ее состав модули выделения структуры текстов, визуализации результатов поиска, определения актуальности и выделения новых тем.

4.1. Выделение структуры текста

Для решения задач контентного анализа немаловажным источником дополнительной информации является структура текста, описывающая видимые человеку взаимосвязи между отдельными информационными элемен-

тами, а также определяющая приоритетность отдельных информационных полей текста.

Логическая структура является одной из базовых характеристик документа для последующего извлечения смысловой информации поскольку различные структурные элементы обладают разным весом с точки зрения важности содержащейся в них информации. Использование алгоритмов контент анализа, кластеризации и категоризации информационных источников по их словарному содержимому может быть существенно улучшено по точности, быстродействию и другим параметрам, если учитывать расположение лексических единиц текста в тех или иных частях структурной модели документа. В результате построения модели логической структуры документа может быть получено другое представление того же документа (наряду с остальной интересующей нас информацией) в виде XML файлов с единым DTD.

Элементами логической структуры являются заголовки различных уровней, абзацы текста, элементы списков, ячейки таблиц, а также отношения вложенности между всеми этими объектами. Представление документа в виде html файла обычно уже содержит элементы разметки, которые достаточно адекватно отражают логическую структуру. Другим вариантом представления документа являются простые текстовые файлы, где структура задается различными способами форматирования текстовых абзацев.

4.2. Определение актуальности сообщений

При определении актуальности сообщений для пользователя требуется учитывать одновременно несколько факторов: степень новизны сообщения, степень соответствия сообщения информационной потребности пользователя, достоверность источника, степень цитируемости сообщения. Одним из подходов определения актуальности является построение функции, отображающей многомерную область возможных значений перечисленных выше аргументов на одномерную область. В качестве такой функции можно брать, например, произведение или корень суммы квадратов параметров.

4.3. Выделение новых тем в информационном потоке

Для облегчения восприятия большого потока новостных сообщений необходимо проводить предварительную тематическую классификацию сообщений с целью выделения тематических групп. Каждая группа представляет набор близких по тематике сообщений который можно описать одним рефератом. В качестве реферата выбирается смысловая единица наиболее значимая с точки зрения структуры текста и наиболее близкая к центру тематического кластера. В силу большого количества сообщений и критичности времени обработки, в качестве метода кластеризации используются различные варианты метода K-средних или другие методы с высокой

производительностью. В качестве результата работы пользователю предоставляется набор тем с кратким описанием и подборкой сообщений, раскрывающих эту тему.

4.4. Визуализация результатов поиска

На текущий момент самым распространенным способ визуализации и отображения взаимосвязи между текстовыми документами является система иерархий вложенных папок, построенная вручную, цель которой — упрощение поиска нужного документа. Такая структура хранения документов удобна только при небольшом их количестве. При увеличении же их числа появляются различные взаимосвязи между документами и группами документов, которые невозможно представить в виде иерархии. Это обстоятельство требует разработки других способов визуализации.

К наиболее известным средствам иерархической визуализации можно отнести TreeMap [7], BotaTree [8], Star Tree [9] и Hyperbolic display [10].

В методе TreeMap на первом этапе все дерево представляется как прямоугольник. Каждое его поддерево представляется как подпрямоугольник основного прямоугольника. При этом построение подпрямоугольников подчиняется следующему правилу: сначала прямоугольник разбивается на прямоугольники с помощью проведения вертикальных линий, потом горизонтальных и снова вертикальных и т.д. При этом площадь каждого подпрямоугольника пропорциональна числу вершин в нем. Помимо отображения на картинке размера (веса) вершины дерева используют раскраску каждого подпрямоугольника для отображения некоторых дополнительных свойств вершин дерева, например, для отображения глубины вершины.

Метод BotaTree представляет результат в виде биологического дерева. Основной аргумент в эффективности данного подхода заключается в том, что в природе биологическое дерево имеет много листьев, и несмотря на их количество мы без труда различаем всю структуру дерева. При построении этого дерева проводится моделирование, в ходе которого проводится расчет таких параметров как толщина, отклонение и тяжесть каждой ветви.

В методе Star Tree корень дерева помещен в центре некоторой окружности, а его дочерние вершины расположены на окружностях меньшего радиуса.

Hyperbolic display является модификацией метода Star Tree с улучшенной навигацией по данным. Основным достоинством данного метода является фокусировка при движении на данных, интересующих пользователя, с сохранением в поле зрения всей совокупности данных.

В работе [11] предлагается механизм визуализации графа в виде дерева. Пользователь может просматривать дерево, а также, предоставляется возможность получить дополнительную информацию о вершине в виде

вершин, связанных с данной. Данный подход ориентирован на однократный проход дерева. Если рассматривать этот инструмент как инструмент для анализа данных и их структуры, то изменение дерева в ходе его просмотра вызывает трудности в представлении структуры данных.

В работе [6] предложены следующие критерии, по которым оценивается качество визуализации иерархий:

- интуитивная ясность структуры визуализация данных;
- простота в навигации по данным;
- возможность просмотр деталей для произвольной вершины или группы вершин;
- эффективное использование пространства, визуализация не должна быть громоздкой.

Визуализатор должен быть ориентирован на нужды аналитика, основной задачей которого является изучение структуры данных и взаимосвязей между ними. Возможны следующие пути решения этих задач. Первый заключается в анализе структуры данных с использованием статистических методов, таких как кластерный, факторный, дисперсионный, дискриминантный анализы, результатом которых являются таблицы и характеристики в виде чисел, что требует их дальнейшего изучения. Все это возможно только в том случае, если человек обладает достаточными знаниями в области статистических методов и имеет некоторый опыт работы с ними. Альтернативный путь решения проблемы заключается в попытке визуализировать данные для удобного и простого просмотра их структуры и взаимосвязей.

5. Заключение

Представленные в работе и опробованные на практике алгоритмы и методы интеллектуального автоматического анализа тестов позволяют значительно упростить предварительный сбор и обработку информации в интересах обеспечения информационной безопасности критически важных объектов о потенциальных угрозах и проявлениях террористической деятельности. Реализованы алгоритмы поиска информации, выделения фактов, автоматической классификации информации и информационных ресурсов. Проведенные эксперименты практически доказывают эффективность использования предложенных методов при построении автоматизированной информационной поисковой системы и соответствия точности и полноты поиска предъявляемым к системе требованиям.

В дальнейшем планируется развитие существующих в системе моделей и алгоритмов, а также реализация новых методов и алгоритмов, позволяющих улучшать качество поиска. К числу таких перспективных методов относятся методы определения актуальности сообщений, выделения новых тем и выделения структуры текста. Помимо этого, несомненный интерес представляют методы графической визуализации, обеспечивающие возможность быстрого визуального анализа результатов поиска.

Литература

[1] Васенин В. А. Научные проблемы противодействи кибертерроризму // Проблемы безопасности и противодействия терроризму. Материалы конференции. МГУ, 2005. С. 49–64.

[2] Васенин В. А., Афонин С. А., Козицын А. С., Шундеев А. С. Поиск в сверхбольших хранилищах данных и высокопроизводительные системы с массовым параллелизмом // Программные системы: теория и приложения. Труды международной конференции. Переславль-Залесский, май 2004 г., том 1, с. 211–228.

[3] Водомеров А. Н., Конев И. М., Степанов Е. А. Некоторые методы организации высокопроизводительных вычислений в распределенной среде // IX международная конференция «Проблемы функционирования информационных сетей», Новосибирск, 2006.

[4] Козицын А. С., Методы уточнения вероятностной рубрикации текстов // Тезисы докладов. Ломоносовские чтения, секция механика. Апрель 2004. Издательство Московского университета, 2004.

[5] Афонин С. А., Козицын А. С. Поиск текстовых документов с учетом их логической структуры // XII международная конференция по вычислительной механике и современным прикладным программным системам (ВМСППС). Тезисы докладов. Т. 1, 2003, с. 74–75.

[6] Титов А. С. Кластеризация на основе гравитационного метода // Информационные технологии и программирование: Межвузовский сборник статей. Вып. 2(7). М.: МГИУ, 2003.

[7] Coulom Remi. Treemaps for Search-Tree Visualization // The Seventh Computer Olympiad Computer-Games Workshop Proceedings, Maastricht, 2002.

[8] Kleiberg E. et al. Botanical Visualization of Huge Hierarchies // Proceedings 1999 IEEE Symposium on Information Visualization (InfoVis'99), IEEE Computer Society, p. 4–9.

[9] Lamping J., Rao R. The Hyperbolic Browser: A Focus + Context technique for Visualizing Large Hierarchies // Proceedings of CHI'95, ACM Conference on Human Factors in Computing Systems, 1995, p. 401–408.

[10] Batagelj V. et al. Clustering Large Datasets and Visualizations of Large Hierarchies and Pyramids Symbolic Data Analysis Approach // Workshop on Symbolic Data Analysis (PKDD'2000), 2000, p. 69–81.

[11] Ming C. Hao et al., Web-Based Visualization of Large Hierarchical Graphs Using Invisible Links in a Hyperbolic Space // HP Laboratories Palo Alto, 2000.

[12] Козицын А. С. Система тематического мониторинга распределенной текстовой информации // Третья международная конференция по проблемам управления (20–22 июня 2006 г.), Москва, 2006. Т. 2. С. 125.

К созданию автоматизированных средств верификации программного кода

Ф. М. Пучков, К. А. Шапченко, О. О. Андреев

1. Введение

Одним из важнейших требований к системе обеспечения информационной безопасности на объектах, потенциально уязвимых в плане кибератак, является защита используемого программного обеспечения (ПО) от возможных сбоев в работе. Это требование становится особенно важным при проектировании информационных систем с высоким уровнем требований к их защищенности, в том числе при разработке и реализации программно-технических средств защиты информации, что отражено в соответствующих Руководящих документах ФСТЭК ([1]). Возникновение подобных сбоев зачастую связано с наличием в программных средствах подобных систем уязвимостей и ошибок, в том числе таких, использование которых злоумышленником может привести к нерегламентированному политикой безопасности повышению его привилегий на узле и являться одним из этапов атаки на компьютерную систему. Кроме того, возникновение сбоев в работе ПО может приводить к аварийному завершению функционирования важных программно-аппаратных компонентов, создавая угрозу отказа для системы в целом. Имея в виду существующие подходы к разработке и последующего сопровождения ПО ([2, 3, 4, 5]), в частности, ПО с открытым исходным кодом, на первый план выходит задача создания эффективных средств аудита исходного кода ПО. К задачам верификации программного кода, как к ключевым при аудите программных средств, относятся:

- обнаружение и устранение уязвимостей ПО (с использованием средств статического анализа кода, тестирования и отладки);
- построение систем формальных доказательств корректности программы или ее частей.

Решение таких задач позволяет обеспечить необходимый уровень защищенности ПО. В связи с изложенным, средства и методы верификации

ПО являются необходимой составляющей общего комплекса мер по обеспечению информационной безопасности в системах с высоким уровнем защищенности (доверия).

В настоящее время эффективных и широкораспространенных автоматизированных средств верификации исходного кода программ не существует. По этой причине, как правило, верификация осуществляется вручную специально подготовленной группой экспертов. Следовательно, существует вероятность возникновения ошибки при работе экспертов, причем при увеличении объема анализируемого кода эта вероятность увеличивается. Указанное обстоятельство является недопустимым при построении информационных систем с высоким уровнем требований к их защищенности. По этой причине при построении таких систем актуальной становится разработка и использование на практике автоматизированных средств обнаружения уязвимостей ПО. Использование таких средств позволит существенно снизить объем рутинной работы, выполняемой экспертами, и повысить точность анализа.

В настоящей публикации излагается подход к созданию автоматизированного средства обнаружения различных классов уязвимостей программ на основе методики статического анализа их исходных текстов. Одним из главных требований к реализации такого подхода является его *консервативность*, что означает гарантированное обнаружение всех возможных уязвимостей, относящихся к определенному классу (при этом допускается наличие произвольного количества ложных тревог). Основными классами выявляемых уязвимостей являются ошибки в программах на языке C или C++ при работе с памятью (переполнение буфера, разыменование недействительного указателя, ошибки при захвате или освобождении памяти, ошибки форматной строки), некорректное преобразование данных (возможное при приведении типов), утечки памяти, переполнения целых типов. В разделе 2 каждый из указанных классов уязвимостей описан более подробно.

В формулировке, подобной приведенной выше, задача создания автоматизированных средств верификации программного обеспечения ставилась в работах [6, 7]. В указанных работах также описываются подходы к созданию инструментальных средств аудита исходного кода программ на наличие потенциальных уязвимостей, в первую очередь связанных с использованием механизмов работы с памятью. Однако методам, описанным в [6, 7], присущи такие недостатки как:

- низкая эффективность анализа программ, содержащих рекурсивные вызовы функций;

- невозможность обработки неявной передачи управления (например, в языке C эта возможность реализуется с помощью указателей на функции).

В настоящей работе будет показано, каким образом, в рамках предлагаемого подхода, можно указанные недостатки устранить.

2. Актуальность проблематики

В настоящем разделе приводятся некоторые статистические данные, подтверждающие актуальность проблемы обнаружения уязвимостей в программах, в частности уязвимостей программ на языках C и C++ различных классов.

В таблице 1 приводятся данные о количестве проектов с открытым исходным кодом, зарегистрированных к началу 2007 года на сайте `http://www.sourceforge.net`. В первой колонке перечислены выбранные языки программирования (ЯП). Во второй колонке приведены сведения о количестве проектов с открытым исходным кодом, написанных с использованием соответствующего ЯП, [1)] выпускающихся под лицензией GPL и имеющих по крайней мере один стабильный релиз. В третьей колонке приведены сведения о количестве проектов с открытым исходным кодом, написанных с использованием соответствующего ЯП, имеющие по крайней мере один стабильный релиз независимо от лицензии распространения. В четвертой колонке приведены сведения об общем числе проектов с открытым исходным кодом, написанных с использованием соответствующего ЯП.

Таблица 1

	GPL, Stable	Stable	All
C	3021	4304	17384
C++	2500	3730	19160
Java	2056	4318	21830
PHP	2578	3303	14979
Perl	1351	1829	6465
Python	671	1103	6004
Lisp	61	80	333

Из приведенной таблицы видно, что, несмотря на развитие высокоуровневых ЯП, проекты с открытым исходным кодом, написанные с использо-

[1)] Таким образом, проекты, написанные с использованием двух и более ЯП из представленных в таблице, будут учтены несколько раз.

ванием языков C и C++, по-прежнему составляют значительную часть от общего числа таких проектов.

Таблица 2 более точно отражает сведения о соотношении использования языков C и C++ по отношению к другим ЯП в различных дистрибутивах операционной системы Linux. Для примера были выбраны дистрибутивы Red Hat Linux 7.1 (апрель 2001) и Debian 3.1 (июнь 2005).

Таблица 2

	Red Hat Linux 7.1 (апрель 2001)	Debian 3.1 (июнь 2005)
C	21,461,000 (71.18 %)	130,847,000 (57 %)
C++	4,576,000 (15.18 %)	38,602,000 (16.8 %)
Java	147,000 (0.46 %)	3,679,000 (1.6 %)
PHP	—	2,144,000 (0.93 %)
Perl	563,000 (1.87 %)	6,415,000 (2.8 %)
Python	285,000 (0.95 %)	4,129,000 (1.8 %)
Lisp	722,000 (2.40 %)	6,919,000 (3.0 %)

В первой колонке перечислены выбранные языки программирования (ЯП). Во второй колонке приведены сведения об общем количестве строк исходного кода, относящегося к соответствующему ЯП, входящего в дистрибутив Red Hat Linux 7.1 ([8]). В третьей колонке приведены сведения об общем количестве строк исходного кода, относящегося к соответствующему ЯП, входящего в дистрибутив Debian 3.1 ([9]).

Таким образом, среди ПО с открытым исходным кодом, наблюдается преобладание программ, написанных с использованием языков C, C++. По этой причине, а также ввиду отсутствия распространенных автоматизированных средств анализа исходного кода, удовлетворяющих современным требованиям, предъявляемым к такому анализу, задача автоматизации процесса аудита исходного кода программ, написанных на языках C и C++, остается актуальной на настоящий момент.

Рассмотрим некоторые классы наиболее распространенных уязвимостей в программах на различных языках программирования. Несмотря на тот факт, что в настоящее время существует и поддерживается большое число баз данных, содержащих сведения об уязвимостях программного обеспечения, до сих пор отсутствует их общепринятая классификация. Тем не менее, можно выделить, а в некоторых случаях даже формализовать, некоторые классы уязвимостей ПО. В таблице 3 в первой колонке приведен перечень рассматриваемых классов. Во второй и в третьей колонках таблицы приведены сведения о количестве уязвимостей, зарегистрирован-

ных центром реагирования на компьютерные инциденты (CERT), а также в базе данных CVE.

Таблица 3

	`http://www.cert.org` (на начало 2007 г.)	База данных CVE (октябрь 2005 г.)
Переполнения буфера	935	3203
Ошибки при обращении к памяти	65	91
Переполнения целых типов	84	232
Ошибки форматной строки	71	415
SQL-инъекции	27	1961
Утечки памяти	28	84
Гонки потоков	27	132
Повторные освобождения памяти	10	5

Приведем краткую характеристику перечисленных в таблице классов уязвимостей.

Переполнения буферов составляют класс уязвимостей, присущих программам, написанным на языках программирования C и C++, при которых в ограниченную область памяти (буфер) записываются данные, превышающие по размеру вместимость буфера. В случае, когда буфер располагается на стеке процесса, возникает потенциальная угроза подмены адреса возврата из функции и загрузки на исполнение кода с привилегиями запущенной программы. Приведенная схема является далеко не единственной, при которой возможно использование отмеченной уязвимости. Более подробное исследование данного вопроса, включая рассмотрение способов предотвращения возможностей использования уязвимостей, связанных с переполнением буферов, можно найти в работе [10].

Ошибки при обращении к памяти составляют класс уязвимостей, характерных для программ, написанных на языках программирования C и C++. В результате реализации уязвимости такого класса программа аварийно завершает работу при попытке обращения к области памяти, выходящей за пределы сегмента, отведенного под выполнение соответствующего процесса. Необходимо отметить, что реализация данного класса уязвимости может возникать и без участия злоумышленника.

Переполнения целых типов (или *арифметические переполнения*) составляют класс уязвимостей, присущих программам, написанных с использованием любых ЯП. Реализация уязвимости возникает при попытке записать целое значение, выходящее за пределы допустимого диапазона, в некоторую область памяти или регистр. В результате такого действия нарушаются предполагаемые арифметические соотношения между

целочисленными переменными в программе (например, при сложении двух положительных чисел результат может оказаться отрицательным). Как следствие, это приводит к дальнейшему некорректному функционированию программы. Необходимо отметить, что переполнение целых типов может приводить к реализации уязвимостей других классов, например, вызывать переполнения буферов или ошибки при обращении к памяти.

Ошибки форматной строки составляют класс уязвимостей, связанных с возможностью передачи злоумышленником в программу произвольной строки (форматной строки), содержащей информацию о структуре обрабатываемых данных. Реализация уязвимости может приводить к некорректному считыванию (записи) данных из памяти. При последующем использовании такой форматной строки злоумышленник получает возможность получить внутренние данные программы, находящиеся на стеке. Ошибки форматной строки могут встречаться в программах, написанных на таких ЯП, как C, C++ и Perl.

SQL-инъекции ([11]) составляют класс уязвимостей, возникающих чаще всего при недостаточно аккуратной проверке и обработке данных, передаваемых от пользователя веб-приложения к СУБД. Для эксплуатации этой уязвимости необходимо определенным образом «подменять» исполняемый SQL-запрос, что позволит получить несанкционированный доступ к данным СУБД, недоступным при регламентированным способе такого взаимодействия. SQL-инъекции чаще всего обнаруживаются в программных продуктах, написанных с использованием скриптовых языков, таких как PHP, Perl и других.

Утечки памяти составляют класс уязвимостей, связанных с операциями выделения/освобождения памяти, которые могут приводить к постоянному увеличению памяти, выделенной для выполнения программы. Неиспользуемые программой участки памяти при этом не освобождаются. Данный вид уязвимостей может встречаться в программах, написанных на любых ЯП. Реализация уязвимостей данного класса может привести к отказу в обслуживании.

Гонки потоков ([12]) составляют класс уязвимостей, связанных с ошибками синхронизации в многозадачных системах. Уязвимости данного класса встречаются в программах, написанных с использованием любых ЯП. Реализация данного класса уязвимостей может привести к неконтролируемому поведению системы.

Повторные освобождения памяти составляют класс уязвимостей, возникающих при попытке освободить недействительный указатель, с которым не ассоциирован какой-либо участок памяти. Уязвимости встречаются, как правило, в программах, написанных с использованием языков

C и C++. Реализация данного класса уязвимостей может привести к аварийному завершению программы, порче данных или другим последствиям.

Метод, рассматриваемый в настоящей работе, позволяет автоматически обнаруживать уязвимости большинства классов из представленных в таблице 3 (за исключением, SQL-инъекций и гонок потоков), что представляет значительную часть от общего числа встречающихся уязвимостей ПО.

3. Подходы к созданию инструментальных средств анализа программ на языке C или C++ на предмет обнаружения потенциальных уязвимостей

В настоящем разделе будут рассмотрены основные особенности существующих методов решения задачи анализа программ на предмет обнаружения в них потенциальных уязвимостей, а также будут проанализированы их достоинства и недостатки. Кроме того, будет представлен новый подход к решению этой задачи, позволяющий частично устранить отмеченные недостатки.

3.1. Существующие подходы

Подходы к решению задач, связанных со статическими методами обнаружения уязвимостей в исходном тексте программ, в том числе, связанных с переполнениями буфера, предлагались и ранее ([6, 7, 13, 14, 15]). В данном подразделе рассмотрим две наиболее известные в данной области работы.

Метод, рассмотренный в работе [6], является одним из первых, относящихся к числу строго формализованных. В указанной работе представлена математическая модель обнаружения уязвимостей, связанных с переполнением буферов, в программах, написанных на языке C. К числу основных особенностей данного метода относятся следующие:

- для каждого указателя, определенного в исходном коде, вводятся две дополнительные переменные, содержащие информацию о размере выделенного для него участка памяти и о длине строки, содержащейся в данном участке;
- с каждой целочисленной переменной связывается целочисленный интервал, моделирующий допустимое для нее множество значений;
- каждый шаг в исходной программе преобразуется к набору операций над интервалами и к набору условий на эти интервалы, позволяющих гарантировать отсутствие ошибок при работе с памятью;

- с помощью алгоритмов целочисленного анализа проверяется истинность полученных условий.

Отдельный интерес представляет работа с функциями, с конструкциями передачи управления внутри функции и сложными типами данных.

Анализ исходного кода проводится для каждой функции отдельно, при этом строится интервал, содержащий ее возвращаемое значение. Такое действие позволит в каждой точке вызова функции использовать выведенный для нее интервал. Следует отметить, что построенный таким способом интервал для возвращаемого значения функции не зависит от интервалов ее параметров, что существенно снижает точность анализа.

Для моделирования некоторых внешних функций, например, функций обработки строк, используются заранее определенные операции с интервалами и условиями на них. Вызовы таких функций подменяются указанными аннотациями.

Рассмотренный метод не позволяет учитывать структуру графа передачи управления в пределах одной функции. Это обстоятельство существенно упрощает алгоритм анализа, однако, вместе с тем, приводит к значительному увеличению числа ложных тревог.

К другим недостаткам метода можно отнести невозможность работы с двойными массивами (например, `char**`) и указателями на функции.

Таким образом, рассмотренный в работе метод может считаться прототипом для построения других, более совершенных средств анализа, однако, и это следует отметить, он неприменим для анализа крупных программных комплексов.

В работе [7] рассматривается автоматизированное инструментальное средство, позволяющее проводить аудит исходного кода программ, написанных на языке C, на предмет наличия ошибок при обращении со строковыми массивами.

Предложенный авторами метод, также как и рассмотренный ранее, позволяет анализировать отдельные функции, определенные в исходном коде программы, независимо от результата анализа других функций. Аналогично рассмотренному ранее методу, с каждым выделенным участком памяти связывается семейство ассоциированных переменных, после чего инструкции, входящие в исходный код программы, преобразуется в инструкции, оперирующие с целочисленными переменными и условиями на них. Истинность указанных условий позволяет гарантировать в исходной программе отсутствие ошибок при работе с памятью.

Для анализа каждой отдельной функции используется множество предусловий, выполняющихся перед вызовом функции, и множество постусловий, которые должны выполняться непосредственно после ее вызова. Та-

кие условия могут формироваться как самим пользователем средства, так и в автоматическом режиме. Однако принципы функционирования алгоритмов автоматической генерации пред- и постусловий в работе [7] не раскрываются. Таким образом, при анализе крупных программных продуктов пользователю придется самостоятельно указывать пред- и постусловия для значительного числа функций, в противном случае анализ приведет к большому числу ложных срабатываний.

К числу других недостатков метода относится невозможность работы с указателями на функции.

3.2. Новый подход к созданию инструментальных средств анализа исходного кода программ, написанных на языках C и C++, на предмет обнаружения потенциальных уязвимостей

В настоящем подразделе рассматриваются особенности архитектуры и режимов работы компонент автоматизированного инструментального средства для анализа исходного кода программ, написанных на языке C, на предмет обнаружения потенциальных уязвимостей (далее — «Анализатор»). Отметим, что в дальнейшем возможно расширение области применимости «Анализатора» на программы, написанные на языке C++. Рассматриваются следующие классы уязвимостей:

- переполнения буферов;
- ошибки при обращении к памяти;
- переполнения целых типов;
- ошибки форматной строки;
- утечки памяти;
- повторные освобождения памяти.

На вход «Анализатор» принимает исходный код программы на языке C и файл, содержащий правила ее сборки (далее — *файл сборки*). Исходный код представляет собой множество «единиц трансляции» (как правило, файлов `*.c` и `*.h`). Файл сборки (например, `Makefile`) содержит информацию о зависимостях между модулями и о порядке выполнения каждой из стадий сборки программы.

На выходе «Анализатор» выдает сообщения о местоположении возможных уязвимостей и их описание.

Общая структура инструментального средства представлена на рис. 1. В ней выделяются следующие три компонента, характерные и для других аналогичных программных комплексов (например, [7]):

- модуль лексического и синтаксического анализа, осуществляющий анализ файла сборки проекта, лексический и синтаксический разбор

анализируемой программы, соединение деревьев разбора (в случае анализа многофайловых проектов);
- модуль, осуществляющий упрощение дерева разбора;
- компонент, осуществляющий преобразование дерева разбора к блок-схеме и анализ блок-схемы.

В последующих подразделах каждый из перечисленных компонентов рассматривается более подробно.

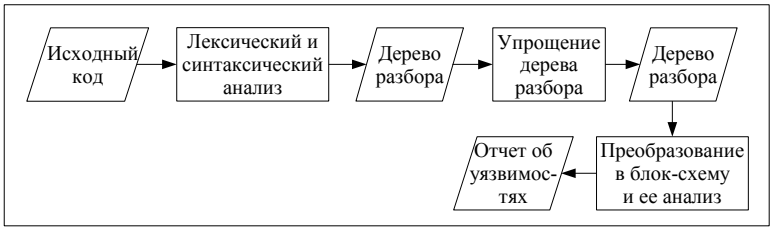


Рис. 1. Структура автоматизированного средства верификации исходного кода программ

3.3. Лексический и синтаксический анализ кода

Модуль синтаксического и лексического анализа осуществляет трансляцию исходного кода программы в дерево разбора в соответствии с правилами грамматики языка C (согласно стандарта ISO 9899:1999 «C99»). Исходный код представляет собой множество файлов, содержащих транслируемые конструкции, и, возможно, файл, содержащий правила сборки программы (файл сборки). При этом интерфейс рассматриваемого модуля имитирует интерфейс компилятора языка C. Это обстоятельство позволяет, в случае использования автоматизированных средств сборки (таких как, например, `make, cmake, scons`), автоматически выполнять подмену вызова компилятора в файле сборки вызовом модуля. Синтаксический и лексический разбор файлов исходного кода осуществляется с использованием автоматизированного средства генерации парсеров `DParser` и дополнительно реализованных средств лексического и синтаксического разбора. Перечислим свойства «Анализатора», гарантируемые подобной структурой модуля:

- возможность интеграции с автоматизированными средствами сборки;
- возможность параллельной трансляции (по аналогии с возможностью параллельной сборки комплекса);

- возможность анализа кода, генерация которого происходит только во время сборки комплекса (в случае, когда участки исходного кода зависят от результатов выполнения / трансляции других участков).

Более подробно последовательность действий представлена на рис. 2.

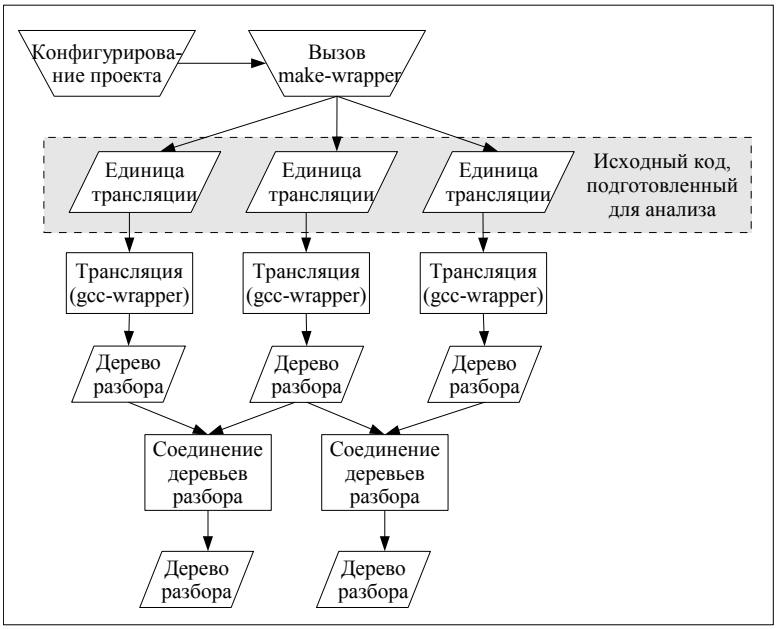


Рис. 2. Схема работы модуля синтаксического и лексического анализа

На первом шаге пользователь инструментального средства анализа исходного кода осуществляет конфигурирование комплекса (в соответствии с инструкцией по его сборке). Далее он вызывает специальную «обертку» для средств сборки (`make-wrapper`),[2] в которой устанавливаются значения переменных (`CC, LD, AR`) и вызывается обычная команда сборки комплекса. Значениями указанных переменных являются пути к соответствующей «обертке» компилятора (`c-compiler-wrapper`).

Далее модуль вызывается автоматически в соответствии с правилами сборки, описанными в `Makefile`. При этом вызов компилятора

```
<c-compiler> <args>
```

[2] В настоящее время поддерживается только средство сборки `make`.

заменяется вызовами

```
<c-compiler> <args> <c-compiler-wrapper> <args>
```

где `c-compiler-wrapper` — «обертка» компилятора языка C, предоставляющая интерфейс к функциям модуля синтаксического и лексического разбора.[3)]

На втором шаге в соответствии с правилами сборки комплекса и в согласно правилам грамматики языка C осуществляется процедура *трансляции* — для каждой единицы трансляции (файла, содержащего исходный код анализируемой программы) выполняется лексический и синтаксический разбор, результат которого сохраняется в виде *дерева разбора*.

На третьем шаге по аналогии со связыванием объектных модулей в исполняемые осуществляется соединение деревьев разбора. Таким образом, для каждого исполняемого модуля исходного проекта будет получено соответствующее дерево разбора.

3.4. Упрощающие преобразования дерева разбора

После преобразования исходного кода программы в дерево разбора, запускается модуль, выполняющий упрощающие преобразования этого дерева. Указанные преобразования не меняют структуры дерева, поскольку результатом каждого шага будет являться дерево разбора некоторой программы на языке C, эквивалентной исходной. Данный этап работы «Анализатора» носит, в основном, рутинный характер. На выходе модуля получается дерево, содержащее в качестве своих поддеревьев основные конструкции языка C. К их числу относятся инструкции присваивания, циклы, операторы проверки условий, явные вызовы функций, операции неявного вызова функции (посредством указателей на функции), операции преобразования типов и некоторые другие.

3.5. Трансляция дерева разбора в блок-схему и ее анализ

Трансляция дерева разбора в блок-схему и анализ блок-схемы является основной частью рассматриваемого инструментального средства. Данный этап работы «Анализатора» существенно отличается от аналогичного этапа в методе, описанном в работе [7].

Для дальнейшего изложения введем несколько понятий.

3.5.1. Основные понятия.

3.5.1.1. Блок-схема. Под *блок-схемой* будем понимать упорядоченное множество инструкций одного из следующих типов: присваивания, условного перехода, безусловного перехода, останова. Каждая инструкция

[3)] В настоящее время такая «обертка» разработана лишь для компилятора `gcc`.

имеет уникальный *идентификатор*, позволяющий осуществлять передачу управления на другую инструкцию блок-схемы. С каждой инструкцией связано *ключевое слово*, определяющее ее тип, а также *тело* инструкции, содержащее параметры операции, выполняемой при каждой передаче управления на рассматриваемую инструкцию. Тело инструкции может быть пустым (например, для инструкции останова).

Инструкции могут оперировать значениями переменных, полный список которых должен быть определен для всей блок-схемы заранее. В рамках исследования задачи анализа исходного кода программ на предмет обнаружения уязвимостей, достаточно ограничиться предположением, что переменные могут принимать лишь целочисленные значения. Инструкции могут содержать традиционные арифметические операции с целочисленными переменными, включая сложение, вычитание, умножение, целочисленное деление. Поддерживаются операции присваивания переменной «неопределенного» значения, что соответствует ситуации, в которой значение переменной не может быть выражено с помощью инструкций присваивания. Логические выражения образуются путем сравнения арифметических выражений (больше, меньше, больше или равно, меньше или равно, равно, не равно). Кроме того, поддерживаются инструкции неопределенного условного перехода, что соответствует ситуации, в которой значение логического выражения не может быть представлено с помощью описанных правил.

Каждая блок-схема, возникающая в процессе работы «Анализатора», соответствует некоторому участку исходного кода. Обычно таким участком является определение некоторой функции исходной программы.

Для представления блок-схем используются следующие синтаксические правила. [4)]

```
translation_unit: (instruction)*
instruction: identifier (assign | assign_unk | condition | goto |
    goto_unk | stop) ';'
identifier: [A-Za-z_][0-9A-Za-z_]* assign: 'assign' variable '='
expression assign_unk: 'assign_unk' variable '= unknown'
condition: 'condition' predicate '?' identifier ':' identifier
goto: 'goto' identifier goto_unk: 'goto_unk ?' identifier ':'
identifier stop: 'stop' variable:
[A-Za-z_@$\mes{?}.\[\]][0-9A-Za-z_@$\mes{?}.\[\]]* expression:
identifier | unsigned_int_const |
    ( expression binary_operator expression ) |
    ( unary_operator expression )
predicate: expression expression pred_sign
```

[4)] Необходимо отметить, что приводимые далее правила являются лишь одним из способов представления блок-схем.

```
unsigned_int_const: [0-9]+
binary_operator: '+' | '-' | '*' | '/'
unary_operator: '--'
pred_sign: '>' | '=' | '<=' | '==' | '!='
```

Рассмотрим содержательный смысл инструкций каждого типа.

Инструкция, соответствующая единице трансляции `assign`, имеющая вид

```
<id> assign <var> = <expression>;
```

обозначает операцию присваивания переменной `var` нового значения, определяемого арифметическим выражением `expression`. После выполнения присваивания управление передается на следующую по порядку инструкцию.

Инструкция, соответствующая единице трансляции `assign_unk`, имеющая вид

```
<id> assign_unk <var> = unknown;
```

обозначает операцию присваивания переменной `var` неопределенного значения. После выполнения присваивания управление передается на следующую по порядку инструкцию.

Инструкция, соответствующая единице трансляции `condition`, имеющая вид

```
<id> condition <predicate> ? <id1> : <id2>;
```

обозначает инструкцию условного перехода и включает операцию проверки условия, определяемого логическим выражением `predicate`, и последующего перехода (передачи управления) либо на инструкцию с идентификатором `id1` в случае истинности логического выражения, либо, в противном случае, на инструкцию с идентификатором `id2`.

Инструкция, соответствующая единице трансляции `goto`, имеющая вид

```
<id> goto <id1>;
```

является инструкцией безусловного перехода (передачи управления) на инструкцию с идентификатором `id1`.

Инструкция, соответствующая единице трансляции `goto_unk`, имеющая вид

```
<id> goto_unk ? <id1> : <id2>;
```

является инструкцией неопределенного условного перехода (передачи управления) либо на инструкцию с идентификатором `id1`, либо на инструкцию с идентификатором `id2`. Выбор следующей инструкции осуществляется случайно и не зависит от предыстории выполнения инструкций блок-схемы.

Инструкция, соответствующая единице трансляции `stop`, имеющая вид

```
<id> stop;
```

является инструкцией останова.

Рассмотрим пример преобразования участка программы на языке C в блок-схему, демонстрирующий предназначение инструкций каждого типа.

```
int foo(int* buf, int n) {          L0:  assign  i = 0;
    int i, sum;                     L1:  condition  i < n ? L2 : L6;
    for(i=0; i<n; ++i) {            L2:  goto_unk ? L4 : L3;
        if (buf[i] > 0)       ==>   L3:  assign_unk  sum = unknown;
            sum += buf[i];          L4:  assign  i = i + 1;
    }                               L5:  goto L1;
    return sum;                     L6:  assign  foo.return = sum;
}                                   L7:  stop;
```

3.5.1.2. Предусловия, условия корректности и инварианты. *Предусловием* блок-схемы, соответствующей функции `f` исходного кода, будем называть предикат, связывающий параметры `f` и глобальные переменные, выполнение которого предполагается перед выполнением начальной инструкции блок-схемы. Предусловия необходимо использовать в функции анализа блок-схемы, когда значения параметров `f` или глобальные переменные связаны некоторыми соотношениями.

Условием корректности будем называть пару вида (`id, predicate`), где `id` — идентификатор некоторой инструкции блок-схемы, а `predicate` — условное выражение. Условие корректности для блок-схемы, соответствующей некоторому участку исходного кода, выражает достаточное условие отсутствия уязвимости в определенной точке этого участка.

Процедура проверки условия корректности заключается в том, чтобы определить, возможно ли, что при выполнении инструкций блок-схемы и в случае истинности предусловий, при передаче управления на инструкцию `id`, значение условного выражения `predicate` окажется ложным. В случае, если указанная ситуация возможна, будем считать, что в соответствующей точке исходного кода присутствует потенциальная уязвимость.

Инвариантом блок-схемы будем называть пару вида (`id, predicate`). Инвариант обозначает условие, связывающее переменные блок-схемы, которое выполняется всякий раз при передаче управления на инструкцию `id`.

Инварианты используются для проверки истинности условий корректности в соответствующей точке блок-схемы. Для автоматической генерации инвариантов в различных точках блок-схемы используется специальные алгоритмы обхода графа, изложенные в работе авторов [16].

Для примера, рассмотренного в предыдущем подпункте, условия корректности определены в точках `L2, L3` и имеют вид `(buf.size - 4*i >= 1)`, где `buf.size` — *ассоциированная переменная* (см. следующий подпункт) для `buf`.

В случае, когда выполнено предусловие `(buf.size == 4*n)`, в точках `L2, L3, L4` могут быть получены инварианты `(i < n)` и `(buf.size == 4*n)`. Это позволит доказать истинность условий корректности и, следовательно, отсутствие уязвимости в функции `foo`.

3.5.1.3. Ассоциированные переменные.. Пусть `p` — указатель на область памяти или массив, объявленный в исходном коде анализируемой программы. С каждым таким указателем свяжем семейство *ассоциированных переменных*, определяемых следующим образом.

- Переменная `p.isNull` принимает значение 1, если указатель равен нулю, и 0 — в противном случае.
- Переменная `p.size` принимает значение, равное размеру буфера или массива (в байтах), доступного в текущий момент по указателю `p`.
- Переменная `p.offset` выражает смещение указателя (в байтах) относительно начала буфера.
- Переменная `p.isString` принимает значение 1, если буфер представляет собой корректную C строку (то есть последовательность байт, расположенную в захваченной на текущий момент области памяти, заканчивающуюся нулевым байтом), и 0 — в противном случае. Необходимо отметить, что переменная `p.isString` является характеристикой буфера, поэтому ее значение не зависит от значения переменной `p.offset`.
- Переменная `p.length` является корректно определенной в случае, если буфер является корректной C строкой. Ее значение равно максимальному числу ненулевых байт, встретившихся в буфере `p`. Переменная `p.length` также является характеристикой буфера, поэтому ее значение не зависит от значения переменной `p.offset`.

Будем считать, что каждой функции, объявленной в исходном коде, присвоен собственный уникальный номер — некоторое целое число. Тогда с каждым указателем `p` на функцию свяжем ассоциированную переменную `p.function`, принимающую значение, равное номеру функции, вызываемой по указателю.

Назначение ассоциированных переменных заключается в том, чтобы моделировать различные операции с указателями и массивами, существенные для обеспечения возможности выявления некорректных обращений с ними, а также условия корректности.

Для подтверждения вышесказанного рассмотрим несколько примеров.

1. Пусть в исходном коде анализируемой программы встретилось выражение `p[i]`, где `p` — указатель типа `int*`. Тогда при формировании множества условий корректности для данного участка кода встретятся условия:

```
p.size > 4*i + p.offset;
4*i + p.offset >= 0.
```

2. Пусть в исходном коде программы встретилось выражение `p = (int*)malloc(40)`. Тогда при преобразовании участка кода, содержащего это выражение, в блок-схеме встретятся инструкции:

```
assign  p.isNull = unknown;
assign  p.size = 40;
assign  p.offset = 0;
assign  p.isString = unknown;
assign  p.length = unknown.
```

3. Пусть в исходном коде программы встретилось выражение `p = foo`, где `p` — указатель на функцию, а `foo` — функция определенная в исходном коде, имеющая номер . Тогда при преобразовании участка кода, содержащего это выражение, в блок-схеме встретится инструкция:

```
assign  p.function = <foo-number>.
```

Использование переменных, ассоциированных с указателями на функции, позволит осуществлять анализ исходного кода программ, в котором присутствует неявная передача управления на функции (при помощи указателей). Например, если в точке вызова функции по указателю `p` возможно существенно ограничить диапазон возможных значений переменной `p.function`, то вместо «заглушки» на место вызова может быть подставлен результат анализа функций с номерами, удовлетворяющими диапазону возможных значений переменной `p.function`.

3.5.1.4. Аннотации для функций исходной программы. *Аннотацией функции* будем называть запись, содержащую информацию об имени аннотируемой функции, множестве предусловий ее вызова, представлении функции в виде блок-схемы, множестве условий корректности и множестве инвариантов для этой блок-схемы.

Аннотация должна гарантировать, что, если перед вызовом функции предусловия были истинны, то при выполнении инструкций блок-схемы, соответствующей определению функции, инварианты аннотации окажутся истинными.

В процессе работы «Анализатора» для всевозможных функций, определенных в исходном коде, аннотации формируются и сохраняются в *базе аннотаций*. Кроме того в этой же базе хранятся аннотации для внешних (библиотечных) функций. База аннотаций представляет собой СУБД, имеющую следующую структуру. Все аннотации расположены в таблице `annotations`, которая имеет атрибуты:

- `key` (уникальный идентификатор аннотации, являющийся первичным ключом таблицы);
- `name` (имя аннотируемой функции);
- `precond` (список условных выражений, представляющих собой предусловия аннотации);
- `flowchart` (описание блок-схемы, соответствующей исходному коду функции);
- `c-conditions` (множество условий корректности, соответствующих блок-схеме);
- `invariants` (список инвариантов блок-схемы).

Отметим, что пара атрибутов `(name, precond)` является составным первичным ключом таблицы (не может быть двух записей с совпадающими значениями указанных атрибутов).

Следующий листинг представляет собой пример аннотации для стандартной библиотечной функции `strcpy`.

```
key = 0
name = "strcpy"
precond = ""
flowchart = "L0 assign dst.isString = 1;
             L1 assign dst.length=dst.offset+src.length-src.offset;
             L2 stop;"
c-conditions = "(L0, src.isNull == 0),
                (L0, src.offset >= 0),
                (L0, src.size >= src.offset),
                (L0, src.isString == 1),
                (L0, src.length >= src.offset),
                (L0, dst.isNull == 0),
                (L0, dst.offset >= 0),
                (L0, dst.size >= dst.offset+src.length-src.offset)
invariants = ""
```

3.5.2. Схема алгоритма. Общая схема работы алгоритма преобразования дерева разбора к блок-схеме и анализа блок-схемы представлена на рис. 3, 4. Алгоритм включает следующие функции.

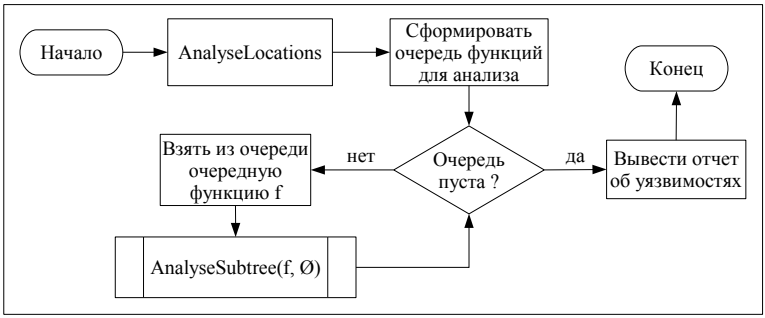


Рис. 3. Общая схема алгоритма преобразования дерева разбора к представлению блок-схемы и анализа блок-схемы

1. Функция `AnalyseLocations` позволяет по дереву разбора программы произвести предварительный анализ соответствия указателям, определенным в исходном коде, возможных участков памяти, на которые эти указатели могут ссылаться. Более подробно работа этой функции рассматривается в пункте 3.5.3.

2. Функция `Generate(f, pred)` позволяет по поддереву определения функции `f` и множеству предусловий `pred` получить блок-схему `fc`, множество условий корректности `ccs` и начальное множество инвариантов `inv`. Функция возвращает тройку `(fc, ccs, inv)`.

Реализация `Generate` носит технический характер, однако интерес представляют правила обработки операций с указателями, рассматриваемые в пункте 3.5.3 и правила получения условий корректности, рассматриваемые в пункте 3.5.4. Кроме того, следует отметить, что вызовы функций, находящиеся в теле `f`, преобразуются в так называемые «заглушки». *Заглушка* представляет собой последовательность инструкций присваивания значений переменным блок-схемы функции `f`, которые могут быть изменены в вызываемой функции.

3. Функция `Analyse(f, fc, pred, ccs, inv)` позволяет произвести анализ данной блок-схемы `fc` и данного множества инвариантов `inv`, в результате которого множество инвариантов будет пополнено и сформирована аннотация для текущей анализируемой функции. Полученная аннотация вида `(f, pred, fc, ccs, inv')`, где `f` — имя текущей анализируемой

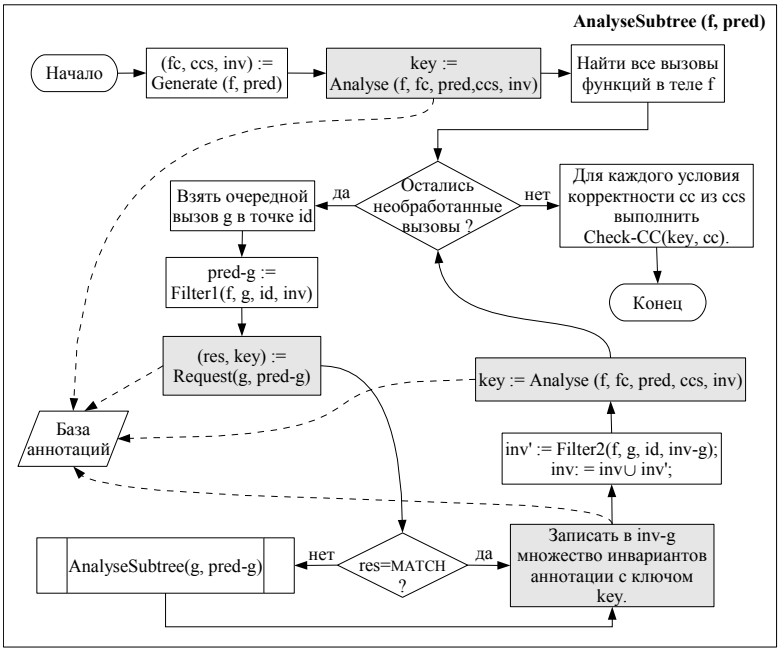


Рис. 4. Схема алгоритма работы рекурсивной функции `AnalyseSubtree(f,pred)`, где `f` — функция, определенная в исходном коде, `pred` — предусловия ее вызова. Серым цветом выделены шаги, на которых происходит обращение к базе аннотаций

функции, `pred` — множество предусловий, а `inv'` — новое множество инвариантов, заносится в базу аннотаций в том случае, если пара `(f, pred)` появляется впервые. В противном случае, выведенное множество инвариантов добавляется к существующей записи. Функция возвращает значение `key`, являющее первичным ключом в записанной аннотации.

Подробное рассмотрение алгоритма построения новых инвариантов, являющегося одним их основных этапов функционирования «Анализатора», выходит за рамки настоящей работы. Формализованное описание указанного алгоритма можно найти в работе авторов [16].

4. Функция `Filter1(f, g, id, inv)` позволяет произвести преобразование множества инвариантов `inv`, относящихся к точке `id` блок-схемы функции `f`, к множеству предусловий вызова функции `g`. При этом выражения, подставленные в качестве аргументов функции `g`, должны быть преобразованы к виду ее параметров. Возвращаемым значением `Filter1` является построенное множество предусловий.

Реализация `Filter1` достаточна проста и сводится к определению и переименованию переменных, соответствующих параметрам функции, ассоциированным с ними переменных, а также глобальных переменных, область видимости которых содержит определение самой функции.

5. Функция `Filter2(f, g, id, inv-g)` позволяет произвести преобразование множества инвариантов `inv-g` блок-схемы функции `g`, относящихся к инструкции останова, к множеству инвариантов блок-схемы функции `f` в точке `id`. Инструкция `id` является последней инструкцией «заглушки» вызова функции `g`. Возвращаемым значением `Filter2` является построенное множество инвариантов функции `f`.

Реализация функции `Filter2` аналогична реализации функции `Filter1`.

6. Функция `Check-CC(key, cc)` позволяет произвести проверку условия корректности `cc` для аннотации, соответствующей первичному ключу `key`.

Реализация функции `Check-CC` основана на сведении задачи выводимости условий корректности из множества инвариантов к задаче линейного программирования. Более подробно указанный подход изложен в пункте 3.5.5.

7. Функция `Request(g, pred-g)` позволяет произвести запрос к базе аннотаций с целью определить, подходит ли пара `(g, pred-g)` под одну из существующих аннотаций. Будем считать, что пара `(g, pred-g)` *подходит* под аннотацию `A`, если предусловие аннотации является более слабым, чем `pred-g`. Если такая аннотация была обнаружена, то функция возвращает пару `(MATCH, key)`, где `MATCH` — константа, обозначающая совпадение, а `key` — первичный ключ обнаруженной аннотации. В случае отсутствия в базе подходящей аннотации, определенным образом формируется одна или несколько новых аннотаций. Все добавленные записи в базу будут «неполными» (атрибуты `flowchart, c-conditions, invariants` пока останутся пустыми).

Важными требованиями к алгоритму работы Request (в случае отсутствия подходящей аннотации) являются следующие:

- пара `(g, pred-g)` должна подходить по крайней мере под одну из новых аннотаций;
- число аннотаций в базе, соответствующих одной функции, не должно превышать некоторого фиксированного значения.

Соблюдение указанных требований позволит избежать бесконечного зацикливания алгоритма анализа исходного кода программ.

В случае отсутствия подходящей аннотации возвращаемым значением `Request` является пара `(REANALYSE, key)`, где `REANALYSE` — констан-

та, обозначающая необходимость произвести повторный анализ функции `g` с новыми предусловиями, определяемыми аннотацией с ключом `key`.

Алгоритм работы функции `Request` может быть достаточно сложным и формальное его описание выходит за рамки настоящей работы. Однако, в 3.5.6 рассмотрен содержательный пример, демонстрирующий поведение функции `Request` в характерных ситуациях.:l

3.5.3. Анализ участков памяти. При анализе исходного кода программ на языке C или C++ необходимо учитывать возможность неявного изменения значений целочисленных и других переменных. Это связано с тем обстоятельством, что указатели, определенные в исходном коде, могут ссылаться на один и тот же объект в памяти. В качестве примера такого поведения программы приведем следующий участок кода.

```
1:  int a, *p;
2:  a = 0;
3:  p = &a;
4:  *p = 1;
```

Оператор присваивания в строке 4 повлечет изменение значения переменной `a`. По этой причине отбрасывание операций разыменования указателя `p` приведет к выводу ложного инварианта `a == 0`. Это, в свою очередь, повлечет нарушение корректности (консервативности) всего алгоритма анализа. Следовательно, необходимы средства обработки подобных ситуаций. С этой целью введем понятие *участка памяти*, как объекта, на который могут ссылаться указатели в различных точках исполнения программы. Такими объектами могут быть локальные переменные или массивы, определенные в текущей функции, глобальные переменные или массивы, а также динамически выделенные участки памяти. Участки памяти однозначно определяются по положению соответствующего объекта в исходном коде и по предыстории (стеку) вызовов функций. В приводимом ниже примере участки памяти определяются следующим образом: `main:8:f:3:malloc`, `main:9:f:3:malloc`, `f:1:n`.[5)]

```
1:  void f(int n) {
2:    ...
3:    malloc(n);
4:    ...
```

[5)] Обозначение участков памяти имеет следующую структуру: `::...:::`, где — имя `i`-й функции в стеке вызовов, — номер строки в исходном коде операции, соответствующей выделению участка памяти, или операции вызова `(i+1)`-й функции, — имя идентификатора, соответствующего участку памяти, или ключевое слово `malloc` для операций динамического выделения памяти.

```
5:  }
6:  int main() {
7:    ...
8:    f(10);
9:    f(20);
10:   ...
11: }
```

Далее в разделе при обозначении участков памяти, в тех случаях, где это не приводит к двусмысленности, будем опускать указание стека вызовов функций и указание местоположения в исходном коде операций, соответствующих этим участкам.

Алгоритм анализа участков памяти должен по дереву разбора в каждой точке `A` исходного кода и для каждого указателя `p` построить набор участков кода, на которые в данной точке может ссылаться указатель.

Работа функции `AnalyseLocations` устроена следующим образом. На первом шаге алгоритма для каждого указателя `p` вводится специальная переменная `p.locations`, ассоциированная с ним, возможными значениями которой могут являться наборы участков памяти. При этом в каждой точке исходного кода, в которой определен указатель `p`, должно выполняться следующее свойство: `p` ссылается (возможно со смещением) на один из участков памяти, идентификатор которого присутствует в наборе `p.locations`.

При выполнении различных операций с указателями участки памяти преобразуются по следующим правилам.

- Операция присваивания указателей `p = q + i`, где `i` — целое число, заменяется на операцию `p.locations = q.locations`.
- Операция вида `p = &x`, где `x` — переменная произвольного типа, заменяется на операцию `p.locations = {x}`.
- Операция вида `p = malloc(n)`, где `n` — целое число, заменяется на операцию `p.locations = {malloc(n)}`.

На втором шаге алгоритма в каждой точке `A` полученного представления дерева разбора для каждого указателя `p`, определенного в этой точке, вычисляется возможное значение переменной `p.locations`. Если в точке `A` определена операция вида

```
p.locations=<value>,
```

где — либо определенный набор идентификаторов участков памяти, либо значение другой переменной, то возможным значением `p.locations` будет . В противном случае `p.locations` определяется в точках, пред-

шествующих A, причем значением p.locations в точке A будет являться объединение ее значений в предшествующих точках.

Необходимо отметить, что результат анализа участков памяти используется на этапе преобразования поддерева определения функции к виду блок-схемы. Рассмотрим некоторые правила такого преобразования.

• Операция разыменования указателя вида *p = обрабатывается следующим образом. Если значение p.locations является пустым набором, то операция является некорректной (разыменование не действительного указателя). Если p.locations включает один участок вида {x}, где x — переменная произвольного типа, то указанная операция преобразуется в соответствии с общими правилами, как эквивалентная операции x = . При этом, если x — переменная простого типа (не указатель), то добавляется условие корректности p.offset == 0. В противном случае, необходимо добавить условие корректности 0 <= p.offset <= x.size. Если p.locations включает несколько участков памяти, то для каждого такого участка s, в блок-схему должна быть добавлена инструкция вида

```
assign_unk  s = unknown.
```

• Операция освобождения памяти вида free(p) обрабатывается следующим образом. Если значение p.locations является пустым, то операция является некорректной. В противном случае для каждого участка памяти s, входящего в p.locations, необходимо добавить инструкции вида

```
assign_unk  s.size = unknown;
assign_unk  s.offset = unknown;
assign_unk  s.is_string = unknown;
assign_unk  s.strlen = unknown.
```

3.5.4. Получение условий корректности. Процедура получения условий корректности по дереву разбора исходного кода, является единственным шагом, выполнение которого зависит от выявляемых классов уязвимостей программ. Таким образом, условия корректности разделяются на классы в соответствии с группами выявляемых уязвимостей.

Рассмотрим указанное разделение.

• К первому классу относятся условия корректности, гарантирующие отсутствие в соответствующей «подозрительной» точке исходной программы различных ошибок при работе с памятью.[6] Условия корректности

[6] В соответствии с таблицей 3, такими ошибками могут быть переполнения буферов, ошибки при обращении к памяти, ошибки форматной строки, повторные освобождения памяти.

должны формироваться для каждой операции разыменования указателя вида `*p` и будут иметь вид:

```
(p.size > p.offset), (p.offset >= 0).
```

Кроме этого для библиотечных функций условия корректности извлекаются из базы аннотаций (пример условий корректности для библиотечной функции `strcpy` приведен в 3.5.1).

• Ко второму классу относятся условия корректности, гарантирующие отсутствие переполнений целых типов (арифметических переполнений). Поскольку отсутствует формальное определение данного класса уязвимостей, охватывающее все возможные случаи их возникновения, рассмотрим несколько подходов для формирования условий корректности. Первый подход заключается в добавлении для каждой инструкции присваивания, связанной с переменной `var`, условия корректности вида:

```
MIN_RANGE <= var < MAX_RANGE,
```

где `MIN_RANGE, MAX_RANGE` определяются типом `var` (например, для переменной типа `int` выполнено: `MIN_RANGE`$=-2^{31}$, `MAX_RANGE`$=2^{31}$). При использовании такого подхода алгоритм анализа будет выдавать большое число ложных предупреждений о наличии уязвимостей в исходном коде.

Более разумным представляется другой подход, при котором аналогичные ограничения накладываются лишь на те переменные, которые входят в условия корректности из первого класса, включая условия корректности для внешних библиотечных функций. Такие переменные являются непосредственно связанными с операциями с памятью. По этой причине, указанный подход позволяет гарантировать, что даже в случае возникновения арифметического переполнения, некорректные операции с памятью будут невозможны.

• К третьему классу будем относить условия корректности, позволяющие гарантировать отсутствие утечек памяти в анализируемой программе. Аналогично классу арифметических переполнений, класс уязвимостей, связанный с утечками памяти, формализовать невозможно. По этой причине представляется разумным осуществлять проверку на наличие утечки памяти в функциях исходного кода, определенных пользователем «Анализатора». С этой целью для каждой функции `f` вводится ассоциированная с ней переменная `f.memory`, значение которой равно «балансу» выделенной / освобожденной памяти в функции `f`. Если `f` содержит вызов `g`, то к соответствующей «заглушке» в блок-схеме функции `f` должна быть добавлена инструкция

```
assign  f.memory = f.memory + g.memory.
```

Если `g` является библиотечной функцией, то значение переменной `g.memory` и его связи со значениями параметров должны определяться из соответствующей записи в базе аннотаций.

Для того, чтобы проверить наличие утечек памяти в функции `h`, необходимо в инструкции останова ее блок-схемы сформировать условие корректности: `(h.memory == 0)`.

3.5.5. Проверка истинности условий корректности. Проверка истинности условия корректности в точке `id` блок-схемы осуществляется путем анализа выводимости его из условий, входящих в систему инвариантов в точке `id`, полученную на этапе анализа блок-схемы. Для достижения указанной цели составляются системы алгебраических уравнений и неравенств, которые затем исследуются на предмет наличия решений. Существуют универсальные алгоритмы решения подобного рода задач, однако их вычислительная сложность слишком велика, чтобы их можно было использовать на практике. Часто оказывается, что большинство ограничений — линейные. Таким образом пропадает необходимость использования указанных сложных алгоритмов. Вместо этого, путем отбрасывания «нелинеаризуемых» ограничений, системы приводятся к виду, характерному для традиционных задач линейного программирования (ЛП). Математические модели, которые получаются при формализации различных видов задач ЛП, в настоящее время хорошо изучены ([17]). Более того — алгоритмы для их решения, основанные на использовании «симплекс-метода», достаточно быстры.

Рассмотрим изложенную схему более подробно. На первом шаге условие корректности приводится к одной из трех форм:

а) $expr \leqslant c$;
б) $expr = c$;
в) $expr \neq c$,

где $expr$ — некоторая линейная комбинация переменных блок-схемы, а c — целочисленная константа. Если привести условие корректности ни к одной из форм нельзя, то вывод объявляется несостоявшимся.

На втором шаге составляется система линейных уравнений и неравенств S, состоящая из условий полученных в точке `id` инвариантов. Все нелинейные ограничения системы инвариантов отбрасываются.

Далее, в зависимости от случая 0а, 0б или 0в, формируется одна или несколько задач ЛП. В случае 0а составляется задача L, состоящая в максимизации линейной формы $expr$ при условиях S. Пусть L^* — решение этой задачи. Критерием того, что условия корректности выполняются в точке `id`, является условие $L^* \leqslant c + 1/2$.

В случае 0б составляются две задачи L_1 и L_2, причем L_1 — это задача максимизации линейной формы *expr* при условиях S, а L_2 — это задача минимизации линейной формы *expr* при условиях S. Пусть L_i^* $(i = 1, 2)$ — решение соответствующей задачи. Тогда критерием того, что условия корректности выполняются в точке `id`, является условие $c - 1/2 \leqslant L_i^* \leqslant c + 1/2$, $(i = 1, 2)$.

В случае 0в составляется задача L, состоящая в поиске решения системы линейных уравнений и неравенств $S \wedge (expr = c)$. Критерием того, что условия корректности выполняются в точке `id`, является условие неразрешимости задачи L.

Отметим, что в «Анализаторе» используется программное средство с открытым исходным кодом GLPK (GNU Liner Programming Kit), с помощью которого возможно:

- исследовать задачу ЛП на предмет наличия решений;
- в случае, когда решение существует, находить оптимальное; [7)]
- исследовать задачу ЛП в предположении, что все используемые переменные принимают только целые значения. [8)]

3.5.6. Пример анализа исходного кода программы, содержащей рекурсивные вызовы функций. Рассмотрим пример анализа исходного кода программы, содержащей рекурсивно вызываемые функции. Пусть анализируемый исходный код представляется следующим листингом (метки, обозначающие номер строки, к коду не относятся и введены для удобства изложения).

```
1:  int sum(int* buf, int n) {
2:      if (n > 0) return (*buf + sum(buf+1, n-1));
3:      else return 0;
4:  }
5:  int main() {
6:      int a[10] = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10};
7:      return sum(a, 10);
8:  }
```

На первом шаге будет сформирована очередь функций для анализа: `main, sum` в указанном порядке. Затем, будет вызвана рекурсивная функция `AnalyseSubtree(main, "")`.

[7)] Данная возможность позволяет строить «контрпример» в виде значений переменных исходной программы и состояние ее памяти, при которых реализуется уязвимость.

[8)] Данная возможность позволяет проводить более точный анализ выводимости условий корректности, поскольку все переменные блок-схемы могут принимать лишь целые значения. Кроме того, риск получения некорректного результата работы симплекс-метода из-за многократных округлений вещественных чисел существенно снижается.

Функция `Generate` сформирует для `main` блок-схему `fc`, множество условий корректности и исходное множество инвариантов `inv`, причем блок-схема будет иметь вид: [9)]

```
L0:  assign  a.isNull = 0;
L1:  assign  a.size = 40;
L2:  assign  a.offset = 0;
L3:  stop;
```

Множество условий корректности и исходное множество инвариантов будут пустыми.

Функция `Analyse` обнаружит следующие инварианты:

```
(L1, a.isNull == 0);
(L2, a.isNull == 0), (L2, a.size == 40);
(L3, a.isNull == 0), (L3, a.size == 40), (L3, a.offset == 0)
```

и запишет их в базу аннотаций для функции `main`. После этого база аннотаций будет содержать единственную запись вида:

```
key = 0
name = "main"
precond = ""
flowchart = ...
c-conditions= ""
invariants = ...
```

Далее при обходе поддерева разбора `main` будет обнаружен единственный вызов функции (а именно, вызов функции `sum` с аргументом `a` в качестве параметра `buf`, с аргументом `10` в качестве параметра `n`).

Функция `Filter1` преобразует множество инвариантов `inv` блок-схемы `fc` в множество предусловий для функции `g=sum`, в результате чего `pred-g` будет состоять из таких предусловий:

```
(buf.isNull == 0), (buf.size == 40), (buf.offset == 0), (n == 10).
```

Поскольку база аннотаций не содержит записей, относящихся к функции `sum`, результатом запроса `Request` будет пара `(REANALYSE, 1)`, а в базу запишется «неполная» аннотация (атрибуты `flowchart, invariants, c-conditions` останутся пустыми) для `sum`:

[9)] Для сокращения записи всюду в данном пункте ассоциированные переменные `.isString` и `.length` будем опускать, поскольку они являются несущественными для анализа данной программы на уязвимости.

```
key = 1
name = "sum"
precond = "(buf.isNull == 0), (buf.size == 40),
           (buf.offset == 0), (n == 10)"
flowchart = ""
c-conditions = ""
invariants = "".
```

Следовательно, анализ `main` будет приостановлен, и рекурсивно вызовется функция `AnalyseSubtree(sum, "(buf.isNull == 0)...")`.

После повторения описанных операций для функции `sum` будет сформирована блок-схема:

```
M0:  condition  n > 0 ? M1 : M3;
M1:  assign_unk  sum.return = unknown;
M2:  goto L4;
M3:  assign  sum.return = 0;
M4:  stop;
```

Множество условий корректности будет иметь вид:

```
(M1, buf.offset < buf.size);
(M1, buf.offset >= 0).
```

Эти условия позволяют гарантировать отсутствие переполнения буфера при операции `*buf` в строке 2 исходного кода.

Множество инвариантов `inv` будет совпадать с множеством предусловий (все инварианты будут относиться к начальной инструкции блок-схемы).

Далее в функции `Analyse` производится анализ блок-схемы, который (с учетом заданных предусловий) обнаружит следующие инварианты:

```
(M0, buf.isNull == 0), (M0, buf.size == 40),
(M0, buf.offset == 0), (M0, n == 10);

(M1, buf.isNull == 0), (M1, buf.size == 40),
(M1, buf.offset == 0), (M1, n == 10);

(M2, buf.isNull == 0), (M2, buf.size == 40),
(M2, buf.offset == 0), (M2, n == 10);

(M3, EMPTY-SET);
```

```
(M4, buf.isNull == 0), (M4, buf.size == 40),
(M4, buf.offset == 0), (M4, n == 10).
```

(Инвариант `(M3, EMPTY-SET)` означает невозможность попадания в точку `M3`.)

Поскольку запись для `sum` с заданным множеством предусловий в базе аннотаций уже существует, новая запись создаваться не будет, а старая (которая является «неполной») будет пополнена соответствующими значениями атрибутов `flowchart`, `invariants`, `c-conditions`. Функция `Analyse` вернет значение первичного ключа для пополненной аннотации.

Далее при обходе поддерева разбора `sum` будет обнаружен единственный вызов функции (а именно, вызов функции `sum` с аргументом `buf+1` в качестве параметра `buf`, с аргументом `n-1` в качестве параметра `n`).

Функция `Filter1` преобразует множество инвариантов, построенное на предыдущем шаге, в множество предусловий нового (рекурсивного) вызова `sum`:

```
(buf.isNull == 0), (buf.size == 40), (buf.offset == 4), (n == 9).
```

Рассмотрим работу функции `Request` в данном случае. В базе уже содержится аннотация для `sum` с предусловиями

```
(buf.isNull == 0), (buf.size == 40), (buf.offset == 0), (n == 10).
```

Предположим, что алгоритм `Request` контролирует изменение значений переменных в предусловиях для одной функции (а сами значения переменных, указанные в предусловиях не столь существенны). Тогда этот алгоритм обнаружит увеличение переменной `buf.offset` на 4 и одновременное уменьшение переменной `n` на 1. Таким образом, путем «линейной интерполяции» может быть сформировано следующее множество предусловий, естественным образом обобщающее указанные предусловия:

```
(buf.isNull == 0), (buf.size == 40), (buf.offset >= 0),
(n <= 10), (buf.offset + 4*n == 40).
```

Однако, поскольку предусловия получены эмпирически, отсутствует гарантия, что все последующие вызовы `sum` будут им удовлетворять. По этой причине необходимо дополнительно добавить предусловия, которые позволят гарантировать этот факт и, тем самым, предотвратить неограниченный рост базы аннотаций. В рассматриваемом случае такими предусловиями является пустое множество. Старые условия будут сохранены в базе, однако дальнейшего накопления аннотаций, соответствующих функции `sum`, происходить не будет, поскольку результатом любого следующего запроса будет значение `MATCH`.

Таким образом, после выполнения `Request` часть базы аннотаций, относящаяся к функции `sum`, будет иметь такой вид:

```
key = 1
name = "sum"
precond = "(buf.isNull == 0), (buf.size == 40),
           (buf.offset == 0), (n == 10)"
flowchart = ...
c-conditions = "(M1, buf.offset < buf.size),
                (M1, buf.offset >= 0)"
invariants = ...

key = 2
name = "sum"
precond = "(buf.isNull == 0), (buf.size == 40),
           (buf.offset >= 0), (n <= 10),
           (buf.offset + 4*n == 40)"
flowchart = ""
c-conditions = "(M1, buf.offset < buf.size),
                (M1, buf.offset >= 0)"
invariants = ""

key = 3
name = "sum"
precond = ""
flowchart = ""
c-conditions = "(M1, buf.offset < buf.size),
                (M1, buf.offset >= 0)"
invariants = "".
```

Возвращаемым значением функции `Request` будет являться пара `(REANALYSE, 2)`.

Следовательно, анализ функции `sum` будет приостановлен и рекурсивно вызовется `AnalyseSubtree(sum, ...(key=2)...)`.

Описанные выше шаги должны быть повторены, однако, инварианты, выведенные в точке `M1`, будут иметь другой вид:

```
(M1, buf.isNull == 0), (M1, buf.size == 40),
(M1, buf.offset >= 0), (M1, 1 <= n <= 10),
(M1, buf.offset + 4*n == 40).
```

Следовательно, после выполнения функции `Filter1`, предусловия очередного рекурсивного вызова функции `sum` будут определяются следующим образом:

```
(buf.isNull == 0), (buf.size == 40),
(buf.offset >= 4), (0 <= n <= 9),
(buf.offset + 4*n == 40).
```

Очередной вызов `Request` вернет пару `(MATCH, 2)`, поскольку полученные в качестве результата работы функции `Filter1` предусловия являются более сильными, чем предусловия, сохраненные в базе аннотаций.

Условий на возвращаемое значение функции `sum` в системе инвариантов получено не было, поэтому множество `inv` на двух последовательных шагах (`Filter2` и `Analyse`) не изменится.

Теперь управление будет передано шагу, на котором (с использованием `Check-CC`) производится проверка выводимости условий корректности функции `sum`. Очевидно, что условия `(buf.offset = 0)` являются следствиями системы инвариантов в точке `M1`:

```
(buf.isNull == 0), (buf.size == 40),
(buf.offset >= 0), (1 <= n <= 9),
(buf.offset + 4*n == 40).
```

По этой причине переполнения буфера в функции `sum`, в предположении истинности предусловий, не происходит.

При возврате к предыдущему вызову `AnalyseSubtree`, цикл по вызовам функций, обнаруженным в теле `sum`, будет завершен и управление снова будет передано шагу, на котором производится проверка выводимости условий корректности функции `sum` с предусловиями, соответствующими записи в базе аннотаций с ключом 1. Поскольку, значения переменных `buf.size` и `buf.offset`, полученные из выведенных в точке `M1` инвариантов, равные 40 и 0 соответственно, удовлетворяют обоим условиям корректности

```
(buf.offset < buf.size), (buf.offset >= 0),
```

то переполнения буфера в функции `sum` при указанных предусловиях также не происходит.

При возврате к самому первому вызову `AnalyseSubtree` (для функции `main`) цикл по вызовам функций, обнаруженным в теле `main`, будет завершен, а поскольку условия корректности для функции `main` отсутствуют, переполнение буфера в ней также невозможно.

Таким образом, все функции, определенные в исходном коде, будут проанализированы; отчет об обнаруженных уязвимостях будет пустым. После этого алгоритм анализа завершит свою работу.

Необходимо отметить, что без учета и преобразования предусловий вызова обосновать отсутствие переполнения буфера в функции `sum` невозможно. Следовательно, ни один из методов, описанных в работах [6, 7], не позволит автоматически доказать корректность приведенной простой программы. Кроме того, моделирование стека вызовов, с помощью которого программа, содержащая рекурсивные вызовы функций, может быть приведена к эквивалентной программе, не содержащей таких вызовов, также в данном случае не привело бы к положительному результату, поскольку при использовании этого подхода необходимы алгоритмы, способные выводить условия, связывающие произвольные элементы этого стека.

3.5.7. Пример анализа исходного кода программы, содержащей указатели на функции. Рассмотрим пример анализа исходного кода программы, содержащей указатели на функции. Пусть анализируемый исходный код представляется следующим листингом (метки, обозначающие номер строки, к коду не относятся и введены для удобства изложения).

```
1:  #include
2:  int op1(const char* str) {
3:     return strlen(str);
4:  }
5:  int op2(const char* str) {
6:     return *str;
7:  }
8:  typedef int (*op_t)(const char*);
9:  const op_t op[2] = { op1, op2 };
10: int main(int argc, char** argv) {
11:    int code;
12:    if (argc < 3) return -1;
13:    if (!strcmp(argv[1], "c"))
14:        code = 0;
15:    else
16:        code = 1;
17:    return op[code](argv[2]);
18: }
```

На первом шаге будет сформирована очередь функций для анализа `main, op1, op2` в указанном порядке. Будем считать, что идентификаторами этих функций являются соответственно значения 1, 2, 3. Затем будет вызвана рекурсивная функция `AnalyseSubtree(main, "")`.

Функция `Generate` сформирует для `main` блок-схему `fc`, множество условий корректности и исходное множество инвариантов, причем блок-схема будет иметь вид:

```
L0:  assign  op.is_null = 0;
L1:  assign  op.size = 2;
L2:  assign  op.offset = 0;
L3:  assign  op[0] = 2;
L4:  assign  op[1] = 3;
L5:  condition  argc < 3 ? L6 : L12;
L6:  goto_unk ? L7 : L9;
L7:  assign  code = 0;
L8:  goto L9;
L9:  assign  code = 1;
L10: assign_unk  argv[2].is_string = unknown;
L11: assign_unk  argv[2].strlen = unknown;
L12: stop;
```

Необходимо отметить, что идентификаторы `op[0]`, `op[1]`, `argv[0].is_null` и другие, аналогичные им, являются обычными целочисленными переменными. Множество инвариантов этой блок-схемы, полученное в результате выполнения функции `Generate`, представляется следующим образом.

```
(L0, argc >= 1),
(L0, argv.is_null == 0),
(L0, argv.size == argc),
(L0, argv.offset == 0),
(L0, argv[0].is_null == 0),
(L0, argv[0].size >= 1),
(L0, argv[0].offset == 0),
(L0, argv[0].is_string == 1),
(L0, argv[0].strlen == argv[0].size - 1),
(L0, argv[1].is_null == 0),
(L0, argv[1].size >= 1),
(L0, argv[1].offset == 0),
(L0, argv[1].is_string == 1),
(L0, argv[1].strlen == argv[1].size - 1)
(L0, argv[2].is_null == 0),
(L0, argv[2].size >= 1),
(L0, argv[2].offset == 0),
(L0, argv[2].is_string == 1),
(L0, argv[2].strlen == argv[2].size - 1),
```

```
(L11, 0 <= argv[2].is_string <= 1).
```

Множество условий корректности, полученное `Generate`, будет иметь вид:

```
(L6, argv.is_null == 0),
(L6, 1 + argv.offset < argv.size),
(L6, argv[1].is_null == 0),
(L6, argv[1].size >= 1),
(L6, argv[1].offset >= 0),
(L6, argv[1].is_string == 1),
(L6, argv[1].strlen >= 0),
(L6, argv[1].strlen + argv[1].offset < argv[1].size),
(L10, op.is_null == 0),
(L10, 0 <= op.offset + code < op.size),
(L10, argv.is_null == 0),
(L10, 2 + argv.offset < argv.size).
```

Далее для краткости будем рассматривать только инварианты, соответствующие инструкции `L10` блок-схемы, в которые входят переменные, имеющие вид `"argv[2]..."` или `"op..."`, а также переменная `code`. Кроме того, будем опускать операции взаимодействия с базой аннотаций.

С учетом предыдущего замечания, функция `Analyse` обнаружит следующие инварианты:

```
(L10, argv[2].is_null == 0),
(L10, argv[2].size >= 1),
(L10, argv[2].offset == 0),
(L10, argv[2].is_string == 1),
(L10, argv[2].strlen == argv[2].size - 1),
(L10, op.is_null == 0),
(L10, op.size == 2),
(L10, op.offset == 0),
(L10, op[0] == 2),
(L10, op[1] == 3),
(L10, 0 <= code <= 1),
```

которые будут записаны в базу аннотаций.

В поддереве определения `main` присутствует только один вызов внешней функции (строка 17), однако этот вызов происходит по указателю, точное значение которого неизвестно. Предварительный анализ функции `main` позволит определить, что значение переменной `code` равно 0 или 1. Кроме того, в точке `L10` также известны точные значения переменных `op[0]`,

op[1]. Следовательно, и это будет установлено на очередном шаге алгоритма анализа, в качестве функции, вызываемой по указателю op[code] в строке 17 исходного кода, может быть либо функция op1, либо функция op2. Далее, в зависимости от реализации того или иного случая, анализ распадается на две ветви.

В первом случае, множество инвариантов в точке L10, связывающих переменные вида "argv[2]...", будет преобразовано к предусловиям вызова функции op1 следующим образом:

```
(str.is_null == 0), (str.size >= 1), (str.offset == 0),
(str.is_string == 1), (str.strlen == str.size - 1).
```

После этого будет вызвана функция

```
AnalyseSubtree(op1, "(str.is_null == 0), ...").
```

Блок-схема, построенная для функции op1 будет иметь вид:

```
M0:  assign  op1.return = str.strlen - str.offset;
M1:  stop.
```

Условия корректности будут иметь вид:

```
(M0, str.is_null == 0),
(M0, str.size >= 1),
(M0, str.offset >= 0),
(M0, str.is_string == 1),
(M0, str.strlen >= 0),
(M0, str.strlen + str.offset < str.size).
```

Легко видеть, что указанные условия корректности будут следовать из предусловий вызова op1.

Во втором случае, множество инвариантов в точке L10, связывающих переменные вида "argv[2]...", будет преобразовано к предусловиям вызова функции op2 следующим образом:

```
(str.is_null == 0), (str.size >= 1), (str.offset == 0),
(str.is_string == 1), (str.strlen == str.size - 1).
```

После этого будет вызвана функция

```
AnalyseSubtree(op2, "(str.is_null == 0), ...").
```

Блок-схема, построенная для функции op2 будет иметь вид:

```
N0:  assign_unk  op2.return = unknown;
N1:  stop.
```

Условия корректности будут иметь вид:

```
(N0, str.is_null == 0),
(N0, str.size >= 1),
(N0, str.offset >= 0).
```

Легко видеть, что указанные условия корректности будут следовать из предусловий вызова `op2`.

Условия корректности, определенные для блок-схемы функции `main`, также следуют выведенных инвариантов. Таким образом, итоговый отчет об уязвимостях будет пустым.

Необходимо отметить, что в методах, описанных в работах [6, 7], функции `op1` и `op2` не будут проанализированы вообще, либо будут проанализированы вне зависимости от контекста вызова их из функции `main`. Следовательно, такой анализ не может считаться достаточно полным.

4. Заключение

В настоящей публикации рассмотрены типовые подходы к решению комплекса задач, связанных с верификацией программного кода, выделены их достоинства и недостатки. В работе описан подход к построению автоматизированного средства верификации исходного кода программ, написанных с использованием языка программирования C, позволяющего выявлять уязвимости различных классов. Важным фактором является то, что данный подход позволяет гарантировать консервативность описанного средства. Кроме того, в работе было показано, что рассматриваемый метод позволяет разрешить вопросы, связанные с наличием в анализируемой программе рекурсивных вызовов функций или неявных вызовов функций, в то время, как в других аналогичных исследованиях указанные проблемы остались без должного внимания.

В заключение отметим, что с помощью описанного средства были проверены на предмет наличия уязвимостей, связанных с некорректной работой к памяти, такие широко распространенные открытые программные средства, как

- `sshd` — демон программы защищенного удаленного доступа к хосту (проект OpenSSH, $\approx$ 70 тыс. строк кода);
- `tar` — средство архивирования файлов ($\approx$ 40 тыс. строк кода);
- модуль `ISDN` ядра ОС Linux 2.0.32;
- модуль `I2C` ядра ОС Linux версии 2.6.13 (в числе прочих, была обнаружена известная уязвимость SA-17384);

- модуль `mod-rewrite` веб-сервера Apache версии 2.0.59 (в числе прочих, была обнаружена широко известная уязвимость CVE-2006-3747).

Литература

[1] Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации // М., 1992.

[2] W. Royce. *Managing the Development of Large Software Systems*: *Concepts and Techniques* // Technical Papers of Western Electronic Show and Convention. 1970, Los Angeles, USA. P. 328–338.

[3] B. Boehm. *A Spiral Model of Software Development and Enhancement* // TRW Defense Systems Group. COMPUTER Journal, May 1988. P. 61–72.

[4] K. Beck. *Extreme Programming Explained*: *Embrace Change*. Addison Wesley Professional, November 2004. P. 224.

[5] K. Fogel. *Producing Open Source Software*. O'Reilly, October 2005. P. 184.

[6] D. Wagner, J. Foster, E. Brewer, A. Aiken. *A First Step Towards Automated Detection of Buffer Overrun Vulnerabilities* // Proceedings of the 2000 Network and Distributed Systems Security Conference, February 2000. P. 423–460.

[7] N. Dor, M. Rodeh, M. Sagiv. *CSSV*: *Towards a Realistic Tool for Statically Detection All Buffer Overflows in C* // Proceedings of the ACM SIGPLAN 2003 conference, San Diego, California, USA, 2003. P. 155–167.

[8] D. Wheeler. *More Than a Gigabuck*: *Estimating GNU/Linux's Size*, `http://www.dwheeler.com/sloc/redhat71-v1/redhat71sloc.html`.

[9] *Measuring Libre Software Using Debian* 3.1 (*Sarge*) *as A Case Study*: *Preliminary Results*. `http://www.upgrade-cepis.org/issues/2005/3/up6-3Amor.pdf`.

[10] C. Cowan, C. Pu, D. Maier, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, Q. Zhang. *StackGuard*: *Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks* // Proceedings of the 7th USENIX Security Symposium, San Antonio, Texas, January, 1998.

[11] K. Spett. *SQL Injection. Are your web applications vulnerable*? `http://www.spidynamics.com/papers/SQLInjectionWhitePaper.pdf`

[12] A. Rubini. *Linux Device Drivers. Chapter* 5: *Concurrency and Race Conditions*. Third edition. O'Reilly, 2005. P. 106–134.

[13] J. Viega, J. T. Bloch, T. Kohno, G. McGraw. *ITS*4: *A Static Vulnerability Scanner for C and C++ Code* // Annual Computer Security Applications Conference, December 11–15, 2000. P. 257–267.

[14] D. Larochelle, D. Evans. *Statically Detecting Likely Buffer Overflow Vulnerabilities* // 2001 USENIX Security Symposium, Washington, D. C., August, 2001. P. 177–190.

[15] `http://www.splint.org/`.

[16] Ф. М. Пучков, К. А. Шапченко *Статический метод анализа програмного обеспечения на наличие угроз переполнения буферов* // Программирование. 2005. № 4. С. 19–34.

[17] Д. Б. Юдин, Е. Г. Гольштейн. Линейное программирование. М.: Государственное издательство физико-математической литературы, 1963. С. 776.

Метод обнаружения несправедливого захвата ресурсов реализациями транспортного протокола Интернет на основе модели производительности

О. Ю. Богоявленская, Ю. А. Богоявленский

1. Введение

Современные сети передачи данных трактуют всех своих пользователей и генерируемые ими потоки как равноправные в смысле доступа к сетевым ресурсам (например, каналам связи и маршрутизаторам), которые они должны справедливо разделять между собой, независимо от конфигурации и загрузки сетевого маршрута или элементов оборудования. В настоящее продолжается интенсивная дискуссия о трактовках термина «справедливый» и количественных метриках, определяющих его [1].

В Интернет реализована децентрализованная технология распределенного управления, предполагающая, что источники потоков данных, не имея полной информации о структуре и загруженности сетевого маршрута, интерпретируют сигналы обратной связи и адаптируют генерируемую ими нагрузку сети. В этом контексте считается, что ресурсы сети разделяются справедливо, если потоки полностью выполняют требования технологии распределенного управления. В современном Интернет функция распределенного управления реализуется протоколом Transmission Control Protocol (TCP) [2]. Протокол TCP контролирует подавляющее большинство потоков на транспортном уровне Интернет и модифицирует пропускную способность соединения согласно интерпретации доступных ему сведений о состоянии сети, с целью предотвращения ее перегрузки [1]. Этот механизм является существенной частью протокола и стандартизован IETF.

Тем не менее, в сети были зафиксированы реализации транспортных протоколов, нарушающие стандартные схемы. Такие реализации либо намеренно пренебрегают предотвращением перегрузки в пользу увеличения собственной пропускной способности, либо неверно трактуют алгоритм

[1] В англоязычной литературе используется термин Congestion Avoidance.

определения текущего размера скользящего окна. Тем самым они производят распределенное деструктивное информационное воздействие на стандартные TCP-соединения, которое приводит к несанкционированному перераспределению ресурсов сетевой инфраструктуры или к резкому снижению ее полезной нагрузки. И в том и в другом случае эти нестандартные реализации представляют с точки зрения реализаций, следующих стандарту, угрозу доступности данных сети и ее целостности. Отметим, что высокая скрытность и распределенный характер такого несанкционированного деструктивного информационного воздействия весьма затрудняют своевременное обнаружение нарушителя. По этим причинам обнаружение потоков, управляемых такими реализациями, является важной и актуальной задачей.

В настоящей работе предложен метод обнаружения нестандартных реализаций транспортных протоколов, основанный на разработанной авторами модели производительности TCP [6]. Последняя позволяет рассчитать производительность стандарта протокола, которая не должна превышаться реализациями. Предлагаемый метод ориентирован на «длинные» соединения, в противовес «коротким» сеансам web-серверов, анализируемых в [3].

2. Основные средства стандартного распределенного управления потоками

Протокол транспортного уровня должен выполнять ряд функций, контролируя соединение на уровне точка-точка. В множество этих функций в том числе входят контроль за доставкой данных и управление характеристиками потока данных. Контроль за доставкой данных обеспечивают подтверждения доставки получателем. Для оптимизации загрузки сети используется механизм скользящего окна, который позволяет отправлять без подтверждения фиксированный объем данных, называемый размером окна. Если все данные окна отправлены, то продолжить передачу можно только после получения подтверждения доставки.

Управление характеристиками потока данных осуществляется посредством управления размером скользящего окна. Мы рассмотрим основной алгоритм TCP, называемый Additive Increase Multiplicaitve Decrease (AIMD). Этот алгоритм изменяет размер скользящего окна, интерпретируя содержание подтверждений получателя. Алгоритм AIMD увеличивает размер окна на единицу, если все данные окна доставлены, и уменьшает размер окна в два раза, если данные были потеряны. Такой механизм позволяет с одной стороны захватывать свободные ресурсы сети и, с другой стороны, предотвращать перегрузку сетевых ресурсов, поддерживая

устойчивое состояние пропускной способности. Очевидно, что такая схема является работоспособной только при условии соблюдения ее всеми потоками, использующими общие фрагменты сетевых маршрутов.

Рядом исследований (проект TBIT [3, 4]) были зафиксированы реализации протокола TCP, которые пренебрегают стандартом AIMD. Цель таких реализаций — увеличение производительности протокола — достигается за счет пренебрежения функцией предотвращения перегрузки. А именно, получив сигнал о потере данных, такие реализации уменьшают размер скользящего окна менее, чем в два раза, не уменьшают его вовсе, или продолжают наращивать.

Угрозы, представляемые такими реализациями можно разделить на два класса. Во-первых, управляемые ими соединения, захватывая ресурсы, не предназначенные им стандартом [2], подавляют производительность стандартных соединений, адекватно реагирующих на потерю данных. Создавая обратную связь со стандартными реализациями, они провоцируют их деградацию, дальнейшие освобождение ими ресурсов сети, которые продолжают захватывать. Таким образом, содержательно их действия эквивалентны атаке с целью несанкционированного захвата ресурса. Атака носит распределенный характер и представляет угрозу для всех стандартных соединений, разделяющих сетевой маршрут.

Во-вторых, множество несправедливых реализаций на маршруте может спровоцировать явление «коллапса насыщения», когда полезная загрузка сети приближается к нулю [5]. В этом случае упомянутое множество производит распределенное деструктивное воздействие, содержательно эквивалентное DoS-атаке (Denial of Service) или flood-атаке, когда маршрутизаторы и каналы передачи данных заполняются большими объемами бесполезного трафика, срывая предоставление сетевых услуг. При «коллапсе насыщения» в сети теряется более 90 % сегментов данных, направленных в нее, в результате чего сеть заполняется повторно передаваемыми сегментами и ее пропускная способность резко падает (Это явление впервые было зафиксировано в UC Berkeley в октябре 1986 г.)

Распределенный характер описанных деструктивных воздействий затрудняет своевременное обнаружение TCP-источников нарушителей, так как само воздействие осуществляется на удаленных сегментах сетевой инфраструктуры и заключается и заключается в искажении доступной атакуемым стандартным TCP-источникам информации об уровне загруженности сети.

Таким образом, наличие в сети соединений, пренебрегающих функцией предотвращения перегрузки, представляет угрозу целостности сети и доступности ее данных. Поэтому необходимо выявлять источники потоков

данных, использующие несправедливые захваты ресурсов нестандартными реализациями транспортного протокола.

3. Производительность стандартного алгоритма AIMD

Изложим кратко результаты работы [6], которые необходимы для понимания следующих разделов настоящей статьи. В этой работе представлена математическая модель стандартного алгоритма AIMD, которая позволяет рассчитать производительность соединения, управляемого этим алгоритмом. Основными параметрами модели являются:

- вероятность потери сегмента [2)] TCP;
- максимальный размер скользящего окна $w_{\max}$ (сетевое или аппаратное ограничение);
- распределение времени кругового оборота RTT (Round Trip Time);
- ограничение пропускной способности сетевого маршрута.

Заметим, что последний параметр может игнорироваться, согласно соображениям, изложенным в [6].) Исходя из этих параметров, полученная модель позволяет рассчитать следующие величины.

Стационарное распределение размера скользящего окна w алгоритма AIMD P_w может быть представлено в виде

$$P_w = \frac{\alpha_w \pi_w}{\sum\limits_{w=2}^{w_{\max}} \alpha_w \pi_w}. \tag{1}$$

Здесь величины π_w удовлетворяют следующим рекуррентным соотношениям

$$\pi_i = \pi_j K_i,$$

где

$$K_{w_{\max}} = \frac{F_{w_{\max}-1}}{1 - f_{w_{\max}}}, \tag{2}$$

$$K_i = F_{i-1}, \qquad j < i < w_{\max}, \tag{3}$$

$$K_{i-1} = \frac{1}{f_{i-1}} \left(K_i - \left(K_{2i}(1 - f_{2i}) + K_{2i+1}(1 - f_{2i+1})\right)\right), \qquad i < j, \tag{4}$$

При этом $F_i = \prod_{k=j}^{i} f_k$ и $j = \lfloor w_{\max}/2 \rfloor$.

Величины α_w определяются в виде

$$\alpha_w = \int_{wt_0}^{\infty} t dR(t) + wt_0 R(wt_0), \tag{5}$$

[2)] Сегмент — название пакета данных, принятое на транспортном уровне.

где t_0 — время, которое требуется источнику данных для отправки в сеть одного сегмента TCP. Детали и соответствующие доказательства представлены в [6].

Стационарное распределение пропускной способности AIMD в раунде будет иметь вид

$$T(x) = 1 - \sum_{w=2}^{w_{\max}} P_w R\left(\frac{w}{x}\right). \tag{6}$$

Выражение (6) имеет место для всех $x < 1/t_0$, $T(1/t_0) = 1$ и $R(x)$ — распределение RTT.

Далее будем обоснованно предполагать, что производительность TCP-соединения, полностью соответствующего [2], не должна превышать теоретическую производительность стандартизованного алгоритма AIMD.

Будем считать несправедливым захватом сетевого ресурса действия реализации TCP, производительность которой превышает теоретическую производительность AIMD.

4. Метод обнаружения несправедливого захвата ресурсов

Распределения (1) и (6) позволяют получить широкий набор характеристик соединения точка-точка и могут служить основой для различных статистических схем обнаружения захвата ресурсов. Структура таких схем существенно зависит от степени детализации данных наблюдений, генерируемых используемой системой мониторинга. Рассмотрим далее две различные статистические схемы обнаружения нестандартных TCP-соединений, предполагающие различные объем и содержание доступных для анализа данных.

1. Высокий уровень детализации данных

Пусть изучается поведение TCP-соединения, установленного некоторой сетевой ЭВМ и пусть известна полная, упорядоченая по времени последовательность размеров скользящего окна алгоритма AIMD, продемонстрированная этим соединением в течение его жизни $\Omega = \{\omega_i\}_{i-1}^N$. Обозначим $n_{ij}(k)$ количество переходов таких, что $\omega_{k-1} = i$ и $\omega_k = j$. Пусть

$$n_{ij} = \sum_{k=1}^{N} n_{ij}(k).$$

Последовательность Ω является траекторией марковского процесса, переходные вероятности которого (см. [6]) имеют следующий вид

$$p_{i,i+1} = (1-p)^i, \quad p_{2i,i} = 1-(1-p)^{2i}, \quad p_{2i+1,i} = 1-(1-p)^{2i+1},$$

где p — вероятность потери TCP-сегмента. Для остальных пар индексов $p_{ij} = 0$. Согласно [7] выражение

$$f_{ij} = \frac{n_{ij}}{\sum_j n_{ij}} \tag{7}$$

является состоятельной оценкой максимального правдоподобия для вероятностей p_{ij}. Очевидно, что если изучаемая реализация протокола TCP следует стандарту IETF, то f_{ij} должны являться оценками вероятностей p_{ij}. Поэтому, предложенные в [8] критерии максимального правдоподобия и χ^2 для проверки гипотезы о равенстве значений переходных вероятностей наблюдаемого процесса значениям p_{ij} позволят сделать вывод о наличии противоречий стандарту наблюдаемого соединения. Заметим, что такая схема не использует распределение (1).

2. Низкий уровень детализации данных

Пусть изучается реализация протокола TCP на некоторой сетевой ЭВМ (будем называть ее «источник»). Наблюдая TCP-соединение источника, получим следующие оценки его характеристик. Ограничение на размер скользящего окна $w_{\max}$, выборку значений RTT (последнее можно заменить парой $E[R]$, $D[R]$ — соответственно математическое ожидание и дисперсия RTT) и

$$p = \frac{N_{\text{ack}}}{N}$$

(N_{ack} — общее количество случаев получения источником троекратного повторного подтверждения[3)], N — общее число раудов). Величина p принимается нами в качестве оценки вероятности потери сегмента данных, так как именно троекратные повторные подтверждения интерпретируются AIMD как сигнал о приближающейся перегрузке сетевого маршрута. Обозначим

$$P = \{w_{\max}, \{\text{RTT}_i\}_{i=1}^N, p\}.$$

Пусть для наблюдения также доступна некоторая величина X, характеризующая соединение и являющаяся функцией перечисленных выше параметров.

В результате наблюдений за k соединениями источника, получим набор оценок параметров $\{P_i\}_{i=1}^k$ и выборки $\{X_i\}$, где X_i — значение выбранной

[3)] В англоязычной литературе используется термин triple acknowledgement.

характеристики, которое было продемонстрировано соединением с параметрами P_i. Размер этих выборок зависит от условий наблюдения и возможностей системы мониторинга.

Выберем значение $0 < \alpha < 1$. Опираясь на распределения (1) и (6), построим функцию распределения выбранной характеристики для наблюдаемых соединений $D_X^i(x) = F(x, P_i)$. Определим для каждого набора параметров величину X_α: $\mathsf{P}\{X > X_\alpha\} = 1 - F(X_\alpha, P_i) = \alpha$. Обозначим X_α^i значение X_α, рассчитанное с параметрами P_i. Будем считать успехом событие $X_i > X_\alpha^i$ и неудачей событие $X_i \leqslant X_\alpha^i$. Наблюдаемые нами выборки $\{X_j^i\}$ таким образом трансформируются в бинарную последовательность успехов и неудач. Последняя, должна быть выборкой из распределения Бернулли с параметром α. Результаты стандартной проверки критерия согласия распределений позволят сделать статистический вывод о соответствии наблюдаемой реализации ТСР и стандарта [2].

Пример. Пусть система мониторинга не сообщает содержание последовательности Ω, но сообщает среднее значение элементов этой последовательности $\widetilde{w}$. Положим $X = \widetilde{w}$. Последнее может быть представлено в виде

$$\widetilde{w} = \frac{\sum_i^N w_i}{N}. \tag{8}$$

Оценка $\widetilde{w}$ является асимптотически нормальной (см., например [9]) и имеет математическое ожидание E_w и дисперсию $\sigma = f(D_w, p, N)$. При этом E_w и D_w, математическое ожидание и дисперсия размера окна w, однозначно определяются распределением (1) и, следовательно, могут быть получены на основе выражений (2), (3), (4), (5). Согласно предложенной схеме, для выбранного значения α необходимо найти w_α, являющееся решением уравнения

$$\mathsf{P}\{\widetilde{w} > w_\alpha\} = N(w_\alpha, E_w, \sigma) = \alpha.$$

Пусть наблюдалось k соединений некоторого источника и соответствнно получена совокупность $\{\widetilde{w}_i\}_{i=1}^k$. Обозначим

$$S_i = \begin{cases} 1, & \text{если } \widetilde{w}_i > w_\alpha^i \\ 0 & \text{иначе} \end{cases}$$

и пусть $\beta = \sum\limits_{i=1}^{k} S_i$. Рассмотрим выражение

$$H = \frac{(\beta - k\alpha)^2}{k\alpha(1-\alpha)} \tag{9}$$

Поведение соединения признается не противоречащим стандарту, если H не превосходит значения χ^2 с одной степенью свободы при выбранном администратором сети уровне значимости.

Заметим, что предлагаемый метод позволяет исследовать соответствие стандарту производительности соединений, но игнорирует средства, которыми эта производительность достигается. Последние могут находиться в формальном противоречии со стандартом (например, применять алгоритмы, отличные от AIMD), но не представляют указанных выше угроз, если достигают производительности, эквивалентной стандартной.

Таким образом, представленный в работе метод, в отличие от специализированных средств (таких как TBIT [4]), может опираться на данные стандартных средств мониторинга (например, tcpdump), не требует запуска дополнительных исследовательских соединений со специальными свойствами. Метод может применяться только для узкого класса угроз, описанных выше.

Литература

[1] Floyd S. Metrics for Evaluation of Congestion Control Mechanisms. IETF Internet Draft, 2006.

[2] Allman M., Paxon V., Stevens W. TCP Congestion Control, RFC2581.

[3] Medina A., Allman M., Floyd S. Measuring Evolution of Transport Protocols in the Internet. CCR, 35(2), 2005.

[4] Padhey J., Floyd S. Identifying TCP behavior of Web Servers. ACM SIGCOMM, August 2001.

[5] Jacobson V. Congestion Avoidance and Control. Proceedings of SIGCOMM'88.

[6] Богоявленская О. Ю., Анализ случайного потока, генерируемого транспортным протоколом с обратной связью, в сети передачи данных. Автоматика и телемеханика, № 12, 2003, с. 60–68.

[7] Ли Ц., Джадд Д., Зельнер А. Оценивание параметров марковских моделей по агрегированным временным рядам. М.: Статистика, 1997, 221 с.

[8] Anderson T. W., Goodman L. A. Statistical Inference about Markov Chain. The Ann. of Math. Stat., 28, 1957, p. 89–110.

[9] Сираджинов С. Х., Форманов Ш. К. Предельные теоремы для сумм случайных векторов, связанных в цепь Маркова. Ташкент: Фан, 1979. С. 171.

Моделирование безопасности управления доступом и информационными потоками в компьютерных системах

П. Н. Девянин

Для анализа безопасности управления доступом и информационными потоками по памяти и по времени между сущностями компьютерной системы (КС) с дискреционным или мандатным управлением доступом построены математические модели КС, которые будем называть ДП-моделями [1]. Первой построена базовая ДП-модель КС с дискреционным управлением доступом, которая является основой всех ДП-моделей.

В ДП-моделях учтены ряд особенностей функционирования современных КС, в том числе:

- различие в условиях реализации в КС информационных потоков по памяти и по времени;
- наличие в современных КС иерархической структуры сущностей и возможность ее использования при реализации информационных потоков по времени;
- возможность кооперации части субъектов КС при передаче прав доступа или реализации информационных потоков;
- возможность реализации в КС доверенных и недоверенных субъектов с различными условиями функционирования;
- возможность противодействия доверенными субъектами КС передаче прав доступа или реализации информационных потоков недоверенными субъектами;
- возможность изменения функциональности субъекта при реализации информационного потока по памяти на функционально-ассоциированные с ним сущности.

Для построения базовой ДП-модели использованы классическая модель *Take-Grant* и ее основные расширения [2, 5], модель Белла—Ла-Падула [4] и ее интерпретации [7], субъектно-ориентированная модель изолированной программной среды [3] и модель систем военных сообщений [6].

В основе базовой ДП-модели используется классических подход, состоящий в том, что каждая моделируемая КС представляется абстрактной системой, каждое состояние которой представляется графом доступов, каждый переход системы из состояния в состояние осуществляется в результате применения одного из правил преобразования графов доступа.

Используем следующие обозначения и определения:

$E = O \cup C$ — множество сущностей, где O — множество объектов, C — множество контейнеров и $O \cap C = \emptyset$;

$S \subseteq E$ — множество субъектов;

$R_r = \{read_r, write_r, append_r, execute_r, own_r\}$ — множество видов прав доступа, где $read_r$ — право доступа на чтение из сущности, $write_r$ — право доступа на запись в сущность, $append_r$ — право доступа на запись в конец сущности, $execute_r$ — право доступа на выполнение (активизацию) сущности, own_r — право доступа на владение сущностью, позволяющее субъекту-владельцу передавать права доступа к сущности другим субъектам или удалить сущность;

$R_a = \{read_a, write_a, append_a\}$ — множество видов доступа, где $read_a$ — доступ на чтение из сущности, $write_a$ — доступ на запись в сущность, $append_a$ — доступ на запись в конец слова, содержащегося в сущности;

$R_f = \{write_m, write_t\}$ — множество видов информационных потоков, где $write_m$ — информационный поток по памяти на запись в сущность, $write_t$ — информационный поток по времени на запись в сущность;

$R_{raf} = R_r \cup R_a \cup R_f$ — множество видов прав доступа, видов доступа и видов информационных потоков, при этом множества R_r, R_a, R_f попарно не пересекаются.

Перечисленные элементы множества R_{raf} являются наиболее распространенными в современных КС, с их использованием, как правило, можно представить любой вид права доступа, вид доступа или вид информационного потока в КС.

Определение 1. Иерархией сущностей называется заданное на множестве сущностей E отношение частичного порядка «$\leqslant$» (то есть отношение, обладающее свойствами рефлексивности, антисимметричности и транзитивности), удовлетворяющее условию:

> если для сущности $e \in E$ существуют сущности e_1, $e_2 \in E$ такие, что $e \leqslant e_2$, $e \leqslant e_1$, то или $e_1 \leqslant e_2$, или $e_2 \leqslant e_1$.

В случае, когда для двух сущностей e_1, $e_2 \in E$ выполняются условия $e_1 \leqslant e_2$ и $e_1 \neq e_2$, будем говорить, что сущность e_1 содержится в сущности-контейнере e_2, и будем использовать обозначение: $e_1 < e_2$.

Определение 2. Определим $H\colon E \to 2^E$ — функцию иерархии сущностей, сопоставляющую каждой сущности $c \in E$ множество сущностей $H(c) \subset E$, удовлетворяющее условиям:

Условие 1. Если сущность $e \in H(c)$, то $e < c$, и не существует сущности-контейнера $d \in C$ такой, что $e < d$, $d < c$.

Условие 2. Для любых сущностей e_1, $e_2 \in E$, $e_1 \neq e_2$ по определению выполняются равенство $H(e_1) \cap H(e_2) = \emptyset$ и условия:

- если $o \in O$, то выполняется равенство $H(o) = \emptyset$;
- если $e_1 < e_2$, то или e_1, $e_2 \in E \setminus S$, или e_1, $e_2 \in S$;
- если $e \in E \setminus S$, то $H(e) \subset E \setminus S$;
- если $s \in S$, то $H(s) \subset S$.

Описанная иерархия сущностей является типичной для современных КС. Например, она соответствует иерархии файлов и каталогов (директорий) на жестких дисках компьютеров, доменной иерархии компьютеров в ОС семейств Microsoft Windows 2000/XP/2003.

Определение 3. Пусть определены множества S, E, $R \subseteq S \times E \times R_r$, $A \subseteq S \times E \times R_a$, $F \subseteq E \times E \times R_f$, $F \subseteq E \times E \times R_f$ и функция иерархии сущностей H. Определим $G = (S, E, R \cup A \cup F, H)$ — конечный помеченный ориентированный граф, без петель, где элементы множеств S, E являются вершинами графа, элементы множества $R \cup A \cup F$ являются ребрами графа. Назовем $G = (S, E, R \cup A \cup F, H)$ графом прав доступа, доступов и информационных потоков или сокращенно графом доступов. При этом в графе доступов будем использовать следующие обозначения:

- вершины из множества S (соответствующие субъектам) в графе доступов будут обозначаться «$\bullet$»,
- вершины из множества $E \setminus S$ (соответствующие сущностям, не являющимся субъектами) в графе доступов будут обозначаться «$\otimes$»,
- каждое ребро графа доступов помечено одним из элементов множества R_{raf},
- каждое ребро из множества R будет обозначаться стрелкой вида, представленного на рис. 1 а) (элементы множества R являются ребрами графа доступов, соответствующими правам доступа субъектов к сущностям),
- каждое ребро из множества A будет обозначаться стрелкой вида, представленного на рис. 1 б) (элементы множества A являются ребрами графа доступов, соответствующими доступам субъектов к сущностям),
- каждое ребро из множества F, помеченное $write_m$, будет обозначаться стрелкой вида, представленного на рис. 1 в), каждое ребро из

множества F, помеченное $write_t$, будет обозначаться стрелкой вида, представленного на рис. 1 г) (элементы множества F являются ребрами графа доступов, соответствующими информационным потокам между сущностями).

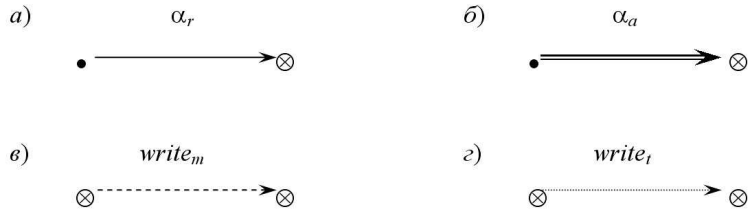


Рис. 1. Обозначения ребер графа доступов:
а) — ребро из множества R, помеченное $\alpha_r \in R_r$;
б) — ребро из множества A, помеченное $\alpha_a \in R_a$;
в) — ребро из множества F, помеченное $write_m$;
г) — ребро из множества F, помеченное $write_t$

Используем также обозначения:
$\Sigma(G^*, OP)$ — система, при этом:

- каждое состояние системы представляется графом доступов;
- G^* — множество всех возможных состояний;
- OP — множество правил преобразования состояний;

$G \vdash_{op} G'$ — переход системы $\Sigma(G^*, OP)$ из состояния G в состояние G' с использованием правила преобразования состояний $op \in OP$.

Если для системы $\Sigma(G^*, OP)$ определено начальное состояние, то будем использовать обозначение:

$\Sigma(G^*, OP, G_0)$ — система $\Sigma(G^*, OP)$ с начальным состоянием G_0.

В базовой ДП-модели определены 16 монотонных и немонотонных правил преобразования состояний:

$take_right(\alpha_r, x, y, z)$, $grant_right(\alpha_r, x, y, z)$, $remove_right(\alpha_r, x, y, z)$, $own_take(\alpha_r, x, y)$, $own_remove(\alpha_r, x, y)$, $create_entity(x, y, z)$, $create_subject(x, y, z)$, $delete_entity(x, y, z)$, $rename_entity(x, y, z)$, $access_read(x, y)$, $access_write(x, y)$, $access_append(x, y)$, $flow(x, y, y', z)$, $find(x, y, z)$, $post(x, y, z)$, $pass(x, y, z)$.

Примеры применения монотонных правил $rename_entity(x, y, z)$ и $flow(x', y', y, x)$ приведены на рис. 2 и 3.

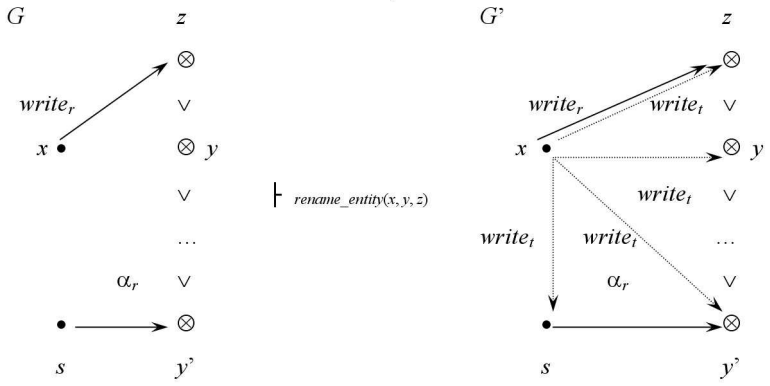


Рис. 2. Реализация информационных потоков по времени при применении правила *rename_entity*(x, y, z) , где $\alpha_r \in R_r$

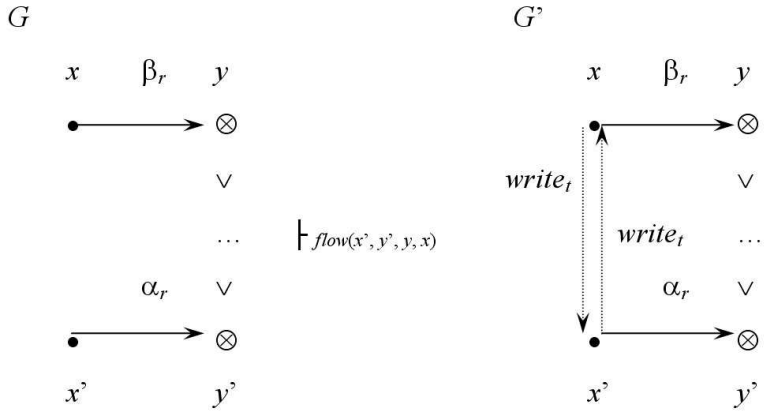


Рис. 3. Пример применения правила *flow*(x', y', y, x), где $\alpha_r, \beta_r \in R_r$

В рамках базовой ДП-модели теоретически обосновано, что при анализе условий передачи прав доступа, реализации информационных потоков по памяти и по времени возможно использование только монотонных правил преобразования состояний, а также определены условия передачи прав доступа и реализации информационных потоков по памяти и по времени для случая, когда все субъекты КС действуют в кооперации.

Определение 4. Пусть $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ — состояние системы $\Sigma(G^*, OP)$ и субъект $x \in S_0$, сущность $y \in E_0$, где $x \neq y$, и пусть

$\alpha \in R_r$ — некоторое право доступа. Определим предикат $can_share(\alpha, x, y, G_0)$, который будет истинным тогда, и только тогда, когда существуют состояния $G_1, \ldots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N)$ и правила преобразования состояний $op_1, \ldots, op_N$ такие, что $G_0 \vdash_{op1} G_1 \vdash_{op2} \ldots \vdash_{opN} G_N$ и $(x, y, \alpha) \in \in R_N$, где $N \geqslant 0$.

Определение 5. Пусть $G_0 = S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ — состояние системы $\Sigma(G^*, OP)$ и сущности $x, y \in E_0$, где $x \neq y$. Определим предикат $can_write_memory(x, y, G_0)$, который будет истинным тогда, и только тогда, когда существуют состояния $G_1, \ldots, G_N = (S_N, E_N, R_N \cup A_N \cup \cup F_N, H_N)$ и правила преобразования состояний $op_1, \ldots, op_N$ такие, что $G_0 \vdash_{op1} G_1 \vdash_{op2} \ldots \vdash_{opN} G_N$ и $(x, y, write_m) \in F_N$, где $N \geqslant 0$.

Определение 6. Пусть $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ — состояние системы $\Sigma(G^*, OP)$ и сущности $x, y \in E_0$, где $x \neq y$. Определим предикат $can_write_time(x, y, G_0)$, который будет истинным тогда, и только тогда, когда существуют состояния $G_1, \ldots, G_N = (S_N, E_N, R_N \cup A_N \cup \cup F_N, H_N)$ и правила преобразования состояний $op_1, \ldots, op_N$ такие, что $G_0 \vdash_{op1} G_1 \vdash_{op2} \ldots \vdash_{opN} G_N$ и $(x, y, \alpha_f) \in F_N$, где $\alpha_f \in \{write_m, write_t\}$ и $N \geqslant 0$.

В рамках базовой ДП-модели обоснованы необходимые и достаточные алгоритмически проверяемые условия передачи прав доступа и реализации информационных потоков по памяти и по времени для случая, когда все субъекты КС действуют в кооперации. При этом особо рассмотрены условия реализации информационных потоков по времени.

Теорема 1. *Пусть* $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ — *состояние системы* $\Sigma(G^*, OP)$ *и сущности* $x, y \in E_0$, $x \neq y$. *Предикат*

$$can_write_time(x, y, G_0)$$

истинен тогда, и только тогда, когда существует последовательность сущностей $e_1, \ldots, e_m \in E_0$, *где* $e_1 = x$, $e_m = y$ *и* $m \geqslant 2$, *таких, что выполняется одно из условий*:

Условие 1. $m = 2$ *и* $(x, y, \alpha_f) \in F_0$, *где* $\alpha_f \in \{write_m, write_t\}$.

Условие 2. *Для каждого* $i = 1, \ldots, m-1$ *выполняется одно из условий*:

- $e_i \in S_0$ *и* $(e_i, e_{i+1}, write_t) \in F_0$;
- $e_i \in S_0$ *и истинен предикат* $can_write_memory(e_i, e_{i+1}, G_0)$;
- $e_i \in S_0$ *и существует сущность* $e'_{i+1} \in E_0$, *такая, что* $e'_{i+1} \leqslant e_{i+1}$ *и истинен предикат* $can_share(\alpha_r, e_i, e'_{i+1}, G_0)$, *где* $\alpha_r \in R_r$;
- $e_{i+1} \in S_0$ *и истинен предикат* $can_share(read_r, e_{i+1}, e_i, G_0)$;
- $e_i, e_{i+1} \in S_0$ *и существуют сущности* $e'_i, e'_{i+1} \in E_0$ *такие, что или* $e'_i \leqslant e'_{i+1}$, *или* $e'_{i+1} \leqslant e'_i$, *и истинны предикаты*

can_share(α_r, e_i, e'_i, G_0) *и can_share*(β_r, e_{i+1}, e'_{i+1}, G_0), *где* $\alpha_r, \beta_r \in$ $\in R_r$.

В ДП-моделях, построенных на основе базовой ДП-модели, в зависимости от анализируемых условий функционирования моделируемых КС могут уточняться условия и результаты применения правил преобразования состояний, значения функции иерархии сущностей, также могут использоваться дополнительные правила преобразования состояний. Условия передачи прав доступа и реализации информационных потоков в КС без кооперации доверенных и недоверенных субъектов также могут быть проанализированы с использованием ДП-моделей (например, ДП-модели без кооперации доверенных и недоверенных субъектов или, сокращенно, БК ДП-модели).

Отношение иерархии сущностей системы $\Sigma(G^*, OP)$ может быть использовано для реализации в КС информационных потоков по времени. Однако субъекты системы могут препятствовать созданию информационных потоков по времени с использованием сущностей, к которым они имеют доступ. Например, на рис. 4 доступ α_a субъекта s к сущности b препятствует возникновению (с использованием находящихся в одной иерархии с сущностью b сущностей c и a) информационного потока по времени от субъекта x к субъекту y.

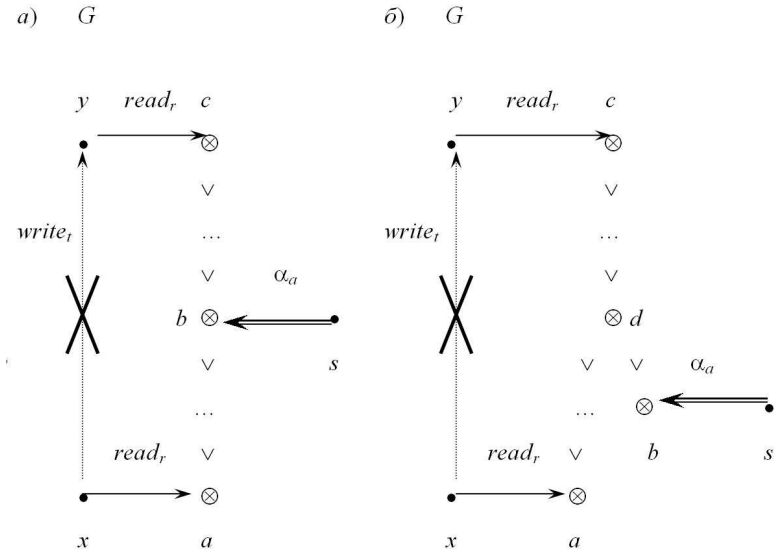


Рис. 4. Примеры, когда невозможна реализация информационного потока по времени с использованием отношения иерархии сущностей

Следовательно, возможно включение в систему доверенных субъектов, которые осуществляют доступы к сущностям с целью предотвращения возможности реализации с их использованием запрещенных информационных потоков по времени.

Определение 7. Любой доступ любого доверенного субъекта к сущности назовем блокирующим.

На основе БК ДП-модели построим ДП-модель с блокирующими доступами доверенных субъектов (или, сокращенно, БД ДП-моделью). При этом используем обозначения:

$E_B \subset E$ — множество сущностей, к которым имеют доступ доверенные субъекты системы $\Sigma(G^*, OP), OP)$;

$A_B \subset A$ — множество блокирующих доступов доверенных субъектов системы $\Sigma(G^*, OP)$, при этом $A_B \subseteq (L_S \cap S) \times E_B \times R_a$.

Также следует внести изменения в определения иерархии сущностей «$\leqslant_B$» и функции иерархии сущностей $H_B()$ с учетом блокирующих доступов доверенных субъектов.

В рамках БД ДП-модели определены и обоснованы алгоритмически проверяемые условия, обеспечивающие невозможность возникновения запрещенных информационных потоков по времени для случая, когда после того, как доверенные субъекты реализуют блокирующие доступы, доступы к сущностям осуществляют только недоверенные субъекты.

Опишем метод предотвращения возможности реализации в КС запрещенных информационных потоков по времени с использованием блокирующих доступов доверенных субъектов. Сокращенно, описание метода включает следующие шаги, определяющие действия в системе $\Sigma(G^*, OP, G_0)$, которые необходимо осуществить при применении метода.

Метод 1. *Условие применения метода.* Пусть определена система $\Sigma(G^*, OP, G_0)$ с начальным состоянием $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ и определены множества доверенных субъектов L_S, недоверенных субъектов N_S и запрещенных информационных потоков N_f.

Шаг 1. Создать в системе доверенный субъект $u \in L_S \cap S_0$, который будет реализовывать блокирующие доступы.

Шаг 2. Для каждого запрещенного информационного потока по времени $(x, y, write_t)$, где x и y — недоверенные субъекты, использовать алгоритм проверки истинности предиката $can_write_time_block(x, y, G_0, L_S)$. Если предикат $can_write_time_block(x, y, G_0, L_S)$ является истинным, рассмотреть все пути (пролеты моста) в G_0, с использованием которых возможна реализация информационного потока. Если для всех запрещенных информационных потоков из N_f по времени предикат

$can_write_time_block(x, y, G_0, L_S)$ является ложным, то закончить применение метода.

Шаг 3. Для каждого пути, определенного на шаге 2, определить его вид. Возможны два вида путей. Если путь первого вида, то с его использованием реализуется информационный поток по памяти. Если путь второго вида, то с его использованием может быть реализован только информационный поток по времени.

Шаг 4. Если пролет моста первого вида, то удалить любое ребро пути (удалить у недоверенного субъекта право доступа к сущности). Перейти на шаг 2.

Шаг 5. Если путь второго вида, реализовать блокирующий доступ доверенного субъекта u к любой сущности, не являющейся субъектом и принадлежащей пути. Перейти на шаг 2.

Теорема 2. *Пусть* $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ *— начальное состояние системы* $\Sigma(G^*, OP, G_0)$. *Пусть определены множества доверенных субъектов* L_S, *недоверенных субъектов* N_S *и запрещенных информационных потоков* N_f. *Тогда в результате применения в системе метода* 1 *для каждого информационного потока* $(x, y, write_t) \in N_f$, *где* x *и* y *— недоверенные субъекты, предикат* $can_write_time_block(x, y, G_0, L_S)$ *является ложным.*

Для анализа условий нарушения безопасности системы путем получения недоверенным субъектом права доступа владения к доверенному субъекту построена ДП-модель с функционально-ассоци-ированными с субъектами сущностями (или, сокращенно, ФАС ДП-модель). В ФАС ДП-модели к определенным в БК ДП-модели правилам преобразования состояний добавлено монотонное правило $control(x, y, z)$, позволяющее субъекту x, реализовавшему информационный поток по памяти к сущности z, функционально ассоциированной с субъектом y, получить к нему право доступа владения (рис. 5). При этом используем обозначение:

$[s] \subset E$ — множество всех сущностей, функционально ассоциированных с субъектом s.

В рамках ФАС ДП-модели сформулированы и обоснованы необходимые условия получения недоверенным субъектом права доступа владения к доверенному субъекту. При этом использованы определения.

Определение 8. Пусть $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ — состояние системы $\Sigma(G^*, OP)$ и недоверенный субъект $x \in N_S \cap S_0$, субъект $y \in S_0$, где $x \neq y$. Определим предикат $can_share_own(x, y, G_0, L_S)$, который будет истинным тогда, и только тогда, когда существуют состояния $G_1, \ldots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N)$ и правила преобразования состояний $op_1, \ldots, op_N$ такие, что траектория $G_0 \vdash_{op1} G_1 \vdash_{op2} \ldots \vdash_{opN} G_N$

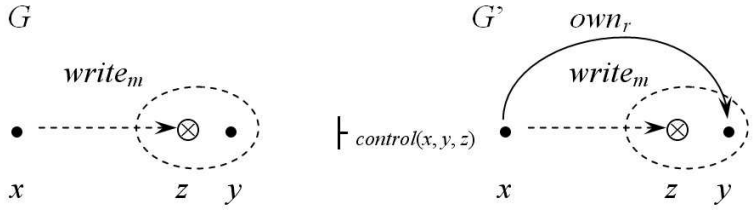


Рис. 5. Условия и результаты применения правила $control(x, y, z)$ ФАС ДП-модели

является траекторией без кооперации доверенных и недоверенных субъектов для передачи прав доступа и реализации информационных потоков, и $(x, y, own_r) \in R_N$, где $N \geqslant 0$.

Определение 9. Доверенный субъект y назовем функционально корректным, если во множество функционально ассоциированным с ним сущностей $[y]$ не входят недоверенные субъекты.

Определение 10. Доверенный субъект y назовем корректным относительно сущности e, не являющейся доверенным субъектом, если субъект y не реализует информационный поток по памяти от сущности e к сущности e', функционально ассоциированной с некоторым доверенным субъектом y'.

Теорема 3. *Пусть* $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ *— начальное состояние системы* $\Sigma(G^*, OP)$, *в котором* $A_0 = F_0 = \emptyset$, *и недоверенный субъект* $x \in N_S \cap S_0$, *доверенный субъект* $y \in L_S \cap S_0$. *Пусть истинен предикат* $can_share_own(x, y, G_0, L_S)$. *Тогда существуют недоверенный субъект* $x' \in N_S \cap S_0$, *доверенный субъект* $y' \in L_S \cap S_0$, *сущность* $e \in [y']$, *такие, что выполняется одно из условий*:

Условие 1. $x' = e$.

Условие 2. $(x', e, \alpha_r) \in R_0$, *где* $\alpha_r \in \{own_r, write_r, append_r\}$.

Условие 3. *Существует доверенный субъект* $y'' \in L_S \cap S_0$, *такой, что истинен предикат* $can_write_memory(y'', e, G_0, L_S)$, *и выполняется одно из условий*:

- *право доступа* $(y'', x', read_r) \in R_0$ *и субъект* y'' *некорректен относительно сущности* x';
- *право доступа* $(x', y'', \alpha_r) \in R_0$, *где* $\alpha_r \in \{write_r, append_r\}$;
- *существует сущность* $e' \in E_0$, *такая, что права доступа* (x', e', α_r), $(y'', e', read_r) \in R_0$, *где* $\alpha_r \in \{own_r, write_r, append_r\}$, *и субъект* y'' *некорректен относительно сущности* e'.

В рамках ФАС ДП-модели опишем метод предотвращения возможности получения права доступа владения недоверенным субъектом к доверенному субъекту с использованием реализации информационного потока по памяти к сущности, функционально ассоциированной с доверенным субъектом. Сокращенно, описание метода включает следующие шаги, определяющие действия в системе $\Sigma(G^*, OP)$, которые необходимо осуществить при применении метода.

Метод 2. *Условие применения метода.* Пусть определена система $\Sigma(G^*, OP, G_0)$ с начальным состоянием $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ и определены множества доверенных субъектов L_S и недоверенных субъектов N_S.

Шаг 1. Исключить из множества прав доступа R_0 права доступа владения недоверенных субъектов к доверенным субъектам.

Шаг 2. Рассмотрев реализацию каждого доверенного субъекта $y \in L_S \cap \cap S_0$, описать множество функционально ассоциированных с ним сущностей $[y]$.

Шаг 3. Для каждого доверенного субъекта $y \in L_S \cap S_0$ исключить недоверенные субъекты из множества функционально ассоциированных с ними сущностей $[y]$.

Шаг 4. Для каждого доверенного субъекта $y \in L_S \cap S_0$ рассмотреть множество функционально ассоциированных с ним сущностей $[y]$. При этом из множества прав доступа R_0 удалить права доступа own_r, $write_r$, $append_r$ недоверенных субъектов к сущностям из множества $[y]$.

Шаг 5. Для каждого доверенного субъекта $y \in L_S \cap S_0$ обеспечить его корректность относительно всех сущностей, информационный поток на запись к которым может реализовать хотя бы один недоверенный субъект.

С использованием ФАС ДП-модели разработаны ДП-модель для политики безопасного администрирования и ДП-модель для политики абсолютного разделения административных и пользовательских полномочий.

В КС с мандатным управлением доступом, как правило, анализируются условия возникновения запрещенных информационных потоков следующих видов.

Определение 11. Определим как запрещенные в КС с мандатным управлением доступом следующие четыре вида информационных потоков.

1. Информационные потоки по памяти и по времени между сущностями одного уровня конфиденциальности (определяются в соответствии с априорно заданной политикой управления доступом и информационными потоками).

2. Информационные потоки по памяти от сущностей с большим уровнем конфиденциальности к сущностям с меньшим уровнем конфиденциальности информации.
3. Информационные потоки по времени от сущностей с большим уровнем конфиденциальности к сущностям с меньшим уровнем конфиденциальности информации.
4. Информационные потоки по памяти от субъектов с низким уровнем доступа к субъектам с высоким уровнем доступа или к сущностям, функционально ассоциированным с субъектами с высоким уровнем доступа.

В известной автору литературе наименее исследованы условия реализации в КС запрещенных информационных потоков третьего и четвертого видов. В то же время результаты проведенных на практике экспериментов показали, что данные запрещенные информационные потоки представляют существенную угрозу безопасности КС$.

Для анализа запрещенных информационных потоков третьего и четвертого видов построим ДП-модель КС с мандатным управлением доступом (далее будем называть мандатной ДП-моделью). При этом дополнительно используем обозначения и определения:

$(L, \leqslant)$ — решетка линейно упорядоченных уровней доступа и конфиденциальности;

$f_s: S \to L$ — функция, определяющая уровень доступа каждого субъекта системы $\Sigma(G^*, OP)$;

$f_e: E \setminus S \to L$ — функция, определяющая уровень конфиденциальности каждой сущности системы, не являющейся субъектом;

$CCR: E \setminus S \to \{true, false\}$ — функция, определяющая способ доступа к сущностям, не являющимся субъектами, внутри контейнеров. Если сущность $e \in E$ является контейнером и доступ к сущностям, содержащимся внутри контейнера e, разрешен без учета уровня конфиденциальности контейнера e, то по определению выполняется равенство $CCR(e) = false$, в противном случае выполняется равенство $CCR(e) = true$.

$N_S(l) = \{s \in N_S: f_s(s) \leqslant l\}$ — множество недоверенных субъектов системы $\Sigma(G^*, OP)$ с уровнем доступа не большим l, где $l \in L$;

$L_S(l) = \{s \in L_S : f_s(s) \leqslant l\}$ — множество доверенных субъектов системы $\Sigma(G^*, OP)$ с уровнем доступа не большим l, где $l \in L$.

Определение 12. Пусть $G = (S, E, R \cup A \cup F, H, (f_s, f_e), CCR)$ — конечный помеченный ориентированный граф без петель, где назначение элементов графа S, E, R, A, F, H соответствует определению 3. При этом для каждой сущности $e \in E \setminus S$ определены значения функций $f_e(e)$, $CCR(e)$, для каждого субъекта $s \in S$ определено значение функции $f_s(s)$.

На траекториях функционирования системы $\Sigma(G^*, OP)$ не используются правила преобразования состояний, позволяющие субъектам брать, передавать и удалять права доступа к сущностям, удалять субъектов или сущности. При проверке возможности предоставления субъекту права доступа к сущности не учитывается содержимое множества прав доступа R.

Определение 13. В состоянии $G = (S, E, R \cup A \cup F, H, (f_s, f_e), CCR)$ системы $\Sigma(G^*, OP)$ доступ $(s, e, \alpha) \in A$, где субъект $s \in S$, сущность $e \in E \setminus S$, вид доступа $\alpha \in R_a$, обладает ss-свойством, если выполняются условия $f_s(s) \geqslant f_e(e)$ и для каждой сущности-контейнера $e' \in E \setminus S$, такой, что $e < e'$ и $CCR(e') = true$, выполняется неравенство $f_s(s) \geqslant f_e(e')$.

Определение 14. В состоянии $G = (S, E, R \cup A \cup F, H, (f_s, f_e), CCR)$ системы $\Sigma(G^*, OP)$ доступы $(s, e_1, read_a)$, $(s, e_2, \alpha) \in A$, где субъект $s \in S$, сущности $e_1, e_2 \in E \setminus S$, вид доступа $\alpha \in \{write_a, append_a\}$, обладают $*$-свойством, если выполняется условие $f_e(e_1) \leqslant f_e(e_2)$.

Определение 15. Состояние системы $\Sigma(G^*, OP)$ называется безопасным в смысле Белла—ЛаПадула, если все доступы состояния обладают ss-свойством и $*$-свойством. Система $\Sigma(G^*, OP)$ называется безопасной в смысле Белла—ЛаПадула, если все состояния системы на всех конечных траекториях ее функционирования безопасны в смысле Белла—ЛаПадула.

Правила преобразования состояний в мандатной ДП-модели определены с использованием БД ДП-модели и ФАС ДП-модели. В рамках мандатной ДП-модели возможно доказательство утверждения, аналогичного утверждению, доказываемому в базовой теореме безопасности модели Белла—ЛаПадула.

Приведем необходимые и достаточные условия, при выполнении которых в системе $\Sigma(G^*, OP)$ возможно повышение недоверенным субъектом своего уровня доступа.

Определение 16. Пусть в состоянии

$$G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0, (f_{s0}, f_{e0}), CCR_0)$$

системы $\Sigma(G^*, OP)$ недоверенный субъект $x \in N_S \cap S_0$. Определим предикат $can_increase_level(x, G_0)$, который будет истинным тогда, и только тогда, когда существуют состояния

$$G_1, \ldots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N, (f_{sN}, f_{eN}), CCR_N)$$

и правила преобразования состояний $op_1, \ldots, op_N$ такие, что траектория $G_0 \vdash_{op1} G_1 \vdash_{op2} \ldots \vdash_{opN} G_N$ является траекторией без кооперации субъектов из множества $S \setminus N_S(l)$ и субъектов из множества $N_S(l)$ для передачи прав доступа и реализации информационных потоков относительно уровня доступа l, и $f_{sN}(x) > l$, где $l = f_{s0}(x)$ и $N > 0$.

Теорема 4. *Пусть уровень доступа* $l \in L$ *и* $G_0 = (S_0, E_0, R_0 \cup \cup A_0 \cup F_0, H_0, (f_{s0}, f_{e0}), CCR_0)$ *— состояние системы* $\Sigma(G^*, OP)$, *которое безопасно в смысле Белла—ЛаПадула и в котором существует недоверенный субъект* $x \in N_S \cap S_0$, *и* $A_0 = F_0 = \emptyset$. *Предикат* $can_increase_level(x, G_0)$ *является истинным тогда, и только тогда, когда для* $l = f_{s0}(x)$ *существует субъект* $y \in S_0 \setminus N_S(l)$, *такой, что* $f_{s0}(y) > l$ *и выполняется одно из условий*:

Условие 1. *Субъект* y *функционально некорректен относительно субъекта* x.

Условие 2. *Существует субъект* $y' \in S_0$, *такой, что* $f_{s0}(y') > l$, *и субъект* y *некорректен относительно сущности* x *и субъекта* y'.

Условие 3. *Существует сущность* $e \in E_0$, *такая, что* $e \in [y]$, $f_{e0}(e) \leqslant l$, *и для каждой сущности-контейнера* $e' \in E_0$, *такой, что* $e < e'$ *и* $CCR_0(e') = true$, *выполняется неравенство* $f_{e0}(e') \leqslant l$.

Условие 4. *Существуют сущность* $e \in E_0$ *и субъект* $y' \in S_0$, *такие, что* $f_{e0}(e) \leqslant l$, $f_{s0}(y') > l$, *и для каждой сущности-контейнера* $e' \in E_0$, *такой, что* $e < e'$ *и* $CCR_0(e') = true$, *выполняется неравенство* $f_{e0}(e') \leqslant l$, *и субъект* y *некорректен относительно сущности* e *и субъекта* y'.

Таким образом, с использованием мандатной ДП-модели показано, что безопасности системы в смысле Белла—ЛаПадула недостаточно для предотвращения возможности реализации запрещенных информационных потоков по памяти четвертого вида. Из теоремы 4 следует, что для повышения субъектом своего уровня доступа необходимо наличие в системе либо некорректных субъектов с высоким уровнем доступа, либо наличие у субъектов с высоким уровнем доступа функционально ассоциированных с ними сущностей с низким уровнем конфиденциальности, доступ к которым может получить субъект с низким уровнем доступа. При этом при повышении субъектом своего уровня доступа используются запрещенные информационные потоки четвертого вида.

Рассмотрим с использованием БД ДП-модели условия реализации в системе $\Sigma(G^*, OP)$ мандатной ДП-модели запрещенных информационных потоков по времени третьего вида, для чего используем мандатную ДП-модель с блокирующими доступами доверенных субъектов (или, сокращенно, БДМ ДП-модель). На рис. 6 приведены примеры реализации с использованием доступов двух кооперирующих субъектов s_x и s_y запрещенного информационного потока по времени от сущности x с высоким уровнем конфиденциальности к сущности y с низким уровнем конфиденциальности.

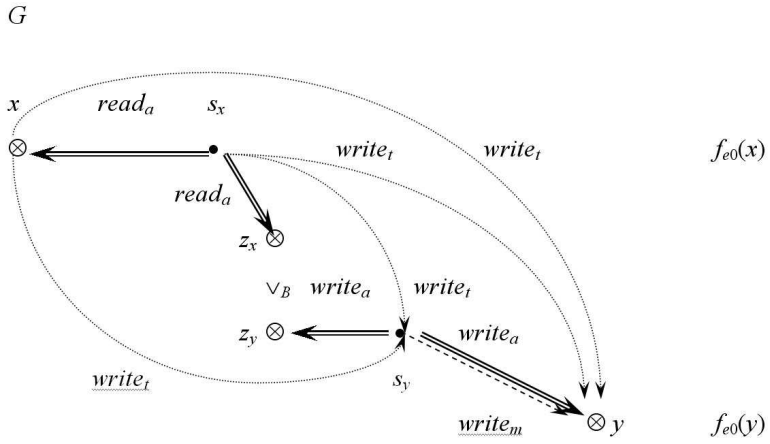


Рис. 6. Пример доступов и информационных потоков в БДМ ДП-модели

На основе мандатной ДП-модели строится мандатная ДП-модель с отождествлением порожденных субъектов (или, сокращенно, ОСМ ДП-модели), в которой все недоверенные субъекты имеют одного общего «предка» и при определении $*$-свойства рассматриваются доступы недоверенного субъекта вместе со всеми доступами порожденных им субъектов. При этом используем следующие определения.

Определение 17. В рамках ОСМ ДП-модели в каждом состоянии $G = (S, E, R \cup A \cup F, H, (f_s, f_e), CCR)$ системы $\Sigma(G^*, OP)$ разобьем множество субъектов S на непересекающиеся множества $s_1^*, s_2^*, \ldots, s_m^*$, такие, что для каждого $1 \leqslant i \leqslant m$ по определению выполняются условия:

- $s_i^* = \{s_i\}$, где $s_i \in L_S \cap S$;
- $s_i^* = \{s \in N_S \cap S : s \leqslant s_i\}$, и не существует недоверенного субъекта $s \in N_S \cap S$, такого, что выполняется условие $s_i < s$.

При этом по определению выполняется равенство $f_s(s_i^*) = f_s(s_i)$.

Определение 18. Для системы $\Sigma(G^*, OP)$ определим систему $\Sigma(G^*, OP^*)$, в которой правила преобразования состояний OP^* заданы в рамках мандатной ДП-модели и БДМ ДП-модели, при этом в каждом правиле если его параметром является субъект $x \in S$, то вместо него в условии применения правила используется класс s^*, такой, что $x \in s^*$.

Определение 19. Пусть $G = (S, E, R \cup A \cup F, H, (f_s, f_e), CCR)$ — состояние системы $\Sigma(G^*, OP^*)$ и недоверенные субъекты $s_1, s_2 \in N_S \cap S$, сущности $e_1, e_2 \in E \setminus S$, вид доступа $\alpha \in \{write_a, append_a\}$, такие, что

или $s_1 \leqslant s_2$, или $s_2 \leqslant s_1$. Доступы $(s_1, e_1, read_a)$, $(s_2, e_2, \alpha) \in A$ обладают $*$-свойством с отождествлением порожденных субъектов, если выполняется условие $f_e(e_1) \leqslant f_e(e_2)$.

Определение 20. Состояние системы $\Sigma(G^*, OP^*)$ обладает $*$-свойством с отождествлением порожденных субъектов, если в состоянии все доступы доверенных субъектом обладают $*$-свойством (по определению 14) и все доступы недоверенных субъектов обладают $*$-свойством с отождествлением порожденных субъектов (по определению 19).

В рамках ОСМ ДП-модели теоретически обосновано, что невозможна реализация запрещенных информационных потоков по времени третьего вида.

На основе мандатной ДП-модели строится ДП-модель для политики строгого мандатного управления доступом (или, сокращенно, ПСМ ДП-моделью). Реализация в системе $\Sigma(G^*, OP)$ строгого мандатного управления доступом позволяет обеспечить защиту от возникновения запрещенных информационных потоков по времени третьего вида.

Определение 21. В состоянии $G = (S, E, R \cup A \cup F, H, (f_s, f_e), CCR)$ системы $\Sigma(G^*, OP)$ доступы (s, e_1, α), $(s, e_2, \beta) \in A$, где субъект $s \in S$, сущности $e_1, e_2 \in E$, вид доступа $\alpha, \beta \in R_a$, безопасны в смысле политики строгого мандатного управления доступом, если выполняется условие $f_e(e_1) = f_e(e_2)$.

Определение 22. Состояние $G = (S, E, R \cup A \cup F, H, (f_s, f_e), CCR)$ системы $\Sigma(G^*, OP)$ безопасно в смысле политики строгого мандатного управления доступом, если все доступы состояния обладают ss-свойством (по определению 13) и все доступы доверенных субъектов обладают $*$-свойством (по определению 14), все доступы недоверенных субъектов безопасны в смысле политики строгого мандатного управления доступом. При этом ко всем сущностям-контейнерам реализованы блокирующие доступы доверенных субъектов, то есть выполняется условие $C \subset E_B$.

В рамках мандатной ДП-модели с использованием ОСМ ДП-модели и ПСМ ДП-модели опишем метод, позволяющий в системе $\Sigma(G^*, OP)$ предотвратить возможность реализации запрещенных информационных потоков по времени третьего вида. При этом используем обозначения:

$EC \subset E_0$ — множество компьютеров системы $\Sigma(G^*, OP)$;

$EC_1, EC_2, EC_3 \subset EC$ — попарно непересекающиеся множества компьютеров системы $\Sigma(G^*, OP)$ такие, что $EC_1 \cup EC_2 \cup EC_3 = EC$.

Сокращенно, описание метода включает следующие шаги, определяющие действия в системе $\Sigma(G^*, OP, G_0)$, которые необходимо осуществить при применении метода.

Метод 3. *Условие применения метода.* Пусть определена система $\Sigma(G^*, OP, G_0)$ с начальным состоянием

$$G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_{B0}, (f_{s0}, f_{e0}), CCR_0) \text{ и } A_0 = A_B, \quad F_0 = \emptyset.$$

Пусть также определены множества доверенных субъектов L_S и недоверенных субъектов N_S.

Шаг 1. Выделить в системе $\Sigma(G^*, OP, G_0)$ компьютеры EC_1, функциональность которых ограничена узким набором функций.

Шаг 2. Для компьютеров из EC_1 обеспечить доверенность всех активизируемых на них субъектов. Реализовать систему управления доступом системы таким образом, чтобы обеспечивалась безопасность в смысле Белла—ЛаПадула всех доступов доверенных субъектов.

Шаг 3. Выделить компьютеры EC_2, на каждом из которых должна быть обеспечена возможность активизации субъектов от имени только одного недоверенного субъекта-пользователя. Реализовать систему управления доступом системы $\Sigma(G^*, OP, G_0)$ таким образом, чтобы обеспечивалась безопасность доступов доверенных субъектов компьютеров из EC_2 в смысле Белла—ЛаПадула, доступов недоверенных субъектов, активизированных от имени субъектов-пользователей компьютеров из EC_2 в смысле Белла—ЛаПадула с отождествлением порожденных субъектов.

Шаг 4. Выделить компьютеры EC_3, на каждом из которых должна быть обеспечена возможность активизации субъектов несколькими недоверенными субъектами-пользователями. Реализовать систему управления доступом системы $\Sigma(G^*, OP, G_0)$ таким образом, чтобы обеспечивалась безопасность доступов доверенных субъектов компьютеров из EC_3 в смысле Белла—ЛаПадула, недоверенных субъектов-пользователей компьютеров из EC_3 в смысле строгого мандатного управления доступом.

Шаг 5. Реализовать всех доверенных субъектов системы $\Sigma(G^*, OP, G_0)$ таким образом, чтобы на всех траекториях функционирования системы доверенные субъекты не создавали недоверенных субъектов.

В заключение следует отметить, что построенные ДП-модели могут быть использованы для анализа безопасности управления доступом и информационными потоками не только в КС с дискреционным или мандатным управлением доступом. Например, после соответствующей модификации возможно применение построенных ДП-моделей для анализа безопасности информационных потоков в КС с ролевым управлением доступом.

Литература

[1] *Девянин П. Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006, 176 с.

[2] *Девянин П. Н.* Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Издательский центр «Академия», 2005, 144 с.

[3] *Щербаков А. Ю.* Введение в теорию и практику компьютерной безопасности. М.: издатель Молгачева С. В., 2001, 352 с.

[4] *Bell D. E.*, *LaPadula L. J.* Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976, MTR-2997, Rev. 1.

[5] *Bishop M.* Computer Security: art and science. ISBN 0-201-44099-7, 2002, 1084 p.

[6] *Lanawehrm E.*, *Heitmeyer L.*, *McLean J.* A Security Model for Military Message Systems. ACM Trans. On Computer Systems, vol. 9, no. 3, p. 198–222.

[7] *McLean J.* The Specification and Modeling of Computer Security. Computer, vol. 23, no. 1, 1990.

Оценка защищенности компьютерных сетей на основе анализа графов атак

И. В. Котенко, М. В. Степашкин

1. Введение

Проектировщики компьютерной сети и (или) системные администраторы (администраторы защиты) должны проводить анализ защищенности проектируемой или эксплуатируемой сети, т. е. проверять, насколько защищаемая система и планируемые для применения или уже используемые механизмы защиты информации и средства обеспечения безопасности, удовлетворяют принятой политике безопасности.

Проведение детального анализа защищенности является задачей, сложность которой постоянно возрастает в связи с усложнением компьютерных сетей, механизмов защиты (реализованных в межсетевых экранах, серверах аутентификации, системах разграничения доступа и т. п.), а также увеличением числа уязвимостей в программном и аппаратном обеспечении.

В связи с этим актуальной задачей в области защиты информации является *разработка новых подходов и эффективных программных средств для детального анализа защищенности компьютерных сетей на этапах проектирования и эксплуатации* [1].

Данная работа направлена на разработку такого подхода и создание *системы анализа защищенности* (*САЗ*), которые базируются на следующих базовых процедурах:

- автоматическая имитация действий злоумышленников на модели сети, соответствующей проектируемой или реальной защищаемой сети;
- автоматическое построение графов атак, отражающих возможные действия злоумышленников при использовании известных уязвимостей и ошибок в проектировании и реализации сети;

)Работа выполняется при финансовой поддержке РФФИ, программы фундаментальных исследований ОИТВС РАН (контракт № 3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза POSITIF (контракт IST-2002-002314) и RE-TRUST (контракт № 021186-2).

- автоматический или автоматизированный анализ защищенности компьютерной сети на основе использования построенного графа атак и разнообразных показателей (метрик) защищенности.

В отличие от других работ авторов [1, 5], в настоящей статье дается представление о полном перечне используемых моделей, рассматривается расширенный вариант системы анализа защищенности, и содержится анализ применимости подхода.

Работа структурирована следующим образом. *Второй раздел* содержит краткий обзор релевантных работ и описание сущности предлагаемого подхода к детальному анализу защищенности компьютерных сетей. В *третьем разделе* рассматривается архитектура и пользовательский интерфейс разработанной системы анализа защищенности компьютерных сетей. В *четвертом разделе* представлен пример одного из экспериментов по использованию данной системы при проектировании компьютерной сети. Анализ применимости подхода содержится в *пятом разделе*. В *шестом разделе* делаются выводы, и определяются направления будущих исследований.

2. Релевантные работы и сущность подхода

В настоящее время существует большое количество *исследований в области анализа защищенности*. В виду ограниченности объема статьи перечислим лишь несколько работ (более подробный анализ работ можно найти в [1]).

В исследовательских работах в области компьютерной безопасности используются различные способы представления действий злоумышленников при реализации сетевых атак:

- деревья атак [9],
- формальные грамматики,
- раскрашенные сети Петри,
- метод анализа изменения состояний,
- причинно-следственная модель атак,
- описательные модели сети и злоумышленников,
- структурированное описание на базе деревьев,
- использование и создание графов атак для анализа уязвимостей [10],
- объектно-ориентированное дискретное событийное моделирование,
- модели, основанные на знаниях и т. д.

В [11] излагаются возможные концептуальные методики анализа рисков для оценки степени защищенности компьютерных систем. В [8] пред-

лагается методика анализа графов атак, рассматривается использование метода верификации на модели, байесовского и вероятностного анализа, описывается генерация событий, возникающих при реализации атак, исследование их влияния на заданную спецификацию сети и отображение полученных результатов на сценарных графах. В [7] предлагается метод оценки защищенности на основе теории игр. В этой работе авторы рассматривают взаимодействие между злоумышленником и администратором как вероятностную игру с двумя игроками и предлагают модель данной игры.

Основное отличие предлагаемого в данной работе подхода от рассмотренных заключается в способе построения графа атак и использовании построенного графа атак для определения семейства различных показателей (метрик) защищенности, задействуемых для качественного анализа заданной конфигурации сети и реализуемой политики безопасности.

Система анализа защищенности (САЗ), использующая предложенный подход, предназначена для функционирования на различных этапах жизненного цикла компьютерной сети, включая этапы проектирования и эксплуатации. На этапе проектирования САЗ оперирует с моделью анализируемой компьютерной сети, которая базируется на заданной спецификации компьютерной сети и реализуемой политики безопасности. На этапе эксплуатации САЗ взаимодействует с реальной компьютерной сетью.

В результате анализа защищенности определяются уязвимости, строятся трассы (графы) возможных атак, выявляются «узкие места» в компьютерной сети, и вычисляются различные показатели защищенности, которые могут быть использованы для оценки общего уровня защищенности компьютерной сети (системы), а также уровня защищенности ее компонентов.

Граф атак отражает возможные распределенные сценарии атак с учетом конфигурации сети, реализуемой политики безопасности, а также местоположения, целей, уровня знаний и стратегий нарушителя. Показатели (метрики) защищенности позволяют оценивать защищенность компьютерной сети с различной степенью детализации и с учетом разнообразных аспектов.

Полученные результаты обеспечивают выработку обоснованных рекомендаций по устранению выявленных узких мест и усилению защищенности системы. На основе данных рекомендаций пользователь вносит изменения в конфигурацию реальной сети или в ее модель, а затем, если необходимо, повторяет процесс анализа уязвимостей и оценки уровня защищенности. Таким образом, обеспечивается требуемый уровень защищенности компьютерной сети (системы) на всех этапах ее жизненного цикла.

В предлагаемом подходе к анализу защищенности компьютерных сетей используются следующие формальные модели, построенные на основе экспертных знаний:

- модель компьютерных атак;
- модель нарушителя;
- модель формирования графа атак;
- модель компьютерной сети;
- модель оценки уровня защищенности.

Модель компьютерных атак служит для описания возможных действий нарушителя и формирования сценариев реализации этих действий [4]. Интегрированная модель атак имеет вид иерархической структуры, состоящей из моделей нескольких уровней:

- комплексного уровня;
- сценарного уровня;
- нижнего уровня (эксплоитов и команд).

Модель комплексного уровня определяет множество высокоуровневых целей, обеспечивая согласование нескольких сценариев, которые могут быть реализованы группой нарушителей.

Модель сценарного уровня определяет только одну высокоуровневую цель и уточняет подцели атаки.

Модель нижнего уровня в иерархии описывает низкоуровневые действия нарушителя, например, запуск программ реализации атак (эксплоитов), выполнение команд операционной системы (ОС) и т. п.

Модель нарушителя задается с помощью следующих параметров нарушителя:

- первоначальное положение (внутренние и внешние нарушители);
- уровень знаний и умений, определяющий возможности нарушителя по реализации атакующих действий (задается перечнем известных нарушителю уязвимостей, средств реализации атаки и т. п.);
- первичные знания об атакуемой компьютерной сети;
- используемый метод формирования сценария (используется ли оптимизация сценария для достижения заданной цели).

Модель формирования графа атак служит для построения графа, описывающего всевозможные варианты реализации атакующих действий нарушителем с учетом его первоначального положения, уровня знаний и умений, первоначальной конфигурации компьютерной сети и реализуемой в ней политики безопасности. Эта модель используется алгоритмом формирования общего графа атак (смотри ниже).

Модель анализируемой компьютерной сети служит для представления используемого в сети программного и аппаратного обеспечения, распознавания действий нарушителя и определения реакции сети на реализуемые нарушителем атакующие действия [4].

Модель оценки уровня защищенности охватывает систему различных показателей защищенности и правил (формул), используемых для их расчета на основе графа атак [1].

Все объекты графа атак можно подразделить на базовые объекты и составные. Вершины графа задаются с использованием базовых объектов. Для формирования различных последовательностей действий нарушителя базовые объекты связываются на графе атак с помощью дуг. Таким образом, формируются составные объекты графа. К базовым объектам общего графа атак относятся объекты, принадлежащие к типам «хост» и «атакующее действие». Множество объектов «хосты» включает все обнаруженные нарушителем и атакуемые им сетевые компьютеры (хосты). Множество объектов «атакующие действия» состоит из всех различимых элементарных действий нарушителя.

Атакующие действия разделены на следующие классы:

1) действия по получению информации о сети (хосте), т. е. разведывательные действия;
2) подготовительные действия (в рамках уже имеющихся у нарушителя полномочий), служащие для создания условий реализации атакующих действий последующих классов;
3) действия, направленные на нарушение конфиденциальности;
4) действия, направленные на нарушение целостности;
5) действия, направленные на нарушение доступности;
6) действия, приводящие к получению нарушителем прав локального пользователя;
7) действия, приводящие к получению нарушителем прав администратора.

Все атакующие действия можно разделить также на две группы:

1) действия, использующие различные уязвимости программного и аппаратного обеспечения, например, «NTP_LINUX_ROOT» (использует уязвимость в сервисе NTP ОС семейства Linux и позволяет нарушителю получить права администратора на атакуемом хосте);
2) обычные действия легитимного пользователя системы, например, «удаление файла».

К составным объектам отнесем объекты типов «трасса», «угроза» и «граф». Трасса атаки — это совокупность связанных вершин общего гра-

фа атак (хостов и атакующих действий), первая из которых представляет хост, соответствующий первоначальному положению нарушителя, а последняя не имеет исходящих дуг. Под угрозой будем понимать множество различных трасс атак, имеющих одинаковые начальную и конечную вершины.

Обобщенный алгоритм формирования общего графа атак основан на реализации следующей последовательности действий:

- действия по перемещению нарушителя с одного хоста на другой;
- разведывательные действия по определению «живых» хостов;
- действия разведки для каждого обнаруженного хоста;
- атакующие действия, использующие уязвимости программного и аппаратного обеспечения;
- общие действия пользователя.

На основе сформированного графа атак строится множество показателей защищенности. Данные показатели могут характеризовать защищенность как базовых, так и составных объектов графа атак. Показатели защищенности можно классифицировать по следующим признакам:

- по разделению объектов графа атак на базовые и составные;
- в соответствии с порядком вычислений;
- в соответствии с тем, используются ли показатели для определения общего уровня защищенности анализируемой компьютерной сети.

Примерами показателей защищенности являются:

- критичность хоста;
- размер ущерба при реализации угрозы;
- количество трасс атак на графе;
- сложность в доступе для атакующего действия, для трассы атаки, для всех трасс;
- степень возможности реализации угрозы;
- общий уровень защищенности и т. д.

Методика экспресс оценки общего уровня защищенности компьютерной сети состоит из следующих этапов [1]:

1) определение уровня критичности $Criticality(h)$ хостов h по трехуровневой шкале ($High$, $Medium$, Low);

2) определение критичности $Severity(a)$ атакующих действий a на основе алгоритма CVSS [3] получения обобщенной оценки критичности атакующего действия;

3) определение размера $Mortality(a, h)$ ущерба, вызванного успешной реализацией атакующего действия a, зависящего от уровней критичности действия и атакуемого хоста h;

4) определение размера $Mortality(T)$ ущерба для всех угроз:

$$Mortality(T) = Mortality(a_T, h_T)),$$

где a_T — последнее атакующее действие угрозы, направленное на хост h_T);

5) определение метрик сложности в доступе для всех атакующих действий ($AccessComplexity(a)$), для всех трасс ($AccessComplexity(S)$) с учетом значений данного показателя для всех действий, составляющих трассу, и всех угроз ($AccessComplexity(T)$) с учетом значений данного показателя для всех трасс, составляющих угрозу;

6) определение степени возможности реализации угрозы ($Realization(T)$) на основе показателя сложности в доступе;

7) определение общего уровня защищенности компьютерной сети ($SecurityLevel$) на базе полученных оценок степени реализации угрозы и размера ущерба, вызванного ее успешной реализацией.

3. Архитектура системы анализа защищенности

Для демонстрации предложенного подхода реализован программный прототип системы анализа защищенности [5].

Архитектура разработанной системы анализа защищенности (САЗ) компьютерных сетей приведена на рис. 1.

На этапе проектирования, САЗ оперирует с моделью анализируемой компьютерной сети (системы), которая базируется на заданных спецификациях анализируемой сети и политики безопасности.

На этапе эксплуатации для построения модели анализируемой сети используется подсистема сбора информации об анализируемой компьютерной сети.

Модуль интерфейса пользователя позволяет пользователю управлять работой всех компонентов системы, задавать входные данные, просматривать отчеты по анализу защищенности и т. п.

Хранилище данных состоит из следующих групп баз данных (БД):

- группа БД о конфигурации анализируемой компьютерной сети и используемой политике безопасности ($NetworkModel$);
- группа БД атакующих действий ($Attacks$).

Группа БД об анализируемой компьютерной сети состоит из следующих баз:

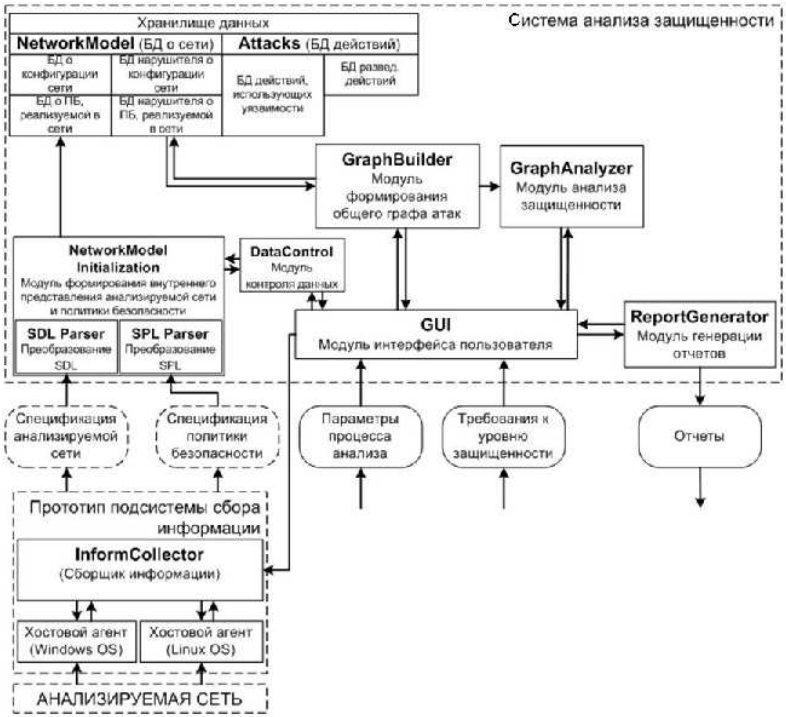


Рис. 1. Архитектура системы анализа защищенности

- БД о конфигурации сети;
- БД о политике безопасности (ПБ), реализуемой в сети;
- БД нарушителя о конфигурации сети;
- БД нарушителя о политике безопасности, реализуемой в сети.

Структурно данные базы данных попарно совпадают (базы о конфигурации сети и реализуемой в ней политике безопасности соответственно) и содержат информацию об архитектуре сети (например, типы и версии используемых операционных систем, приложений, список открытых портов и т. п.) и правил, описывающих функционирование сети.

БД о конфигурации сети является внутренним представлением спецификации анализируемой сети, которое используется для определения результатов выполнения атакующих действий во время построения общего графа атак.

БД нарушителя о конфигурации анализируемой сети является ее внутренним представлением (так, как ее представляет себе нарушитель).

Данное представление является результатом выполнения последовательности атакующих действий.

БД о политике безопасности, реализуемой в анализируемой сети, содержит общие правила, описывающие функционирование сети, например, «локальные пользователи хоста *H* не могут запускать приложение *A*». На основе *БД нарушителя о политике безопасности* возможно планирование последовательности выполняемых нарушителем действий (например, если согласно политике безопасности только локальные администраторы могут читать файл *F*, тогда нарушитель должен получить эти права, т. е. должен реализовать некоторую последовательность действий, направленных на получение прав администратора).

Группа баз данных атакующих действий состоит из следующих баз:

- БД действий, использующих уязвимости;
- БД разведывательных действий.

БД действий, использующих уязвимости (в отличие от других баз данной группы) строится на основе внешней базы данных уязвимостей.

БД разведывательных действий содержит действия, направленные на удаленное получение информации о хосте или сети. Описание разведывательных действий не содержится во внешних базах уязвимостей. Информацию о методах и средствах реализации нарушителем разведывательных действий можно получить лишь экспертным путем.

NetworkModel Initialization преобразует информацию о конфигурации сети и реализуемой в ней политике безопасности, задаваемых пользователем (эта информация задается при помощи специализированных языков System Description Language (SDL) и Security Policy Language (SPL)) во внутреннее представление.

DataControl используется для обнаружения некорректно заданных или отсутствия необходимых для процесса анализа защищенности данных. Например, пользователь может ввести ошибочное имя сервиса или указать, что порт 21 открыт, но не определить какое приложение обрабатывает поступающие на данный порт запросы.

GraphBuilder строит общий граф атак, эмулируя действия нарушителя в анализируемой компьютерной сети и используя информацию о доступных атакующих действиях различных типов (атакующие действия, использующие уязвимости, разведывательные действия, обычные действия легитимных пользователей), о конфигурации сети и реализуемой в ней политике безопасности. Данный модуль расставляет в вершинах графа метрики защищенности базовых объектов, на основе которых *GraphAnalyzer* рассчитывает метрики составных объектов.

ReportGenerator служит для агрегации полученных в процессе анализа защищенности данных (информации об обнаруженных уязвимостях, рекомендаций по повышению уровня защищенности) и формирования на их основе единого отчета.

Подсистема сбора информации служит для сбора информации от программных хостовых агентов и формирования на основе данной информации спецификаций, описывающих конфигурацию сети и реализуемую в ней политику безопасности.

Хостовые программные агенты используются для сбора необходимых для создания модели анализируемой компьютерной сети данных. Так, например, данные агенты могут реализовывать анализ конфигурационных файлов операционной системы и различных программных средств.

InformCollector служит для сбора информации, поступающей от хостовых агентов, ее представления на SDL и SPL и ее передачи компонентам САЗ (модулю *NetworkModel Initialization*).

4. Пример работы системы анализа защищенности

Рассмотрим пример работы системы анализа защищенности на тестовой компьютерной сети, структура которой представлена на рис. 2.

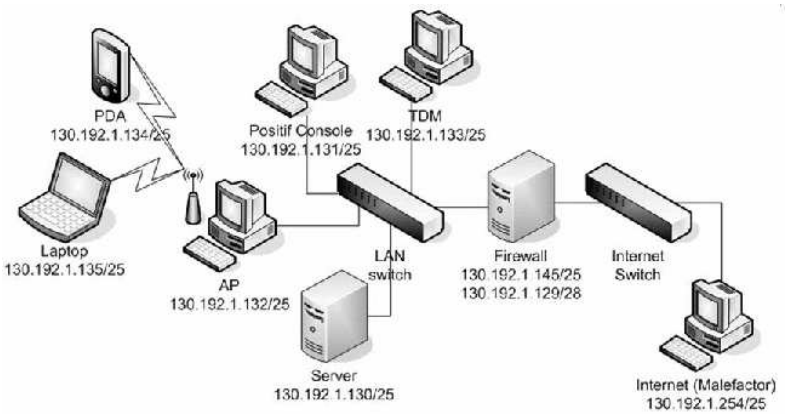


Рис. 2. Структура тестовой компьютерной сети

Во время построения общего графа атак автоматически выполняются следующие основные изменения в представлениях нарушителя об атакуемой сети (здесь рассмотрен фрагмент работы системы):

1) после реализации атаки «ping» (с учетом таблицы маршрутизации трафика) нарушитель узнает о существовании хоста «Server»;

2) нарушитель реализует атаку, использующую уязвимость в ftp-сервисе и позволяющую получить удаленному злоумышленнику права локального администратора;

3) нарушитель использует полученные права на хосте «Server» для сбора всей доступной информации, анализируя которую, злоумышленник понимает, что используется перенаправление портов (port forwarding), и хост «Server» подключен к другому сетевому концентратору. Следовательно, нарушителю выгодно перейти на хост «Server», так как такой переход открывает нарушителю доступ в другой сегмент сети;

4) перейдя на «Server», нарушитель реализует атаку «ping» и узнает о существовании множества других хостов, которые он последовательно пытается атаковать.

Общий граф атак для тестовой компьютерной сети представлен на рис. 3.

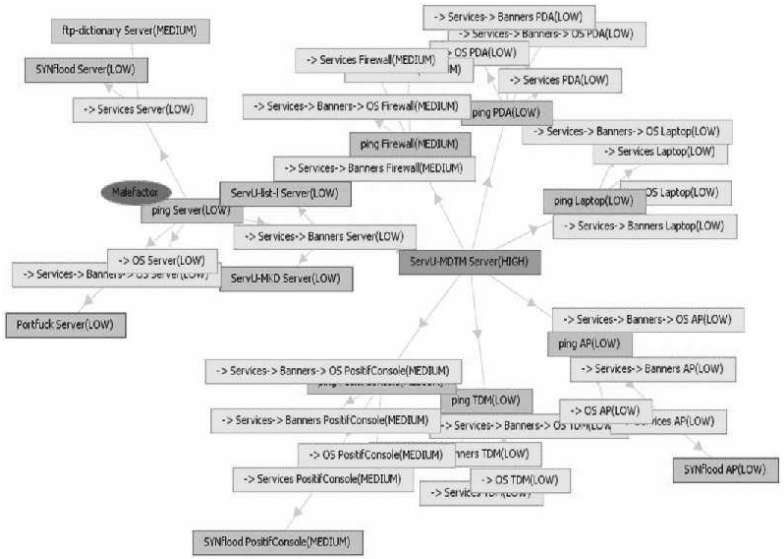


Рис. 3. Общий граф атак для тестовой компьютерной сети

Основными результатами процесса анализа защищенности в данном случае являются:

1) множество обнаруженных уязвимостей (например, уязвимость «ServU-MDTM»);

2) множество метрик защищенности (например, количество трасс атак, проходящих через хост «Server»).

В результате анализа защищенности для тестовой компьютерной сети был получен «красный» уровень защищенности (в предположении, что администратор задал четыре возможных уровня защищенности для компьютерной сети — «красный», «оранжевый», «желтый», «зеленый»; эти уровни перечислены здесь в порядке убывания критичности). Дальнейшими действиями пользователя должны стать:

1) устранение обнаруженных уязвимостей и «узких» мест (обновление конфигурации сети и реализуемой политики защищенности);
2) повторный анализ защищенности сети, заданной обновленными спецификациями.

5. Анализ применимости подхода

Предлагаемый подход обладает следующими особенностями:

- использование для анализа защищенности комплекса различных моделей, построенных на экспертных знаниях;
- учет разнообразия местоположения, целей и уровня знаний злоумышленника;
- использование при построении графа атак не только параметров конфигурации компьютерной сети, но и правил реализуемой политики безопасности;
- учет как собственно атакующих действий (по использованию уязвимостей), так и разрешенных действий пользователя и действий по разведке;
- возможность исследования различных угроз безопасности для различных ресурсов сети;
- возможность определения «узких мест» (хостов, ответственных за большее количество трасс атак и уязвимостей, имеющих наиболее высокую возможность компрометации);
- возможность задания запросов к системе вида «что если», например, какова будет защищенность при изменении определенного параметра конфигурации сети, правила политики безопасности;
- применение для построения графа атак актуализированных баз данных об уязвимостях (например, NVD [6]);
- использование для расчета части первичных показателей защищенности подхода CVSS [3];

- применение для вычисления показателей защищенности качественных методик анализа риска (в частности, модифицированной методики оценки серьезности сетевой атаки SANS/GIAC и методики FRAP [2]).

Эти особенности говорят в пользу применения данного подхода. Система анализа уязвимостей, основанная на применении данного подхода, позволяет *автоматически* определить уязвимости, возможные трассы атак, «узкие места» в компьютерной сети, важные для проектировщика или администратора безопасности показатели защищенности, в том числе общий уровень защищенности компьютерной сети.

Однако он не является панацеей и имеет ряд ограничений, поэтому для детального анализа защищенности должен применяться в комплексе с другими средствами анализа. В частности, он базируется на использовании для построения графа атак только известных уязвимостей (из актуализированных баз уязвимостей) и зависит от уровня детальности задания входных данных, т. е. спецификации компьютерной сети и политики безопасности.

Существенным ограничением для использования данного подхода в больших сетях является *вычислительная сложность алгоритмов формирования графа атак и анализа графа атак*.

Сложность алгоритма формирования графа атак определяется числом выполненных нарушителем действий. Данное число зависит, главным образом, от количества хостов в анализируемой сети N_H и количества используемых уязвимостей (эксплоитов) из внутренней базы данных уязвимостей N_V.

Рассмотрим компьютерную сеть, состоящую из n хостов, на каждом из которых существуют уязвимости, позволяющие нарушителю получить полный контроль над хостом и перейти на него для атаки других хостов.

На данной сети нарушитель во время сканирования хостов может в предельном случае обнаружить все n хостов и реализовать последовательно для каждого из них все доступные атакующие действия и переходы на захваченные хосты.

Поэтому сложность алгоритма формирования графа атак можно приближенно вычислить по следующей формуле:

$$\begin{aligned} F(N_H,\, N_V) &= N_H N_V F(N_H - 1,\, N_V) \\ &= N_H N_V (N_H - 1) N_V F(N_H - 2,\, N_V) = N_V^{N_H} N_H!. \end{aligned}$$

Сложность *алгоритма анализа графа атак* определяется сложностью алгоритма обхода графа атак в глубину и равна $O(V + E)$, где V — множество вершин графа атак; E — множество ребер графа атак.

Как видно из приведенных выше соображений, данный подход сталкивается с комбинаторным ростом сложности. Он может быть с успехом применен для небольших компьютерных сетей, но его нельзя использовать без соответствующей модификации для больших сетей.

Для уменьшения сложности в работе предлагается использовать следующие подходы:

1. Разбиение сети на фрагменты, *распараллеливание вычислений* для каждого фрагмента и последующее объединение решений.
2. Использование *агрегирования и абстрагирования представлений атакующих действий и* (*или*) *объектов сети*:
   - *По атакующим действиям*. Вид агрегирования или абстрагирования выбирается в соответствии с предложенной моделью атак. Примеры объектов агрегирования по атакующим действиям:
     - основные стадии реализации атак (разведка, первоначальное внедрение, повышение привилегий и др.),
     - класс атаки (переполнение буфера, отказ в обслуживании и т. д.),
     - подкласс атаки (например, конкретный вид переполнения буфера).

     Подход заключается в том, чтобы при построении графа атак можно объединять множество вершин, представляющих действия одного типа, в одну вершину (например, действия ping и «получение баннеров сетевых сервисов» в набор действий «разведка»).
   - *По объектам сети*. Агрегированными объектами сети могут являться объединение нескольких хостов сегмента, сегмент сети, объединение нескольких сегментов сети. Таким образом, анализируемая сеть может разбиваться на агрегированные объекты, каждый из которых представляется в виде одного объекта. Такой объект может характеризоваться множеством параметров, присущим всем его компонентам (хостам, сетевым концентраторам). В качестве элементов данного множества параметров могут выступать перечень типов операционных систем, используемых на хостах сегмента, перечень используемых сетевых сервисов и т. д. Упрощение графа атак в данном случае достигается за счет того, что вместо множества вершин, в которых целью атакующих действий будут выступать хосты, на графе будет отображено го-

раздо меньшее количество вершин, в которых целью атакующих действий выступают сегмент сети агрегированные объекты.
- *Комбинирование* различных подходов к использованию агрегирования и абстрагирования.

3. *Комбинирование распараллеливания, агрегирования и абстрагирования.*

6. Заключение

В работе предложен подход к анализу уязвимостей и оценке уровня защищенности компьютерных сетей, предназначенный для реализации на различных этапах жизненного цикла компьютерных сетей, основанный на генерации графов атак и вычислении показателей защищенности.

В работе рассмотрена архитектура разработанной системы анализа защищенности, представлены примеры экспериментов по использованию данной системы, дан анализ сложности алгоритмов формирования графа атак и предложены подходы для ее уменьшения.

Предлагаемый подход характеризуется использованием для анализа защищенности комплекса различных моделей, построенных на экспертных знаниях (компьютерных атак, нарушителя, формирования графа атак, компьютерной сети, оценки уровня защищенности), позволяет учитывать местоположение, цели и уровень знаний злоумышленников, основан на использовании не только параметров конфигурации компьютерной сети, но и правил реализуемой политики безопасности, дает возможность исследования различных угроз безопасности для различных ресурсов сети, позволяет определять «узкие места» в сети, т. е. хосты, ответственные за большее количество трасс атак и уязвимостей, имеющих наиболее высокую возможность компрометации, и базируется на применении актуализированных баз данных об уязвимостях.

Направлениями дальнейших исследований является совершенствование используемых в подходе моделей (компьютерных атак, оценки уровня защищенности, в частности системы показателей защищенности и правил их вычисления), развитие программного прототипа системы анализа защищенности и проведение дальнейшей экспериментальной оценки предложенных решений. В настоящее время авторами ведется разработка параметризованного по точности и вычислительной сложности комплекса различных алгоритмов формирования графа атак.

Литература

[1] Котенко И. В., Степашкин М. В. Метрики безопасности для оценки уровня защищенности компьютерных сетей на основе построения графов атак // Защита информации. INSIDE. № 3, 2006.

[2] FRAP. Facilitated Risk Analysis Process. `http://www.peltierassociates.com/`.

[3] CVSS. Common Vulnerability Scoring System. `http://www.first.org/cvss/`.

[4] Kotenko I. V., Stepashkin M. V. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science. Springer-Verlag, vol. 3685, 2005.

[5] Kotenko I. V., Stepashkin M. V. Analyzing Network Security using Malefactor Action Graphs // IJCSNS International Journal of Computer Science and Network Security, vol. 6, № 6, 2006.

[6] NVD. National Vulnerability Database. `http://nvd.nist.gov/`.

[7] Lye K., Wing J. Game Strategies in Network Security // International Journal of Information Security, February, 2005.

[8] Jha S., Sheyner O., Wing J. Minimization and reliability analysis of attack graphs // Technical Report CMU-CS-02-109. Carnegie Mellon University, 2002.

[9] Schneier B. Attack Trees // Dr. Dobb's Journal, 1999. Vol. 12.

[10] Iglun K., Kemmerer R. A., Porras P. A. State Transition Analysis: A Rule-Based Intrusion Detection System // IEEE Transactions on Software Engineering, 1995, vol. 21, № 3.

[11] Chapman C., Ward S. Project Risk Management: Processes, Techniques and Insights. Chichester, John Wiley, 2003.

Часть V

СЕМИНАР-КРУГЛЫЙ СТОЛ «БОРЬБА В СЕТИ: НАУЧНЫЕ, ПОЛИТИЧЕСКИЕ И ЮРИДИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРТЕРРОРИЗМУ»

Противостояние в Интернет: моделирование противодействия распределенным кибер-атакам

И. В. Котенко, А. В. Уланов

1. Введение

Актуальной угрозой безопасности Интернет являются *атаки «распределенный отказ в обслуживании»* (Distributed Denial of Service, DDoS). Они могут привести не только к выходу из строя отдельных хостов и служб, но и остановить работу корневых DNS-серверов и вызвать частичное или полное прекращение функционирования Интернета.

Эффективная защита от атак DDoS должна строиться на основе распределенной многокомпонентной системы, и включать механизмы предупреждения и обнаружения атаки, определения ее источников и противодействия. Очевидно, что чем большим количеством информации обладает система защиты, тем точнее можно обнаружить атаку. Однако из-за отсутствия в сети Интернет единого управления в большинстве случаев невозможно получить данные о трафике во всех указанных подсетях. Наиболее вероятная ситуация — сбор данных в промежуточной и (или) защищаемой сети, например, от своего поставщика услуг Интернет (ISP).

Важной задачей, требующей решения для создания интеллектуальных информационно-безопасных распределенных вычислительных систем, является задача формализации противодействия нарушителей и систем защиты в сети Интернет и, в частности, исследования атак DDoS и разработки эффективных средств защиты от них.

В работе рассматривается развитие изложенного в [1] подхода к многоагентному моделированию атак DDoS и защиты от них для исследования безопасности Интернет.

)Работа выполняется при финансовой поддержке РФФИ, программы фундаментальных исследований ОИТВС РАН (контракт 3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проекта Евросоюза POSITIF (контракт IST-2002-002314)и RE-TRUST (контракт 021186-2).

Используя разработанную среду моделирования, авторы исследуют различные способы противодействия атакам DDoS, представляя компоненты атаки и защиты в виде команд агентов.

Основное отличие результатов, изложенных в данной статье, от предыдущих работ [1, 2, 3] *заключается в следующем*:

- разработана модифицированная архитектура среды моделирования,
- реализована кооперация между различными командами агентов защиты, как компонентами систем защиты различных организаций и поставщиков услуг Интернет,
- проведены многочисленные эксперименты по исследованию различных способов кооперации команд агентов защиты и адаптации поведения команд для повышения эффективности защиты.

Работа построена следующим образом. Во *втором разделе* кратко описываются предлагаемый подход к моделированию и модели команд злоумышленников и команд защиты. В *третьем разделе* рассматривается разработанная система (среда) моделирования. В *четвертом разделе* представлены основные исследуемые параметры и допущения, принятые при моделировании. Примеры экспериментов описаны в *пятом разделе*. В *шестом разделе* делаются выводы, и определяются направления будущих исследований.

2. Модели команд злоумышленников и защиты

Формализуемые процессы представляются в виде взаимодействия различных команд программных агентов в динамической среде, задаваемой на основе модели сети Интернет [1]. Агрегированное поведение системы проявляется посредством локальных взаимодействий отдельных агентов. Предполагается, что агенты осуществляют сбор информации из различных источников, оперируют нечеткими знаниями, прогнозируют намерения и действия других агентов, пытаются обмануть агентов соперничающих команд, реагируют на действия других агентов.

При формализации данной задачи выделяются различные классы команд агентов: агенты-злоумышленники, агенты защиты и агенты-пользователи. Агенты различных команд могут находиться в отношении безразличия, сотрудничать или соперничать, вплоть до явного противоборства.

Агенты команд атаки подразделяются, по крайней мере, на два класса: «демоны», реализующие атаку, и «мастер», выполняющий действия по координации остальных компонентов системы. На предварительном этапе демоны и мастер устанавливаются на доступные узлы сети. Класс атаки задается следующим набором параметров: интенсивностью

посылки пакетов и способом подмены адреса отправителя в пакете («IP spoofing»): без подмены, постоянный, случайный, случайный с реальными адресами.

В соответствии с общим подходом к защите от DDoS атак, выделены следующие классы *агентов команд защиты*: обработки информации («сэмплеры»), обнаружения атаки («детекторы»); фильтрации («фильтры»); «агенты расследования». Сэмплеры осуществляют сбор сетевых данных для последующего обнаружения аномалий или злоупотреблений детектором. Фильтры ответственны за фильтрацию трафика атаки по правилам, предоставляемым детектором. Агент расследования пытается обезвредить агентов атаки. Команда агентов защиты совместно реализует определенный исследуемый механизм защиты. Команды агентов защиты могут *взаимодействовать по различным схемам*. В одной из них при обнаружении начала атаки действует детектор команды, на защищаемую сеть которой направлена атака (сети-жертвы). Он посылает запрос агентам-сэмплерам других команд с целью получения информации, которая может быть релевантной указанной атаке. Сэмплеры других команд отвечают на запрос, посылая необходимые данные. В случае обнаружения вероятного источника атаки детектор сети-жертвы посылает информацию об адресе агента атаки детектору команды, в сети которой может находиться этот агент, с целью его деактивации.

3. Система моделирования

Для реализации представленного подхода предполагалась разработка многоуровневой инструментальной среды, отличающейся от известных средств агентно-ориентированного моделирования (такие системы как: CORMAS, Repast, Swarm, MadKit, MASON, NetLogo и др.), в первую очередь, использованием в качестве базиса средств имитационного моделирования, позволяющих адекватно имитировать сетевые протоколы и процессы. Поэтому для реализации подхода используется архитектура системы моделирования, включающая базовую систему имитационного моделирования (Simulation Framework), модуль (пакет) моделирования сети Интернет (Internet Simulation Framework), подсистему агентно-ориентированного моделирования (Multi-agent Simulation Framework) и модуль (библиотеку) имитации процессов предметной области (Subject Domain Library).

Компонент Simulation Framework представляет систему моделирования на основе дискретных событий. Остальные компоненты являются надстройками или моделями для Simulation Framework.

Компонент Internet Simulation Framework — комплект модулей, позволяющих реалистично моделировать узлы и протоколы сети Интернет. Наивысший уровень абстракции в моделировании IP — это сеть, состоящая из IP-узлов. Узел может быть маршрутизатором или хостом. IP-узел отвечает компьютерному представлению стека протоколов Интернет. Предполагается, что модули, из которых он состоит, организованы так, как происходит обработка IP-дейтаграммы в операционных системах. Обязательным является модуль, отвечающий за сетевой уровень (реализующий обработку IP) и модуль «сетевой интерфейс». Дополнительно можно подключать модули, реализующие протоколы транспортного уровня.

Компонент Multi-agent Simulation Framework реализует многоагентное моделирование и использует модуль имитации процессов предметной области. Данный компонент представляет собой библиотеку модулей, задающих интеллектуальных агентов, реализованных в виде приложений. При проектировании и реализации модулей агентов подразумевается использование элементов абстрактной архитектуры FIPA. Для взаимодействия агентов реализован язык коммуникаций. Передача сообщений между ними происходит поверх TCP-протокола, реализованного в компоненте Internet Simulation Framework. Каталог агентов является обязательным только для агента, координирующего действия других. Агенты могут управлять другими модулями с помощью сообщений.

Компонент Subject Domain Library — это библиотека, служащая для имитации процессов предметной области, а также модули, дополняющие функциональность IP-узла: таблица фильтрации и анализатор пакетов.

С использованием OMNeT++ INET Framework и программных моделей, разработанных на C++, эта архитектура была реализована для многоагентного моделирования атак DDoS и механизмов защиты от них. INET Framework представляет собой пакет имитации протоколов и узлов Интернет. В нем детально реализованы основные протоколы, используемые при атаках DDoS (HTTP, TCP/IP, UDP), благодаря чему в моделируемых сетях идет обмен сетевыми пакетами, соответствующими реальным с точностью до флагов в их заголовках.

Также реализованы типовые узлы сети (клиенты, серверы, маршрутизаторы) и модели каналов связи (учитывающие пропускную способность и задержку распространения сигнала). Пакет позволяет моделировать поведение сети, состоящей из десятков тысяч узлов быстрее реального времени.

На рис. 1 представлена иерархия объектов пользовательского интерфейса (слева направо показаны вложенные объекты «сеть», «хост», «агент»). В процессе исследования можно переходить от одного уровня

иерархии представления объектов к другому и анализировать параметры функционирования различных объектов.

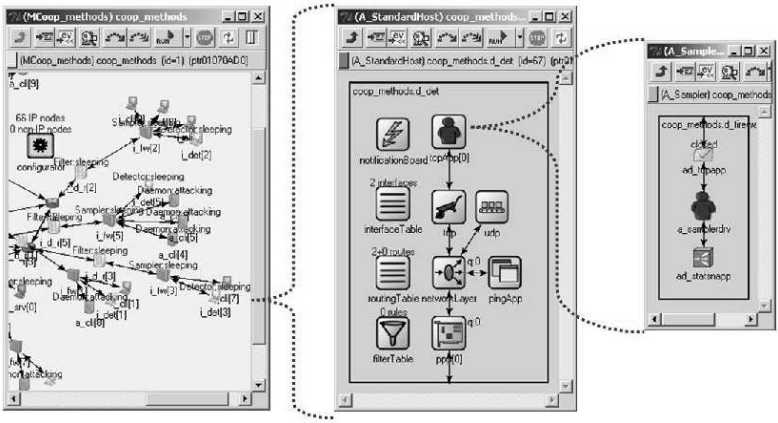


Рис. 1. Иерархия объектов пользовательского интерфейса

Существует возможность распараллеливания моделирования, благодаря чему отдельные части сети можно моделировать на разных компьютерах и, таким образом, увеличить размер модели. Данная возможность пока не реализована и является направлением дальнейших исследований. Модели агентов, реализованные в Multi-agent Simulation Framework, представлены типовым агентом, агентами атаки и агентами защиты. Subject Domain Library содержит различные модели узлов, например, атакующего, брандмауэра и др., а также модели приложений (механизмы реализации атак и защиты, анализаторы пакетов, таблицы фильтрации).

4. Основные параметры и допущения, принятые при моделировании

Созданная среда моделирования позволяет проводить различные эксперименты с целью исследования стратегий реализации атак и перспективных методов защиты.

В процессе экспериментов можно варьировать топологию и конфигурацию сети, структуру и конфигурацию команд атаки и защиты, механизмы реализации атак и защиты, параметры кооперации команд и др. На основе экспериментов проводятся измерения различных показателей эффективности механизмов защиты, и выполняется анализ условий и возможности их применения.

Сети, используемые для моделирования, состоят из различных подсетей, являющихся, например, зонами ответственности различных провайдеров. Выделяются подсеть защиты, где расположен ресурс, являющийся целью атаки, промежуточная подсеть, в которой находятся узлы, создающие типовой трафик, а также подсети атаки, где располагаются команды атаки.

Сети генерируются с помощью алгоритмов, позволяющих создавать конфигурации, близкие к сети Интернет. Использовалось допущение, что сеть состоит из маршрутизаторов, клиентских узлов, в том числе узлов с агентами и каналов связи.

Сеть строится как случайный граф в соответствии со степенным законом распределения вероятностей ранга узла (количества узлов, связанных с текущим). Были выбраны следующие параметры сети: минимальное количество соединений — 2; количество маршрутизаторов — 10; вероятностный параметр (степень) — 2,25.

Было использовано допущение, что в каждом домене имеется только один маршрутизатор и случайное количество клиентских хостов. Маршрутизаторы соединены между собой волоконно-оптическими каналами связи OC-48 с пропускной способностью 2.4 Гбит. Клиентские хосты используют канал связи Ethernet 100Mbit.

Для *защиты* могут использоваться различные методы, например, Hop counts Filtering (HCF), Source IP address monitoring (SIPM), Bit Per Second (BPS) и др. HCF заключается в применении сформированных в режиме обучения таблиц подсетей и количества скачков до них. В SIPM используется предположение, что во время атаки появляется большое количество новых адресов клиентов. BPS позволяет обнаружить атакующих по превышению порога нормального трафика.

Для команды атаки в процессе экспериментов варьируется интенсивность атаки в пакетах в секунду и способ подмены адреса отправителя. *Для команд защиты в процессе экспериментов варьируются* используемые методы защиты и параметр кооперации, задающий количество используемых в командах сэмплеров. Конфигурация сети изменялась с помощью задания различного количества легитимных клиентов.

Исследуются следующие *параметры эффективности механизмов защиты*: доля отброшенного легитимного трафика (false positive); доля пропущенного трафика атаки (false negative); время реакции на атаку.

5. Примеры экспериментов

Проведено большое количество разнообразных экспериментов. В одном из экспериментов исследовалась *эффективность различных меха-*

низмов защиты (HCF, SIPM и BPS) при использовании одной команды агентов защиты.

Эффективность механизмов защиты исследовалась в зависимости от следующих входных параметров: тип атаки: способ подмены адреса отправителя; время обучения; внутренние параметры методов; интенсивность атаки; конфигурация сети (количество легитимных клиентов).

В результате экспериментов оказалось, что интенсивность атаки и конфигурация сети не сильно влияют на характер исследуемых зависимостей. При уменьшении интенсивности атаки метод BPS перестает определять атаку, так как не может сопоставить большой трафик заданным адресам. Конфигурация сети, в том числе количество клиентов, влияет на время обучения методов. Это связано с тем, что методам необходимо обработать данные от как можно большего количества узлов.

Можно сказать, что метод BPS при малом времени обучения «закрывает» защищаемую систему и не пропускает ни легитимный трафик, ни трафик атаки. При длительном обучении метод пропускает большую часть легитимного трафика, но вместе с тем уязвим к методам случайной подмены адреса при атаке. Последнее связано с тем, что метод не может сопоставить большой трафик постоянно меняющемуся набору адресов. Оптимальное время обучения находится в районе 60 секунд. При этом количество ложных срабатываний около 10–20 %, а количество пропусков атак — от 15 до 40 % для разных видов атак.

Метод HCF работает (но показывает посредственные результаты, так как количество пропусков атак равно 75 %) при обучении средней продолжительности (составляющей около 50 секунд), но только для одного типа атаки — при атаке с методом подмены адреса на адрес из диапазона адресов, используемых в данной сети.

Метод SIPM достаточно хорошо работает при небольших временах обучения, но требует дополнительной настройки (порога новых IP-адресов и порога CUSUM). Чем меньше порог новых адресов, тем чувствительнее метод и тем больше ложных срабатываний. Оптимальное время обучения — около 25 секунд. При этом наблюдается меньше 10 % ложных срабатываний и от 15 до 30 % пропусков атак.

При оптимальных временах обучения меньший процент ложных срабатываний обеспечивает метод SIPM — меньше 10 %. Процент пропусков у BPS и SIPM находится примерно на одном уровне для разных видов подмены адреса при атаке (от 15 до 30 %).

В проведенных экспериментах время реакции всех методов, кроме HCF, составило около 40 секунд. Это время, в основном, требуется на обмен сообщениями между агентами сэмплером, детектором и фильтром и применение правил фильтрации. В методе HCF фильтрация возможна только

локально (на том же узле, где этот механизм защиты установлен). С этим связано очень малое время реакции на атаку с методом подмены адреса на адрес из диапазона адресов, используемых в данной сети.

Была исследована зависимость ложных срабатываний и пропусков атак от внутренних параметров метода SIPM (интервала сбора данных, сдвига интервала, порога для количества новых IP-адресов, порога для числа превышений). Найдены оптимальные значения этих параметров.

Проводились *эксперименты по исследованию различных схем кооперации команд защиты*. Эксперименты продемонстрировали, что использование кооперации нескольких команд защиты и комбинированное применение различных методов защиты приводит к существенному повышению эффективности защиты. Наилучшие результаты (наибольшее снижение трафика атаки, как на входе, так и в защищаемой подсети, наименьший трафик сообщений между агентами) наблюдались при кооперации команд защиты на уровне фильтров и полной кооперации.

Также проведены *эксперименты по исследованию адаптивного поведения команд защиты в кооперативных режимах* в зависимости от поведения команд атаки. Исследовалось применение различных схем адаптации на основе подхода, изложенного в [4]. Лучшей адаптивной схемой адаптации оказалась схема с кооперацией на уровне сэмплеров (рис. 2).

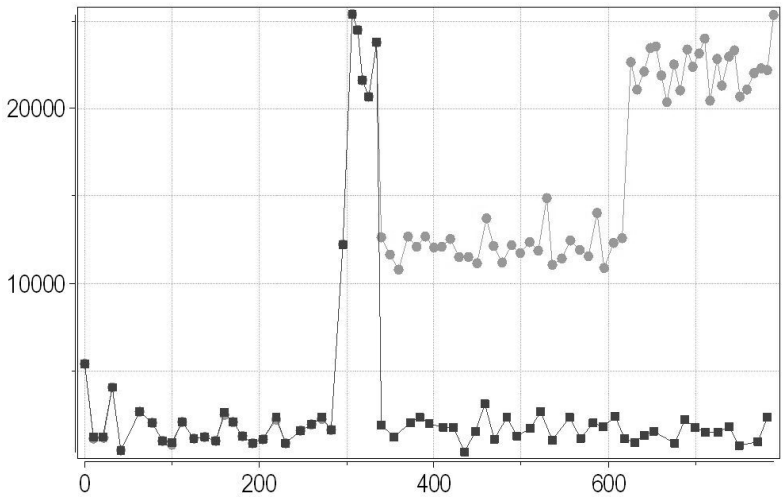


Рис. 2. Трафик на входе (серый) и внутри (черный) атакуемой подсети для адаптивной схемы с кооперацией на уровне сэмплеров в режиме защиты

Атака начиналась на отметке 300 секунд и осуществлялась без подмены адреса отправителя. Агенты защиты, пользуясь методом BPS, обнаруживали атаку и применяли правила фильтрации. После начала атаки для адаптивной схемы с кооперацией на уровне сэмплеров, команде защиты удалось фильтровать трафик атаки и обезвреживать некоторых демонов (рис. 2, 300–600 секунд).

При изменении метода атаки (атака осуществляется с подменой адреса на случайный) рос только трафик на входе в защищаемую подсеть (рис. 2, после 600 секунд). В этом случае команда защиты применяла метод SIPM. Внутри подсети трафик так и оставался на приемлемом уровне. Это связано с тем, что при обучении в режиме кооперации на уровне сэмплеров, команды защиты получали данные от сэмплеров других команд из других подсетей. Этих данных оказалось достаточно для метода SIPM, чтобы сразу блокировать атакующих, изменяющих свой адрес на случайный.

6. Заключение

В работе предложен подход к моделированию кибернетического противостояния в Интернет.

Подход реализован в разработанной среде моделирования, позволяющей моделировать атаки, направленные на нарушение доступности информационных ресурсов, и механизмы защиты от них.

Проведено большое количество экспериментов, в которых исследовались параметры эффективности механизмов защиты от топологии и конфигурации сети, структуры и конфигурации команд атаки и защиты, механизмов реализации атак и защиты и параметров кооперации команд защиты.

Эксперименты показали, что использование кооперации команд защиты приводит к существенному повышению эффективности защиты.

В дальнейшем планируется совершенствование среды моделирования, в частности, детальная реализация новых кооперативных механизмов защиты, более глубокое исследование эффективности механизмов кооперации различных команд и внутрикомандного взаимодействия агентов, реализация развитых механизмов адаптации и самообучения агентов.

Литература

[1] Котенко И. В., Уланов А. В. Программный полигон и эксперименты по исследованию противоборства агентов нападения и защиты в сети Интернет // Математика и безопасность информационных технологий. Материалы конференции МаБИТ-05 в МГУ. М.: МЦНМО, 2005.

[2] Kotenko I., Ulanov A. Simulation of Internet DDoS Attacks and Defense // 9th Information Security Conference. ISC 2006. Proceedings. Lecture Notes in Computer Science, vol. 4176, 2006.

[3] Kotenko I., Ulanov A. Agent Teams in Cyberspace: Security Guards in the Global Internet // International Conference on CYBERWORLDS. CW2006. Proceedings. IEEE Computer Society, 2006.

[4] Zou C. C., Duffield N., Towsley D., Gong W. Adaptive Defense Against Various Network Attacks // SRUTI: Steps to Reducing Unwanted Traffic on the Internet. Boston, 2005.

Концептуальные положения обеспечения информационной безопасности объектов национальной информационно-телекоммуникационной инфраструктуры

В. А. Васенин, М. В. Большаков, В. Б. Савкин

Введение

Данная статья посвящена описанию концептуальных положений обеспечения информационной безопасности, которые с необходимостью должны приниматься во внимание при проектировании и в процессе функционирования объектов национальной информационно-телекоммуникационной инфраструктуры (НИТИ), обеспечивающих управление критически важными объектами (КВО). Далее будет использоваться понятийный аппарат для анализа объектов, который подробно описан в работе [2]. В частности, под КВОИ далее будут пониматься объекты НИТИ, обеспечивающие управление КВО.

Необходимость обеспечения информационной безопасности критически важных объектов не вызывает сомнения. Однако, существует конфликт между интересами организаций, владеющих и управляющих ресурсами КВО и интересами обеспечения государственной безопасности. Например, внедрение дополнительных механизмов защиты приводит к существенному удорожанию инфраструктуры поддержки функционирования объекта и увеличению затрат как на ее создание, так и на обеспечение ее эффективной работы. По этой причине, с точки зрения государства следует найти компромисс между уровнем защищенности КВОИ [1)] и затратами, необходимыми для ее обеспечения. Приоритет национальных интересов в некоторых случаях приводит к необходимости финансирования работ по

[1)] Под уровнем защищенности КВОИ будем понимать степень соответствия средств его защиты от деструктивных информационных воздействий требованиям по безопасности, которые формируются на основе заранее принятых принципов,особенностей объекта защиты и положений регламентирующих документов.

созданию и эксплуатации дополнительных средств обеспечения безопасности КВО.

Таким образом, форма и содержание, а также применяемые способы и методы обеспечения информационной безопасности в значительной степени зависят от характеристик конкретного защищаемого объекта, в частности от степени критичности [2)] объекта ([3]). Однако, их применение должно опираться на концептуальные положения и базовые наборы требований по организации работ по созданию и обеспечению безопасности информационных технологий (БИТ), используемых в объектах НИТИ, в том числе, закрепленных международными стандартами.

1. Базовые положения и цели обеспечения информационной безопасности критически важных объектов НИТИ

Анализ существующих стандартов и тенденций в области обеспечения безопасности сложных систем позволяет выявить, что понятие безопасности КВО [3)], с позиций государства близко понятию «функциональная безопасность» введенным в стандарте ISO/IEC 61508:1-6.

Понятие функциональной безопасности в основе своей предполагает обеспечение безопасности объектов различных типов от непредумышленных, случайных деструктивных воздействий при отсутствии злоумышленного влияния на систему [5]. В современных комплексах, содержащих информационно-вычислительные и телекоммуникационные ресурсы, обеспечение перманентно усложняющейся функциональности объекта (целей, задач, способов и регламентов их решения) ложится на систему автоматизации управления объектом. Такие системы включают различные активы, которые могут быть подвержены деструктивным информационным воздействиям. В их числе информационные ресурсы, в виде данных, обрабатываемых и передаваемых с помощью сетей связи, современные информационно-вычислительные и телекоммуникационные технологии, а также инструментальные средства и оборудование, которые их поддерживают. Однако,

[2)] Степень критичности здесь и далее понимается в смысле уровня ущерба, то есть потерь материально-технического, политического, социального характера или других, которые возникают в случае деградации (частичной или полной) отдельных элементов или системы управления КВО в целом, произошедшей вследствие деструктивного информационного воздействия на систему управления объектом.

[3)] Здесь и далее в настоящей работе речь идет об информационной безопасности, а точнее, о безопасности информационных технологий, используемых в составе информационно-вычислительно-телекоммуникационных системам управления критически важными объектами, которая далее для краткости именуется «безопасностью».

основным ресурсом, который лежит в основе всех процессов, протекающих в подобного рода системах является информация. На сегодняшний день большинство сложных систем управления технологическими процессами реализуется с помощью электронно-вычислительных машин (ЭВМ) различной сложности, объединенных сетевыми структурами, с использованием программных средств, реализующих алгоритмы управления, в том числе — баз данных, которые обеспечивают информационную поддержку программных средств прикладного уровня. При этом режимы функционирования систем управления такого сорта практически значимыми объектами, как правило, налагаются «жесткие» ограничения на используемые ресурсы, время отклика, корректность реализации и целый ряд других параметров. Выход из строя или работа компьютерной системы управления технологическим процессом в нештатном режиме с большой вероятностью приводит к значительному ущербу, в том числе, связанному с гибелью людей, чрезвычайными ситуациями. На подобные системы в первую очередь ориентированы стандарты и средства обеспечения функциональной безопасности. Область анализа состояния функциональной безопасности в работе систем имеет дело с ситуациями отказов и потерей работоспособности систем по причине, обусловленной действием непредумышленных факторов, случайных дефектов, и, как следствие, деградацией или потерей функциональности программного обеспечения, аппаратуры, а также с рядом других обстоятельств [5].

Вместе с этим, необходимо отметить, что безопасность компьютерных систем в большей мере связана с «информационной безопасностью», рассматривающее ситуации, при которых деструктивное воздействие, как правило, предполагается умышленным. Значительный рост производительности вычислительных процессоров и объемов запоминающих устройств обеспечил возможность создания компьютерных систем для оперативной обработки, анализа, систематизации и хранения больших объемов данных. Такие системы получили широкое применение в информационно-вычислительных комплексах, управляющих объектами в различных сферах национально-хозяйственного комплекса. Основной целью такого типа систем является обеспечение пользователя удобным инструментом поддержки принятия решений через доверенное хранение, накопление, быстрый поиск и обработку информации. В рамках данных систем пользователю необходимо иметь полный контроль над информацией. По этой причине, в первую очередь, выдвигаются требования к обеспечению целостности, конфиденциальности и доступности информации для администрирующего персонала и авторизованных пользователей системы. Обеспечение защищенного использования информации в системах такого сорта основано на принципах, которые декларирует сфера информационной безопасности.

Область анализа информационной безопасности в большей степени связана с защитой от предумышленных деструктивных воздействий на ресурсы подобных систем.

Для каждого из упомянутых выше аспектов обеспечения безопасности существует класс критически важных объектов, в котором задача обеспечения соответствующего типа безопасности или их комбинации является определяющей. В ряде случаев понятия функциональной и информационной безопасности близки и неразрывно связаны друг с другом. Однако, и это необходимо отметить, они имеют существенные различия в методах и способах, которые применяются для их обеспечения.

При анализе защищенности КВО понятия функциональной и информационной безопасности часто становятся неотделимы и отражают разные аспекты функционирования системы. Полная картина угроз и рисков реализации деструктивных информационных воздействий может быть достигнута только в результате анализа обоих аспектов обеспечения безопасности КВО в их взаимосвязи. Необходимо следовать комплексному подходу, который заключается в использовании традиционных методов обеспечения информационной безопасности, однако в сочетании с более глубокими методами анализа функциональных свойств и состояния системы. Строгая и полная идентификация и оценка угроз позволит обосновать необходимость применения конкретных методов обеспечения функциональной и информационной безопасности КВО на различных этапах жизненного цикла системы.

Меры по обеспечению информационной безопасности КВО направлены на достижение и поддержание необходимого (заранее определенного) уровня функциональной и информационной безопасности КВО путем защиты его информационно-телекоммуникационной составляющей, которая осуществляет управление объектом.

2. Основные задачи обеспечения информационной безопасности КВО

Основной целью обеспечения информационной безопасности КВО является организация эффективного противодействия реализации угроз информационной и функциональной безопасности КВО. Она достигается путем решения следующей задачи.

Необходимо осуществить разработку и документальное оформление требований по безопасному использованию активов подлежащего защите объекта. Решение этой задачи основывается на применении последова-

тельности следующих процедур на этапах разработки, эксплуатации и модернизации объекта:

- разработка моделей обеспечения информационной безопасности КВО на основе анализа уязвимостей, угроз и оценки рисков их реализации;
- формирования требований к обеспечению безопасности;
- создания адекватных способов и методов защиты от различных проявлений угроз при заданных требованиях безопасности.

На каждом из отмеченных выше этапов жизненного цикла перечисленные процедуры призваны уточнить состав и функциональность системы, выбрать адекватные методы нейтрализации потенциальных угроз. Проведение данных процедур на этапе эксплуатации объекта позволяет оценить эффективность применяемых механизмов защиты, необходимость их пересмотра или введения новых, дополнительных мер обеспечения безопасности объекта. Традиционно данную задачу решают посредством процедуры управления рисками. С точки зрения государства необходимо налагать требования на методику проведения оценки и снижения рисков деструктивных информационных воздействий на КВО, а также на перечень рассматриваемых рисков в зависимости от структуры и исполняемых КВО функций.

Информация о структуре и исполняемых объектом функциях может быть использована при проведении идентификации, кластеризации и категоризации КВО, по методике изложенной в [3]. Анализ позволяет определить категорию значимости или степень критичности объекта, положение в дереве критических инфраструктур, выделить общие требования к обеспечению информационной безопасности, методы и средства по поддержанию работы объекта в штатном режиме.

Отдельно выделим задачу поиска и реализации мер, позволяющих организовать и осуществить контроль и поддержку соответствия реальной системы методам и средствам, полученным в результате решения первой задачи. Решение данной задачи призвано обеспечить защиту объекта от угроз неисполнения или неэффективности принятых мер обеспечения информационной безопасности объекта и связанных с ними рисками деструктивных информационных воздействий.

3. Комплексный подход к обеспечению информационной безопасности КВО

Решение задач обеспечения безопасности КВО должно проводиться на основе использования комплексного подхода, предполагающего сочетание

мер законодательного, организационно-административного, процедурного и программно-технического уровней.

Законодательный уровень обеспечения информационной безопасности КВО включает в себя перечень законодательных актов, стандартов и другие нормативные документы, регламентирующие вопросы защиты объекта от деструктивных кибервоздействий, а также способы их толкования и применения, к конкретному объекту.

Основой мер организационно-административного уровня, то есть мер, предпринимаемых руководством организации, является политика безопасности. Под политикой безопасности на верхнем уровне ее формирования понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов (активов), которая на нижележащих уровнях ее реализации трансформируется в систему мер и способов предоставления этих активов, механизмов и средств их реализации, обеспечивающих защиту от деструктивных информационных воздействий.

К процедурному уровню относятся меры безопасности, осуществляемые персоналом, призванным поддерживать положения политики безопасности объекта защиты. Выделяются следующие традиционные ([1]) группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Меры программно-технического уровня направлены на контроль защищенности компьютерных активов — оборудования, программ и данных. Такой контроль достигается использованием средств и систем защиты активов для реализации требований по безопасности в рамках подсистем управления доступом, регистрации и учета событий, контроля целостности и других программно-технических сервисов.

На законодательном уровне решаются следующие задачи:

- определение положений законодательных актов и нормативных документов федерального и отраслевого уровня, регламентирующих международных и отечественных стандартов применение которых необходимо для проектирования и реализации комплекса мер и средств обеспечения информационной безопасности КВО;

- определение на основе нормативных документов и регламентирующих стандартов набора требований к подсистеме информационной безопасности и ее компонентам, включая требования по категорированию информации.

На административном уровне осуществляется решение следующих задач:

- ведение реестра ресурсов подлежащих защите, включая тех, которые содержат информацию ограниченного распространения;
- определение набора сервисов, позволяющих обеспечивать доступ пользователей к информационным ресурсам КВО; выработка типовых профилей пользователей КВОИ, ведение реестра таких профилей;
- разработку политики информационной безопасности КВО, как набора административно-управленческих процедур, правил и способов безопасного с позиций деструктивных информационных воздействий использования его ресурсов.

К числу задач на процедурном уровне реализации информационной безопасности КВО относятся следующие:

- выбор эффективных с позиции обеспечения информационной безопасности объекта процедур управления и контроля за возможными действиями персонала;
- решение вопросов физической защиты компонентов информационной системы, как на основе существующих решений, так и с возможностью их модификации;
- формирование и реализация перечня мероприятий, выполняемых персоналом и направленных на поддержание работоспособности информационных систем, в первую очередь, система мониторинга состояния функциональности (работоспособности) основных информационно-телекоммуникационных компонентов объекта защиты;
- формирование, утверждение и реализация плана реагирования персонала на нарушения режима информационной безопасности;
- формирование плана восстановительных работ.

Как результат решения перечисленных задач должны быть разработаны регламенты, процедуры и планы мероприятий по организации режима обеспечения информационной безопасности КВО.

На программно-техническом уровне обеспечения информационной безопасности КВО поддерживается решение следующих задач:

- обеспечение архитектурной безопасности решений, связанных с хранением, обработкой и передачей информации ограниченного распространения;
- обеспечение непротиворечивости и полноты механизмов безопасности (решение задачи достигается проектированием системы обеспечения информационной безопасности КВОИ и встроенных механизмов безопасности в соответствии с нормами отечественных и международных стандартов, с использованием анализа рисков создаваемой системы);
- выработка и реализация[4)] проектных решений по сервисам идентификации и аутентификации пользователей в КВОИ;
- выработка и реализация проектных решений по сервисам разграничения доступа в КВОИ;
- выработка и реализация проектных решений по сервисам мониторинга и аудита деятельности пользователей и администраторов в КВОИ;
- выработка и реализация проектных решений по сервисам контроля защищенности и контроля целостности;
- выработка и реализация проектных решений по сервисам криптографической защиты информации КВОИ;
- выработка и реализация проектных решений по сервисам информационного и межсетевого экранирования;
- выработка и реализация проектных решений по сервисам обеспечения отказоустойчивости и обеспечения безопасного восстановления;
- выработка и реализация проектных решений по сервисам управления режимами работы и конфигурацией КВОИ.

Решение указанных задач необходимо проводить с учетом стадий жизненного цикла КВО, как автоматизированной системы (АС) (ГОСТ 34.601-90, ГОСТ Р 51583-2000) и рекомендаций международных стандартов ISO/IEC 13335, ISO/IEC 15408, ISO/IEC 17799, рассматривая систему обеспечения информационной безопасности КВОИ как составной элемент КВО. Далее более подробно остановимся на содержании мер на административном уровне обеспечения информационной безопасности КВОИ.

3.1. Меры обеспечения информационной безопасности КВО на административном уровне

Одним из самых важных в плане обеспечения надлежащего уровня информационной безопасности КВОИ и, вместе с тем, самым сложным для практической реализации, контроля и регулирования является ее ад-

[4)] Под реализацией здесь понимается создание программной и/или аппаратно-программной компоненты.

министративный уровень. Формирование программы работ в области информационной безопасности в комплексе с мерами, обеспечивающими их исполнение созданной программой, является главной целью реализации мер административного уровня противодействия информационным угрозам деструктивного характера. Исполнение планируемых программой мер достигается путем регламентированного выделения необходимых для этого ресурсов и всестороннего контроля их исполнения.

Основой программы является политика информационной безопасности[5)] объекта защиты, отражающая используемые подходы владеющей объектом или эксплуатирующей его организации к защите информационных активов объекта от деструктивных кибервоздействий, а также методы, применяемые для создания самой политики безопасности. Под политикой информационной безопасности на верхнем уровне её формирования понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов, активов КВО.

Организационно, КВОИ представляет собой сложную структуру отдельных административных единиц, назовем их предприятиями, на основе скоординированных действий которых обеспечивается разработка и поддержка КВО в работоспособном состоянии. Каждое такое предприятие, как правило, представляет совокупность объектов недвижимости, оборудования и инструментальных (включая программно-технические) средств и организаций, обслуживающих их с целью поддержания штатных режимов работы КВОИ и,соответственно, КВО. Перечень таких организаций может включать в себя: телекоммуникационные компании, обеспечивающие каналы передачи данных; компании, осуществляющие системную интеграцию и поддержку установленного программного обеспечения; организации, осуществляющие поставку и ремонт средств вычислительной техники, реализующих функциональность КВОИ, и подобные им хозяйствующие структуры, вообще говоря различных форм собственности. Каждая из организаций, участвующая в процессе поддержки функционирования КВОИ может иметь собственную политику информационной безопасности. Объединение этих политик должно быть непротиворечивым и взаимодополняющим, что позволяет представить совокупность политик в виде единой, общей политики КВОИ. Такая общая политика информационной безопасности КВОИ может быть сформирована как изначально на основе политик составляющих его объектов и эксплуатирующих их организаций,так формироваться в «режиме последействия» как объединяющая (интегрирующая) их поли-

[5)] Для краткости далее, когда это ясно по контексту изложения, политику информационной безопасности будем называть политикой безопасности.

тика. Далее, под политикой информационной безопасности КВОИ будем понимать вышеописанную объединенную политику, а под организацией — виртуальную организацию, структурно представляющую собой объединение организаций, осуществляющих создание и поддержку функционирования отдельных объектов в составе КВОИ на основе договорных отношений. Основные положения единой политики и мероприятия по контролю ее исполнения должны планироваться и проводиться отдельной организацией, осуществляющей стратегическое управление деятельностью всех взаимодействующих организаций, которые обеспечивают поддержку функционирования КВОИ.

Первым и одним из самых важных шагов в процессе разработки положений политики безопасности КВОИ является создание документа, отражающего концептуальные положения обеспечения информационной безопасности, который в самой общей трактовке можно назвать «Концепцией обеспечения информационной безопасности». Концепция создается на основе всестороннего анализа функций и свойств объекта управления на предмет возможных методов их реализации и возникающих для объекта угроз деструктивных информационных воздействий. Для этого необходимо исследовать вопрос применимости существующих подходов и технологий их реализующих, а также проанализировать возможные способы и средства обеспечения информационной безопасности на основе этих технологий на предмет целесообразности и эффективности их применения.

Концепция раскрывает стратегические положения обеспечения информационной безопасности на всех этапах жизненного цикла КВОИ, фиксирует набор архитектурных и структурных решений используемых для создания КВОИ, а также регламентирует общие подходы к формированию мер обеспечения информационной безопасности. На законодательном уровне концепция отображает отношение к положениям отдельных законодательных актов, к нормативно-регламентирующим документам и стандартам, оказывающим влияние на информационную безопасность КВО. Она фиксирует методологию их использования для поддержки процессов создания и безопасного функционирования КВО. На административном уровне концепция описывает подходы и методы, используемые для разработки политики безопасности КВОИ, отражающие состав и основные положения включенных в нее документов. На процедурном уровне выделяются обязательные к исполнению пользователями и администрирующим персоналом меры общего характера обеспечения информационной безопасности КВО. На программно-техническом уровне концепция фиксирует архитектуру используемых программно-технических средств, а также структуру создаваемого комплекса.

Изменение Концепции с необходимостью влечет за собой пересмотр и изменение выработанного комплекса мер по защите КВО от деструктивных информационных воздействий, в частности, — политики безопасности КВОИ, процедурных и программно-технических мер, противоречащих изменениям в Концепции. Концепция должна включать декларацию о необходимости перманентного уточнение базовых положений и целей, задач и принципов, используемые для поддержания информационной безопасности КВО.

Концепция информационной безопасности также должна содержать необходимый анализ функциональной безопасности КВОИ, выделять основные угрозы и методы противодействия им. Такой анализ должен сопровождаться разработкой и исследованием комплекса взаимоувязанных моделей, каждая из которых отражает некоторые функциональные, архитектурные и структурные особенности создаваемого программно-аппаратного решения. В рамках моделей должны быть выделены максимально общие угрозы информационной безопасности, совокупность которых по всем моделям с должной полнотой покрывает множество угроз. На основе такого подхода Концепция получается гибкой и расширяемой. В случае возникновения новых классов угроз, или новых типов программно-аппаратных решений она может быть пересмотрена или дополнена новыми моделями и механизмами, отражающими свойства добавленных сущностей.

Данный подход был применен при создании концепции информационной безопасности Федерального центра обработки данных (ФИЦ), более подробно с результатами работы можно ознакомиться в [4].

Процесс создания политики безопасности КВОИ, по сути, является продолжением исследований, выполненных на этапе формирования концепции информационной безопасности, и содержит более детальную проработку мер и решений, описанных в концепции.

Сформированная и зафиксированная документально политика информационной безопасности КВОИ и программа ее реализации должна быть выполнимой на практике, краткой и понятной, а также не приводить к существенному снижению производительности отдельных структурных элементов, составляющих объект. Содержание политики безопасности должно быть доведено до сотрудников, принимающих участие в его эксплуатации. Сотрудники должны обладать достаточными правами для исполнения всех обязанностей, возложенных на них согласно положений политики безопасности. Одна из основных целей политики безопасности состоит в том, чтобы обосновать и внедрить средства защиты КВОИ от деструктивных информационных воздействий, адекватные основным целям и задачам возлагаемым на объект. Выбор политики информационной безопасности представляет собой сложный и многоэтапный процесс. Решающую роль

при формировании содержания политики играет необходимость создания и поддержания режима информационной безопасности объекта, а также сложившиеся в организации административные регламенты, включая электронные, и поддерживаемая «культура» их исполнения (правила и приоритеты при исполнении указаний, методы обеспечения коммуникаций между сотрудниками и подобные им неформализованные процедуры). Следует отметить, если правила политики безопасности намного более «жесткие», чем те, которые сложились, то они будут либо игнорироваться, либо сотрудниками будут найдены способы обхода правил, декларируемых политикой информационной безопасности.

На основе политики безопасности разрабатывается программа обеспечения информационной безопасности, регламентирующая набор и содержание процедурных мер, используемых в КВОИ для реализации каждого из уровней комплексного подхода к реализации такой программы. Обычно выделяют две составляющих программы:

- стратегическую — содержит стратегические планы работ по обеспечению безопасности, документально зафиксированные руководством, например, периодичность и методику проведения переоценки рисков, контроль соответствия текущего состояния политике безопасности и работа с внешними контролирующими организациями;
- тактическую — содержит рекомендации и руководства по работе с конкретными сервисами КВОИ, необходимо для исполнения непосредственными администраторами сервисов.

Следует заметить, что все меры используемые для обеспечения информационной безопасности КВОИ на процедурном и программно-технических уровнях так или иначе должны быть отражены в политике информационной безопасности и программе обеспечения информационной безопасности, что позволяет повысить прозрачность всей организации в целом и упростить оценку защищенности и проверку соответствия реальных мер декларируемым.

Заключение

В данной статье рассмотрены подходы к выработке концептуальных положений обеспечения информационной безопасности объектов национальной информационно-телекоммуникационной инфраструктуры. Обосновывается необходимость контроля со стороны государства за составом и реализацией используемых на объектах механизмов обеспечения информационной безопасности. Предложена адаптация комплексной системы мер

обеспечения информационной безопасности, раскрыта роль и содержание административно-организационного уровня противодействия деструктивным информационным воздействиям.

В продолжение данной работы, для каждого из классов КВО, выделенных на основе методики из [3], предполагается:

- уточнить списки мер, направленных на обеспечение информационной безопасности;
- сформировать шаблоны содержания концепции обеспечения информационной безопасности КВО;
- детально проработать наиболее важные положения политики обеспечения информационной безопасности.

Литература

[1] Основы информационной безопасности: курс лекций: учебное пособие / Издание третье / Галатенко В. А. Под редакцией академика РАН В. Б. Бетелина / М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006.

[2] *Васенин В. А.* Научные проблемы противодействия кибертерроризму. Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. Интеллектуальный Центр МГУ. 2–3 ноября 2005 г. М.: МЦНМО, 2006 г.. С. 49–63.

[3] *Васенин В. А.*, *Пучков Ф. М.* Информационная безопасность объектов критически важных инфраструктур: вопросы идентификации, кластеризации и категоризации.

[4] *Васенин В. А.*, *Большаков М. В.*, *Савкин В. Б.* К вопросу обеспечения информационной безопасности в Федеральном центре управления информационно-технологическими ресурсами. Международная конференция «Проблемы функционирования информационных сетей». Материалы конференции (Новосибирск, 31 июля–3 августа 2006 г.). ЗАО РИЦ Прайс Курьер, Новосибирск, 2006. С. 59–66.

[5] *Липаев В. В.* Функциональная безопасность программных средств. М.: СИНТЕГ, 2004, 348 с.

Terrorist Use of the Internet

J. Bird

Introduction

1. At the risk of disillusioning the audience or of being over simplistic, I hope this presentation will serve to underline the fact that terrorist use of the internet is really the same as everyone else's' use of the internet. Incitement to violence or planning a terrorist act — which can hardly be said to be new phenomena — are the exceptions to 'normal' behaviour which can now be expressed through a new medium. The fact that terrorists too appreciate what more and more of us realise to be a valuable tool for outreach is unsurprising but has prompted frenzied discussion of the key question, how to limit terrorist outreach whilst not crippling the world wide web for the rest of us.

2. The internet is an open medium, it excludes none, invites participation and brings billions of people within reach. The opportunities it offers for public debate and particularly for experts to argue in open forum are huge drivers for democracy but they are equally valid for the dissemination of minority views, whether these are acceptable or unacceptable to the majority.

3. Azzam Publications site 2001:

"It is easy to spread news, information, articles and other information over the internet. We strongly urge Muslim internet professionals to spread and disseminate news and information about the jihad through email lists, discussion groups and their own websites. If you fail to do this and our site closes down before you have done this, we may hold you to account before Allah on the day of Judgement!"

> **Note:** *Although this is an example which refers to terrorism based on an interpretation of Islam, the same is true of any other group promoting violence* (*only they will be held accountable to someone else*!)

There have been extensive publications of the role of the internet in terrorism but for today I have opted to reduce them to 5 key functions: communications, media impact, research, belonging and alternative reality.

[)] This is the author's own view and in no way represents an official NATO position.

4. Communications

4.1. Terrorists need to communicate. For many of us, and many of them, this is the basic, sometimes the only, use of the internet. Email in its simplest form, messages that get sent in seconds, mostly reliably and which wait in mailboxes for the recipient to log on and reply. This is generally one-to-one communication although copy addressees can be added. Similarly, voice contact using VOIP (Voice over internet protocol) is growing and is usually for one-to-one calls although conference calls are possible. These methods presuppose those communicating know each other or at least have been recommended to each other through a mutual contact.

4.2. More general communications include blogs, chat rooms, drafting areas etc where messages can reach a wider (random) audience or more limited (password controlled) audience.

4.3. Although there is a general appreciation that intercept is possible and the use of encryption using commercial packages is generally on the rise, it seems no more prevalent amongst terrorists than amongst law abiding individuals. Al-Qa'ida (AQ) has used it on occasion but its use amongst large commercial enterprises is widespread.

4.4. Stenography is seemingly discussed more by security services than by terrorists and is more challenging and hence less immediately appealing.

4.5. If the aim is to reach more than a small number of people then we are into the next category

5. Media impact

5.1. The broad requirement for a terrorist ideology is for it to be spread to new recruits, to win over new enthusiasts and sow doubts about the validity of the status quo in the mind of opponents and neutral bystanders. Wide-reaching propaganda and the manipulation of public opinion is essential for the continuance of terrorism and the internet is an ideal medium as it offers multimedia richness — music, videos, voice-overs, animations etc can be included by even relatively inexperienced webmasters — which appeals particularly to the young or less literate.

5.2. Most terrorist or extreme ideological groups have established a web presence; it is cheap and easy to look professional. Merely by having a website they add to their own perceived validity and legitimacy. In this they behave exactly like small pressure groups or commercial outlets serving niche markets and simultaneously make themselves available for direct contact by interested parties.

5.3. Ensuring that a cause or activities related to it received public attention used to depend on attracting the attention of journalists from TV, radio or

print media, editors, political influence or competing stories often pushed such issues from the headlines but on the web terrorist groups can retain direct control over their messages — no more editorial liberties! No more sidelining by the latest pop star controversy! As many gruesome pictures and shocking headlines as the group wants and whenever it wants.

5.4. AQ has to convey its strategy and focus to increasingly dispersed followers whose enthusiasm has to be constantly whipped up if they are to remain dedicated to the cause. As Sahab agency distributes messages from the leaders (UBL and Zawahiri) and martyrs' testaments (e.g. after London) for use on AQ associated sites. These are also mirrored at other locations or linked or posted to other sites. They can generally be viewed alongside videos of executions and attacks, memorial listings of martyrs etc.

5.5. Unfortunately terrorist web postings are monitored not only by security services but by journalists who, increasingly, are rebroadcasting web material through conventional media outlets and increasing the media impact achieved by the terrorists. This can also be the fate of disinformation (such as casualty figures).

6. Research

6.1. For terrorists, as for school children and the general population, the internet is the world's greatest library. As Rumsfeld is often quoted "using public sources, openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy". Though internet sources are of varying reliability, it can be consulted for technical information of various sorts — maps, plans, transport systems, entrances to buildings, security procedures, instructions on mixing explosives, constructing suicide belts, extracting toxins, conspiracy theories, religious texts, and their interpretations (both valid and misguided), current anti-terrorist programmes can be checked and information on weapons likely to be deployed against terrorists can be downloaded.

6.2. The difficulty in verifying and authenticating sources means that the least selective (youngest, least well educated, unbalanced, unquestioning) most vulnerable members of society are exposed to undue influence. This is perhaps most clearly seen amongst converts who are avidly looking for 'the truth' and are unsure where it is to be found.

7. Belonging

7.1. The web presence of terrorist groups on the net differs only in content from that of other groups which bring together those with a common interest from amongst the vast range of individuals on line. Extremist or terrorism-related websites are the cyber equivalent of sewing groups or book

clubs and they provide a reassuring feeling of being part of an intimate community rather than a misfit or a loner. Unlike book clubs, however, terrorists may deploy spotters to keep an eye on communications from members of websites with similar interests to see if they have potential as real life recruits

7.2. Terrorist groups develop their own language of icons and graphic art, merely by looking at a site you can tell if it is tailored to your tastes (Joni Fighel of the ICT gives a fascinating, multicoloured, rapid fire presentation of horses, flags, roses, pointing fingers etc). These are the web equivalents of membership badges or scarves, in-house jargon and the like.

7.3. Linking those with common interests effectively regardless of geography carries out AQ's strategy of disseminating its ideology worldwide. Despite the intrinsic differences of different theatres of unrest/insurgency/terrorism such as Indonesia, Chechnya, Afghanistan, Saudi Arabia, Iraq etc. those with an interest are given a gut feeling that they are part of a worldwide movement, often referred to as 'global jihad'.

7.4. Finding others like yourself can lead to introspection, a spiral of reaffirmed ideas and isolation from the physical society in which you exist. This is the route which self-radicalisation follows amongst small groups of likeminded contacts.

8. Alternative Reality

8.1. In an extension of finding others who share your views on life (or whose views you suddenly realise you share) is a degree of escapism. You have the chance to be who you always thought you were and to express your 'true' feelings and 'core identity' no matter how difficult that has always been for the mainstream world to accept. You can live a parallel life, behave as the good neighbour, the football coach, the selfless charity worker etc in real life but give voice to your violent, discriminatory even fundamentally unbalanced views on the net. You can have a different status — as a help, a source of information, everyone's best mate when you log on and feel a misfit and resentful of your situation when you step out of your front door. Similarly you can meet your flat mate on line and never recognise his alter ego.

8.2. You can replace the routine, grey nature of daily life with a seemingly endless diet of movies, chat rooms, congratulatory or inspiring messages from your heros on line. You can choose how anonymous you wish to be — a low profile porn viewer or a would-be hero.

9. Additional uses to note:

- Hezbollah and Hamas (like the far Right) are concentrating efforts on children with a view to hardening opinions and tolerance of violence at

an early age (Prof Gabi Weimann of the University of Haifa provides examples of such sites).
- Fundraising.
- Souvenir selling.
- Eventual possibility of cyber attacks by terrorists (Omar Bakri Mohammed of al Muhajiroun in the UK claimed in 2002 that AQ were planning this).

Problems with countering terrorist internet use

10. As we have seen, terrorist use is not noticeably different from everyman's use of the internet. Large groups of people world wide feel alienated on the basis of religious intolerance, but also more generally on the grounds of deprivation, be it physical, territorial, spiritual, financial, educational etc. They are entitled (under the International Covenant on Civil and Political Rights and under the European Convention on Human Rights) to their opinions, to express themselves freely, to communicate, to seek out likeminded individuals and associate with them and to discuss their understanding of a better world (provided they do not advocate hatred — national, racial or religious — that constitutes incitement to discrimination, hostility or violence).

11. We must not forget that what happens on the internet does not equate to mobilisation to action in real life. Stating one's support for right wing extremism or violent jihad is not the same as taking up arms. Nor is the spectrum of Islamic self-help and teaching (from immigrant community self help sites, through Dawa, to discussions of fundamentalist interpretations of religion) terrorism. Until violence is a real possibility, civil liberties — particularly freedom of expression and freedom of religion must win out.

12. States are obliged to prevent terrorism and providing material support to terrorism or even the extension to the provision of expertise, advice or assistance can be legislated against. States are currently divided as to how public support for terrorism or its glorification can be legislated against (lengthy discussions at the OSCE, COE etc).

13. Freedom of expression is not an absolute right as it may not be used to destroy the rights of others. Suppression of views can, however, give those views more credibility than if they could be freely expressed so such action may be self defeating. It can also increase alienation and hence ratchet up radical views. Any restrictions on free speech restrict democracy, as do restrictions on the media whose open scrutiny is a key to the maintenance of democracy.

14. Hence the international lawyers' insistence on proportionate limitations. I recommend you to the publications of the Office for Democratic Institutions and Human Rights.

15. Enacting new laws is not necessarily the answer — it is illegal to fly a plane into a building but it didn't stop it being done. Laws also suffer from boundaries and the internet is very short of these, prosecution over a range of national legislations is notoriously difficult.

What else can we do?

16. Monitor, trace the most offensive ideologues, the most effective recruiters or efficient weapons trainers and (ideally) take action against them, counteract rabid views with 'balanced' ones, limit what is published, shut down sites?

17. There are problems with all of these. Not least the labour involved in policing the vast extent of the net, or the linguistic and cultural knowledge which is required (and usually in short supply), or the theological training needed for imams to be able to provide effective counter arguments to rabid proselytisers in favour of violent jihad.

18. If a site becomes a problem it can be shut down, but does that achieve anything? Usually not — suppressed sites have sprung up again within hours or days based in different countries, on different servers, with different IP addresses but with the same content. Such disruption may trigger a move to password protection or even encryption thus making the job of monitoring more difficult.

19. Azzam Publications site Nov. 2001:

"We expect our website to be opened and closed continuously. We urgently recommend any Muslims that are interested in our material to copy all the articles…and disseminate them…. This way, even if our sites are closed down, the material will live on with the Grace of Allah."

20. Overall the internet's value far exceeds the penalty we pay in terrorist use of it; it is a tool for democracy and human rights, it enables culture to speak to culture — or at the very least compare itself with the norms of others. The overall aim being mutual respect and tolerance.

21. Tariq Ramadan — a leading Muslim Brotherhood figure, well known for his books on Western Muslims — said, following the cartoons issue, "There are no limits to free speech but there are civic limits". "Free speech should be used wisely so as not to provoke sensibilities". "Just because you have the legal right to do something, doesn't mean you have to do it".

22. Once an idea is made public on the net it replicates fast — a huge challenge but also a huge opportunity — why should it be only for the promotion of violence? Key discussions now appear to centre on what alternative ideologies can be offered, how they can be made as attractive as terrorism and how they can be made to flow naturally without the usual grinding associated with government involvement (however peripheral).

Note: *Possible solutions might include*:

- *Addressing social conditions leading to alienation and aggression*.
- *Promoting Arab soaps ridiculing militant extremists*.
- *Imams on line correcting incorrect interpretations — undermining terrorist ideology*.
- *Imams teaching familiarity with the Koran to remove religious base for violence and worst extremes of interpretation* (*Saudi and Kuwaiti initiative in prisons*, *other examples in schools and universities*).

Conclusions

23. Terrorism has not changed dramatically in its move to a new medium. Most of the issues are old, though the problems are exacerbated by the reach and anonymity of the web. Cyber attacks by terrorists are not yet an established phenomenon. Countering terrorist action with legislation is not a full solution, the grass roots action is to prevent alienation by improving social conditions. Possible actions include monitoring, removal of the worst excesses and making efforts to counter violent ideologies. Suppression is as much a problem as a solution so shutting down websites must be a last ditch solution for sparing use only. The internet's value to us exceeds the penalty we pay in terms of terrorist use of it and I, personally, look forward to continuing to use a free internet.

Психологические модели и методы в исследованиях ресурсов развития терроризма

Ю. П. Зинченко, Р. С. Шилко

Терроризм является мультидисциплинарной, в том числе и психологической проблемой, поскольку вовлечение в террористическую деятельность основывается на использовании и манипулировании хронически неудовлетворенными потребностями существенной части населения, и в этом качестве может быть соответствующим образом исследовано.

Провоцирующими факторами порождения и развития терроризма исследователями признаются: обострение социального неравенства, ослабление семейных и социальных связей, отчуждение, недостатки воспитания, негативные последствия миграции, разрушение культурной самобытности, маргинализация населения, разрушение самоидентичности человека, становящиеся индивидуальными психологическими проблемами, а также распространение средствами массовой информации идей и взглядов, ведущих к росту экстремизма, неравенства и нетерпимости, несовершенство системы образования и подготовки кадров, отсутствие жизненных перспектив, другие, в первую очередь, экономические факторы.

Хотя предпосылкой современного терроризма в первую очередь служат кризисные экономические и социальные явления, терроризм опирается на глубинные свойства человеческой природы, что подтверждено классическими исследованиями.

Предполагается, что закономерности формирования, структурирования и функционирования комплексного психического образования, обозначаемого в школе А. Н. Леонтьева как «образ мира», у лиц, вовлеченных в террористические организации, имеет существенное сходства с образом мира лиц, характеризующихся либо отдельными чертами зависимости, либо зависимостью в психопатологическом смысле этого слова. Технология порождения террориста является не уникальной, а лишь одной из современных технологий, посредством которых структурируется образ мира, самоидентификация подвластного этим технологиям субъекта, что может стать основой для построения теоретических моделей и практических методик диагностики лиц, входящих в группы риска, эффективной профилактической работы, коррекции, реабилитации и формирования системы

психологически ориентированного мониторинга антитеррористической деятельности.

Аксиологической и идейной основой терроризма являются внутренняя убежденность террориста, экстремиста, радикала в служении абсолютной, высшей, единственной истине и, как следствие, вытекающий из нее фанатизм и готовность утверждать ее любыми средствами.

Д. В. Ольшанский указывает на наличие определенных требований со стороны террористических организаций к своим членам. К основным требованиям относятся следующие:

1. Безграничная преданность делу организации, доходящая до готовности пожертвовать своей жизнью в любой момент.
2. Выдержка, дисциплинированность и способность соблюдать конспиративность.
3. Безусловное повиновение решениям вышестоящих распорядителей.
4. Участие в оценивании новых привлекаемых в группу членов и готовность быть самому оцениваемым членами группы.

Люди, становящиеся членами террористических групп, — выходцы из разных социальных слоев общества. Поэтому мотивация, определяющая их радикально-настроенное поведение, достаточно разнообразна. Вместе с тем можно говорить о трансформации личности террористов и о тенденции к доминированию у них определенных личностных черт. Прежде всего, это агрессивность, которая развивается в том числе и как реакция на фрустрацию — субъективно невозможную ситуацию удовлетворения важных потребностей. Кроме того, это склонность к эскстернализации — возложению ответственности за неудачи на внешние обстоятельства и поиск внешних факторов для объяснения неадекватности собственного поведения объективно предписанным условиям.

Потребность в принадлежности к определенной группе относится к одной из базовых. Благодаря этой потребности обеспечивается социализация человека и формирование у него чувства самоидентичности. Часто членами террористических организаций становятся выходцы из неполных семей, а также люди, которые по тем или иным причинам испытали трудности адаптации к существующим социальным институтам, в частности, потеряли или вообще не имели работу. Чувство отчуждения от общества, возникающее в подобных ситуациях, становится основой для маргинализации ценностно-смысловой сферы личности человека. Это приводит к трансформации исходной потребности в принадлежности к определенной группе и в итоге заставляет человека присоединиться к группе, которая кажется ему столь же антисоциальной, как и он сам. Таким образом, характерной чертой личности террористов является сильная потребность во включен-

ности в группу подобных людей, обеспечивающая процесс самоидентичности. Террористами не становятся сразу, в одночасье. Прежде, чем стать частью террористической группы, человек зачастую проходит через изменение смысловых ориентиров собственной жизни, апатию, депрессию, вызванные социальной дезадаптацией.

Среди факторов, определяющих формирование террориста, исследователи называют следующие:

1) ранняя социализация;
2) нарушения нарциссического типа;
3) конфликтные ситуации;
4) личные связи с членами террористических организаций.

Идентификация с террористической группой обеспечивает ее членов социальной ролью, хотя и негативной. Выйти из группы для террориста крайне трудно, почти невозможно. Покинуть террористическую организацию для террориста значит потерять самоидентичность. Зачастую террорист имеет столь низкую самооценку, что для него отказаться от по сути дела заново обретенной самоидентификации практически невозможно. Нападки на группу воспринимаются террористом как нападки на него лично. Соответственно, любые действия, направленные на противодействие террористической группе, способствуют увеличению групповой сплоченности.

По мере того, как террорист проникается идеологией своей организации, он усваивает абсолютистскую риторику. Объекты окружающего мира предстают для него через призму простых и однозначных характеристик: свои и чужие, правильное и неправильное. При этом нивелируется возможность для проявления сомнения.

Одним из возможных источников становления террористической организации является радикализм. Не все радикалы становятся террористами, но многие террористы начинали свою деятельность с радикализма.

Радикализм обычно связан с идеями и представлениями о необходимости кардинального и решительного переустройства существующих социально-политических отношений в обществе. При этом радикализм предполагает отрицание существующей структуры общественных отношений и выдвижение новой, альтернативной, которая рассматривается как единственно возможная и правильная для выхода из сложившейся несправедливой и неприемлемой социально-политической действительности.

Ключевое отличие радикализма от экстремизма состоит в том, что радикализм предполагает важную идеологическую составляющую в социальном переустройстве. И только на ее основе разрабатывает определенные методы достижения конкретных целей. Экстремизм может существо-

вать и без четко обозначенной идеологической составляющей, фокусируясь главным образом на методах и средствах борьбы.

Среди основных функций радикализма исследователями выделяются следующие пять:

1) информационная (свидетельствующая о нестабильности социальных процессов);
2) снижение социальной напряженности;
3) давление на политические институты;
4) корректировка социально-политических представлений;
5) стимулирование социальных преобразований.

Проблема психологического сопровождения формирования эффективной системы противодействия различным аспектам террористической деятельности должна решаться не обособленно от других гуманитарных проблем, а именно в контексте их общих закономерностей, детерминируемых современными технологиями. Проблема противостояния технологиям терроризма не имеет технического решения. Однако вполне решаемой представляется задача разработки на основе современной психологической теории программ и методов, существенно уменьшающих число индивидуумов с ментальностью террористов.

Комплексный анализ взаимоотношений современного терроризма и средств массовой информации

Е. Л. Вартанова, Е. Е. Пронина, Н. В. Ткачева

В глобальном обществе средства массовой информации становятся главным инструментом и основным объектом террористических атак. Именно поэтому необходимо рассматривать информационную безопасность самым широким образом, вводя в это понятие как безопасность электронных сетей, связи банков данных, так и безопасность общества от воспевания и героизации насилия и террора в СМИ. Причем данная трактовка информационной безопасности не может носить абстрактный и академический характер. Такого рода информационная безопасность должна стать одной из целей общенациональной информационной политики.

Особенностью современного терроризма является активное использование информационно-психологического воздействия как важного элемента манипуляции сознанием и поведением людей. Действия террористов рассчитаны не только на нанесение материального ущерба и угрозу жизни и здоровью людей, но и на информационно-психологический шок, воздействие которого на большие массы людей создает благоприятную обстановку для достижения террористами своих целей.

Большинство развитых стран сталкиваются сегодня с необходимостью противостояния терроризму, выработки национальной стратегии и межгосударственного сотрудничества. Специфика собственно российской ситуации, однако, состоит в удивительном разногласии общества по вопросам, касающимся общей безопасности: отчужденность и даже враждебность многих СМИ по отношению к государству, правоохранительным и силовым органам в ситуации тотальной террористической угрозы; отсутствие у населения веры в защиту со стороны государства, отсутствие у государства недвусмысленной и четкой позиции в отношении террористов и их идеологии и т. д. Невозможность консолидации власти, СМИ и гражданского общества в чрезвычайных обстоятельствах является одним из центральных феноменов современного состояния проблемы информационной безопасности. Показателем кризиса стала неспособность журналистско-

го сообщества содействовать национальному объединению перед лицом опасности.

С конца 80-х годов в связи с социально-экономической трансформацией и политической реструктуризацией государства самой насущной задачей общества стало национальное самоопределение, становление новой российской идентичности. Но СМИ так и не смогли взять на себя функцию форума национального самоопределения, что привело к дезориентации и распылению активности общества. Идейный вакуум увеличивает вероятность проникновения террористической идеологии в СМИ. Формируется своеобразная спираль нарастания кризисных явлений в общественном самосознании, «порочный круг» самопрограммирования на поражение в борьбе с терроризмом. Становится все более очевидно, что без позитивной самоидентификации, осознания своих интересов политическое, духовное и иное противостояние террористической угрозе невозможно.

Причины вовлечения СМИ в сферу влияния террористических группировок

Анализ показывает, что причины вовлечения СМИ в сферу влияния экстремистов могут быть различными, но *в основе лежит отсутствие представления о национальных интересах как в самих СМИ, так и в обществе в целом*. Следует в то же время различать факторы, оказывающие влияние на поведение рядовых журналистов, и факторы, определяющие политику СМИ как социальных институций.

Среди причин вовлечения журналистов в сферу влияния террористов в качестве наиболее важных можно отметить:

1. отсутствие профессиональных этических принципов, моральная неразборчивость, потеря перспективы, социального оптимизма (утрата смысла журналистской деятельности);
2. преобладание узкокорпоративных интересов над общенациональными (отсутствие системы санкций за нарушение принципов профессиональной деятельности и вред, наносимый национальным интересам, неразработанность профессиональных стандартов и норм);
3. правовая и физическая незащищенность журналиста (зависимость от работодателя, корпоративное давление, страх мести со стороны экстремистов, лоббистских группировок);
4. внутриличностные причины: психологическая некомпетентность, непонимание собственных психических процессов (неконтролируемая эмпатия, сочувствие «угнетенным»), отсутствие навыков эмоционального самоконтроля и саморегуляции («стокгольмский син-

дром»), недостаточно развитые способности логического мышления, неструктурированная, диффузная система ценностей (тщеславие, стремление играть влиятельную роль, желание получить эксклюзив любой ценой и т. д.);

5. принадлежность к референтным группам с маргинальной и экстремистской ориентацией (этническим, социальным, политическим), преследующим цели разложения существующего общества.

Вовлечение владельцев СМИ в сферу влияния террористических группировок и позиция СМИ в отношении терроризма определяются другими причинами. В их числе наиболее важную роль играют:

1. Приоритет личных и коммерческих интересов руководства СМИ перед общенациональными.
2. Отсутствие контроля со стороны гражданского общества и государства за соблюдением национальных интересов в работе СМИ.
3. Непрозрачность источников финансирования СМИ (финансирование со стороны экстремистских организаций, партий и групп приводит к конфликту интересов конкретных СМИ с национальными интересами).
4. Неограниченная власть и правовая неподконтрольность владельцев СМИ.
5. Психологическая некомпетентность руководства СМИ, неосведомленность о возможных последствиях информационных кампаний, неспособность к социальному прогнозированию.

Различие причин вовлечения в сферу влияния террористов на индивидуальном и институциональном уровнях свидетельствует о том, что и меры должны приниматься разные: например, для рядовых сотрудников необходим психологический ликбез, а также система защиты профессиональных и личных прав журналистов, для организаций и руководителей — строгий финансовый контроль и юридическая ответственность за нарушение принципов профессиональной деятельности и несоблюдение правил информационно-психологической безопасности общества. Важно предусмотреть систему адекватных предупреждающих мер. Ответственность владельцев СМИ должна быть повышена и приведена в соответствие с их коммерческой выгодой. В то же время рядовые журналисты должны быть максимально защищены журналистским сообществом и правовыми нормами от произвола и преследования со стороны руководства СМИ, а также лиц и групп, стремящихся реализовать собственные интересы в ущерб общественным.

Текстовые индикаторы террористической направленности публикаций

Контроль со стороны общества за деятельностью СМИ требует не только четкого осознания манипулятивных приемов, применяемых террористами, но и надежных текстовых индикаторов данных технологий.

Наиболее распространенными приемами воздействия на общественное мнение в интересах террористических организаций являются следующие:

1. *Создание негативного образа государства, силовых структур и органов правопорядка* (с целью вызвать отчуждение населения от власти, противодействовать консолидации общества). При этом используются как обвинения в плохой организации необходимых мероприятий, огульная критика, дискредитация всех предпринимаемых действий государства и служб противодействия террористам, так и упреки в несоблюдении прав человека, жестокости и несправедливости по отношению к террористам.

2. *Формирование позитивного образа террориста* (с целью привлечения на свою сторону, ослабления сопротивления, создания иллюзии безопасности, размывания убеждений и т. д.). Достижению этих целей способствуют: выражение сочувствия, «понимание мотивов», признание полной или частичной справедливости требований экстремистов; мифологизация или демонизация агрессора, формирование представлений о его могуществе и непобедимости; замалчивание, преуменьшение нанесенного ущерба, поиск смягчающих обстоятельств; предоставление слова террористам, легитимизирующее их намерения и действия.

3. *Запугивание аудитории* (с целью деморализации, провоцирования панических настроений, страхов и тревоги). Этой цели служит демонстрация «актов возмездия», устрашающие прогнозы, прямое цитирование угроз, нагнетание тревоги, создание ощущения хаоса, бессмысленности происходящего, беспомощности и т. д.

4. *Создание негативного самообраза у аудитории* (с целью дискредитировать коллективную идентичность, препятствовать национальному объединению, обратить энергию сопротивления на поиск виновных в собственной среде и т. д.). Для этого жертвам террористической агрессии приписывается изначальная «историческая», родовая вина; попытки самозащиты расцениваются как проявления жестокости, жадности, эгоизма; под видом «самокритики» допускается неуважение к традициям и ценностям аудитории, дискредитируются те черты национального характера, которые обеспечивают сопротивление, и возвеличиваются те, кото-

рые формируют податливое поведение; одна часть аудитории настраивается против другой, активизируется поиск «внутреннего» врага.

5. *Организация акций в поддержку требований террористов* (с целью создания иллюзии о массовости поддержки соответствующих идей и привлечения отдельных представителей общественности на свою сторону).

6. *Дискутирование вопросов*, *не подлежащих обсуждению* (вопросы территориальной целостности России, принцип невмешательства иностранных государств), абсурдизация реальности с целью провоцирования сомнений, подрыва рационального мышления, размывания убеждений аудитории.

Вышеописанные методы воздействия обнаруживаются в следующих текстовых коррелятах, свидетельствующих о попытках реструктурирования общественного мнения:

1. *Негативно окрашенная и сниженная лексика*, *характеризующая антитеррористические действия* государственных институтов, спасателей, силовых органов.
2. *Позитивно окрашенная лексика*, *характеризующая самих террористов*, *их мотивы*, *намерения и акции*.
3. Мифологическая структура текста по проблемам экстремизма и терроризма: *формирование символов*, *мифов и штампов* (приводит к снижению функций сознательной регуляции поведения, содействует развитию фобий и панических реакций, повышает внушаемость и импульсивность, чревато развитием массовых психозов).
4. Гедонистическая структура текста: *глумление*, *издевательство*, *мизеризация*, *инфантилизация* (размывает структуру базовых ценностей и ориентиров, поселяет неуверенность, разрушает ценностно-ориентационное единство общества, препятствует конструктивному решению проблем, восстановлению после травмы, деморализует перед лицом опасности).
5. *Дискредитация жертв агрессии*: *представление террористических акций как заслуженного наказания*, ссылки на историческую вину, политические просчеты, экономическую несправедливость.

Сегодня становится очевидным, что недостаточно только отслеживать патологические паттерны в потоке информации. Необходимо придать новые силы процессам национальной консолидации и самоидентификации. Для этого необходимо включить все механизмы, связывающие прессу и гражданское общество, усилить ответственность СМИ перед обществом.

Общественный контроль является главным условием начала процессов самоорганизации и саморегулирования в структурах СМИ.

Саморегулирование придает смысл и стержень деятельности журналистов и медиаинститутов, служит естественным иммунитетом против террористических и антиобщественных идей. Государство должно предусмотреть рычаги влияния общества и общественного мнения на СМИ. Это необходимо для превращения СМИ в подлинную саморегулирующуюся систему, независимую от структур и группировок, представляющих угрозу общественным интересам.

При всей важности саморегулирования для самих СМИ, проблема заключается в том, что СМИ не могут самостоятельно инициировать и развивать систему саморегулирования. Саморегулирование существует только *наряду* с системой общественного регулирования и постольку, поскольку действуют реальные санкции со стороны общества. Это означает, что саморегулирование активно работает только там, где существует отлаженная система «обратной связи»: Общество → СМИ. Алгоритм её функционирования представлен на рис 1.

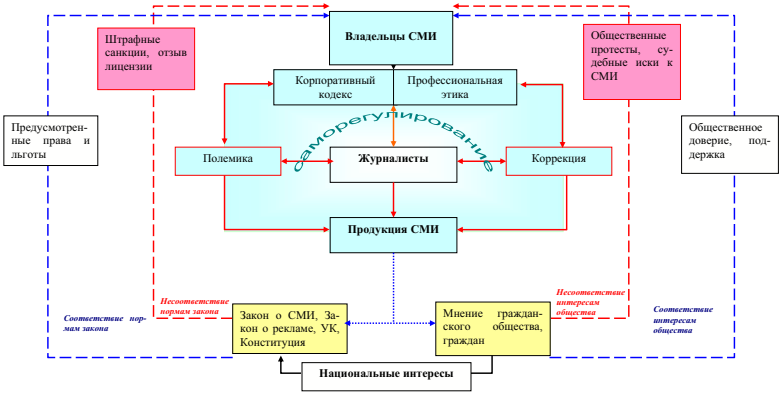


Рис. 1. «Обратные связи» в процессах саморегулирования СМИ

Согласно принципу саморегуляции, только сами журналисты имеют непосредственный доступ к производству и контролю информационной продукции. Общество оценивает продукцию только после её публикации. Отсутствует предварительная цензура. Однако работают механизмы «обратной связи». Продукция СМИ, не соответствующая интересам общества и нормам закона, отражающим эти интересы, по механизму отрицательной обратной связи влечет за собой определенные санкции в отношении владельцев СМИ, начиная от общественных акций протеста и администра-

тивных взысканий вплоть до судебных разбирательств и отъема лицензии. Большую роль играют и положительные обратные связи, которые выражаются в общественной поддержке, высоком статусе соответствующих изданий и предусмотренных законом правах и льготах для СМИ. Мнение общества, поддержанное законодательной и исполнительной властью, нельзя отклонить, и это вынуждает СМИ активизировать инструменты саморегулирования во избежание общественного недовольства и санкций разного уровня.

Важным механизмом саморегулирования является формирование общественного мнения самих журналистов в процессе развертывание полемики между изданиями и каналами, а также здравой критики отдельных выступлений, материалов и политики изданий (на схеме: левая сторона контура саморегулирования — «полемика»). По мнению многих профессионалов, в журналистике в настоящее время практически отсутствует полемика и не сформировано общественное мнение, которое могло бы противодействовать авторитаризму и деловой или политической ангажированности владельцев СМИ.

Интересным средством активизации профессиональной дискуссии может служить создание журналистских медиасайтов по проблемам профессиональной этики, как, например, сайт американских журналистов `www.journalism.org`. Сайт создан комитетом обеспокоенных журналистов (The Committee of Concerned Journalists) при поддержке участников Проекта по достижению наивысшего качества в журналистике (The Project for Excellence in Journalism). Комитет обеспокоенных журналистов — это консорциум репортеров, редакторов, продюсеров, издателей, собственников и профессионалов. Свою задачу они видят в создании общенациональной дискуссии о стандартах работы журналистов. Различные разделы сайта посвящены обзорам и контент-анализу СМИ, практическим рекомендациям и специальным форумам.

Кроме того, СМИ могут создавать различные структуры по осуществлению непосредственного взаимодействия с аудиторией подобно Комиссии по жалобам на прессу в Великобритании (на схеме — самокоррекция). Это позволило бы СМИ предупреждать возможные конфликты и взрывы общественного недовольства, избегать судебных разбирательств и исков. В этом плане уже предприняты определенные шаги. В 2005 году создана Общественная комиссия по жалобам на прессу, которая состоит из 2 палат: представителей медиа и аудитории. Комиссия еще находится на стадии формирования и не начала свою работу. Успех в её деятельности зависит от того, будет ли она ориентирована на самокоррекцию или на поиск «прикрытия». Но и при самом благоприятном варианте следует понимать, что подобные структуры, созданные на средства медиа, являются

именно способом внутренней саморегуляции *СМИ* и не могут выполнять функции общественного контроля, как бы они при этом ни назывались.

Наличие действенного механизма общественного контроля необходимо как Обществу, так и СМИ. Саморегулирование СМИ представляет в этом смысле часть саморегулирования более широкой системы: Общество $\Longleftrightarrow$ $\Longleftrightarrow$ СМИ. Общество нуждается в СМИ как важнейшем инструменте осознания и реализации национальных интересов, а СМИ могут сохранить непредвзятость и независимость от интересов владельцев и инвесторов только следуя общественным интересам и опираясь на поддержку со стороны общества в целом.

Организация системы общественного регулирования СМИ

Говоря о необходимости внешнего контроля для активизации внутренних процессов саморегулирования СМИ, следует учесть, что глобальный, *сетевой* характер современных СМИ соответствует только *сетевому* характеру гражданского общества и не может эффективно регулироваться иначе, как структурами этого общества. Попытки сосредоточить функции контроля в локальном центре, присвоить их отдельному социальному институту, сколь угодно авторитетному и правомочному, заранее обречены на провал, так как сетевая, «распыленная» структура СМИ не поддается точечному контролю. Невозможно отследить и откорректировать все процессы, одновременно протекающие на разных уровнях многомерной системы.

Функции текущего контроля необходимо препоручить структурам гражданского общества и непосредственно гражданам, заинтересованным в собственной безопасности. Важно *напрямую* связать потребителя и производителя информационной продукции, гражданское общество и СМИ, обеспечив действенность, правомочность и легитимность *прямых* связей «Общество → СМИ». Конструктивная воля и роль государства в решении проблемы безопасности состоит в том, чтобы вооружить гражданские структуры реальными возможностями воздействия на СМИ, включая принятие решений о пригодности/непригодности (безопасности/вредности) того или иного информационного продукта для обращения в структуре массовой коммуникации.

Общественный контроль по определению, в соответствии с сущностью самого Гражданского общества, должен строиться на сетевых принципах и принципах местного самоуправления. Только сетевая структура контроля способна взаимодействовать одновременно со всеми СМИ на всей терри-

тории страны, учитывая все аспекты их деятельности. *Сетевая* система контроля предполагает, что отдельные структуры сети на местах, в регионах должны быть в целом аналогичны во всех отношениях центральным органам и работать относительно самостоятельно, обладая практически теми же полномочиями, что и центральные органы, только в отношении местного вещания.

Основной функциональной единицей такой сети может стать Совет по СМИ[1)] под эгидой какого-либо авторитетного в данном регионе общественного представительства: Общественной палаты, Гражданской ассамблеи (гг. Пермь, Новосибирск, Нижний Новгород), Общества защиты прав потребителей и т. д. В центре страны (гг. Москве, Санкт-Петербурге) может быть создан Высший совет по СМИ при одной из центральных общественных организаций (Общественная палата, Общество потребителей). *Однако Высший совет не является ни управляющим, ни головным.* Высший Совет принимает протесты на работу центральных каналов вещания. Принятые им решения могут рассматриваться как прецедентные (моделирующие) местными советами по их желанию. Местное вещание регулируется местной общественностью.

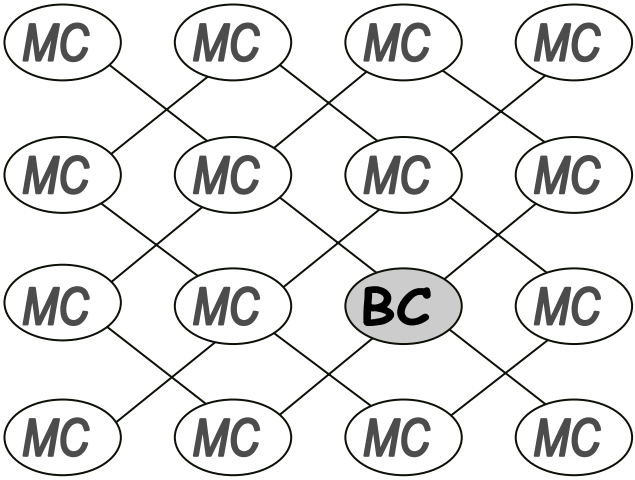


Рис. 2. Сетевая структура органов общественного контроля СМИ: МС — местный Совет по СМИ, ВС — Высший Совет по СМИ

[1)] Например, такое название имеет орган регулирования и контроля вещания во Франции (CSA) — Высший совет по аудиовизуальным средствам информации.

Принципы деятельности Совета по СМИ

Совет по СМИ (в том числе Высший Совет по СМИ) — общественный орган с функциями, аналогичными судебным.

Основная задача Совета по СМИ — защита национальной (местной) аудитории от информации, наносящей вред моральному, духовному состоянию общества, противоречащей интересам каких-либо социальных слоев и групп населения: детей, подростков (включая вопросы воспитания и защиты молодежи от информационного насилия), женщин, профессиональных сообществ и т. д., а также приносящей моральный и материальный ущерб конкретным гражданам.

Конкретные лица, группы граждан (например, родители) и общественные организации вправе обращаться с заявлениями и протестами в Высший и местные Советы по СМИ. Совет по СМИ определяет степень безопасности/вредности (пригодности/непригодности) представленной на рассмотрение продукции СМИ.

Заявления рассматриваются в соответствии с имеющимися нормативными документами по СМИ. При отсутствии соответствующих правил и законов или при их недостаточности и несовершенстве Совет может начать разбирательство по принципу открытого судебного состязательного процесса перед лицом жюри, аналогичного жюри присяжных и состоящего из представителей срединных слоев общества (о принципах формирования жюри см. ниже). Принимая решение, члены жюри не связаны никакими указаниями.

Решения общественного Совета по СМИ относительно безопасности/вредности (пригодности/непригодности к обращению) конкретного информационного продукта являются *окончательными*.

Принципиально важно, чтобы в спорных и вопиющих случаях (а именно такие случаи должны становится предметом разбирательства Совета по СМИ) приоритет безусловно отдавался мнению общественности, даже если оно не может быть строго аргументировано.

Чувство общественного самосохранения является самым надежным и главным гарантом адекватного решения, минимизируя возможность ошибки, хотя и не исключая её полностью. Решение, принятое самой аудиторией, является формой выражения общественного интереса и потому единственно легитимным и справедливым. *Права граждан и аудитории в целом выше прав СМИ, как права личности выше прав организаций.*

Деятельность Совета строится по принципу прецедентного права, то есть принятое в конкретном случае решение может рассматриваться далее как модельное для аналогичных ситуаций.

На основе вынесенного вердикта о безопасности/вредности информационного продукта (по аналогии с виновностью/невиновностью в судебном процессе) Совет вправе потребовать от Министерства Печати, Антимонопольного комитета и других исполнительных органов принять необходимые меры по пресечению вредной деятельности тех или иных издателей, наказания виновных (штрафы, отъем лицензии) или компенсации нанесенного ущерба.

Величина штрафа, характер наказания для различных случаев предварительно устанавливаются на совместных переговорах Общественного Совета с соответствующими исполнительными органами (так называемых, гражданских переговорах) и закрепляются на определенный период.

Совет вправе:

- инициировать расследовательскую деятельность в отношении конкретных СМИ;
- обращаться с запросами по деятельности конкретных СМИ в Антимонопольный комитет, Налоговую инспекцию, Министерство Печати и т. д. и получать всю необходимую информацию;
- в случае затяжки принятия мер исполнительными органами организовывать общественные акции протеста, вплоть до бойкотирования соответствующих изданий, пикетирования исполнительных органов и т. д.;
- выходить с законодательными инициативами и поправками к существующим нормативным актам по СМИ в Государственную Думу, Министерство Печати, Антимонопольный комитет и т. д.

Решения Совета должны широко освещаться в СМИ и специальных изданиях, бюллетенях.

Структура Совета по СМИ

Совет по СМИ организуется при крупной общественной организации — Общественной палате или Обществе потребителей.

Совет обладает функциями, аналогичными судебным.

Совет состоит *из двух частей*:

1) представителей общественности в количестве 12 (24) человек *с правом голоса — Общественное жюри*,

2) специалистов в области психологии, медицины, права (4 человека) в качестве постоянных *консультантов*.

(Во Франции в аналогичный Совет входят также судьи.)

Решения принимаются путем голосования членами общественного Жюри простым большинством голосов при условии присутствия не менее 2/3 от общего состава Жюри на момент голосования.

Для участия в Совете *со стороны общественности* выдвигаются представители *срединных слоев* населения, имеющие высшее образование. Кандидатуры выдвигаются местными общественными организациями, родительскими комитетами, попечительскими советами. Жюри формируется путем случайного выбора из представленных кандидатур (по аналогии с практикой формирования жюри присяжных).

Со стороны специалистов в совет входят психологи, медики и юристы, выступающие в Совете в качестве консультантов. Они предоставляют Совету необходимую информацию, организуют исследовательские пробы, рекомендуют привлечь дополнительных внешних специалистов в случае надобности.

В состав Совета *не могут быть включены* в качестве членов представители СМИ, бизнеса и шоу-бизнеса, политических партий, исполнительных структур государства, так как в этом случае высоко вероятно возникновение конфликта интересов. Не могут являться членами жюри также «звезды», известные и популярные люди, так как необходимо избежать харизматического воздействия на аудиторию, какого бы то ни было намека на PR. Авторитет и харизма конкретной личности не должны подавлять самостоятельного мышления граждан, затемнять существо дело и мешать трезвому принятию решений.

Участие специалистов и экспертов в работе Совета ограничено консультированием, проведением экспертизы, развертыванием аргументации в пользу того или иного мнения в ходе состязательного процесса. *Решения принимаются исключительно голосованием членов общественного Жюри.* Специалисты и эксперты не участвуют в голосовании. Это обусловлено тем, что компетентность специалистов ограничена диапазоном имеющихся знаний, уровнем развития представлений о влиянии СМИ, наличным методическим инструментарием, различиями теоретических подходов, экономическими интересами и статусными притязаниями. В этой ситуации результат экспертизы далеко не всегда однозначен, а споры могут длиться вечно. Решение должно приниматься теми, кто в первую очередь будет «расплачиваться» своим здоровьем и благополучием за распространение вредной продукции СМИ. Наука может ждать, пока будут проставлены все точки над i, а конкретные люди, сегодня подвергающиеся опасности, нет.

Именно общественность является основной движущей силой в решении вопросов информационной безопасности в международной практике на

всех этапах: инициирования разбирательства, экспертизы и принятия решения. Если общественность будет отстранена от участия в этих вопросах, то решение проблемы окажется долгим, трудным и даже вряд ли вообще возможным. *Только обеспечение приоритета прав личности в области информационного производства гарантирует общее оздоровление общества.*

Повышение уровня компетентности общества как условие адекватной работы СМИ

Следует, однако, иметь в виду, что общественное сознание и самосознание — это не столько процесс самовыражения, сколько процесс *самостановления*. Растущая активность граждан в отстаивании своих прав свидетельствует о росте общественного и национального самосознания во всем мире и в нашей стране. Этот процесс характеризуется повышением осведомленности и компетентности граждан в экономических, политических и всех других вопросах, затрагивающих жизненные интересы национальной аудитории в целом и каждого человека в отдельности. Мощный импульс развитию коллективного самосознания дает свободный, открытый доступ к информации, повышающей общественную компетентность. То же можно сказать о профессиональном самосознании и этических кодексах специалистов в области СМИ: журналистов, психологов, социологов и др. И потребитель информации, и её производитель, и исследователь-эксперт должны знать о закономерностях, механизмах и последствиях массовых информационных процессов. Широкая осведомленность всех слоев общества о технологиях и методиках воздействия, возможном вреде для личности и социума тех или иных информационных технологий поставит надежный заслон соблазну коммерческой и политической эксплуатации аудитории и самих СМИ. Это обуславливает первоочередную необходимость развития системы медиаобразования как для широкой общественности, так и для профессионалов.

Основным условием развития системы саморегулирования СМИ и активизации общества в сфере взаимодействия со СМИ является становление общественного самосознания. Вследствие этого наряду с задачей создания системы общественного контроля необходимо содействовать повышению уровня медиапсихологической грамотности населения и профессиональной среды.

Задачи и каналы медиаобразования для широких кругов населения и медиапрофессионалов несколько различны.

Таблица 1. Структура и функции медиаобразования

Уровень	**Задачи медиаобразования**	**Содержание обучения**	**Организационные формы**
Гражданское общество, аудитория СМИ	1) повышение компетентности в области механизмов работы СМИ, защита от манипулятивного воздействий; 2) формирование навыков грамотного использования СМИ в собственных интересах потребителя, 3) развитие критического мышления и самосознания аудитории.	1) основные закономерности воздействия СМИ на аудиторию, анализ содержания СМИ — *медиакритика* 2) практическое освоение доступных технологий работы СМИ — *медиапрактика*	1) систематическое предметное обучение в рамках среднего и высшего образования, 2) общественные дискуссии по проблемам СМИ в массовой коммуникации, 3) развитие системы непрофессиональных СМИ в школах, вузах, районах, 4) широкое освещение деятельности Общественных советов по СМИ, результатов общественной экспертизы
Журналисты	1) профилактика профессионального выгорания; обучение навыкам психологической саморегуляции; 2) обеспечение профессиональной и психологической независимости журналиста; 3) поддержание высоких стандартов качественной журналистики; 4) обеспечение соответствия деятельности журналистов интересам национальной аудитории; 5) создание условий для саморегулирования и самоорганизации журналистского сообщества.	1) изучение содержания СМИ в контексте массовых психодинамических процессов — *медиааналитика*; 2) профилактика и реабилитация информационных травм аудитории; содействия росту национального самосознания — *медиатерапия*; 3) современные информационные психотехнологии, анализ и моделирования контента массовой коммуникации — *управление информационными кампаниями*; 4) *психологическая самопомощь*.	1) система профессионального образования, 2) специализированные тренинги, семинары, 3) центры психологической помощи журналистам; 4) профессиональные дискуссии по проблемам СМИ, 5) создание органов саморегулирования, 6) разработка внутренних корпоративных и этических норм профессиональной деятельности.

Возрастающая важность и актуальность медиаобразования граждан в современной России определяются двумя ключевыми моментами. С одной стороны, медиаобразование выполняет функцию важного средства защиты от манипулятивного воздействия СМИ, являющихся инструментом в руках политиков и других властных элит. С другой — медиаобразование может способствовать осознанному участию россиян в медиасреде и медиакультуре, что, несомненно станет одним из ключевых моментов эффективного развития гражданского общества.

Подготовка специалистов для системы саморегулирования СМИ

Первоочередное значение для регулирования деятельности СМИ имеет подготовка и обучение специалистов в области: 1) исследования и экспертизы СМИ, 2) информационной безопасности, 3) медиатерапии, 4) психологической помощи журналистам, 5) собственно медиаобразования.

Непосредственные задачи таких специалистов:

1) анализ СМИ, политико-экономический, лингвистический и психотехнический анализ сообщений массовой коммуникации, экспертиза информационной продукции;

2) изучение эффектов воздействия СМИ на массовую аудиторию, разработка проблем информационно-психологической безопасности аудитории;

3) моделирование контента СМИ в зависимости от типологии и аудитории медиаканалов;

4) разработка системы медиатерапии, планирование практических мероприятий по психологической реабилитации, формированию позитивной «Я-концепции» аудитории посредством СМИ и т. д.;

5) развитие системы психологической помощи журналистам.

Подготовка указанных категории специалистов обеспечит в дальнейшем надежный фундамент для развития системы общественного контроля и саморегуляции СМИ. Эта задача решается в русле таких новых направлений науки как моделирование СМИ, медиапсихология [2)], критика теорий СМИ, разрабатываемых на факультете журналистики МГУ.

Работа по подготовке кадров для системы медиаобразования, медиааналитики и медиатерапии потребует координации деятельности различных научных организаций, учебных институтов, практических служб и специалистов в области журналистики, психологии, практической психотерапии, медицины катастроф, социально-психологической помощи населению (Союз журналистов, ф-т психологии МГУ, ин-т психологии РАН, психотерапевтические профессиональные организации, психологические службы помощи и т. д.).

Головной организацией по развитию концепции, структуры и учебных программ для подготовки специалистов в области медиапсихологии может стать факультет журналистики МГУ, обладающий в настоящее время необходимыми теоретическими и методическими разработками (в частности,

[2)] Пронина Е. Е. Категории медиапсихологии // Проблемы медиапсихологии. РИП-холдинг, 2002.

Пронина Е. Е. Психология журналистского творчества // М:, МГУ, 2003.

моделью спецотделения «Медиапсихология»), организационными возможностями (система второго высшего образования, выездные школы и семинары для региональных журналистов, зарубежной русской прессы и т. д.), широкими связями с профессиональными союзами, центральными СМИ (так, например, факультет проводит ежегодные общероссийские и международные научно-практические семинары и конференции по проблемам журналистики и медиаобразования) и соответствующими учебными курсами.

Специалисты в области информационно-психологической безопасности и медиатерапии могут быть подготовлены на базе журналистского, филологического, психологического, медицинского или юридического высшего образования (в зависимости от направления дальнейшей деятельности в СМИ) в соответствующих учебных заведениях или в рамках спецотделений на факультетах журналистики.

Подводя итог проведенному анализу, можно сказать, что проблема защиты СМИ от использования террористами есть прежде всего проблема восстановления функций СМИ как инструмента саморегулирования общества, средства осознания и отражения национальных интересов. Полноценная реализация данной функции требует развития обратных связей «Общество $\Longleftrightarrow$ СМИ», активизации общественной реакции на деятельность средств массовой коммуникации. Это позволит СМИ «самонастраиваться» в интересах общества, а не чьих-либо иных. Качество СМИ, таким образом, во многом определяется уровнем активности, взыскательности и требовательности общества. По этой причине программа стимулирования процессов саморегулирования СМИ предусматривает не только формирование надежных обратных связей «Общество $\rightarrow$ СМИ», но и содействие становлению общественного мнения, способного оказывать влияние на СМИ. Для решения данной задачи предалагаемая организационная модель взаимодействия общества со СМИ поддержана мерами по развитию: 1) общественного самосознания, 2) профессиональной рефлексии и ответственности журналистов, и, наконец, 3) системы подготовки квалифицированных специалистов в области анализа СМИ, медиапсихологии и медиатерапии.

О международной практике и российском сегменте страхования риска «террористический акт»

И. Б. Котлобовский

Явление «терроризм» имеет многовековую историю, однако в последнее время оно приобретает такие масштабы, что становится настоящим вызовом безопасности человечеству.

Только за последние несколько лет произошли крупные террористические акции: 11 сентября 2001 г. в Нью-Йорке и Вашингтоне США, 24 августа 2004 г. потерпели катастрофу два пассажирских авиалайнера в РФ, погибло 90 человек, 1 сентября 2004 г. в Беслане, где погибли и пострадали сотни ни в чем не повинных детей, в 2004 г. на железной дороге в Испании, в 2005 г. в Лондонском метро и на курортах Египта и Турции. Эти события показали, что небольшая группа террористов или даже один человек способна «организовать» катастрофу, оказывающую влияние на весь мир. Во многих странах вырабатываются меры по пресечению и предотвращению действий террористов, по управлению рисками террористических актов.

Одной из важнейших и пока нерешенных проблем является проблема возмещения ущерба от террористических актов. Ущерб может носить катастрофический характер: убытки от террористического акта 11 сентября 2001 г. во Всемирном торговом центре превысил 100 млрд. долл. Погибло свыше 3 тыс. человек, пострадали тысячи людей и сотни организаций. Как правило, террористические акты наносят не только прямой, но и косвенный ущерб. После террористического акта 11 сентября наступила депрессия на рынке авиаперевозок: самолеты летали полупустыми, что привело к банкротству двух крупнейших авиакомпаний — «Sabena» и «SwissAir».

Во многих случаях остаются неурегулированными вопросы ответственности за возмещение ущерба от террористических актов, лимитов ответственности и определения источников финансирования возмещения убытков. Это приводит к многочисленным судебным тяжбам, как после теракта на Дубровке, большим социальным и политическим издержкам.

Как показывает исторический опыт, испытанным инструментом для компенсации убытков от непредвиденных событий является страхование. Однако до недавнего времени страхование риска терроризма не приме-

нялось. Только в конце XX столетия это стало востребованным. Именно страховщики возместили убытки более чем на 50 млрд. долл. после террористического акта 11 сентября 2001 г. во Всемирном торговом центре в Нью-Йорке. Это событие послужило толчком к росту спроса на страхование от террористических актов.

В последние годы многие государства создали национальные системы страховой защиты на случай террористических актов, основанные на участии в возмещении причиненного вреда страховых организаций, перестраховщиков и их пулов, в том числе и с участием государства. И хотя до настоящего времени в научных кругах не выработано единого мнения о соответствии риска «терроризм» критериям рисков, принимаемых на страхование, на практике страхование подобных рисков имеет место.

Крупные страховые и перестраховочные компании начали оценивать возможности страхования риска терроризм с 1972 г. после трагических событий на летних Олимпийских играх в Мюнхене. Однако лишь некоторые государства задумывались о создании национальной системы страховой защиты на случай терроризма (например, Великобритания и Испания).

После 11 сентября специальные схемы страхования от террористических актов были созданы в ряде зарубежных государств. Некоторые государства пересмотрели законодательные принципы, учитывая необходимость общественной солидарности в покрытии ущербов в результате террористических атак. В ряде случаев государством установлено обязательное страхование/перестрахование риска терроризм, предусмотрено создание пулов из государственных и негосударственных средств, других объединений страховых компаний, позволяющих урегулировать крупные потери. Ряд страховых компаний разработал специальные страховые продукты, предусматривающие страхование от риска терроризм.

Северная Ирландия

В 1978 г. в стране начала действовать специальная компенсационная программа Criminal Damage Compensation Scheme, обеспечивающая выплату страхового возмещения по ущербам в имуществе, вызванным терактами или действиями незаконных группировок (насчитывающих более трех лиц).

Испания

В Испании существует государственная страховая компания Consorcio de compensación de seguros (CCS), которая гарантирует покрытие для «экстраординарных рисков», таких как землетрясение, извержение вулканов, наводнение, буря, терроризм, гражданские беспорядки. Покрытие включено в страховые договоры, заключаемые частными страховыми ком-

паниями, которые собирают дополнительные страховые премии от имени CCS.

В соответствии с принципами разгосударствления страховой отрасли, которые были проведены в жизнь в начале 1990-х гг., CCS в настоящее время обеспечивает выплаты по «экстраординарным рискам», в том числе по риску терроризм в двух случаях:

- если эти риски исключены по полису частной страховой компании;
- если риск покрыт частной страховой компанией, но предъявленный к ней иск не может быть удовлетворен в силу неплатежеспособности компании (либо у компании приостановлены платежи в связи с проведением аудиторской проверки).

В первом случае CCS действует как прямой страховщик, во втором — как гарантийный фонд.

Выплаты, осуществляемые CCS, обеспечивают минимальную страховую защиту, установленную национальным законодательством.

Добровольное страхование «экстраординарных рисков» предполагает систему дополнительных страховых взносов, которые перечисляются в CCS. Таким образом, в полной мере реализуется принцип солидарной раскладки по катастрофическим рискам.

В результате событий 11 сентября 2001 г. в страховое покрытие в связи с перерывами в производстве (business interruption) также включается риск терроризм.

Великобритания

В Великобритании в связи с террористическими выступлениями членов IRA в начале 1990-х гг. был создан специальный перестраховочный пул Pool RE, принимающий в перестрахование риски прямых страховщиков, включающих риск терроризм в полисы страхования имущества юридических лиц.

Участие в Pool RE не является обязательным, но перестраховочная защита распространяется только на участников пула (в настоящее время около 200 страховых компаний).

Существуют определенные территориальные ограничения по перестрахованию. В территорию страхования включается территория Соединенного королевства за исключением Северной Ирландии, острова Мэн и Нормандских островов.

Страховое покрытие основывается на особом определении терроризма, данного в документах пула.

Английское правительство выступает в качестве «перестраховщика последней инстанции» в случае неплатежеспособности пула.

Начиная с 2003 г. для страховщиков, входящих в Pool RE, используется новая система расчета максимальной ответственности. Первоначально была установлена максимальная ответственность каждого страховщика — 100 тыс. английских фунтов стерлингов на один застрахованный объект по одному страховому полису. В 2003 г. была установлена максимальная ответственность всей страховой отрасли по риску терроризм в размере 30 млн. ф. ст. на одно страховое событие / 60 млн. ф. ст. на год; ответственность каждого страховщика рассчитывается на основе его рыночной доли.

В течение 2003–2005 гг. было предусмотрено постепенное увеличение размеров максимальной ответственности, с тем, чтобы к 2006 г. она составляла 100 млн. ф. ст. на одно событие / 200 млн. ф. ст. на год.

Начиная с 2002 г. к числу возмещаемых ущербов по риску терроризм относятся ущербы в имуществе предприятий и в связи с остановкой производства, вызванные всеми опасностями (ранее только от огня и взрыва). С 2003 г. покрывается ущерб от радиоактивного заражения в результате террористической атаки.

Австрия

В стране существует специальный пул по страхованию риска терроризм Terrorism pool.

Начиная с 1 января 2003 г. австрийский пул обеспечивает автоматическую защиту для коммерческих рисков до 5 млн. евро. Риски от 5 до 25 млн. евро могут быть переданы в пул при уплате дополнительной премии; риски, превышающие 25 млн. евро могут быть застрахованы на факультативной основе.

К числу исключений по условиям страхования относятся ущербы, вызванные биологическим и химическим заражением.

Максимальная ответственность пула составляет 50 млн. евро на год, ответственность каждого страховщика — участника пула определяется пропорционально его рыночной доле.

Риски, переданные в пул, перестраховываются на мировом рынке перестрахования. Емкость перестрахования составляет 150 млн. евро в год. В настоящее время рассматривается вопрос о возможности покрытия австрийским правительством ущерба, превышающего 200 млн. евро.

Франция

С 1 января 2002 г. под контролем государства действует специальный пул GAREAT (Gestion de l'assurance et de la rЙssurance des risques attenants et actes de terrorisme).

Пул страхует и соперестраховывает риски, превышающие 6 млн. евро, по полисам, обеспечивающим возмещение прямого ущерба в связи с огневыми и техническими рисками.

Пул действует по принципу среднегодового лимита убытка. За выплаты в пределах 400 млн. евро полностью отвечают прямые страховщики. За выплаты, превышающие 400 млн. евро, отвечают перестраховщики (договор второго уровня — 1,1 млрд. евро, превышающий 400 млн.; договор третьего уровня — 250 млн., превышающие 1,5 млрд. евро). Указанные договоры перестрахования заключаются на мировом рынке перестрахования. Четвертый уровень — неограниченная ответственность сверх 1,5 млрд. евро — гарантирован французским правительством через CCR (Caisse centrale de reassurance). CCR, в соответствии с национальным законодательством, перестраховывает страховые компании, предоставляющие покрытие на случай «естественных катастроф».

Германия

С 1 ноября 2002 г. в стране проводит операции специально созданная страховая компания Extremus Versicherungs-AG.

На страхование принимаются различные виды имущества юридических лиц (здания, отдельные помещения, инженерное и производственно-технологическое оборудование, инвентарь, товарно-материальные ценности и т. п.), если страховая сумма превышает 25 млн. евро на застрахованный объект/страховой полис. Среднегодовой лимит ответственности страховщика установлен в размере 1,5 млрд. евро. К числу страховых событий относятся: пожар, взрыв, умышленные действия третьих лиц, падение или столкновение летательных аппаратов, вызванные терактами.

Не подлежат возмещению убытки, вызванные военными действиями, гражданской войной и гражданскими беспорядками, воздействием ядерного взрыва, радиации или радиоактивного заражения, химического и биологического заражений, непредвиденной остановкой производства.

Extremus покупает перестрахованную защиту на сумму 3 млрд. евро на одно страховое событие. Договор первого уровня покрывает ущербы до 1,5 млрд. евро и заключается исключительно со страховщиками и перестраховщиками, работающими на немецком рынке. Договор второго уровня (1,5 млрд. евро и выше) размещается на мировом рынке перестрахования. Ущербы свыше 3 млрд. евро обеспечиваются государственной гарантией в 10 млрд. евро на каждый страховой случай. Государственная гарантия действует до конца 2005 г.

Соединенные Штаты Америки

26 ноября 2002 г. Президент США подписал Акт по страхованию террористических рисков — Terrorism Risk Insurance Act 2002 (TRIA 2002),

в соответствии с которым на период 2002–2005 гг. предусматривалась специальная программа участия правительства США в возмещении ущербов, вызванных террористическими актами. Впоследствии она была продлена

Для участия в программе необходимо соблюдения ряда условий. Противоправные действия должны квалифицироваться как террористическая атака государственными органами. Страховые компании должны предоставлять адекватные покрытия по риску терроризм в заключенных страховых договорах. Общий застрахованный ущерб должен превышать 5 млн. долл. США. Программа распространяется на страхование имущества, включая страхование на случай перерывов в производстве, и ответственности юридических лиц. Действие программы охватывает всех страховщиков, осуществляющих операции на территории США и заключающих договоры по соответствующим видам страхования.

Федеральное правительство может обеспечивать до 90 % превышения выплат над собственным удержанием страховщика. Удержание страховщика рассчитывается на основе данных об условиях страховых договоров (начисленные страховые премии, страховые суммы, размеры франшизы).

Владельцы полисов страхования имущества и ответственности, покрывающих риск терроризм, уплачивают дополнительные страховые премии, которые перечисляются страховыми компаниями в Федеральное казначейство.

Максимальная ответственность Федерального правительства и страховщиков установлена на уровне 100 млрд. долл. на каждый год действия программы.

Специальные схемы страхования существуют также в Австралии, Канаде, Нидерландах, Швейцарии, ЮАР, Израиле.

Кроме участия в специальных схемах страхования риска терроризм, крупные страховые компании заключают «традиционные» договоры страхования от террористических актов.

В качестве примера можно привести полис американской компании AIG Property Terrorism Insurance.

Это специальный полис страхования имущества американских многонациональных компаний (финансовых институтов, производственных и сельскохозяйственных предприятий, снабженческих и торговых организаций) от риска терроризм на территории США и за ее пределами.

Лимит ответственности страховщика по ущербу составляет 150 млн. долл.

Возмещению подлежат прямой ущерб имуществу и прямой ущерб, связанный с остановкой производства, вызванные пожаром, взрывом, падением летательных аппаратов в результате террористического акта. Стра-

хование от террористических актов может быть дополнением к договорам страхования имущества или осуществляться по отдельному договору.

Страховое покрытие строится по принципу страхового события — все ущербы, вызванные одной или сходными причинами, рассматриваются как один страховой случай.

Период простоя, по истечении которого возникает ответственность страховщика, составляет 30 дней.

Минимальная страховая премия составляет 50 тыс. долл. США.

Если территория страхования включает Нью-Йорк и другие главные города США, то это специально оговаривается в договоре. Обычно эти условия предполагают увеличение франшизы. На территориях других государств, где предусмотрено страхование от террористических актов на добровольной или обязательной основе, имущество может быть застраховано и на иных условиях. Исключается из территории страхования Великобритания, где соответствующее страхование осуществляется Pool Reinsurance Company Ltd.

Принятие решения о выплатах осуществляются в течение 48 часов после получения полного комплекта всех необходимых документов о страховом случае.

Для Российской Федерации развитие риска терроризма является вполне актуальным. По данным Федеральной службы безопасности с 1999 по 2005 гг. в РФ произошло более 1000 взрывов с признаками терроризма.

В 2002 г. в РФ был образован «антитеррористический пул», объединяющий 25 крупнейших страховых компаний с общим лимитом ответственности в 35 млн. долл. С этого времени было заключено более 500 договоров страхования рисков терроризма. Однако все эти договоры обращены на имущество: крупные торговые центры, банковские и производственные здания, посольства и т. д. А вот жизнь и здоровье потенциальных жертв пока в РФ не страхует никто.

31 марта 2005 г. в Государственную Думу поступил законопроект «Об обязательном страховании ответственности за вред, причиненный в результате террористической акции, совершенной в местах массового пребывания людей», не принятый до сих пор.

В силу катастрофического характера убытков от террористических актов, одним из условий поддержки страхования от терактов являются государственные гарантии. В заявлении «Аэрофлота» по проблемам страхования «военных» рисков говорится, что «ОАО «Аэрофлот» присоединяется к мнению Международной организации гражданской авиации (ИКАО), что террористические акции направлены против государств, а авиакомпании и инфраструктура воздушного транспорта просто используются в качестве средства. В этой ситуации Правительство России должно обратить вни-

мание на необходимость поддержки российских авиаперевозчиков предоставлением государственных гарантий по страхованию гражданской ответственности по рискам терроризма. От решения Правительства РФ зависит развитие и финансовая устойчивость гражданской авиации».

Вместе с тем, до сих пор остается нерешенным ряд принципиальных вопросов:

- каковы могут быть объекты страхования;
- каковы должны быть формы страхования: обязательная или добровольная;
- какова должна быть степень участия государства в обеспечении гарантий этого вида страхования;
- каковы могут быть лимиты ответственности в случае нанесения вреда жизни или здоровью пострадавшего;
- как должна формироваться цена по данному виду страхования.

По всем этим вопросам нет единства мнений или отсутствуют нормативные документы, что обуславливает актуальность исследований по разработке методических основ и научно-практических рекомендаций по осуществлению страхования от террористических актов с учетом международного опыта является целью данного исследования.

Целесообразность страхования риска «терроризм» в Российской Федерации определяется следующими факторами:

- стимулировать эксплуатантов опасных производств и устроителей массовых мероприятий снижать степень подверженности застрахованных объектов террористическим актам;
- определить гарантированные размеры компенсации жертвам и пострадавшим в результате террористического акта;
- определить порядок и источники компенсации ущерба экологии в результате террористического акта;
- унифицировать порядок компенсации убытков в результате террористического акта в рамках добровольного страхования.

Использование механизма страхования для возмещения ущерба, причиненного в результате террористического акта, предполагает, с одной стороны, максимальное использование потенциала, ранее созданных правовых институтов и уже существующих видов страховых отношений в смысле приспособления их к особенностям страхования риска «террористический акт», с другой — разработку новых норм права и классов страхования, призванных обеспечить возмещение вреда, причиненного в результате террористических актов.

В настоящее время на отечественном страховом рынке представлены некоторые виды страховых продуктов, включающие защиту от риска «терроризм», в то время как спрос на подобные страховые продукты еще только начинает формироваться. В условиях дисбаланса между спросом и предложением на рынке страхования (перестрахования) риска «терроризм» могут использоваться некоторые рекомендации, разработанные на основе международного опыта подобного страхования. В частности, возможно:

- введение обязательного страхования: все имущественные риски автоматически включают риск «террористический акт» с целью финансирования и обеспечения возможных потерь;
- введение дополнительной нетто-ставки в страховые взносы по страхованию иному, чем страхование жизни: т. е. дополнительный платеж, который позволит собрать адекватную сумму страховых взносов для максимального вовлечения рынка перестрахования, в том числе международного;
- распределение бремени потерь, т. е. процент участия в возможных последствиях всех участников (а именно страхователей, страховщиков, перестраховщиков, а также государства) должен быть равномерным, при этом: часть убытка лежит на страхователе (застрахованном); прямые страховщики собирают определенную долю страхового взноса, а остаток вносят в централизованные фонды; небольшие убытки непосредственно выплачиваются прямыми страховщиками, а крупные убытки компенсируются с помощью объединений/пулов; пул прибегает к перестрахованию на непропорциональной основе, тем самым вовлекается в рынок перестрахования, что, в свою очередь, позволяет достигнуть равномерного распределения возможных убытков.

Литература

[1] Вестник авиации и космонавтики, 2005, № 1, с. 67.

[2] Terrorism Risks in Property Insurance and their Insurability after 11 September 2001 // Swiss Re, 2003, N 1; Турбина К. Е. Правовые аспекты страхования на случай терроризма // Страховое право, 2004, № 4; Турбина К. Е., Мальковская М. А. Организация страховой защиты на случай терроризма // Финансы, 2004, № 7.

Имитационные модели и игры в противодействии терроризму

Д. Н. Кавтарадзе

Форс-мажорные обстоятельства — это хорошо спланированная акция, только внешне выглядящая как случайность.

Мнение страховых агентов

Аннотация

Экстремальные ситуации требуют эффективных инструментов управления: долгосрочной стратегии, подготовленных прогнозных моделей и сценариев возможного развития событий, сил и средств быстрого реагирования, расчета социально допустимого риска и др.

Штабные учения, деловые игры, имитационные игровые модели, имеют в России многовековую практику и могут применяться в современных условиях проявления экстремальных явлений и терроризма.

Введение

Терроризм как явление приобрел характер, значимый для государственной целостности.

Противодействие этому явлению потребовало мобилизации как силовых, так и гуманитарных ресурсов. Поиск новых средств анализа этого явления привел к созданию системных и динамических моделей, сложность которых создала психологический разрыв между разработчиками моделей и их потребителями. Преодолеть этот разрыв помогают имитационные игровые модели. Участники игр, принимая решения, осваивают модели, действуют в условиях приближенных к реальности, входят в понимание проблемы в процессе личной деятельности, в результате чего обретается понимание сложности проблемы, и находятся пути ее решения.

В истории отечественных разработок военных игр содержится опыт, предостерегающий нас от избыточных надежд на восприятие результатов удачно проведенной игры как, безусловно, значимой, убедительной[1], что убедительно продемонстрировала имитационная модель «ядерной зимы» (рис. 1).

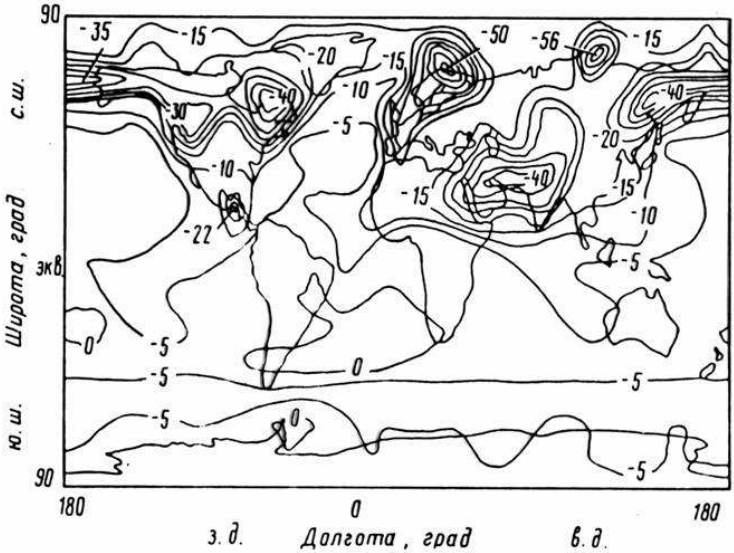


Рис. 1. Имитационная модель «ядерной зимы» показала наступление глобальных последствий не оставляющих шансов на выживание. Географическое распределение изменения температуры воздуха у земной поверхности на 40-е сутки после ядерного конфликта

Обеспечение целостного восприятия проблемы позволяет придать значение деталям, «малым рискам», которые обычно воспринимаются как малосущественные и, даже, как несуществующие[2]. Эти особенности психологии восприятия учитываются и успешно преодолеваются в имитационных играх, благодаря действиям участников и проявлению «неожиданных последствий» буквально иллюстрируя притчу:

[1] Kavtaradze Dmitri. Simulation Games: Limits of Impact. 37th Annual Conference of International Simulation and Gaming Association (ISAGA). St. Petersburg. 3–7 July 2006.

[2] Ковалев Е. Е., Иванов В. И. и др. Новая техника и вопросы безопасности человека (методологические аспекты), Вопр. философии, 1981, **1**, 5, с. 49–59.

Не было гвоздя —
Подкова пропала.
Не было подковы —
Лошадь захромала.
Лошадь захромала —
Командир убит.
Конница разбита —
Армия бежит.
Враг вступает в город,
Пленных не щадя,
Оттого, что в кузнице
Не было гвоздя.

Самуил Маршак

Восприятие мелочи достигается навыком профессионализма подобно знакомой многим картине: в кабинет врача входит пациент. После нескольких шагов врач произносит:

— крестцовый радикулит.
— Да. А как вы узнали?
— Вы «фиксируете спину» (т. е. она искусственно напряжена больным, чтобы избежать боли при движении).

Задача научить восприятию малых рисков требует преодоления «гипноза обыденного сознания», «здравого смысла», выходу за границы обыденного сознания. Этому могут помочь специальные упражнения. Например, такое. Посмотрите в течение 3–4 секунд на рис. 2, закройте рисунок и запишите на листке как стояли фигуры.

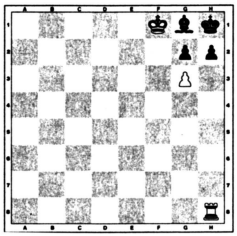


Рис. 2. Постарайтесь за 3–4 секунды запомнить, как стоят шахматные фигуры

Записали?! Посмотрите еще раз и сверьте, правильно ли вы восприняли шахматную композицию. Скорее всего, вполне полно. Отлично! А вот одному человеку не удалось. Он так прямо и заявил: «Да не помню я, как они стояли, только белые дают мат в два хода!». Это был шахматный гроссмейстер. Они увидел смысл расположения фигур, а мы с вами — порядок.

Здесь проявляются различные структуры мышления, которые в быту мы называем разными логиками. Преодолеть расстояние между логическими конструкциями необычайно трудно, это требует сомнения в собственной

правоте (иначе, зачем нам «другая логика»?), а сомнение может и должно получить доказательное подтверждение. Этим средством выступает практика, в том числе практика имитационной игры. Важно, что результаты практики одновременно наблюдают многие участники, что не гарантирует одинаковых выводов, но уменьшает меру взаимного непонимания [3)].

Имитационные игры — это средства постижения смысла. В управлении сложными системами смысл часто ускользает от человека, а пустяковые «человеческие детали поведения и их оценки» определяют вероятность аварии, отказа [4)].

Это в полной мере относится к масштабным событиям, включая аварию на ЧАЭС: среди шести причин которая, каждой была «невозможной», и имела место в результате человеческого поведения [5)].

В различных отраслях хозяйства постепенно находят применение попытки осмысления, а в ряде случаев, математического анализа случаев отказа, поломки, выхода из строя, аварий, чрезвычайных ситуаций включая террористические акты. Можно отметить постепенный переход от чисто описательных исследований к попыткам обобщения, выявления природы вероятностных процессов, их моделирования и, по возможности, прогнозирования и предупреждения.

Так математическая модель [6)] показала и объяснила, что причиной выхода из строя элементов системы вне зоны форс-мажорных обстоятельств (после окончания влияния внешних воздействий) являются *внутренние источники возмущений*. Существенной особенностью построенной модели является возможность выхода из строя при распространении импульсных воздействий по системе наиболее надежных элементов. Этот факт красноречиво подчеркивает *прямую зависимость надежности элемента от его положения в структуре*, *а также зависимость стойкости всей системы от выбранной при проектировании структуры*. Найденные в ходе исследования модели явление относятся к классу синергетических эффектов [7)], прогнозирование которых на начальных этапах исследования не тривиально.

[3)] Следуя проф. А. А. Брудному, повторим: «дураков не так уж много: люди просто не понимают друг друга».

[4)] Аварии на атомных электростанциях. МИФИ, 1998.

[5)] Информация об аварии на Чернобыльской АЭС и ее последствиях, подготовленная для МАГАТЭ. Атомная энергия, 1986. Т. 61, вып. 5, с. 301–320.

[6)] Кочкаров А. А., Малинецкий Г. Г. Обеспечение стойкости сложных систем. Структурные аспекты. ИПМ им. М. В. Келдыша, РАН, Москва, 2005. `http://www.keldysh.ru/papers/2005/prep53/prep2005_53.html`.

[7)] Малинецкий Г. Г. Хаос. Структуры. Вычислительный эксперимент: Введение в синергетику. Сер. «Кибернетика: неограниченные возможности и возможные ограничения». М.: Наука, 1997.

Это подтверждает правомерность распространения закона Ч. Перроу «нормальных аварий» на широкий круг систем, как социальных, так и техногенных. Имеет место системный эффект, для восприятия которого необходим охват всей системы, что в линейной системе управления представляет психологическую и интеллектуальную проблему, однако воспроизводима в имитационных игровых моделях.

Нарастание интенсивности террористических актов в различных странах, преследующих достижение максимальной социальной реакции, позволило нам в 2005 г. выдвинуть рабочую гипотезу о применимости к этому явлению закона Вебера — Фехнера, согласно которому при увеличении силы раздражения в геометрической прогрессии (1, 2, 4, 8, 16 и т. д.) интенсивность ощущения увеличивается в арифметической прогрессии (1, 2, 3, 4, 5 и т. д.). Этот закон устанавливает существование логарифмической зависимости силы ощущения от физической интенсивности раздражителя. Логарифмическая зависимость силы *ощущения* (E) от физической интенсивности *раздражителя* (P): $E = k \log P + c$, где k и c — некоторые постоянные, определяемые данной *сенсорной системой*. В отношении рассматриваемой проблемы функции сенсорной системы выполняют СМИ.

Наша рабочая гипотеза получила подтверждение исследованиями группы английских ученых в 2006 г. под руководством профессора Оксфордского университета Нейла Джонсона (Neil Johnson). Им удалось выявить математические закономерности, характеризующие террористическую активность как таковую, безотносительно к конкретной специфике регионов, где она наблюдается. Статистика приводящих к жертвам терактов подчиняется экспоненциальной зависимости. Отметим, что это открывает возможность предсказания уровня активности террористических групп в отдельных регионах на основании уже имеющейся статистики на основании базовой динамики этого явления, так же как ранее это было сделано при моделировании распространения эпидемии гриппа или другого контагиозного заболевания.

Разработка гуманитарных методов анализа и противодействия экстремизму привела к формулированию ряда положений для построения имитационных динамических моделей этих событий и освоения навыков управления их развитием. В основу имитационной игры «Координация»[8)], разработанной на факультете государственного управления МГУ, была принята базовая динамика развития экстремальной ситуации по модели Ричмонда. Рассмотрение экстремальной ситуации проводилось в определенном пространственно-временном интервале — хронотопе, за пределами которого,

[8)] Рукопись и отчёт по теме «Социально-психологические методы повышения эффективности антитеррористических мероприятий», МГУ, 2006.

безопасность как качество системы не рассматривается и не обеспечивается. Было учтено, что восприятие малых рисков психологически приводит к представлению, что их вообще нет. Однако действительность иная [9]:

«Полиция приграничных районов Германии и Франции ищет связку ключей от дверей ядерного центра в Филиппсбурге. Ее потерял оператор этой крупнейшей атомной электростанции, расположенной в земле Баден-Вюртенберг в непосредственной близости от границы с Францией. В связке находилось 12 ключей, включая и от дверей в так называемой «красной зоне», куда доступ ограничен даже для работников станции. В результате власти были вынуждены в экстренном порядке сменить 150 замков на всех дверях АЭС с тем, чтобы исключить возможное проникновение посторонних лиц. Между тем пока не ясно, были ключи похищены с определенной целью или просто потеряны беспечным сотрудником АЭС. По факту пропажи ключей уже возбуждено уголовное дело».

При построении имитационной игры в процессе принятия решений и выработки мер противодействия терроризму был учтён закон Акоффа — сложность принятия решения не линейно возрастает по мере увеличения информации: чем больше объем массив информации, тем сложнее, дольше принимается решение. Таким образом, приоритет предпринимаемых действий и противодействий оказывается в прямой зависимости от структурной организации противостоящих сторон.

Таким образом, гуманитарный анализ обнаруживает ряд психологических барьеров, препятствующих мерам противодействию терроризму: не восприятие малых вероятностей, их ничтожная оценка, неадекватный перенос представлений о поведении технических систем на социальные процессы, структурное несоответствие противодействующих структур структуре организации противника, неопределенность в рассмотрении обратной связи и ее оценке, не определенность хронотопа события [10], не разработанность механизма координации противодействия терроризму, включая преемственность в системе госслужбы и др.

При разработке имитационной игры возникает обобщение многообразия экстремальных ситуаций как проблемы не решенной интеллектуально. В связи с таким представлением была поставлена и решена задача разработки и испытания имитационной (деловой) игры [11], моделирующей

---

[9] В Германии утеряны ключи от ядерного центра 9.04.2006. Страна.Ru. ИТАР-ТАСС.

[10] Surin A., Kavtaradze D. Paradoxes of Security: Limits of Efficiency. Proceedings of the Third International Security Conference, ISC Security, Terrorism and Privacy in Information Society, Düsseldorf, 27–28 October, 2005, p. 209–221.

[11] См. Duke Richard Games. The Futures Language, N.Y., 1964, Greenblat Cathy Stein Designing Games and Simulations. An Illustrated Handbook, SAGE, 1988; Кавтарадзе Д. Н.

противодействие терроризму и выработку государственной долгосрочной стратегии.

Цель усилий участников — приобретение представлений, адекватных проблеме, и опыта управленческих решений, выработки документа отвечающего уровню федеральной (национальной) стратегии на основе опыта долговременной имитации взаимодействующих систем.

Разработанная имитационная игра «Координация» предназначена для групп государственных служащих высшего и среднего звеньев от 8 до 25 человек, проводится в течение 4–5 часов и направлена на целостное восприятие проблемы, учета временной протяженности, получение опыта реализации принимаемых концепций и стратегий, учета последствий и внесение корректив в изначальную стратегию. Психологическая гипотеза разработки игры заключалась в том, что государственные служащие должны *одновременно*:

- осваивать проблему в процессе ее решения,
- на опыте приходить к координации усилий,
- разрабатывать стратегический управленческий документ.

Имитационный игровой эксперимент — позволяет группе вначале приобрести совместный опыт действий, затем путем проб, анализа ошибок выработать внутренне непротиворечивый образ проблемы и на основе имитации управления противодействия терроризму выработать ряд стратегий. Таким образом, стратегия — результат опыта освоения проблемы конкретной группой участников, целостного видения критических узлов и попыток их управленческого решения. Игра рассматривается как инструмент выработки проекта государственного документа федерального и международного уровня.

Для разработки модели была принята структура вертикали государственной организации (рис. 3).

Разработка «масштабных мероприятий» издавна требовала различных средств и инструментов. Вспомним, что Наполеон Бонапарт проводил разработку планов баталий, втыкая булавки с разноцветными головками на карту боевых действий. Технические возможности моделирования несоизмеримо выросли, однако человеческое восприятие остается ограниченным и, подчас, неспособно адекватно воспринять и использовать громаду технических удобств и сервиса. Неудивительно, что гуманитарные методы находят все большее применение в разработке и обеспечении сложных систем.

Обучение и игра, М.: 1998; Крюков М. М. Эколого-экономическое игровое имитационное моделирование: методический аспект, М.: ТЕИС, 2006 и др.

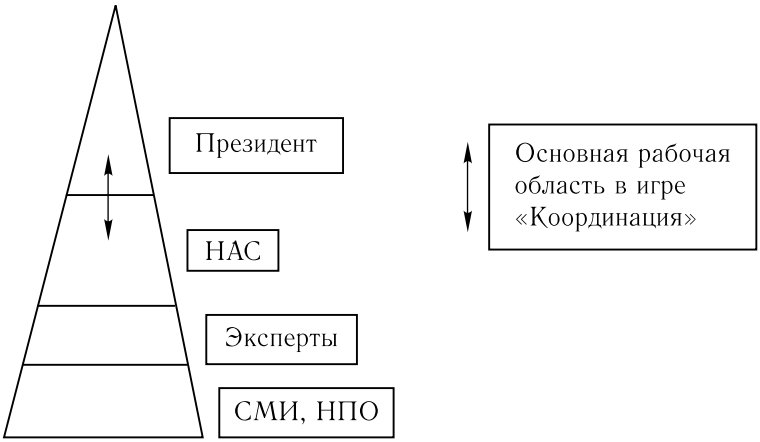


Рис. 3. Структура вертикальной организации имитационной игры «Координация»

Описание целостной картины взаимодействия, важнейшая, определяющая роль контекста событий, вполне успешно оформляется в сценарных понятиях.

Трагически провидческим оказываются произведения литературы. В 1999 г. Том Клэнси опубликовал книги «Долг чести» и «Слово президента», где он с поразительной точностью описал трагедию 11 сентября 2001 года. В 2002 году опубликован сценарий фильма Н. Собакарь «Постановщик» [12)], раскрывший методом художественного анализа возможный механизм разработки и осуществления террористического акта. Сценарий остался вне анализа антитеррористических служб, что стало понятным лишь после событий в Беслане, в которых поразительно совпадают сценарий и реальные драматические события.

Сценарный подход в разработке имитационных моделей привёл к признанию того, что получаемый «инструмент» обоюдоострый: «В открытой печати сообщалось о парадоксальных побочных результатах разработки в США стратегий борьбы с терроризмом и их испытания: «в Лос-Аламосе (США) создали антитеррористическую «матрицу» — математическую модель возможных террористических атак. Модель воспроизводит американские города вместе с жителями и инфраструктурой и позволяет увидеть, к чему может привести то или иное неожиданное воздействие. Однако, эта модель представляет собой инструмент… состязания с террористами. Судите сами: «Детали эксперимента не разглашаются. Как заметил один из его участников, Джеймс Смит, если доступ к модели получат злоумышлен-

[12)] Собакарь Н. Постановщик. Искусство кино, № 8, 2002.

ники, она может подсказать им наиболее уязвимые места. «Это полноценное руководство по совершению масштабных преступлений», — сообщил он журналистам, — «мы пытаемся быть лучшими террористами, чем сами террористы». Некоторые эксперты сомневаются в целесообразности проекта. По их словам, имитация каждой атаки обходится в десятки миллионов долларов, тогда как сама модель претендует на описание слишком сложных систем и далека от совершенства» [13)].

До сих пор остается вне должного анализа и учета фактор отношений доверия в общинах, этнических сообществах. Между тем, эти виды объединений основаны на доверии группы неформальных участников. Например, Интернет-энциклопедия самодеятельных авторов — Wikipedia — имеет более трех миллионов авторов. Которые лично доверяют друг другу — это компьютерное братство доверия. Вспомним Э. Хемингуэя — «все, что у них осталось (солдат, вернувшихся на родину — США — Д. К.) — это чувство фронтового братства» [14)]. Следует признать правомерность объединения (даже дистантного) людей по принципу взаимного, априорного доверия, братства без кавычек. Появление новых социальных факторов в системе «государство — террористические действия» может быть исследовано в имитационных играх.

Для получения представления об имитационной игре «Координация» приведем пример сценария и картосхему (рис. 4).

После размещения всех групп в различных комнатах свободное передвижение прекращается. При необходимости используется нарочный, локальная сеть интернет с выделенным сервером. Питание приносится в комнату. Посещение туалетных комнат по одному человеку с сопровождающим так же, как абитуриентов во время приемных экзаменов. Пользование мобильными телефонами не разрешается. Принимается размерность времени 20 минут = 1 год в игре.

1 *год*. Зачитывается послание — желаемые элементы стратегии — Президента для НАС (Национальный антитеррористический совет). Знакомство игроков с документами, должностными обязанностями и консультация с экспертами, включая телефонные звонки, Интернет. Эксперты распределяют обязанности, выбирают руководителя заседаний, уточняют структуру, изучают документы. Распределяется бюджет государства на этот год (заполняются экономические карточки). Готовится записка в НАС. После ее рассмотрения и оценки предложений НАС направляет предложения записка Президенту. Каждые 15–30 минут вскрывается конверт «Случайное событие».

[13)] Washington Post, Lenta.ru, 2005.

[14)] Хемингуэй Э. Прощай, оружие!, М.: 2005.

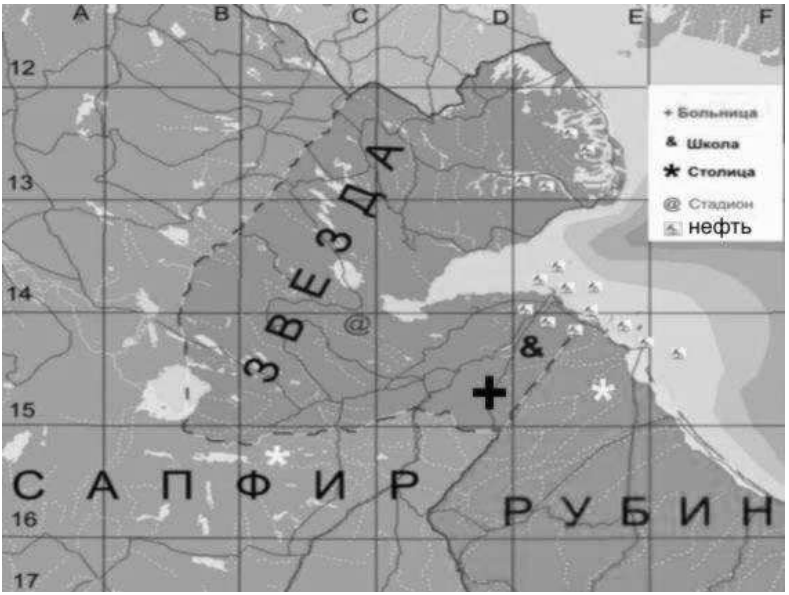


Рис. 4. Картосхема региона

2 *год*. Президент поручает НАС разработать (один-два вариантов стратегии) и предлагает ускорить работу и т. д. НАС проводит в своей комнате встречу с двумя экспертами (возможен вариант передачи экспертам ТЗ). Каждые 20 минут вскрывается конверт «Случайное событие». Эксперты получают информацию и видеозапись действий террористов. Запрашивают статистику, документы, проводят консультации, пользуясь интернетом, телефоном. Эксперты и НАС получают информацию от СМИ. Выполняют указание и предлагают вариант(ы) стратегий в записке НАС. После ее рассмотрения и оценки предложений НАС направляет предложения записка Президенту. Распределяется государственный бюджет противодействия терроризму на этот год.

3 *год*. Внеочередное вскрытие конверта «случайное событие». Эксперты получают информацию и видеозапись действий террористов. Поручение Президента подготовить варианты решения по событию, министры с экспертами экстренно заседают и совместно принимают варианты решения. Эксперты и НАС получают информацию от СМИ. Передают предложения с фельдъегерем Президенту, и он делает выбор. Решение публикуется в СМИ. СМИ сообщило о реакции общества на предложенное НАС решение. Выясняется, что решение не выполнено. Начат поиск виновного.

Члены НАС и эксперты осознают опасность тупикового решения. Распределяется бюджет государства на этот год.

4 *год*. НАС, эксперты запрашивают администратора игры о статистических данных, включая рейтинги членов НАС. СМИ публикует результаты опроса общественного мнения об эффективности деятельности государственных служб. Внеочередное вскрытие конверта «Случайное событие». Распределяется бюджет государства на этот год.

5 *год*. Отчет председателя экспертов перед НАС. Отчет НАС Президенту. Внеочередное вскрытие конверта «Случайное событие». Распределяется бюджет государства на этот год.

Пресс-конференция НАС со СМИ. Журналисты представляют различные углы освещения проблемы. Представитель НАС отбирает вопросы, поступившие от журналистов, и отсевает 30 % по своему усмотрению.

Выборы Президента (обеспечивается административной группой).

Вторая «пятилетка»

В случае избрания нового Президента состав НАС меняется на 80 %, экспертов на 30 %. Смена состава обеспечивается администратором игры из резерва участников. Новые исполнители ролей знакомятся со своими задачами, прежние участники могут наблюдать дальнейший ход игры по телевидению.

Повторяется цикл 1–5 года.

Третья «пятилетка»

Проводится также как и вторая.

Завершение имитации определяется руководителем игры. Участникам предлагают короткий отдых до 10 минут и написание короткого отчета.

Одновременно короткие отчеты пишут наблюдатели.

Через полчаса проводится послеигровое обсуждение проблемы.

Оно проводится руководителем НАС при поддержке администратора игры и длится не более 30–45 минут.

Роли Президента и лидеров экстремистов не озвучиваются — они представлены в «Координации» виртуально через группу управления игрой.

После завершения обсуждения администратор игры просит внести дополнения в отчеты участников и подводит процедурный итог сессии имитационной игры и рассматривает варианты текстов «Стратегии».

В основу структуры игры была положена системно-динамическая модель Б. Ричмонда описывающая палестино-израильский конфликт на протяжении длительного времени. Задача заключалась в разработке игры, в результате участия в которой создавался целостный образ проблемы и приобретался опыт управления конфликтом как системой. Приве-

дем пример причинно-следственной диаграммы, освоение которой простым разглядыванием не удается (рис. 5). Однако в процессе деятельности в такой системе удается вначале лично освоить эффективное поведение в ней, а затем осмысленно рассматривать предложенные связи уже как отражение совершенных действий и потому понятных.

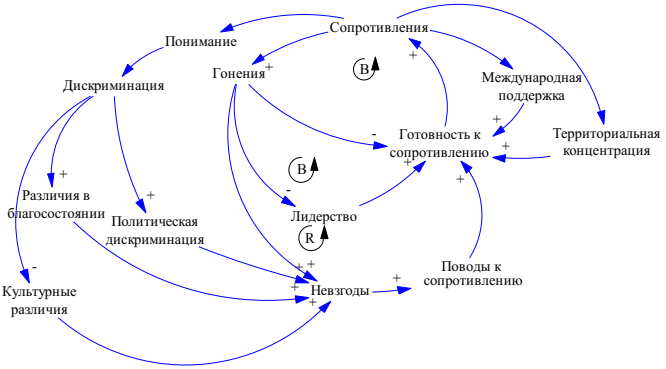


Рис. 5. Каузальная схема Б. Ричмонда, описывающая палестино-израильский конфликт на протяжении длительного времени (перевод А. О. Брылевой)

Сложность современного мира, снижение возможности *прямого* государственного контроля развития, а подчас, и проявления экстремизма делает необходимым разработку опосредованных, непрямых мер обеспечения государством своих интересов, служащих безопасности граждан. Эти методы относятся к гуманитарной сфере и требуют определения границ их эффективности.

В настоящий период времени становления государственности в России имеет место поиск различных форм применения гуманитарных методов, в том числе для ответа на вопрос «что такое безопасность?» в мире сверхсложных систем (Perrow, 1984). Закон постулирует: «сверхсложные системы несут риск сами в себе. При отказе одного или двух элементов, сверхсложная система приобретает свое собственное поведение, научно предвидеть которое не удается. Эти «побочные», но неотъемлемые свойства сверхсложных систем стали определять границы их применения. Зависимость сложности систем и риска отображается графически (рис. 6).

Опасность и безопасность — взаимодействующие системы. Поэтому опережение создания мер безопасности по отношению к опасности несет новые риски, хотя и отсроченные. Конкретные виды обеспечения безопасности мозаичны. Интегрируясь, они становятся все более универсальными, но приобретают также черты сверхсложных систем, которые имеют

Рис. 6. Интервал социально приемлемого риска при разработке новой технологии и технических устройств (Кавтарадзе, 1994)

собственные риски. Поскольку время действия системы безопасности не бывает вечным, то необходим расчет жизни системы безопасности и учет приоритетов разных субъектов безопасности. Отметим практически полное отсутствие анализа «логики неудач» [15)] и причин их порождающих в работе систем безопасности [16)], за исключением отдельных журналистских расследований. Имитационные игры с необходимостью обеспечивают проведение такого анализа.

Гуманитарные меры эффективны, будучи организованы в идеологическую систему, и практику толерантности. Представляется, что базой для выстраивания и совершенствования этой системы послужила ФКЦП по проблеме профилактики экстремизма (утверждена в 2001 г.) как практически ориентированная научная программа. Эта ФКЦП подготовила возможность рассмотрения проблемы в более широком спектре. Одним из направлений исследований стало разработка и апробация методов моделирования гуманитарных методов противодействия терроризму. Её развитие поможет планировать *внутренне непротиворечивую систему мер* снижения рисков экстремизма и терроризма. Научная основа необходима в силу наибольших гарантий состоятельности как её замысла, так и её управлением.

Имеет место становление как собственно государственных институтов и мер противодействия терроризму, так и осмысление, и изучение его природы, ресурсов и потенциала идеологической и социальной экспансии.

Поскольку современные теракты — результат теоретической и организационной подготовки сравним элементы военных и террористических доктрин (см. табл. 1). Иными словами, следует рассмотреть как теоретическую базу этого явления, так и практическую сторону их осуществления для их должного отражения в содержании моделей.

[15)] Дернер Д. Логика неудач, Смысл, 1997.

[16)] Многоплановый анализ хода чеченской компании содержится в книге А. Куликов, С. Лембик. Чеченский узел. Хроника вооруженного конфликта 1994–1996, М.: 2000, 304 с.

Таблица 1

Военные действия	**Терроризм**
Бесконтактность	Внетерриториальность
Информационная война	Использование СМИ
Точечные высокоточные удары	Точечные, «локальные» цели
Новые виды оружия	Заимствование у ВС нового оружия
Новый стандарт войны	Новый стандарт акта терроризма (пояс смертника)
Выявление и уничтожение базы противника	Восхождение уровня целей и смыкание с военными целями государства.

Послеигровой анализ и обсуждение позволяют ответить на вопросы об «устройстве» игры [17] Следует предостеречь читателя от попыток показать слушателям каузальную схему до начала игры и дать комментарии. Понимание схемы и модели требует личного пережитого опыта как основы осмысления графической схемы. При этом особое внимание необходимо уделить этнополитическим конфликтам [18].

Имитационные игры открывают аналитические, управленческие и обучающие возможности и позволяют учесть последствия ошибок в управлении экстремальными событиями [19]. Таким образом, участниками достигается [20] *понимание* этого сложного явления.

[17] Barry Richmond, Chris Soderquist (2001). Адрес модели в Интернете: `http://www.iseesystems.com/resources/SOTM/conflict.zip`.

[18] Кавтарадзе С. Д. Этнополитические конфликты на постсоветском пространстве, 2005; Bahadir K. A., Victor Asal, The dynamic of ethnic terrorism. System Dynamics Conference Proceedings, 2004

[19] Merilyn P. Moving from Blame to Accountability. Organizational Learning at Work. Embracig the challenges of the New Workplace, Pegasus Communication Inc., 1998, p. 75–87; Moorhead Kennedy, Martha Keys Hostage Crisis, NY, 1988.

[20] Важные консультации были получены от Jeannette Heldens (Radboud Universiteit Nijmegen, The Netherlands), Sharyl Cross (George C.Marshall European Center For Security Studies, Germany), Victor Asal (SUNY, USA).

Prototypes and Schemata of Terrorism: Semantic Mapping and Problem Solving Processes

A. A. Brudny, E. S. Molchanova

The paper is designed to explore two parts of the usual knowledge about terrorism. The first, prototypical part is used to create a "University students"' definition of terrorism. The second, schematic part shows a communicational function of terrorist act, no matter how awful the consequences of the act could be. The authors predict that, as any communication, terrorism as a phenomenon will exist until it will be considered to be functional even among a few groups of people.

Creating a concept is one of the first steps in the process of explanation some phenomenon in order to give to the creator and to the others an illusion of its understanding. This process is now described (Rob Plotnik, 2002) with the help of two main terms: *prototypes* and *schemata*. The prototype has been defined as a hypothetical, "most typical" instance of a category (Anderson, 1980), while schema refers to a unit of knowledge that consists of linked actions or decisions (John Best, 1995). So, usual knowledge about something may be relatively divided into two parts: prototypical and schematic. Prototypical part is absorbed from the number of the most common answers on question "what is…?" This part of the concept is an abstraction — an average mental image of all available representations of a phenomenon. The schematic part includes the average decisions formed on the basis of the principle "If (what is)…. That…" These two parts of a concept are dynamic and changeable according to the evolution of the phenomenon itself. We would like to accent the bilateral link between the external, relatively "independent" and "real" characteristics of something and the process of concept creation. The more loosed and complex the thing is, the more the number of its representations, the more indefinite its prototype and the more ambiguous the process of problem solving could be.

This paper is designed to research "what is…" and "if…that…" parts of "*terrorism*" and to predict some possible ways of evolution both the concept and the phenomenon.

The first part of knowledge: "what is terrorism?"

The official notion of terrorism is defined by Title 22 of the U.S. Code as *politically motivated violence perpetrated in a clandestine manner against noncombatants* (cited by Charles L. Ruby, 2002). This definition includes four propositions:

1) *terrorism* is a violence;
2) *terrorism* is politically motivated (action);
3) *terrorism* is (an action) perpetrated in a clandestine manner;
4) *terrorism* is (an action) against noncombatants.

So, the "official" branch of the semantic tree may be represented in the following way:

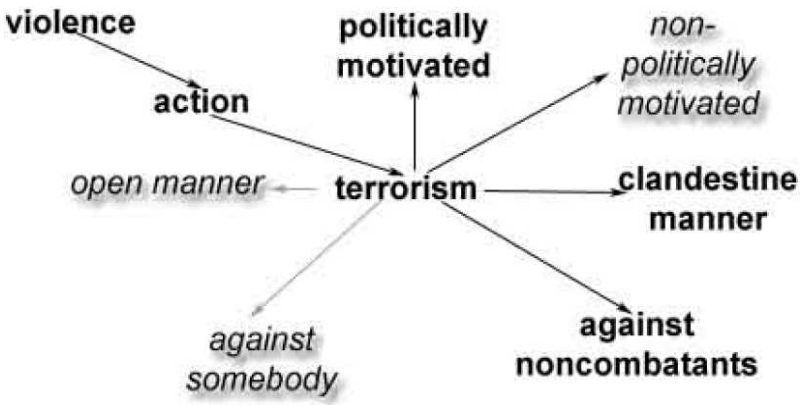


Fig. 1. A part of a semantic tree of "terrorism"

The set is loose and it demonstrates the possible ways (they are shown in gray letters) of widening both the concept and the phenomenon. Only by generation this simple set we may receive three additional hypotheses about terrorism: it may be (1) non-political, (2) perpetrated in a non-clandestine (open) manner (3) against various groups of people. Interestingly, Jerrold M. Post, giving his categorization of terrorism, emphasizes the existence of political and *non-political* (criminal and pathological) terrorism (Jerrold M. Post, 2002).

In order to create a "non-official" prototypical part of *terrorism* in University students we asked sixty volunteers to answer two simple questions ("What is terrorism?" and "What terrorisms are there?") and then we de-

livered a simple ranking procedure to define a "core" and "periphery" of the semantic set which was the result of semantic mapping process.

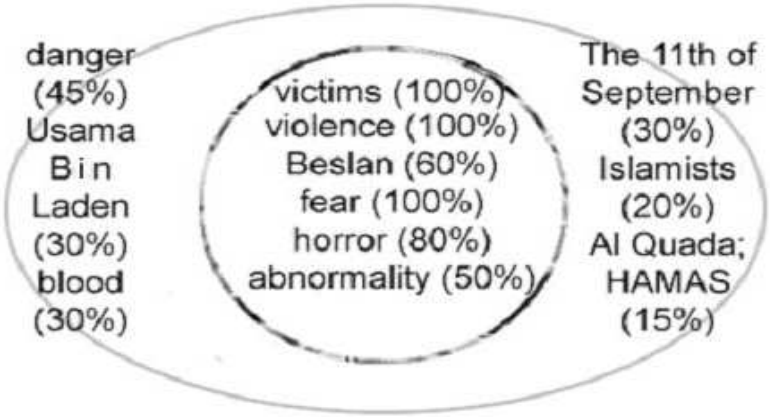


Fig. 2. "What is terrorism?" Two levels of core of the semantic set

About 50% of our respondents consider terrorism to be a kind of "abnormality" in the meaning of abnormal behavior. Although the notion of abnormal behavior is polysemantic and includes the definition of, at least, four different types of what is "normal" and "abnormal", the term "abnormality" is closely associated with the term "psychic disorder". Post (Post, 1984, 1987, 1990) in his comparative researches on the psychology of terrorists does not reveal major psychopathology, agreeing with the finding of Crenshaw "the outstanding common characteristic of terrorists is their normality" (Crenshaw, 1981).

Figure 3 demonstrates the results of a similar procedure with the answers on "What terrorisms are there?"

Interestingly that the adjective "political" is only in the fourth position, nevertheless, it is in the very core of the set.

Figure 4 demonstrates our trial to create a definition and classification of terrorism on the basis of the core of the semantic set in sixty University students.

So, *terrorism*, according to University students,*is a differently motivated violence. The form of terrorism depends on* (1) *its diffusion* (*international terrorism*), (2) *an object and a subject of violence* (*domestic terrorism*, *professional terrorism*) *and* (3) *open or clandestine manner of terrorist act. Victims and fearful states of mind are obligatory consequences*.

Fig. 3. What terrorisms are there? Core of the semantic set

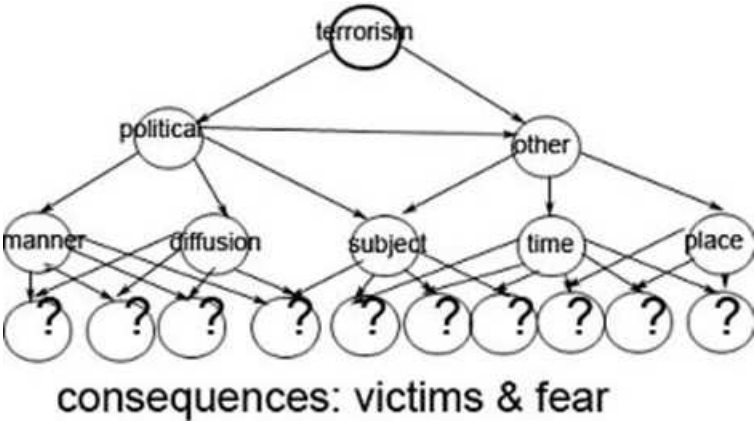


Fig. 4. Classification matrix of the notion

The second part of knowledge: "If (terrorism)...that..."

The second, schematic part of the concept is the basis of individual solving problem processes and plays a programming role in case of definite (terrorist) conditions. If (terrorism), that ...(what I am going (1) to do (2) to feel (3) to see (4) to hear (4) to judge at the moment of terrorist act, just after the event and some time after the event)? If terrorism, what my model of mind would be? If terrorism, what my emotional state would be? If terrorism, could I become a victim? a terrorist? The answers on these questions and many others provide a

kind of "programmed" solving problem process and, what is probably of more importance, may save or change individual sense of significance. We propose to divide the schema of the concept into two parts: the first part should be consciousness with the main primary goal to defense somebody's sense of significance. Second, unconsciousness part is really programming algorithm and it can be clarified only at the moment of definite circumstances.

In order to analyze the second, schematic part of the concept, we asked our sixty volunteers to complete the simple sentence "If terrorism, that…" They wrote all possible completions of the sentence during five minutes without hesitation and then stopped. The same ranking procedure was delivered to pick up the most frequently occurring variants, which are shown on the figure 5.

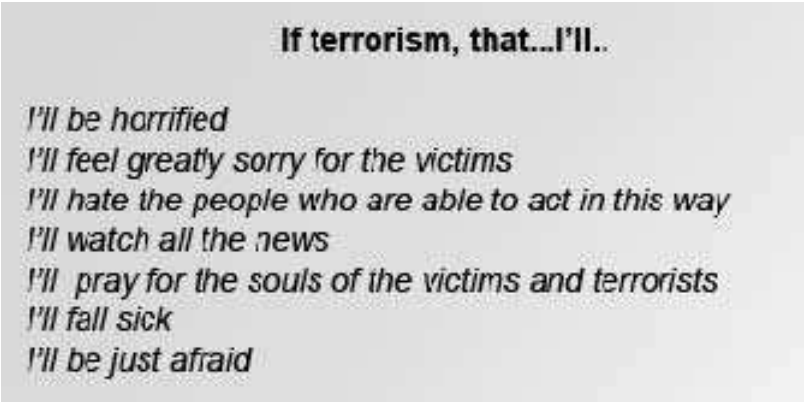


Fig. 5. The most frequently occurring variants of the possible completions of the sentence "If terrorism, that…"

One of the general conclusions of the received results is that *the terrorist act is committed in order to create a fearful state of mind in an audience different from the victims*. It's necessary to mention that our respondents were just TV observer of terrorist acts and weren't active participants of them. Another general conclusion can be formulated in a following way: *terrorism, no matter how awful it's consequenses may be, is now a form of communication with predictable results between groups of people* (fearful states of mind both in victims and in an audience different from the victims). As any communicational activity, it will be exist until it will be considered to be functional.

Литература

[1] Charles L. Ruby. The Definition of Terrorism. Analysis of Social Issues and Public Policy. V. 2, issue 1, p. 9. December 2002.

[2] Cristina Jayme Montiel. Other Terrorism, Psychology, and Media. Peace and Conflict. Journal of Peace Psychology. 2002, vol. 8, no. 3, P. 201–206.

[3] Herbert H. Blumberg. Understanding and Dealing With Terrorism: A Classification of Some Contributions From the Behavioral and Social Sciences. Peace and Conflict. Journal of Peace Psychology. 2002, vol. 8, No. 1, p. 3–16.

[4] C. R. McCauley, E. M. E. Segal. Social psychology of terrorist groups. In C. Hendricks. 1987.

[5] Richard V. Wagner. Terrorism: A Peace Psychological Analysis. Journal of Social Issues, 2006, vol. 62, no. 1, p. 155.

[6] J. Post. Notes on a Psychodynamic Theory of Terrorism. Terrorism, 1984, v. 7, no. 3, p. 241–256.

[7] J. Post. When Hatred is Bred in the Bone: Psycho-cultural Foundations of Contemporary Terrorism. Political Psychology, 2005, vol. 26, no. 4.

О необходимости исследования и моделирования процессов взаимодействия метацивилизаций современности по критерию всеобщей информационно-психологической безопасности

В. И. Таирян, Е. И. Таирян

В настоящей работе, продолжающей [1], обосновывается необходимость исследования и моделирования процессов взаимодействия метацивилизаций современности по критерию всеобщей информационно-психологической безопасности.

В условиях глобализации, являющейся основным лейтмотивом современного этапа развития человечества, проблема контакта, взаимопроникновения, диалога и столкновения культур (цивилизаций) стоит особенно остро. Яркий пример этому — всплеск международного терроризма.

Рост цивилизационного самосознания

Процессы экономической модернизации и социальных изменений во всем мире размывают традиционную идентификацию людей с местом жительства, одновременно ослабевает и роль нации-государства как источника идентификации. Образовавшиеся в результате лакуны по большей части заполняются религией, нередко в форме фундаменталистских движений. Подобные движения сложились не только в исламе, но и в западном христианстве, иудаизме, буддизме, индуизме. Возрождение духовных ценностей создает основу для идентификации и сопричастности с общностью, выходящей за рамки национальных границ — для объединения государств и цивилизаций в метацивилизации. Наблюдаемый при этом рост цивилизационного самосознания диктуется раздвоением роли Запада. С одной стороны, Запад находится на вершине своего могущества, а с другой, в состоянии духовного кризиса. Последнее является мощным стимулом для незападных цивилизаций сохранить собственные ценности. На вершине своего могущества Запад сталкивается с незападными странами, у которых

достаточно стремления, воли и ресурсов, чтобы придать миру незападный облик.

Расширение экспансии Запада

В настоящее время расширяется глобальная информационно-культурная и информационно-идеологическая экспансия Запада, осуществляемая по мировым телекоммуникационным сетям и через средства массовой информации. Многие страны вынуждены принимать специальные меры для защиты своих сограждан, своей культуры, традиций и духовных ценностей от чуждого информационного влияния.

Попытки Запада распространить свои ценности: демократию и либерализм — как общечеловеческие, сохранить военное превосходство и утвердить свои экономические интересы наталкиваются на сопротивление других цивилизаций.

Правительствам и политическим группировкам все реже удается мобилизовать население и сформировать коалиции на базе идеологий, и они все чаще пытаются добиться поддержки, апеллируя к общности религии и цивилизации. Особенно провокационной в связи с этим выглядит «теория» С. Хантингтона о столкновении цивилизаций, в соответствии с которой неизбежен глобальный конфликт между христианской (прежде всего ее православной частью) и мусульманской цивилизациями. Примерами применения подобных взглядов могут служить военные провокации между сербами и албанцами, а также прямая военная агрессия США против Югославии, Ирака, Афганистана и других суверенных государств. Наблюдая с экранов телевизоров за «странной» войной в Ираке, мир увидел появление войн нового поколения — информационно-психологических, в которых боевые действия играют подчиненную сервисную роль, а план вооруженной кампании строится по правилам и в соответствии со сценарием пиар-воздействия на собственных граждан, на граждан политических союзников и оппонентов и на международное сообщество в целом.

Метацивилизации

Смену мировоззрения на рубеже третьего тысячелетия подготовила революция в области коммуникаций и информации, достигшая таких масштабов, каких не могли себе даже представить предшествующие поколения. Массовая компьютеризация, внедрение новейших информационных технологий привели к впечатляющему рывку вперед в сферах образования, бизнеса, промышленного производства, научных исследований и со-

циальной жизни. Информация превратилась в глобальный, в принципе неистощимый, ресурс человечества, вступившего в новую эпоху развития цивилизации — эпоху интенсивного освоения информационного ресурса и «неслыханных возможностей» феномена управления. Именно *информация*, *управление и организация*, как могучие локомотивы прогресса, умчали развитые страны в новую Западную Американо-Иудаистскую метацивилизацию.

Современный мир вряд ли может управляться национальным государством. В «новом американском веке» (как охарактеризовал наступившее столетие 42-й американский президент Клинтон) Соединенные Штаты уже не являются национальным государством в том смысле, как это было сформулировано в рамках и категориях вестфальской системы. Америка обретает особый статус, становясь своеобразной страной-системой, чьи рубежи — не административно-политические границы национальной территории, а зона жизненных интересов, которая имеет выраженную тенденцию к распространению на всю планету.

Процесс трансформации в квази-имперские состояния, в новые политические интегрии — явление, характерное не только для Соединенных Штатов. Подобные изменения и трансформации в разных, порой существенно различающихся между собой, формах наблюдаются и в других частях мира. И государство «Шенген», и страна-регион Большой Китай, вбирающий в себя Гонконг, Макао, Тайвань и связанный тысячей нитей с диаспорой хуа-цяо, и бродящий по планете призрак возрождаемого халифата — все это специфические модификации страны-системы.К этой категории следует отнести и Россию в постсоветском пространстве СНГ — то ли реликт, то ли зародыш некоего организма, чье целеполагание никак не укладывается в конструкты «национального государства», вернее — формирование нового уровня цивилизаций — метацивилизации. При наличии современных средств транспорта и связи процессы взаимодействия и взаимообмена между метацивилизациями приобретают все большие масштабы. «*Ни национальные правительства*, *ни локальные власти не смогут собственными силами справиться с проблемами*, *порожденными растущей взаимозависимостью*».

Означает ли глобализация — в ее нынешних формах — неизбежное столкновение цивилизаций с возможным драматическим исходом? Если исходить из того, что никаких общих интересов у человечества нет, то ситуация получается вроде бы безысходная. Но общий интерес, в конечном счете, все-таки существует. Это интерес выживания — необходимость предотвращения трансформации локальных межцивилизационных конфликтов в полномасштабные войны между метацивилизациями, на корню пресекающая вероятность порождения экстремизма и терроризма со

стороны любой из противоборствующих метацивилизаций. В противовес модным концепциям «столкновения цивилизаций» человечество должно и обязано отстаивать идею сохранения гуманной общечеловеческой перспективы — формирования нового глобального консенсуса в диалоге метацивилизаций.

Взаимодействие (конфликт) метацивилизаций — информационно-психологические технологии

Конфликт между Западом и конфуцианско-исламскими государствами (с*оставляющими ядра восточных метацивилизаци*й) в значительной мере (хотя и не исключительно) сосредоточен вокруг проблем ядерного, химического и биологического оружия, баллистических ракет и других сложных средств доставки такого оружия, а также систем управления, слежения и иных электронных средств поражения целей. Незападные страны отстаивают свое право приобретать, производить и размещать любое оружие, которое они считают необходимым для собственной безопасности.

Однако сегодня даже наличие ядерного оружия не решает проблем национальной безопасности, т. к. борьба перемещается на уровень сознаний, а войны трансформируются в «локальные» конфликты. Как пишет американский специалист С. Стрейндж, «в мире многосторонней, претерпевшей диффузию власти наше собственное сознание становится нашим единственным компасом». Этот компас сегодня пытаются «вывести из строя», воздействуя на общество психологически, применяя по отношению к нему новое могущественное оружие по нескольким каналам, наиболее эффективным из которых является канал информационный.

В ходе специфических военных операций, заключающихся в воздействии на массовое сознание, психологическая составляющая является наиболее значимой. В то же время использование информационных каналов для подобного рода психологического воздействия делает эффективность таких операций максимальной, если за критерий эффективности брать скорость изменения массового сознания, масштабность воздействия и соответствие конечного состояния сознания масс желаемому.

В любом случае, как бы ни было сильно и могущественно государство, неграмотность и неразборчивость населения к воздействиям на психологическом уровне, некритичность к получаемой информации, способны привести к массовым негативным социально-психологическим явлениям, которые вполне могут вывести государственную систему из состояния равновесия.

В одном из докладов Объединенной комиссии по безопасности, созданной по распоряжению министра обороны и директора ЦРУ в США, говорится: «…Уже признано, что сети передачи данных превращаются в поле битвы будущего. Информационное оружие, стратегию и тактику применения которого еще предстоит тщательно разработать, будет использоваться с «электронными скоростями» при обороне и нападении. Информационные технологии позволят обеспечить разрешение геополитических кризисов, не производя ни одного выстрела. Наша политика обеспечения национальной безопасности и процедуры ее реализации должны быть направлены на защиту наших возможностей по ведению информационных войн и на создание всех необходимых условий для воспрещения противоборствующим США государствам вести такие войны…».

Информационно-психологические войны сегодня выступают в качестве мощного дестабилизирующего фактора, способного существенно ослаблять любое не готовое к защите государство и оказывать негативное воздействие на массовое сознание, что предъявляет особые требования к разработке грамотной и эффективной программы в области государственной информационной безопасности, и свидетельствует о необходимости исследования и моделирования процессов взаимодействия метацивилизаций современности по критерию всеобщей информационно-психологической безопасности.

Общая модель взаимодействия метацивилизаций

Авторами исследована и построена общая модель взаимодействия цивилизаций, которая состоит из теоретико-игрового, теоретико-вероятностного и экспертного модулей.

Теоретико-игровой модуль реализует биматричную коалиционную игру, цена которой соответствует индексу информационно-психологической безопасности игроков (системы).

Теоретико-вероятностный модуль реализует марковские процессы и позволяет определять финальные вероятности состояний с заданными значениями индекса безопасности системы.

Экспертный модуль позволяет осуществить сбор и анализ данных, необходимых для вышеназванных двух модулей общей модели.

Литература

[1] Таирян В. И., Таирян Е. И. О доктрине создания сети региональных информационно-психологических поясов безопасности. Материалы международной

научной конференции по проблемам безопасности и противодействия терроризму (Москва, МГУ, 2005). М.: МЦНМО, 2006. С. 438–443.

[2] Шерстюк В. П. Проблемы информационной безопасности в современном мире.

[3] Стрельцов А. А. Обеспечение информационной безопасности России. Теоретические и методологические основы. М.: МЦНМО, 2002 (избранные материалы книги).

[4] Сальников А. А., Ященко В. В. Методологические проблемы противодействия кибертерроризму.

[5] Манойло А. В. Информационно-психологическая война: факторы, определяющие формат современного вооруженного конфликта. Материалы V Международной научно-практической конференции «Информационные технологии и безопасность» (Крым, Партенит, июнь 2005 г.). Киев: 2005. Вып. 8. С. 73–80.

[6] Крутских А. В. Война или мир: международные аспекты информационной безопасности.

[7] Неклесса А. Картография Нового мира. Экономические стратегии. 2001. № 1.

[8] Почепцов Г. Г. Информационные войны. М.: Рефл-Бук, 2000.

[9] Володенков С. В. Информационно-психологические войны и массовое сознание. Философский факультет МГУ им. Ломоносова. Отделение «Связи с общественностью».

[10] Rosenau J. Along the Domestic — Foreign Frontier: Exploring Governance in a Turbulent World. Cambridge, 1997. P. 115.

[11] Strange S. The Retreat of the State. Cambridge, 1996. P. 199.

Роль религии в развитии безопасности и противодействии терроризму

В. Кадыров

Тезисы доклада

- Усиление роли религии в обществе во время переходного периода становления государственных структур.
- Правильные познания в религии, истории и культуры религии один из главных моментов искореняющих тягу людей к террористическим структурам и организациям.
- Фундаментом многих террористических структур и организаций является религиозная основа.
- Вмешательство религии в политику приводит к конфронтации сторон и вовлечение людей в террористические структуры.
- Своевременная совместная работа и взаимодействие государственных структур с религиозными общинами снижает процент увеличения террористической угрозы.
- Полный контроль и правильное понимание новых направлений в религии со стороны государственных структур исключает возможность их участия и содействия в террористических организациях.
- Привлечение религиозных деятелей к полноправной общественной жизни общества, активное участие религиозных организаций во всех сферах общества: снизу доверху, еще один шаг к усилению безопасности и противодействие терроризму.

С каждым годом стремительно растет ритм жизни. В мире происходят катастрофы, аварии, террористические акты и другие события — все эти процессы напрямую связаны с процессом развития общества. С темпами развития нашего общества одновременно происходит и явный рост развития террористической угрозы в мире. Развитие террористической угрозы является чумой нынешнего столетия и в то же время является бизнесом приносящий колоссальные доходы, унося при этом жизни людей. Многие

страны пытаются решить проблему становления общества форсированными методами,что приводит к возможности большого процента ошибок, параллельно развивающихся с показателями роста общества в целом.

Религия является частью жизни для большинства людей. Церкви, секты, деноминации и культы привлекают людей, смысл жизни которых частично или полностью связан с религией. Социологи наверняка знают почему и зачем так происходит. Исходя из того что жизнь в нашем обществе преподносит все больше сюрпризов, на этом фоне, происходит усиление влияния религии на общество в целом. Если построить диаграмму экстремальных событий и увеличение числа людей приобщающихся к религии, то мы заметим пропорциональный зависимый друг от друга рост этого соотношения. Люди самостоятельно ищут пути решения многих проблем в обществе, в том числе и проблему безопасности, как это не банально, находя ответ в канонах религии, которую они исповедают.

Человек, не найдя ответов в обычной жизни, может все глубже искать этот ответ в религии, и здесь очень важно не упустить момент. Правильно организовать понимание религии на всех этапах развития общества. Ведь у любого государства есть образовательные ресурсы — такие как школы, институты, университеты и многие другие структуры, где любой человек может получить правильное понимание религиозных истин, а не искаженные понятия о религии которые используют террористы для привлечения в свои ряды все большее количество людей.

Надеюсь, Вы согласитесь что религия — сложный механизм, можно сказать, один из самых древних методов государственного правления на нашем земном шаре. Выражение о религии *государство в государстве* — говорит само за себя.

Можно только представить насколько религия охватывает наше общество. Я думаю, важно понять, что организация правильного понимания всех религиозных направлений в обществе, искоренит тягу к отчуждению от нормальных правил поведения. Любая религия, я имею ввиду основные направления, такие как буддизм, христианство, ислам и другие, имеют глубокие корни в истории и культуре развития. Это очень важный момент. Ведь вовлечение в ту или иную религию людей, дает возможность постоянно создавать вокруг них необходимый информационный портал. В зависимости от уровня образованности и культуры человека, он может однозначно воспринять ту или иную информацию. Многие террористические организации созданы по принципу религиозного направления, национальных меньшинств, несвоевременная и неправильная информация об истории и культуре религии может привести к притоку людей в эти террористические структуры. Это в свою очередь даст террористическим организациям основной *ресурс — людей* для выполнения своих задач.

Большую роль в религию имеют религиозные руководители. Религиозные деятели многих концессий должны быть очень осторожны в своих высказываниях, так как их речь и мысли являются основой понимания жизни практически для большинства числа верующих. Можно привести пример — недавнее высказывание в своем выступлении главы Римской католической церкви Папы Римского Бенедикта XVI (напомним, что, находясь в Германии, он в одной из своих речей процитировал византийского императора, утверждающего, что пророк Мухаммед не принес в мир ничего, кроме насилия), которое вызвало протесты и гневную реакцию мусульман, привело еще к большей эскалации напряженности во многих регионах мира, следовательно дало еще одну возможность террористическим организациям привлечь в свои ряды необходимых людей.

Я считаю, государственные структуры должны проводить совместную работу с религиозными общинами, контролировать их процессы воздействия на общество, организовывая со своей стороны правильное понимание религии в обществе. Это сложный процесс, для создания этого механизма необходимо привлечь все научные ресурсы. Пример такого взаимодействия можно привести в некоторых странах, где удается наладить полный контакт между религией и государством. В таких странах как Россия, Азербайджан, Казахстан и других странах. Благодаря политике президента России В. В. Путина произошло одно из главных событий, объединение Русской православной церкви, раскол в которой произошел после революции 1917 года. Это значит что Россия исключила одну из причин развития терроризма на своей территории. В Азербайджане, практически нет проблем между религиозными общинами, нет и проблем террора на религиозной основе, очень многие проблемы руководители религиозных концессий решают сообща, в чем заслуга правильной политики поставленной еще во времена правления Гейдара Алиева. Я думаю, постоянное просвещение людей в вопросах истории и культуры всех направлений в религии и связь между основными религиями, с самого раннего возраста, даст правильное истолкование основ религий, и тем самым уменьшит вовлечение людей в террористические организации,что в свою очередь приведет к усилению безопасности.

В то же время (наряду с 4 основными религиями такими как буддизм, иудаизм, христианство, ислам) существует много религиозных направлений разного характера. Можно назвать их своего рода ответвлениями в основных религиях. Возникновение этих направлений в религии можно и нужно контролировать, так как полностью запретить и искоренить их не представляется возможным. Комплексная профилактика и терапия со стороны государственных структур может предотвратить влияние на религиозные структуры террористических организаций.

Я думаю, проблема состоит в том, что государственные структуры пытаются полностью запретить их, а не разобраться, в результате чего эти течения в религии возникают. Террористические организации активно развиваются в ногу со временем, технически и хорошо подготовлены физически и психологически, и очень умело используют людей не реализовавшихся в обществе. Учитывая психологию человека, которого недопонимают в обществе, террористические организации без особых усилий вербуют их в свои ряды. Анализ тенденций террористических актов за последние годы показывает, использование в своих действиях, людей готовых принести себя жертву,на основе религиозных побуждений, так называемых *шахидов*. Тем самым процесс предотвращения террористического акта усложняется отсутствием страха у этих исполнителей — *шахидов*.

Я думаю, нужно консолидировать возможности религиозных общин (структур), ведь они имеют очень большое влияние на своих прихожан.

Полноправное привлечение религиозных деятелей к полноправной общественной жизни общества, возможности их самостоятельного участия в работе исполнительных и законодательных структур государств даст положительный эффект в развитии безопасности и противодействию терроризму.

Я думаю, мы прекрасно понимаем, что религия, независимо от вероисповедания, на сегодняшний день имеет огромное количество последователей и влияние, как на людей, так и на различные сферы общества. Общество должно задействовать этот огромный потенциал и информационный ресурс в своих целях обеспечения безопасности путем противодействия терроризму.

Противоречия глобальной информационной среды как источник роста трансграничной преступности и международного терроризма

Р. А. Шаряпов

В наши дни под влиянием современной информационно-технической революции, изменений в техносфере и инфосфере, роста значения информации формируется глобальная электронная среда, в которую все больше переносятся важнейшие составляющие политической, экономической, социальной и культурной деятельности. Эта среда интенсифицирует обмен информацией, мнениями, идеями, услугами, товарами, здесь создаются различные виртуальные сообщества по интересам. Происходят глубокие перемены в политической жизни общества, обеспечивая гражданам доступ к самой различной информации, возможность вести диалог между властными и гражданскими структурами, выходить на практически неограниченную аудиторию.

Формирование глобальной информационной среды оказывает существенное влияние на структуру мировой экономики, которая становится гораздо динамичнее, генерируя множество новых видов бизнеса. Особенно интенсивно развивается электронная торговля. Так, по данным ЮНКТАД, в 2000 г. продажи через Интернет составляли 354,9 млрд. дол., а в 2001 г. — уже 615,3 млрд. (так, стоимость продаж через Интернет в ЕС составила в 2001 году 86 млрд. дол., а суммарная стоимость электронной торговли в ЕС составила в 2001 году примерно 430 млрд. долл. США [1)]).

Появление Интернет фактически ознаменовало начало активного формирования глобального информационного общества. Возникают условия для экономического роста отдельных стран, их интенсивного включения в мировые интеграционные процессы, в формирующееся общее (а в перспективе — единое) информационное пространство. Поэтому каждое государство стремится к развитию национальной информационной инфраструктуры, всемерному участию во внедрении информационных инноваций.

Однако, как ни заманчивы перспективы глобальной интеграции, на этом пути человечество поджидают много серьезных проблем, вызовов и угроз.

[1)] `http://www.un.org/russian/esa/unctad/e-trade2005_sum.pdf`.

Так, параллельно с вышеотмеченным ростом электронной торговли и трансакций. совершаемых в глобальной сети Интернет, в силу трансграничного характера электронного бизнеса, возникают и немалые проблемы, касающиеся, например, налогообложения. Учитывая, что за счет собираемых налогов формируются фонды для социальных выплат, расходов на образование и здравоохранение во всех странах, становится понятным, возрастающее влияние, которое оказывает информационная революция на рост потенциально конфликтогенных социальных противоречий.

Немалые опасения вызывает проблема так называемого, «цифрового неравенства». Как отмечают специалисты, общество внутри стран и разные по уровню развития государства, разделяются на тех, кто имеет доступ к новейшей информации и услугам посредством современных информационно-коммуникационных технологий, и тех, кто ими не располагает. Согласно «Докладу об информационной экономике», составленном Конференцией ООН по торговле и развитию, на начало 2006 года число пользователей Интернета в мире составило 1 млрд. 20 млн. 614 тыс. человек. По сравнению с 2005 годом этот показатель вырос на 19,5 %. В первую тройку стран по числу интернет-пользователей вошли США — около 200 млн., Китай — 111 млн. и Япония — 85,29 млн. человек [2)].

В то же время, по данным «Internet World Stats» на начало 2007 года количество пользователей Интернета в Африке составило немного более 33 млн. человек (т. е. только 3 % от общемирового числа пользователей), а в Латинской Америке (без стран Карибского региона) — около 68 млн. человек (что составляет 6,1 % от общемирового числа пользователей) [3)].

Неравенство в доступе к информации в информационную, по своей сути эпоху, неизбежно влечет за собой углубление традиционно существовавших видов неравенства — социального, экономического, политического, как между развитыми и развивающимися государствами в целом, так и между различными социальными группами внутри стран. Это означает, что сверхприбыли от базисных нововведений в информационном секторе (информационную ренту) присваивают, в основном, лидеры глобальной гонки, среди которых выделяются транснациональные корпорации, имеющие свои штаб-квартиры в развитых странах, в первую очередь, в США, которые оттеснили Японию, Западную Европу и новые индустриальные страны.

Такая система создания и практического использования интеллектуального капитала прочно закрепляет существующие диспропорции, еще боль-

---

[2)] `http://www.unctad.org/en/docs/sdteecb20061_en.pdf`.

[3)] `http://www.internetworldstats.com/stats.htm`.

шие, чем в мировом распределении доходов. Развитые страны полностью доминируют в фундаментальных и прикладных исследованиях. В 1993 г. в 10 передовых странах было сосредоточено 84 % мировых НИОКР. Затраты на НИОКР в Северной Америке составляли более 42 % мировых расходов на эти цели, в то время как в Латинской Америке и Африке, вместе взятых, — менее 1 % [4].

Неудивительно, что в настоящее время развитые страны владеют 97 % патентов в мире. На их долю приходится более 90 % трансграничных доходов от патентов и лицензий. Ныне действующие международные режимы, гарантирующие права на интеллектуальную собственность, таким образом, способствуют маргинализации бедных стран, технологический разрыв между сопричастными знаниям и обделенными ими увеличивается [5].

Эти и другие проявления неравенства, сопровождающие формирование глобальной информационной среды, характеризуются отечественным исследователем М. Делягиным как *базовое социальное противоречие эпохи глобализации*. Его субъектами стали: с одной стороны — так называемое «информационное сообщество», состоящее из представителей интеллектуального труда, участвующее в разработке и применении информационных технологий, в особенности, технологий формирования сознания, и все остальные слои и группы современного общества, члены которых являются простыми объектами систематического применения указанных технологий, — с другой стороны [6].

Указанное противоречие представляет собой лишь внешнее проявление глубокого фундаментального процесса — перехода контроля за общественным развитием из рук владельцев капитала в руки владельцев уникальных знаний и умений, прежде всего в сфере управления. В итоге принципиально важной особенностью новой «информационной» элиты, является ее значительно меньшая демократичность.

В свою очередь, поляризация любых социальных групп, либо политических сил, прямо или косвенно, способствует возникновению конфликтов. На это обращают внимание как отечественные, так и западные ученые. Так, немецкий исследователь Г. Гейдер, специализирующийся на проблемах безопасности, считает, противоречивые тенденции, порождаемые информационной революцией дополнительным проблемным фактором, поскольку всем этим могут воспользоваться террористы и преступники» [7].

---

[4] Постиндустриальный мир и Россия. — М.: 2001, с. 68, 73.

[5] Яковец Ю. В. Глобализация и взаимодействие цивилизаций. — М.: 2003, с. 390.

[6] Делягин М. Г. Мировой кризис: Общая теория глобализации: курс лекций. — М.: 2003, с. 51; Современные международные отношения и мировая политика. Отв. редактор — член-корреспондент РАН, проф. А. В. Торкунов. — М.: 2004, с. 188.

[7] Gebhard Geider. Sicherheit im Informationszeitalter. Informationen zur politische Bildung. Bonn: 2002, № 274, S. 55.

Действительно, противоречия формирующейся глобальной информационной среды, неспособность противостоять гораздо более сильному (в военном и информационном отношении) противнику побуждает некоторых политических субъектов к поиску асимметричных ответов. Одним из вариантов таких ответов могут стать, и зачастую становятся, действия террористического характера. Современная война развитого государства против страны, находящейся на более низком уровне экономического и технологического развития, сочетает в себе переплетение боевых действий и террористических акций, что мы сегодня и наблюдаем в Афганистане, Ираке, на Ближнем Востоке. Асимметрия действий воюющих сторон, таким образом, также является одной из черт облика войн в условиях формирования глобальной информационной среды [8)].

Стремительное развитие современных коммуникационных технологий предоставило в распоряжение сторонников насилия огромные возможности для достижения своих целей Информатизация общественной жизни не только способствует нарастанию социальных диспропорций, и, тем самым, создает социальную базу терроризма среди отставших, и иллюзию собственного бесконечного превосходства среди преуспевших групп и обществ. Средства массовых коммуникаций еще и способствуют распространению идей нетерпимости и насилия, как среди первых, так и среди вторых. Размышляя по этому поводу, Дж. Гербнер отмечает: «В истории человечества бывали и более кровожадные эпохи, но ни одна из них не была до такой степени пропитана образами насилия, как наша. И кто знает, куда нас унесет этот чудовищный поток зримого насилия ... просачивающийся в каждый дом через мерцающие экраны телевизоров в виде сцен безупречно отрежиссированной жестокости» [9)].

В ряде стран были проведены широкомасштабные исследования о воздействие СМИ на зрительскую аудиторию. Они показали, что в среднестатистической семье телевизор работает до семи часов в день. Две из каждых трех программ в прайм-тайм и субботние утренние часы содержат сюжеты насилия. К моменту окончания средней школы ребенок просматривает по телевидению около 8000 сцен с убийствами и 100 000 других действий с применением насилия [10)].

Телевидение, демонстрируя насилие на телеэкране, смещает акценты в системе человеческих ценностей и приводит к тому, что зрители, в особенности дети, начинают рассматривать насилие как желаемый и «мужественный» стиль поведения, используемый для восстановления справед-

---

[8)] Ефимов Н. Н. Глобализация: военный аспект. `http://www.postindustrial.net/content1/show_content.php?table=free&lang=russian&id-`.

[9)] Цит. по: Майерс Д. Социальная психология. Санкт-Петербург: 1998, с. 517.

[10)] См. там же.

ливости. Среди любой аудитории неизбежно присутствует определенный процент людей (таковы законы статистики), воспринимающих полученные стандарты и образцы поведения как руководство к действию, а терроризм начинает восприниматься ими как вполне приемлемый метод политической борьбы.

Стихийно, или подчиняясь чьей-либо манипуляции, эти люди начинают искать единомышленников, используя многочисленные каналы коммуникации. Особое место среди них занимает новый, невиданный прежде информационный феномен — Интернет. Ввиду отсутствия какого-либо контроля, он активно используется для распространения сведений, выгодных террористам, для получения конфиденциальной информации или выведения из строя жизненно важных структур. Немецкий аналитик Г. Гейдер, заостряет внимание на таком факторе, как анонимность распространения информации в Интернет [11]. Понятно, что иллюзия безнаказанности, возникающая вследствие этого, только развязывает террористам руки. Исходя из этого, приходится признать, что, используя достижения научно-технического прогресса, деструктивные силы добиваются консолидации своих рядов.

Переход к действиям террористического характера, так же сопровождается учетом и использованием информационных факторов общественной жизни. Это непременное условие как террора «сверху», так и терроризма «снизу». Например, террористическая, по своему характеру, война 1999 года в Югославии, предварялась массированной информационной кампанией по созданию негативного образа сербов в массовом сознании американцев и даже европейцев, как патологически жестоких убийц [12].

Эффективность информационного воздействия, при условии использования соответствующих ресурсов, может быть очень велика. Так, например, известный американский юрист и аналитик Р. Нейдер подчеркивает, что сразу после 11 сентября 2001 г. в причастность к терактам С. Хусейна верили 3 % американцев, а в результате массированной пропагандистской кампании, проведенной в американских СМИ к началу войны в Ираке, в это верили уже 47 % населения США [13].

В свою очередь, представители сепаратистского терроризма, так же используют все методы очернения господствующего режима, представляя себя в выгодном свете, как «борцов» за светлые идеалы. Например, террористическая тактика баскской ЭТА предполагает предупреждения населения накануне проведения терактов, во избежание многочисленных жертв

[11] Geider G. Sicherheit im Informationszeitalter. Informationen zur politische Bildung. Bonn: 2002, № 274, S. 54.

[12] Делягин М. Г. Мировой кризис: Общая теория глобализации: курс лекций. М.: 2003, с. 492

[13] Черной Л. С. Глобализация: прошлое или будущее. М.: Академкнига, 2003, с. 247

среди непричастных к политическому противостоянию граждан. Так представители данной организации соблюдают ограничения в масштабах своих акций, благодаря которым диалог с противником — официальными властями, продолжается в более благоприятной среде общественного мнения [14].

В отличие от предшественников, нынешние террористы рассчитывают на крупномасштабный социально-психологический эффект среди тех, составляет зрительскую аудиторию событий. Используя страх, апеллируя к инстинкту самосохранения, они создают сильный психологический прессинг, при котором деморализованные и запуганные люди оказывают давление на представителей власти, вынуждая сделать то, что выгодно террористам. Переоценить роль средств массовой информации, в данном процессе просто невозможно, такие характеристики СМИ, как публичность, распространение информации на огромную аудиторию, зачастую находящуюся в разных уголках земного шара, многократно увеличивают возможности и потенциал террористов.

Драматически освещая, в погоне за рейтингами, происходящие террористические акты, они бесплатно рекламируют деятельность террористов и создают атмосферу паники и страха, так необходимую последним. К таким выводам приходят очень многие террологи, например, Б. Нетаньяху считает решающим фактором в распространении терроризма доступ к масс-медиа [15]. О потребности террористов в освещении своих идей и действий через масс-медиа пишет и Д. Шредер, который, так же предостерегает от сопутствующей мифологизации любых проявлений терроризма: «легенды могут помогать террористам» — пишет он [16].

Еще один немаловажный аспект данной проблемы состоит в том, что современные информационные сети могут использоваться не только как вспомогательные (хотя и очень необходимые) средства террористической деятельности, но как объекты поражения. Компьютерный терроризм, о котором смело можно говорить уже сегодня, в будущем, вероятно, станет одной из самых распространенных форм террористической деятельности. В докладе объединенной комиссии США по безопасности и обороне (февраль 1994 г.) говорится, «что сети передачи данных превращаются в поле битвы будущего. Информационное оружие, стратегию и тактику применения которого еще предстоит тщательно разработать, будет использоваться ... при обороне и нападении» [17].

---

[14] Мороз Р. И. Терроризм как форма политического экстремизма. Дисс. канд. полит. наук. М.: 2004, с. 118.

[15] Terrorismus: Gewalt mit politischen Motiv. Dieter Schroeder [Muenchen], 1986, S. 183.

[16] Terrorismus: Gewalt mit politischen Motiv. Dieter Schroeder [Muenchen], 1986, S. 15.

[17] Цит. по: Изиляева Л. О. Терроризм как социально-политическое явление. Дисс. канд. полит. наук. Уфа: 2004, с. 95.

Действительно, при современной сложности и уязвимости компьютерных систем, управляющих потенциально опасными объектами промышленной и военной инфраструктуры, можно смело предположить, что эффект от применения компьютерного терроризма можно сравнить с эффектом от применения оружия массового поражения.

В заключение следует отметить, что, рассматривая особенности глобальной информационной среды, важно не упускать из вида паразитирующие на противоречиях ее формирования идеологические аспекты террористического насилия. Именно идеология связывает воедино разрозненные факторы влияния на человека, о многих из которых мы уже говорили выше, усиливает их действие за счет синергетического эффекта и направляет ход мыслей и, в конечном итоге, действия вовлеченных индивидов.

Через «возвышенные мотивы» обычно вовлекают молодежь, которая в силу умственной и моральной незрелости легко принимает радикальные национальные, социальные или религиозные идеи. Вовлекают ее чаще всего через тоталитарные (т. е. полностью подавляющие волю людей и подчиняющие их только воле «вождя», или «идее борьбы»), религиозные или идеологические секты. Корыстный терроризм, наемничество в разнообразных формах имеют несколько другой генезис, хотя очень часто прикрываются различными «идеями», но и в этом случае роль современных средств коммуникации очень велика.

К вопросу о разработке операционных сред с открытыми исходными текстами, ориентированных на обеспечение безопасности государственных информационных систем

А. Н. Курбацкий

Недавно Майкл Дуглас (осень 2006 года), вице-президент Sun Microsystems, привел один из факторов, способствующих росту популярности открытых исходных текстов в ИТ-индустрии: «Разработчик от открытых кодов получает следующее преимущество: его интеллектуальный вклад может базироваться на его интеллектуальной собственности многих других разработчиков, и доступ к означенной собственности он получает бесплатно Sun Microsystems не может принять к себе на работу всех самых талантливых людей мира. Но если мы откроем для них свой программный продукт, они будут его использовать. Вот это и будет тот объем, который принесет результаты. Мы можем пользоваться интеллектуальными ресурсами сотен тысяч талантливейших людей».

Модель разработки программного обеспечения с открытыми исходными текстами (open source) не относится к числу новых и оригинальных. По сути, лет 30–40 назад, когда еще только происходило становление ИТ-индустрии и, в частности, индустрии разработки программного обеспечения (ПО), обычным явлением было массовое использование открытых исходных текстов. Процесс разработки рассматривался в значительной мере как творческий процесс, как искусство. Однако становление ИТ-индустрии постепенно приводило к превращению разработки ПО в технологический процесс, рутинное производство. Быстрая коммерциализация разработки, переход к массовому коробочному ПО сопровождались закрытием исходных текстов.

Новый эволюционный виток привел к тому, что программное обеспечение с открытыми исходными текстами в последние несколько лет стало активно рассматриваться как альтернатива в первую очередь Windows-программному обеспечению. Особенно это становится характерным для государственного сектора. Наиболее известны государственные проекты в Юго-Восточной Азии: Китае, Южной Корее, Японии, Вьетнаме,

Таиланде и др. Достаточно интенсивно развиваются такие проекты в Европе, в частности в Германии, Великобритании, Франции, Дании, Финляндии, Австрии; в Латинской Америке, включая Бразилию, Венесуэлу. Мотивация таких проектов различна. Например, по политическим мотивам — избавление от излишней американской опеки, зависимости от американских корпораций: чем больше средств государственные органы расходуют на их программное обеспечение, тем больше государственные структуры становятся зависимыми от них. Особенно такая зависимость неприемлема для оборонной сферы государства. По этой причине необходимо обеспечение информационной безопасности в широком смысле, а это отчасти может быть решено при использовании открытых стандартов. По финансово-экономическим мотивам: необходимость борьбы с явным «пиратством», недостаточно эффективное обеспечение интеллектуальной собственности, в частности, патентной, лицензионной деятельности. Последнее время стала актуальной еще одна мотивация: быстрое развитие собственной ИТ-индустрии, связанное с поиском локомотивных проектов.

Когда в ИТ-профессиональной среде возникают споры вокруг программного обеспечения операционной среды Windows и продуктов с открытыми исходными текстами, они как правило сразу переходят в плоскость функциональности продуктов или разгораются вокруг вопросов безопасности. Особенно популярными стали дискуссии по проблемам обеспечения информационной безопасности той или иной операционной средой. Все эти сравнения, несомненно, полезны, но они обычно отражают текущую ситуацию, без особого прогнозирования, и поэтому полезны для решения тактических задач. Если же говорить о решении значимых государственных стратегических задачах в области ИТ, то необходим комплексный подход.

Часто предметом дискуссий является стоимость затрат на развитие той или иной операционной среды. Одна из стандартных ошибок в дискуссиях заключается в том, что величина затрат сводится в основном к затратам на покупку операционной системы. Интегральная же стоимость состоит из стоимости непосредственно операционной системы и средств разработки, стоимости разработки (включая затраты на освоение системы), стоимости последующих модификаций системы, стоимости лицензий, стоимости сопровождения, стоимости обеспечения информационной безопасности. Вместе с тем основными затратами являются затраты на разработку и адаптацию приложений для конечных пользователей, затраты на подготовку специалистов для той или иной операционной среды, затраты на разработку соответствующих учебных программ и курсов для различных уровней образования, включая системы повышения квалификации и переквалификации.

Следует отметить, что концепции создания и развития двух анализируемых операционных сред существенно отличны друг от друга. Анализ опыта их использования и современного состояния рынка показывает, что операционная среда Linux достаточно популярна на рынке серверных систем — на этом рынке нет однозначного лидера. На рынке же настольных систем по-прежнему доминирует Windows, в первую очередь, из-за огромного числа пользовательских приложений. Операционная среда Linux наиболее популярна у IT-профессионалов, включая разработчиков программного обеспечения, сетевых администраторов, специалистов по информационной безопасности и представителей смежных областей. Часто из-за попыток применения операционных сред в несвойственных для них областях и возникают неправильные оценки перспектив. По этомй причине нельзя утверждать, что данные операционные среды только конкуренты, в определенном смысле они и дополняют друг друга.

Если обсуждать целесообразность массового продвижения операционной среды с открытыми исходными текстами, в частности, Linux в Беларуси в противовес операционной среде Windows, то можно отметить следующее. В 2003 году был подготовлен проект «Разработать защищенную операционную систему для информационно вычислительных систем государственных органов на базе операционных систем с открытым кодом» для включения в Государственную программу информатизации Республики Беларусь на 2003–2005 г. и на перспективу до 2010 года «Электронная Беларусь». Пользователями предлагаемой операционной среды должны стать органы государственного управления, от надежности, защищенности и живучести информационных систем которых зависит эффективность работы народно-хозяйственного комплекса страны, органы кредитно-финансовой системы, информационные системы управления крупными экологически опасными промышленными объектами, вывод из строя которых, может привести к техногенным катастрофам, информационные системы управления крупными энергетическими объектами и т. п. Иными словами областью применения операционной системы являются информационные и управляющие системы с повышенными требованиями к надежности и безопасности, последствия аварий которых связаны с ущербом национальной безопасности, безопасности персонала, населения, окружающей среды, крупными финансовыми потерями, то есть так называемые критичные системы. Необходимость в создании подобной системы вызвана тем обстоятельством, что получившие в Беларуси наибольшее распространение операционные системы обладают низкими показателями защищенности и надежности. Причиной этого являются их архитектурные особенности, в которых ради достижения максимальной функциональности и скорости работы приложений было пожертвовано надежностью и безопасность

систем. Создавшееся положение усугубляется еще и тем, что, например, операционные среды семейства Windows, являясь коммерческими продуктами, поставляются без исходных текстов, в результате чего встраивание в них дополнительных средств защиты затруднено. Предварительный анализ показал, что в настоящее время базовые функциональные возможности операционных сред с открытыми текстами, не уступают возможностям коммерческих операционных сред, а доступность их исходных кодов для широкой аудитории независимых специалистов, служит определенной гарантией отсутствия в них скрытых возможностей. Этот же фактор доступности кодов может обеспечивать быстрое и качественное устранение уязвимостей безопасности, время от времени обнаруживающиеся в данных операционных средах.

В результате реализации проекта планировалось, что будет создан опытный образец защищенной операционной системы, пригодной для работы в качестве программной платформы как сетевых серверов, так и клиентских рабочих мест. Защищенная операционная среда должна была стать операционным ядром для разработки систем управления государственными информационными ресурсами, в первую очередь для критичных систем. Планировалось, что в реализации проекта примут участие ведущие центры в области ИТ-разработок. Данный проект рассматривался как один из базовых для развития современных информационных технологий в Республике Беларусь и мог стать локомотивным проектом, в частности, в рамках реализации Парка высоких технологий.

Для того, чтобы показать пилотное значение такого рода проектов, сделаем небольшой экскурс в историю. Анализ, проведенный еще в середине 90-х годов нашей инициативной группой, текущего состояния ИТ-индустрии в Беларуси показал, что существовал ряд факторов, сдерживающих развитие этой отрасли. В качестве основных таких факторов рассматривались следующие:

- неадекватность и консервативность существующей системы подготовки, повышения квалификации и переподготовки кадров международным стандартам и динамически изменяющейся ситуации на мировом рынке информационных технологий;
- отсутствие профессионально подготовленных ИТ-менеджеров среднего и высшего звена;
- отсутствие эффективной системы маркетинга;
- повышенную осторожность зарубежных партнеров при контактах с отечественными компаниями, связанную с недостаточностью и искаженностью информации о Беларуси в целом и об ее ИТ-индустрии, в частности;

- монополизацию рынка телекоммуникаций и Интернет и неэффективное использование существующей телекоммуникационной инфраструктуры;
- неразвитую правовую базу.

В республике практически отсутствовала политика государственного регулирования и поддержки разработки и экспорта ИТ-технологий. Только в результате одобрения Указом Президента Республики Беларусь от 6.04.1999 г. № 195 Концепции государственной политики в области информатизации и последующего подписания Президентом Республики Беларусь Указа № 234 от 3 мая 2001 г. «О государственной поддержке разработки и экспорта информационных технологий» предложены основные направления такой политики и созданы реальные предпосылки для опережающего развития экспортно ориентированной ИТ-индустрии.

Благодаря государственной поддержке была создана научно-технологическая ассоциация «Инфопарк». Инициатором создания ассоциации, на основании Указа, выступил Белорусский государственный университет. Согласно Указу № 234, Ассоциация создавалась в качестве одного из инструментов развития отечественной индустрии разработки информационных технологий, прежде всего индустрии программирования. Сегодня членами Ассоциации является более 40 юридических лиц — предприятия различной формы собственности, в т. ч. предприятия с иностранными инвестициями и иностранные юридические лица, основной вид деятельности которых — разработка и экспорт информационных технологий, включая программные средства. Согласно экспертным оценкам, Научно-технологическая ассоциация «Инфопарк» объединяет более 50 % всех разработчиков программного обеспечения Беларуси.

Когда в среде экспертов рассматривались базовые принципы государственной политики в сфере развития и экспорта ИТ, одной из основных идей было стимулирование разработок информационных технологий, которые впоследствии будут внедряться на глобальном рынке. Однако на этом рынке сформировано вполне устойчивое понятие налоговой конкуренции. Конкурируют между собой не только компании, но и целые страны. За привлечение интеллектуальных ресурсов. За привлечение высокотехнологичного бизнеса. Для этого государства создают у себя все более благоприятные налоговые условия, позволяющие предприятиям снижать свои издержки. Наша страна такой шаг сделала приняв 22 сентября 2006 года Декрет Президента Республики Беларусь № 12 «О Парке высоких технологий».

В нашем понимании успех реализации проекта Парка высоких технологий (ПВТ) зависит от чёткого осознания того, что его идея должна

разделяться на две важные составляющие: ПВТ как среда и ПВТ как инфраструктура. При этом мы рассматриваем данный проект как эволюционирующий.

ПВТ как среда — это система отношений субъектов ПВТ с принципиально значимыми институтами (органы государственного управления, учреждениями науки и образования и т. п.), а также система нормативных актов, создающих условия для развития высоких технологий, включающих специальные режимы: налогообложения, таможенный и др.

ПВТ как инфраструктура — это здания, сооружения, коммуникации и система сопутствующего сервиса, представляющие собой систему технопарков.

На первом этапе целесообразно осуществить реализацию проекта пилотного технопарка с последующим тиражированием его опыта при строительстве всей системы. В идеальном варианте — это существующая инфраструктура, рядом с которой возможно новое строительство.

Разработчики проекта ПВТ выбрали его базовым направлением информационные технологии с фокусом на заказном программировании. Между тем, такого рода программирование не вполне отвечает сегодняшним критериям высоких технологий. В силу того, что из всего национального сектора информационно-коммуникационных технологий, в числе немногих других его составляющих, действительно конкурентоспособным на мировом рынке является растущая белорусская индустрия программирования. Она может рассматриваться в качестве основополагающего направления развития ПВТ.

Положительным опытом развития отечественной индустрии программирования является создание механизма, обеспечившего самоорганизацию предприятий индустрии. Этим механизмом является ассоциация «Инфопарк», объединяющая предприятия различной формы собственности. Профессионально компетентные институты такого рода, могли бы оказывать действенную помощь в формировании и функционировании среды и инфраструктуры ПВТ, а также содействовать работе государственных органов в практическом осуществлении проекта ПВТ.

Возвращаясь к проекту создания собственной операционной среды с открытыми исходными текстами и построению соответствующих систем управления государственными информационными ресурсами, в первую очередь для критичных систем, как одному из пилотных, локомотивных проектов ПВТ, способному стимулировать в определенной степени быстрое развитие собственной ИТ-индустрии, следует отметить следующее.

Процесс выполнения такого достаточно масштабного и комплексного пилотного проекта должен существенно стимулировать и активизировать

для развития ИТ-индустрии условия (которые изменяются в сторону улучшения эффективности крайне медленно):

- законодательно-нормативные;
- экономические;
- социальные;
- образовательные;
- обеспечения информационной безопасности;
- технологические и методологические.

Как следствие, возможна активизация и совершенствование политических условий.

Теперь о собственно технологических и формально методологических аспектах проекта разработки операционной среды открытыми исходными текстами. Коль скоро ставится задача разработки собственных операционных систем и инструментальных средств проектирования, имеет смысл закладывать в их фундамент современные и прогрессивные научные разработки (в частности — формальные модели), а не базироваться только лишь на теоретических разработках полувековой давности. Рассмотрим, в частности, иерархичность — одно из фундаментальных свойств сущего. Отражение иерархии преследует две основные цели: 1) позиционирование объектов в системе, т. е. задание *структуры* этой системы и 2) создание условий для *наследования* объектом свойств в зависимости от его положения в иерархии.

В программировании и проектировании в целом для отражения иерархии широко применяется формальная модель «дерево» — ациклический ориентированный граф, который имеет одну корневую вершину и в котором каждый узел может иметь строго одного родителя. Эта формальная модель, реализующие ее структуры и алгоритмы являются фундаментом многих компонентов информационных систем (в том числе операционные системы) и инструментальных средств проектирования.

Модель «дерево» адекватна многим реальным структурам, что объясняет широту и успех ее применения. В то же время существует множество реальных структур, в которых объект может входить сразу в несколько иерархических ветвей и/или наследовать свойства нескольких предков в иерархии. Природа не случайно создала для живых существ двух родителей — не будь наследования свойств от двух объектов, а не от одного, не было бы эволюции. Другой пример: попробуем представить себе технологию программирования, которая допускает вызов подпрограммы только из одной «родительской» программы. Таким образом, для многих ситуаций возможность множественности родителей объекта допускается естественным образом, но есть еще много других ситуаций, для которых модель

«дерево» неприменима, но по инерции используется, являясь тормозом процесса создания эффективных решений уже начиная с уровня мышления проектировщика.

Проектировщики должны отражать в проектируемых системах естественно присущую реальным структурам множественную иерархичность. Однако в доступных инструментальных средствах заложена, как правило, модель «дерево», которая не допускает множественность родительских объектов. Поэтому проектировщики вынуждены разрабатывать сложные частные решения, чтобы обойти ограничения этой формальной модели. Более прогрессивный путь состоит в том, чтобы снять ограничения на уровне самой модели.

Модель «диаграмма» так же, как и «дерево» — ациклический ориентированный граф, но она не содержит ограничений на число родительских объектов узла и число корневых узлов («дерево» — частный случай «диаграммы»). По этой причине она адекватна гораздо большему числу реальных структур. Модель эта (в частности, под названием «диаграмма решений») известна давно, но широкое практическое применение получила в середине 1980-х, когда для работы с нею был предложен ряд алгоритмов. С этого момента она стала применяться в ряде областей, что быстро дало огромный скачок в уровне возможностей и эффективности. Можно привести огромный список литературы по применению модели «диаграмма решений» в последние несколько десятилетий (а не «дерево решений», о чем много писалось раньше).

Разрабатываемые в НИЛ Информационно-технологических систем БГУ информационные системы имеют модель «диаграмма» в фундаменте и в некоторых инструментальных средствах, в частности — в языке XPL обработки XML-данных. Опыт проектирования этих систем показывает, что нам часто удается легко и естественно решать такие задачи, которые, не будь этой модели, либо решались бы очень сложно, либо не только не решались бы, но даже не ставились в силу априори предполагаемой нереальности их решения. Другими словами — ориентация на модель «диаграмма» взамен модели «дерево» влияет не только на уровень эффективности реализации, но и на постановочный уровень задач, решаемых информационной системой.

Реализация модели «диаграмма» на базовых уровнях (на уровне ОС, инструментальных средств проектирования систем управления государственными информационными ресурсами, в первую очередь для критичных систем) означала бы определенный прорыв в технологии программирования и позволила бы выйти на качественно новый уровень функциональных возможностей информационных систем.

Один из главных факторов, сдерживающих широкое распространение систем управления информационными ресурсами — это трудоемкость программирования и необходимость использовать для этого квалифицированных программистов. Это так, если рассматривать задачу создания новой системы как в существенной степени программистскую. Технология, использующая математический аппарат семантических сетей и диаграмм решений, позволяет существенно упростить проектирование систем управления информационными ресурсами, уменьшая число квалифицированных программистов и повышая при этом защищенность проектируемых систем.

Обеспечение безопасности инфотелекоммуникационных объектов при воздействии электромагнитного импульса

В. А. Иванов, Е. В. Гречишников,
А. А. Двилянский

Современная эволюция информационного противоборства указывает на растущую тягу к целевым стратегиям, которые используют наиболее фундаментальную уязвимость — прекращение информационного потока внутри систем управления различного предназначения. Модель, используемая для современного информационного противоборства, рассматривает систему управления и поддерживающие его коммуникации как цель наивысшего приоритета для воздействия. Не менее важно, что современные электронные воздействия концентрируются на разрушении и уничтожении коммуникаций и собирающих информацию сенсоров. В связи с этим появление оружия, основанного на новых физических принципах генерации электромагнитного импульса (ЭМИ) наносекундной длительности, с высокой концентрацией плотности энергии, и имеющейся информации по его преднамеренному применению для электромагнитного подавления инфотелекоммуникационных объектов (ИТКО), в том числе и в террористических целях, объективно, с теоретической и практической точки зрения, определяет необходимость разработки соответствующих моделей исследования и конкретных методов по обеспечению безопасности ИТКО [1, 2].

В качестве количественной меры оценки уровня защищённости ИТКО от ЭМИ предлагается использовать вероятностную характеристику [3, 4, 6]. Вероятность выживания ИТКО при данном воздействии может быть как условной, так и безусловной.

Условной она будет в том случае, когда вычисляется в предположении, что воздействие поражающего фактора состоялось

$$P(_i) = \mathsf{P}[U_p(_i) > U(_i)], \tag{1}$$

где $U_p(_i)$, $U(_i)$ — сохранившийся и минимальный заданные уровни работоспособности ИТКО соответственно.

Безусловная вероятность выживания ИТКО характеризует его живучесть в течение определенного периода Δt:

$$P(_i,\ \Delta t) = P_{\prime}(_i,\ \Delta t)P(_i), \tag{2}$$

где $P_{\prime}(_i,\ \Delta t)$ — вероятность того, что в течение Δt элемент подвергнется предполагаемому поражающему воздействию.

Если живучесть ИТКО оценивается вероятностью выживания, то первоначально она вычисляется по анализируемому фактору — Φ (который и представляет собой рассматриваемый ЭМИ), а затем по формуле суммы вероятностей совместных событий (элемент системы кроме воздействия ЭМИ может подвергаться и другим внешним воздействиям) находится интегральная вероятность выживания ИТКО:

$$P(_i,\ \Delta t) = 1 - \sum_{\forall\ \Phi \in \Phi_n} (p(\Phi) + p(\Phi_1) + \ldots + p(\Phi_2)). \tag{3}$$

В зависимости от расстояния от источника внешнего воздействия до ИТКО, мощности ЭМИ, его длительности и времени воздействия, условий расположения ИТКО, применения мероприятий и средств защиты ИТКО, вероятность поражения ИТКО, являющегося целью, определяется по формуле:

$$P = \left(1 - e^{-\rho^{2R^2/P^2}}\right), \tag{4}$$

где $\rho = 0,477$ — постоянная нормального закона; R — радиус поражения воздействующего фактора; P — вероятное отклонение пучка импульса от центра цели (ИТКО).

Безусловная вероятность поражения ИТКО электромагнитным импульсом определяется равенством:

$$P = PP\left(1 - e^{-\rho^{2R^2/P^2}}\right), \tag{5}$$

где $0 < P < 1$ вероятность применения ЭМИ по ИТКО; P — вероятность попадания электромагнитного импульса по ИТКО с учетом технической надежности генератора ЭМИ и преодоления им различного рода противодействий.

Электронное средство вычислительной техники «выживет» с вероятностью:

$$P = 1 - P = 1 - PP\left(1 - e^{-\rho^{2R^2/P^2}}\right). \tag{6}$$

С учетом возможного воздействия по ИТКО нескольких видов деструктивных воздействии в течение рассматриваемого периода вероятность его выживания:

$$P(_i,\ \Delta t) = \prod_{j=1}^{n} \left[1 - P = 1 - P_j P_j \left(1 - e^{-\rho^{2R_j^2/P_j^2}}\right)\right]. \tag{7}$$

На основе исследований предлагается ряд следующих действенных практических мероприятий по защите ИТКО от деструктивного воздействия ЭМИ [5, 6, 7, 8, 9, 10, 11]:

- средства ИТКО должны быть расположены в объектах оборудованными специальными устройствами типа грозозащиты, минимизирована длина кабельных вводов, особенно в вертикальной плоскости;
- размещать средства ИТКО в экранированном помещении или специальном экранированном блоке для защиты ее от опасного воздействия электрического и магнитного полей ЭМИ;
- в качестве экранирующего материала корпусов ИТКО применять листовой композиционный материал с внутренним барьерным слоем, а также полимерных композитов выполненных по технологии структур из дифракционных решёток, обладающим нелинейными свойствами, а размеры корпусов и их технологических отверстий должны находиться в строгих геометрических пропорциях;
- корпуса ИТКО экранировать покрытием из фольгоизола (металлическая фольга толщиной 0,2 мм, ожидаемое значение коэффициента ослабления $= 115$ дБ) и если отверстия в них относительно малы, то их можно отнести к неоднородным экранам со сплошной проводящей поверхностью;
- применить ресурсораспределительный подход на этапе компоновки элементов в пределах монтажной плоскости при помощи алгоритма последовательного обратного размещения и распространить принцип компенсации дестабилизирующего воздействия ЭМИ характеристиками устойчивости элемента к воздействию на этапе формирования стратегии размещения элементов;
- использование на узлах сети (ЭВМ, маршрутизатор, коммутатор, модем, сервер) схемной защиты, в том числе двух- или трехступенчатой защиты с применением разрядников, нелинейных полупроводниковых ограничителей, различных фильтров;
- прокладывать сетевого кабеля на участках небольшой длины в стальных трубах;
- прокладывать стальные тросы вдоль сетевых кабелей;
- применять кабелей сети питания в свинцовой оболочке, но с высокой электрической прочностью изоляции жил (не менее 10 кВ) при одновременном включении разрядников на входах аппаратуры;
- заземлять металлопокровы (оболочки и бронезащиты) кабелей цепей питания;
- включать разрядники в специальных устройствах линейной защиты (УЛЗ) вдоль кабеля между жилами и металлопокровом;

применять кабели в алюминиевой оболочке на протяжении всей топологии ЛВС ИТКО.

Литература

[1] Иванов В. А., Двилянский А. А. Оценка живучести объекта ЭВТ в условиях преднамеренного воздействия ЭМИ СВЧ. Сборник докладов и тезисов Межвузовской научно-практической конференции «Проблемы обеспечения безопасности в системах связи и информационно-вычислительных сетях», Голицынский пограничный институт ФСБ РФ, 2005.

[2] *Иванов В. А., Двилянский А. А.* Обоснование необходимости защиты локальной вычислительной сети от воздействий электромагнитных импульсов ультракороткой длительности с различными спектральными характеристиками // Сб. научных трудов Академии Спецсвязи России. 2004. № 16. С. 114–118.

[3] Дудник Б. Я., Овчаренко В. Ф., Орлов В. К., Филин Б.П, Холин А. В., Шурмин А. В. Надёжность и живучесть систем связи. М.: Радио и связь, 1984. С. 208.

[4] Голенкевич Т. А. Прикладная теория надёжности: Учебник для вузов по специальности «Автоматизированные системы управления». М.: Высшая школа, 1985. с. 186.

[5] Кочкаров А. А., Малинецкий Г. Г. Обеспечение стойкости сложных систем. Структурные аспекты. М.: Институт прикладной математики им. М. В. Келдыша РАН, 2005. с. 36.

[6] Барсуков В. С. Каналы силового деструктивного воздействия на компьютерные системы. Jetinfo, 2000, № 2.

[7] Антипин В. В., Годовицын В. А., Громов Д. В., Кожевников А. С., Раваев А. А. Влияние мощных импульсных микроволновых помех на полупроводниковые приборы и ИМС. М.: Зарубежная радиоэлектроника 1995. № 1, с. 37–52.

[8] Горячев В. А., Захаров С. М. Характеристики электромагнитных наводок в линиях связи микропроцессоров. М.: Успехи современной радиоэлектроники 2002, № 7, с.4–104.

[9] Иванов В. А., Двилянский А. А. Метод расчета электрического поля проникающего в металлические экраны ЭВМ при воздействии электромагнитного импульса. Сборник НТ, Выпуск 19. Орёл: Академия ФСО России, 2005. С. 158–165.

[10] Шубинский И. Б. и др. Активная защита от отказов управляющих модульных вычислительных систем. СПб.: Наука, 1993. 284 с.

[11] Мырова Л. О., Чепиженко А. З. Обеспечение стойкости аппаратуры связи к ионизирующим и электромагнитным воздействиям. М.: «Радио и связь», 1988.

ПРИЛОЖЕНИЕ 1

Между киберземлей и кибернебом: Цензура в Сети рухнет первого декабря (интервью с директором группы перспективных исследований сетевой безопасности Кембриджского университета Р. Рогозинским)

Л. И. Левкович-Маслюк

Рафал Рогозинский (Rafal Rohozinski) — директор группы перспективных исследований сетевой безопасности Кембриджского университета (Advanced network research group). Наша беседа с ним началась на мехмате МГУ поздно вечером 26 октября, сразу по завершении очень интересной международной конференции по безопасности и противодействию терроризму, где Рафал вел круглый стол «Борьба в Сети».

Однако в аудиториях внезапно отключили свет — как оказалось, перед зданием началась генеральная репетиция лазерного шоу с научно-просветительским подтекстом, за которой наблюдал лично ректор Садовничий. И сразу все как-то так закрутилось, что завершать беседу пришлось уже почти через месяц по электронной почте. Рафал слал свои ответы сначала из Кембриджа, а потом — с Западного берега известной многим по Библии великой реки Иордан.

В Палестине Рафал ведет полевые исследования по одному из главных своих проектов — в прошлом году он семь месяцев прожил на Западном берегу, изучая, как ИТ меняют палестинское общество. СМИ периодически сообщают о новых сражениях Интерфады (Interfada): так называют по аналогии с Интифадой идущие в Интернете серии атак и контратак произраильских и пропалестинских хакерских групп во всем мире. Гораздо меньше известно о взрывном росте инфотеха в самой Палестине. В частности, Интернет и мобильная связь сегодня — основная связующая структура деятельности главных политических сил Палестины, ХАМАС и ФАТХ.

)Опубликовано в журнале «Компьютерра» № 44 (664) от 1 декабря 2006 года.

На Западном берегу есть перемены

Рафал, вы напрямую общаетесь с этими организациями?

— Да, конечно, мы в прямом контакте — это часть нашей работы.

Эта работа связана с кибервойной Израиля и Палестины, Израиля и Хезболлы?

— Нет, в Палестине мы просто хотели увидеть, как население пользуется ИКТ-инфраструктурой.

В мирных целях?

— Во всех целях. Например, в политических: для информации, для координации. В глазах, скажем, израильтян ХАМАС — террористическая структура. Но в реальности это также и политическая структура. Если мы члены одной политической организации — как мы можем взаимодействовать, вырабатывать общую позицию? Если вы живете в Газе (Gaza), а я живу, например, в Рамалле (Ramallah) — вряд ли мы встретимся. Все общение идет по Интернету, по мобильному телефону. Сегодня на заседании конференции был очень интересный разговор — о том, что вебсайты террористической организации надо контролировать, закрывать и т. д. Но в Палестине, например, вебсайты не очень популярны. Зато там очень популярны службы мгновенных сообщений (instant messengers). Пару лет назад ХАМАС проводил массовый митинг. Участников собрали на него при помощи чата. Тысячи людей одновременно подключаются к одному чату — и связь налажена.

Что же показали ваши исследования?

— Выводы простые. Группы, которые были разобщены, сейчас очень быстро, очень эффективно координируются за счет ИКТ. Причем они работают с этими технологиями гораздо лучше, чем госорганы Палестины. Как обычно, сетевые структуры быстрее на все реагируют, быстрее могут организоваться, определиться с фактами, манипулировать информацией. Посмотрите на проблемы вооруженных сил (ВС) США в Ираке. США имеют новейшее оборудование, лучших специалистов. Но структура военных сил — та же, что пятьдесят лет назад. Они просто не могут быстро реагировать. А их противники — могут!

Но ведь полвека назад тоже были регулярные армии и партизанское движение, с которым армии не могли справиться.

— Да, но полвека назад партизаны могли работать только в географически ограниченном пространстве. Сейчас же, например, иракские повстанцы работают не только в Рамади (Ramadi) и Багдаде. Они могут заказывать и использовать ресурсы в Сирии, в Европе и т. д. Когда они

сообщают информацию о себе, она сразу идет на весь мир. Поэтому такие структуры сегодня много мощнее, чем полсотни лет назад.

Неужели Америка с вашей — Европы — помощью не может контролировать все эти коммуникации? Уж наверно, США не пожалели денег, чтобы создать в Ираке сеть прослушивания и просматривания всего, что только можно.

— Да, конечно, это так.

Что же не срабатывает?

— Вы знаете, легко создать сеть, оборудование. Но вот Израиль уже давно создал очень хорошую сеть прослушивания важных для него территорий. К тому же очень многие израильские военные хорошо говорят по-арабски. То есть в принципе они должны иметь возможность все предвидеть, все отслеживать, и очень эффективно. Но вот как-то не получается. По-моему, причина в том, что им не хватает «этнографической разведки». Мало слушать разговоры, надо понимать, что они означают — понимать контекст. И хорошо, если только двое людей разговаривают. А если это тысячи людей — распределенная сеть, как организация ХАМАС, или Хезболла, или организация инсургентов в Ираке, отследить все контексты практически невозможно.

Может быть, решающий фактор в такой войне не технический, а что-то иное: идеи, жертвенность?

— Да, наверное, это так. Но поразительно, что и, казалось бы, чисто техническая борьба часто выигрывается такими организациями, как ХАМАС или Хезболла. Возьмите ВС Израиля — это пример идеального воплощения того, что называется network centric warfare: широчайшее использование сетевых структур в военных целях. Но — именно и исключительно в военных. Хезболла же в недавней войне избрала совершенно иную стратегию, где самым важным был информационный удар в более широком смысле слова. Каков результат? Израиль проиграл по информационной части, хотя в чисто военном плане мог уничтожить хоть весь Ливан. Это был большой сюрприз и для Израиля, и, по-моему, для США.

Но заметьте, что эта информационная победа была обеспечена современными техническими средствами. Хезболла прослушивала даже военные коммуникации израильских сил и очень эффективно использовала полученные данные. Например, когда они перехватывали сообщения о том, кто погиб в израильских войсках, то сразу же, первыми, сообщали об этом на весь мир.

Кто Хезболле помог так оснаститься?

— Считается, что помог Иран, но мне кажется — вряд ли. Я думаю, они сами это сделали. Потому что в принципе это не сложно. Просто надо придумать. Они придумали.

Значит, у них работают хорошо образованные люди?

— Да, конечно, такие люди у них есть, технические кадры достаточно высококвалифицированные. Но главное — они понимают, как можно, используя ИКТ, обойти военную силу, которая их превосходит.

Откуда же у них такие специалисты, когда они появились?

— Я не могу комментировать кадровые ресурсы Хезболлы как таковой. Но факт, что ИТ-специализация в этом регионе становится все более популярной. Сегодня только в одной Палестине работает четырнадцать университетов. В каждом из них есть факультет компьютерного образования. Палестинские айтишники считаются едва ли не лучшими в арабском мире. И в Ливане, и в Палестине университеты готовят больше специалистов по ИКТ, чем по любой другой специальности. Одна из причин — в той же Палестине просто не существует других возможностей заработать хорошие деньги на месте. К тому же арабский рынок ИКТ един, в том числе из-за языка. И если ты квалифицированный специалист по компьютерам, то можешь работать и в Дубаи, и в Саудовской Аравии.

Самое интересное, что наиболее продвинутый в техническом плане университет — это университет ХАМАС в Газе. Он называется Исламским университетом Газы (Islamic University of Gaza), но все знают, что это университет ХАМАС. Там самая сильная кафедра мультимедиа, самые лучшие интернет-услуги.

Удивительно.

— Я был в Наблусе, это один из городов на севере Палестины. Там лагерь беженцев, несколько тысяч человек. Жизнь у них ужасная — каждый день стрельба, то и дело рейды израильских войск. Но при всем этом в лагере есть беспроводная связь, кабельная сеть, скоростное подключение к Интернету, а также как минимум четырнадцать интернет-кафе. Мне жутко интересно было — почему в лагере беженцев так много интернет-кафе?!

Ну и почему?

— Потому что компьютер там — это основа жизни вообще. Это единственное средство, чтобы выходить в мир, чтобы зарабатывать деньги, чтобы хоть чем-то заниматься.

В Палестине кто-нибудь занимается программным аутсорсингом?

— Они начинают. Они стараются. Но это очень тяжело. Потому что зарубежные инвесторы, которые могли бы вложить в Палестину деньги, пока выжидают. Тем не менее там уже есть своя ассоциация ИТ-бизнеса

(Palestinian Information Technology Association, PITA), которая объединяет около ста сорока маленьких предприятий. Они занимаются и софтом, и хардом. Есть очень развитое опенсорсное сообщество. Работают с ориентацией на арабский мир в целом, но иногда и на внутренний рынок тоже. Есть большой проект — поставить компьютеры во всех школах. Правительство решило, что ПО для школ должно быть только свободное — чтобы молодежь понимала, что можно дальше все это развивать самим, что мир ПО не сводится к Microsoft.

В 2002 году, когда израильские войска заняли Рамаллу и другие города Западного берега, многие университеты были закрыты. Тогда студенты из Bir Zeit University в течение трех месяцев сделали виртуальный университет — портал под названием Ritaj (`ritaj.birzeit.edu/register/?return%5furl=%2f`), чтобы люди могли продолжать учебу через компьютер. Потому что по жизни это было нужно, невозможно было без этого жить.

Вот почему у них такие хорошие ИТ-специалисты — потому что жизнь им дала не слишком много других возможностей. По той же причине там (как мне показалось, во всяком случае) намного больше людей старшего возраста, которые пользуются компьютером, чем в других странах, в том числе на Западе.

Кто оплачивает все эти компьютеры, сети — арабские шейхи?

— Сами палестинцы. Люди там готовы тратить сорок процентов своей зарплаты на сотовый телефон, на компьютер. Кстати, у каждого палестинца как минимум три сотовых телефона. Тоже удивительно.

Как палестинцы относились к тому, что вы приехали изучать их жизнь? С учетом того, что вы прибыли из Англии — почти из Америки, можно сказать.

— Ни малейших сложностей не было, даже наоборот. Но я ведь не только изучал, я им помогал в плане деловых, технических связей, консультировал — взаимодействовал, в общем. Кстати, среди палестинцев, которым больше сорока, очень много русскоговорящих, и когда они узнавали, что моя фамилия Рогозинский, видели, что я неплохо говорю по-русски, — сразу появлялся контакт (хоть я и не русский, а поляк).

Но главное, что существует некая культурная общность людей, которые занимаются компьютерами — по всему миру. Это выше того, что у нас может быть разная вера, разные этнические корни. И конечно, когда у нас одни цели, одни интересы, это очень помогает найти общий язык.

А есть ощущение, что из этого сообщества айтишников вербуются солдаты кибервойны, или даже активисты террористических групп?

— Несомненно, и это подтверждается тем, о чем я говорил выше: Израиль не смог подавить связь и командование Хезболлы, а Хезболла прослу-

шивала израильские коммуникации. Но главное оружие в руках Хезболлы или ХАМАС — не их умение писать компьютерные вирусы, а использование Интернета, радио, телевидения для перевода войны в виртуальную и в политическую плоскость, туда, где огневая мощь уже не играет решающей роли.

Как вы думаете, развитие ИТ в Палестине, рост образования в целом, современные средства связи — все это поможет установлению мира?

— В конце девяностых было много надежд и у палестинцев, и у израильтян, что ИТ может стать одним из мостов к миру. Масса энергии, огромные деньги были затрачены на создание технопарков, находящихся одновременно по обе стороны границы в Газе и на Западном берегу. На самом деле, бум в ИТ-образовании в Палестине как раз и начался с этих инициатив, так как все ожидали, что палестинские программисты будут работать в совместных израильско-палестинских компаниях, и эти компании будут успешны за счет соединения израильских ноу-хау с палестинскими предпринимательскими и программистскими талантами. Потенциал считался огромным, во всяком случае в масштабах арабоязычного рынка. Но увы, когда рухнул мирный процесс, рухнули и надежды на технологии как мост к прекращению конфликта. После возведения разделительной стены между Израилем и Палестиной, после разрыва всех созданных тогда связей трудно говорить об этих планах иначе как о несбывшейся мечте. Однако некоторый оптимизм внушает то, что израильские и палестинские специалисты продолжают встречаться, продолжают общаться, и на этом, человеческом уровне ничто еще не потеряно.

Парадоксы кибервойны

Часто приходится слышать термин — «кибервойна», но что это такое, по-моему, мало кто понимает. С одной стороны, известно, что до сих пор в мире не отмечено ни одного случая серьезной кибератаки, имевшей террористический характер. С другой стороны, вы цитировали недавно опубликованный американский доклад «Defence Science Board Report» 2000 года, где в качестве двух главных «необычных» (unconventional) угроз США названы: применение ядерного оружия негосударственными акторами и вывод из строя (также негосударственными акторами) национальной информационной инфраструктуры с помощью кибероружия. То есть кибероружие, кибертеррор ставится по грозности на одну доску с атомной бомбой. Что же это такое?

Рис. 1. Блок-пост «Каландия» на границе Палестины. Сотовая антенна служит израильтянам для мониторинга телефонной связи на Западном берегу

— Когда-то в СССР был начальником Генштаба маршал Огарков, и его можно назвать отцом концепции информационной войны. Эта концепция вытекала из его идей о революции в военном деле, обусловленной научно-технической революцией. Но в практической области развитие этих идей гораздо быстрее пошло на Западе. В середине девяностых стало ясно, что если страны мира будут широко использовать сетевые технологии (не обязательно военные), то появляется возможность атаковать эти сети программным путем, а также с помощью оружия, которое специально сделано для уничтожения коммуникационных инфраструктур, и военных, и гражданских. Это и было информационное оружие в первоначальном смысле. Но тогда же стало ясно, что нельзя это понятие ограничивать одним направлением. Например, Мартин Либицкий (Martin Libicki), очень заслуженный сотрудник RAND Corporation, в своей классической статье 1995 года «What is Information Warfare?» выделял семь форм информационного оружия, связанных с управлением и командованием, разведкой, психологическим воздействием, электронной борьбой, хакерством, экономической информацией и, наконец, собственно кибероружие для борьбы в «виртуальном мире (in virtual realm)». Тогда большой акцент был сделан на то, чтобы создать группировки, подразделения, занятые исключительно information operations — боевыми операциями в информационной сфере (сейчас таких группировок много). В начале девяностых появилась программная статья «Cyberwar is coming» Джона Аркиллы (John Arquilla) и Дэвида Ронфельдта (David Ronfeldt) где впервые было сказано о том,

что не только вооруженные силы государств могут использовать средства коммуникации в военных целях — но и другие группировки: политические, террористические, какие угодно. В этой же статье было введено понятие сетевой войны (netwar) — использование сетевой методологии, чтобы организовать свою деятельность. В отличие от этого, кибервойна (cyberwar) — это использование технологии, кибероружия (cyber weapons).

Но что же это за оружие — программные средства, аппаратные средства? Где сейчас передний край в этой области, какие там высшие достижения?

— Достижения, несомненно, есть. Но об этом в деталях никогда никто не говорит. Почему? Во-первых, потому, что совершенно неясно, как наличие этих средств борьбы согласуется с международным правом, относящимся к военным действиям. Во-вторых, опыт показывает, что очень легко в случае применения этого оружия определить, кто его использовал. Американские военные, например, говорят, что в истории многократно принималось решение не использовать такое оружие — именно потому, что боялись — если используют, то будет ясно, откуда это идет. Третья вещь: никто на самом деле не знает приемов. Не знают, как это оружие эффективно применить. Ведь его невозможно даже толком испытать. В США сейчас идет работа над тем, чтобы как-то согласовать эти средства с международным правом. Одновременно они пытаются выработать меры, способы оценки эффективности этого оружия. Все это не секретно, но делается на таких, знаете, полуоткрытых обсуждениях и полузакрытых конференциях.

Сегодня на заседании кто-то сказал, что четыре американских университета получили от правительства несколько миллиардов долларов на разработку нового поколения кибероружия.

— Я этим заявлением докладчика тоже был удивлен, до этого ничего подобного не слышал. Конечно, денег в этой области тратится много, — на защиту от вирусов, от компьютерных атак. Но о разработке средств для кибератак обычно никто не говорит, и вряд ли что-то публикуется в прессе.

Хорошо, мы не знаем, как действует кибероружие, его не испытывают — но что оно должно сделать? Какой цели достичь? Что произойдет в результате его применения?

— Насколько я могу судить, главная цель нынешних разработок — не разрушать компьютеры и сети противника, а делать более эффективной разведку. Получать пользу от перехвата данных через вирусы и им подобные программы.

А можно себе представить такое — началась война, тут же нажимается кнопка, и спутники связи противника отключаются?

— Ну, я думаю, вряд ли это получится. (Смеется.) Помимо всего прочего — давайте посмотрим на этот вопрос с точки зрения США. В Ираке больше восьмидесяти процентов каналов связи, которые американцы используют для военных коммуникаций, арендованы у коммерческих провайдеров. Поэтому, если США ударит таким оружием по инфраструктуре противника, то воздействие на них самих будет гораздо больше, чем на противника! В Афганистане то же самое. Конечно, у ВС США есть свои закрытые, сильно защищенные каналы, но они очень узкие, и военные вовсю пользуются коммерческими.

Фильтрация вслепую

Вы говорили, что сетевым структурам партизанского типа очень трудно противодействовать в информационной войне. С этим столкнулся Израиль в Палестине и в Ливане, в какой-то мере — США в Ираке. У вас есть теория о причинах этого?

— Я изучал такой вопрос: на противника какого типа рассчитаны те мощные меры противодействия в информационной войне, которые сейчас есть у высокоразвитых стран?

А эти меры действительно очень мощные, и прогресс за последние годы, особенно после событий 9/11 был огромным. Это можно увидеть по результатам учений по противодействию кибератакам, проведенных американскими ВС в 1997 году (Eligible Receiver) и в 2005 году (Silent Horizon). В обоих случаях это были внезапные атаки группы под условным названием «Красные» (Red Team) хакеров из АНБ, стремившихся получить контроль над критически важными сетями. В 1997 году эти учебные атаки, по-видимому, были весьма успешными — в СМИ сообщается, что «Красные» перехватили управление некоторыми компьютерами Тихоокеанского командования США, а также системами аварийного жизнеобеспечения крупнейших американских городов. В 2005 году ничего подобного сделать им не удалось. Получается, что от какого-то противника защита создана — но от какого? Этот ли противник сегодня нам угрожает?

С моей точки зрения, такая защита от кибератак не имеет никакого отношения к тем информационным ресурсам, которые действительно эффективно используются экстремистскими группами, в том числе и террористическими.

Почему?

— Дело в том, что эти группы не занимаются никаким хакерством. Они используют Интернет самым обычным образом — для переписки, чатов, форумов. Подавляющее техническое превосходство в данном случае

не срабатывает. Это показал хотя бы пример с Израилем и Хезболлой, о котором мы уже говорили. Нужна не другая технология, а другая тактика.

Главное оружие экстремистских групп — символическое содержание их акций. Исследования, в том числе прямые беседы с недавними активистами таких групп показывают: они просто не рассматривают кибератаки как возможность для достижения своих целей — именно в силу низкого символического содержания кибератак. Интернет используется ими для сбора и пересылки денег, вербовки сторонников, связи, распространения информации о своих действиях, взглядах, чтобы сеять страх и преувеличивать свою значимость.

Любые попытки технически подавить эту активность приводят к обратным результатам: создают дополнительный мобилизующий эффект. Нужны меры совершенно другого типа, совсем не кибернетические: международная координация, обмен информацией между спецслужбами, а самое главное — нужно вводить этих акторов и сообщества, которые их поддерживают, в русло обычной политической жизни.

В связи с этим — каков может быть эффект «фильтрации контента», которая практикуется в довольно многих странах?

— Я считаю, что подобные меры — это одна из основных опасностей, к которым ведет «кибернетическая» борьба против терроризма и экстремистских групп. Наша программа ONI (OpenNet Initiative, opennetinitiative.net) как раз призвана на строго научной основе изучить эту практику и последствия, к которым она приводит. Эту программу реализуют четыре ведущих университета: Кембридж, Гарвард, Оксфорд и Университет Торонто. Соответственно, есть четыре ведущих исследователя, два из которых, Рон Диберт (Ron Deibert) из Торонто и я, участвовали в московской конференции.

Как же вы это изучаете?

— Тут сочетаются два подхода — в сущности, так же работает и разведка! — технический и «человеческий». При помощи специального ПО на те или иные сайты в изучаемой стране наши эксперты заходят дистанционно, физически находясь в Канаде или в Англии, но через те серверы, которые используют жители изучаемой страны. И тогда мы сразу видим, к каким ресурсам доступ у них ограничен. Эти сайты могут быть видны извне, но оказываются закрытыми для населения страны. На втором этапе в страну выезжают наши специалисты, с ноутбуками, на которых установлен соответствующий софт, и на месте собирают информацию, к каким ресурсам ограничен доступ. После всего этого выпускается доклад, который находится в свободном доступе на вебсайте программы.

Какие страны вы уже обследовали?

— Вьетнам в 2005–06 годах, Йемен (2005), Тунис (2005), Сингапур (2004–05), Китай (2004–05), Белоруссию во время президентских выборов этого года….

Ну и что в Белоруссии обнаружилось?

— Обнаружилась неожиданная для многих вещь: оппозиционные ресурсы и сайты независимых медиа там не подавлялись (по крайней мере в период выборов) хотя, как показали наши же исследования, такая возможность у властей была. Доступ к ним был практически свободным, хотя и не без некоторых трудностей. А самая мощная система фильтрации контента и ограничения доступа — китайская. Она подкреплена еще и хорошо проработанной законодательной базой. Впрочем, многие международные медиа-ресурсы в Китае доступны.

В 2007 году мы будем выпускать большое сравнительное исследование более чем сорока государств, включая восемь стран СНГ. Туда же войдут результаты и по фильтрации Интернета в странах Европы и Северной Америки — в этих странах такая практика тоже имеется, причем в некоторых случаях она связана с очень неоднозначными юридическими и этическими обстоятельствами.

Как технически эта фильтрация делается?

— Практически всегда используются коммерческие системы уровня предприятия. У этих систем, надо сказать, есть серьезные недостатки. Например, их очень трудно точно настроить на тот контент, который вы желаете блокировать. Поэтому иногда блокируется заодно и безобидная информация — Рон Диберт в своем докладе приводил пример, как в одной из стран стал вдруг недоступен вебсайт американского посольства, так как в слове «usembassy» система отреагировала на порнографическую, по ее мнению, строку «ass». С другой стороны, не так трудно обойти блокировку, которую обеспечивают эти системы.

Хакеру нетрудно, а обычному человеку вряд ли.

— А мы разрабатываем необходимый софт и выкладываем его для бесплатной загрузки. Рон Диберт — директор находящейся в Торонто Citizen Lab, технического центра программы ONI. Как раз эта лаборатория отвечает за технологию обхода цензуры. Официальный выпуск Psiphon, основного свободного продукта для этой цели, намечен на первое декабря 2006 года. В честь этого состоится специальное мероприятие в Торонто под названием «Protect the Net».

А правительства не будут возмущаться?

— А что они могут сделать?

ПРИЛОЖЕНИЕ 2

Доктринальное лидерство (интервью с заместителями директора ИПИБ МГУ В. В. Ященко и А. А. Сальниковым)

Л. И. Левкович-Маслюк

Думали мы, думали в редакции — чем развлечь читателя в последнем номере уходящего года, да не придумали ничего лучшего, чем загрузить под завязку материалами про террор и интеллектуальную борьбу с ним.

Этого чтения должно, по расчетам, хватить на весь период наших традиционных зимних каникул. В разделе «Анализы» Михаил Ваннах дает общий анализ «информационного измерения» террора. В теме номера Бёрд Киви знакомит нас с передовыми идеями по анализу и защите жизненно важных инфраструктур — информационных в первую очередь. Открывает же тему обстоятельная беседа об угрозах этим инфраструктурам, исходящих из киберпространства. Ну и разумеется, о защите от них. Может ли кто-нибудь перекрыть движением мышки наши драгоценные трубопроводы, обесточить провода, запутать расписание поездов — и что делается для того, чтобы никто не мог?

Обо всем этом я допытывался у очень компетентных людей с впечатляющими титулами. Наши собеседники сегодня — два заместителя директора Института проблем информационной безопасности МГУ — Валерий Ященко (советник Ректора МГУ) и Алексей Сальников (национальный эксперт в Научном комитете Россия-НАТО по кибертерроризму). Как обычно, когда речь идет о вещах деликатных, вопросы были об одном, а ответы оказались о другом. Зато теперь нам легко придумать вопросы к этим ответам — и увидеть, что эти вопросы проясняют едва ли не больше, чем ответы.

Честно признаюсь — был в планах еще и репортаж с переднего, можно сказать, края кибероборoны одной из самых мощных и знаменитых, и абсолютно жизненно важных «инфра». Там вопросы и ответы состыковать пока совсем не удалось. Может быть, удастся в недалеком будущем. Тогда мы узнаем еще чуть больше о том, чего толком не знает никто.

)Опубликовано в журнале «Компьютерра» № 47–48 (667–668) от 22 декабря 2006 года.

Обгоняем, но отстаем

Заглянув в обзор, выпущенный немецким Федеральным департаментом информационной безопасности (BSI, Bundesamt fur Sicherheit in der Informationstechnik), я обнаружил там удивительную вещь — авторы утверждают, что по состоянию на 2002 год (обзор вышел в 2004 году) у многих из девятнадцати изученных ими стран нет национальной стратегии по информационной защите национальных же критических инфраструктур. В том числе — у Великобритании, Японии, Новой Зеландии, самой Германии, а также и у России.

Ященко: Если так, то авторы не владеют материалом. В России была принята самая первая в мире национальная доктрина обеспечения информационной безопасности (ИБ) — в сентябре 2000 года. Там отражен весь спектр угроз ИБ — от угроз критическим сетевым структурам до угроз в духовной сфере. После этого мы долго учили всех остальных, как это делать. А американцы родили свои стратегии гораздо позже.

История такова. Хартия построения информационного общества была подписана президентами G8 в июне 2000 года, и к этому времени была уже готова наша доктрина. А в июне 2001 года в МГУ прошла международная конференция по ИБ, в которой участвовали 45 стран. Я занимался ее организацией и могу рассказать о некоторых деталях. К нам приезжал тогдашний директор Центра Маршалла (Европейского центра исследований по вопросам безопасности им. Джорджа К. Маршалла, `www.marshallcenter.org`) подписывать договор с ректором МГУ о проведении этой конференции, в том числе на деньги Центра, а общий бюджет был порядка 1 млн. долларов. С марта по май мы трижды встречались с западными экспертами по ИБ, обсуждали программу и повестку дня. Одним из главных камней преткновения был сам термин «информационная безопасность». Закончилось это очень смешно — за месяц до конференции американцы поставили прямое и жесткое условие своего участия: чтобы в докладах ректора МГУ Виктора Садовничего и первого заместителя секретаря Совбеза Владислава Шерстюка (ныне директора нашего института) термин «информационная безопасность» не использовался. Мы были вынуждены заменить его на термин «информационная этика». (Причины такой их позиции очень понятны, но не будем сейчас в это углубляться.) И только после 11 сентября 2001 года американцы поняли, что они не самые умные. Что у них многое не так, многое неправильно. После чего, в феврале-марте 2002-го, они по линии Совбеза пригласили нас сделать серию докладов на семинаре в Вашингтоне, по нашей доктрине ИБ. Ну а в марте 2003 года Буш подписал документы о национальной стратегии США по ИБ — три «Национальные стратегии»: защиты киберпростран-

ства, защиты информационных сетей высших органов власти и защиты критически важных объектов. Много взяли у нас, но выкинули всю гуманитарную составляющую — у нас в доктрине очень много места уделено вопросам культуры, создания единого образовательного пространства и т. п. Они все это выкинули и не понимают важности этих вещей до сих пор. События 9/11 на них, конечно, сильно подей твовали. Эти уроки изучаются до сих пор, и глубочайшим образом. Мы с Алексеем были в мае в Нью-Йорке, провели там пару семинаров в университете SUNY (State university of New York), послушали очень интересные доклады. Например, по заказу мэрии Нью-Йорка университет проводил исследование, и оказалось, что в ходе событий 9/11 выявилась масса нестыковок между базами данных ФБР, полиции, пожарных (аналог нашего МЧС). Пожарные получают сигнал от спецслужб: горит дом, надо кого-то спасать, приезжают — нет такого адреса! Это — к вопросу о стратегии.

А у нас все это уже в идеальном состоянии?

Сальников, *Ященко* (*в один голос*): Нет! Конечно, нет. Но на политическом уровне наша стратегия была самой передовой. Потом уже мы отстали в реализации. Американцы нас обогнали, потому что выделили большие деньги на реализацию всех этих идей. Тем не менее в доктринальном смысле мы до сих пор впереди.

Один на один с триадой

Все-таки в общей доктрине ИБ от 2000 года упоминается, если не ошибаюсь, только информационная инфраструктура — либо страны в целом, либо та, что связана с обороной или госуправлением. Акцента на критических инфраструктурах (ИС) в более широком понимании там нет. Вы ведь только что закончили в вашем институте исследование по ИБ критических ИС. Можно ли рассказать о результатах, о подходах к этой проблематике? Причем желательно как можно нагляднее — хотя я знаю, что вы больше занимались концептуальными вопросами, например, что считать «критическим», а что не считать. Да, необыкновенно важно формулировать стратегию, концепцию в этих вопросах. Но ведь всех волнуют более приземленные вещи. Вот метро, вот линия электропередач, вот железная дорога — кто всемуэтому угрожает из киберпространства? Чем это грозит? Как строится защита? Кто сражается с той и с другой стороны?. Какими средствами?

Я.: Вопрос только об информационной безопасности или о безопасности в целом?

В целом — но с упором на ИБ!

Я.: Если в целом, то этим занимаются у нас много и давно. Есть масса документов. Закрыты только технические детали, стратегия открыта. Хотя понятие «критически важные ИС» у нас стали употреблять в документах только три года назад.

У нас есть список критических объектов, угроз им?

Я.: Список есть. Секретный, естественно, на уровне конкретных предприятий. Но идеология понятна — туда входят опасные производства, военные системы управления. Транспорт, связь, финансы, здравоохранение, телемедицина….

С.: Это те структуры, информационное воздействие на которые может привести к гибели и травмированию людей.

От кого же надо все это защищать?

С.: Сейчас принято рассматривать триаду противников. Во первых — киберхулиганы. Это, как правило, одиночки или небольшие преступные группы. Типичная угроза от них — воруют номера банковских карт через Интернет. Следующий уровень — кибертерроризм. Здесь уже действуют организации, часто — распределенные, сетевые по структуре. Третий уровень задействует уже силы государства, — информационная война.

Я.: Вот в это лучше не углубляться, дело очень тонкое — даже Рафал Рогозинский, известный эксперт из Кембриджа, у нас на конференции недавно рассказывал, что с юридическими вопросами тут большие сложности (см. «Компьютерра» № 664. — Л. Л.-М.).

Но понятие информвойны существует, и есть страны, которые могут владеть технологией такой войны. Причем их больше, чем стран, которые обладают ядерным оружием, потому что материальная база гораздо доступнее.

С.: Классический пример информвойны, о котором много пишут, но неизвестно, было это на самом деле или нет, — начало операции «Буря в пустыне». Якобы у Хусейна в этот момент процентов восемьдесят систем управления войсками вдруг отключились. Но с примерами сложно. Любая структура, тем более критически важная, всегда постарается как можно скорее закрыть любую информацию о попытке информатаки на нее.

Особенно если атака была успешной. Ибо это очень серьезный удар по имиджу. Поэтому найти достоверную информацию такого типа, боюсь, практически невозможно. Возьмите известную историю, когда половина западного побережья США вдруг лишилась электроэнергии. Сразу стало ясно — был какойто сбой информационного характера. Скорее всего, просто технический сбой. Но может быть — чье-то воздействие. Кто это может определить по доступным публикациям? Никто. Данных нет.

Я.: Единственное, с чем сейчас все согласны, — ни в России, ни в мире пока не зафиксировано ни одного акта кибертерроризма. Но, кстати, не потому, как думает Рафал, что террористам неинтересен «символический эффект» таких атак! Мы с ним постоянно ведем дискуссии на семинарах и конференциях — он неправ, дело тут в другом. Но это уже отдельная тема.

Существуют у нас в стране хакерские группы, которые профессионально занимаются взломом сетей, добычей «чувствительной» информации? Разработкой программ для всего этого? Созданием вирусов, троянов?

Я.: Не забывайте — мы с вами находимся в Московском государственном университете! У нас исследуются научные проблемы ИБ. А такие вопросы — компетенция МВД, управления «К».

С.: Да, хакерские группы есть, и, как я понимаю, достаточно глубоко законспирированные. Мы с многими госструктурами дружим, конечно, в том числе и с МВД — но какие группы им известны, что там с ними происходит, управление «К» не говорит никому и никогда. Это их компетенция.

Это же все-таки бизнес, хоть и криминальный. Денежные потоки, видимо, можно отследить?

Я.: Первым делом искать, кто платит, — типичнейшая ошибка в этой области. Ситуация другая: очень многие, особенно дети, совершают свои «киберпреступления» по совершенно другим мотивам — они фанатики всяческого «взлома».

Недавно читал беседу двух американских ИБ-специалистов, они говорят как раз обратное: что появился «new bad guy», вместо классического хакерафаната — хорошо оплачиваемый (криминалом) профессионал.

Я.: Есть такое явление. Но «массовка» — это фанаты. На международных конференциях об этом часто говорят.

У нас «государственные хакеры» испытывают на прочность защиту ИС, как в Америке? Вашему институту такое не предлагали?

С.: Если бы нам предложили, мы бы отказались. Ведь есть же стандартные процедуры для таких вещей. Сертификация средств защиты в ФСБ, например, и есть учебный взлом — чаще на бумаге, но иногда и натурно.

Я.: Любые такие заключения об уровне ИБ делаются в рамках закона о контроле. Приходит комиссия на предприятие и проверяет соответствующий регламент в рамках полномочий. Если это предусмотрено, могут промоделировать и кибератаку.

Как вы оцениваете динамику безопасности наших ИС?

Я.: Состояние дел улучшается — в целом. Но по конкретным предприятиям ничего комментировать не можем.

Мониторинг, сертификация, рынок

На конференциях в вашем институте математики всегда делают массу докладов о моделях атак, методах обнаружения вторжения в локальную сеть и т. п. Но это теория, а на практике — насколько хорошо мы сегодня умеем обнаруживать информационные атаки?

Я.: Это проблема глобального масштаба — мониторинг кибератак, отслеживание проникновения в сети. Причем проблема не только технологическая, но и политическая — например, мы не можем мониторить серверы на чужой территории, даже внутри страны мы не все сети можем мониторить. Есть множество корпоративных сетей — в том числе у Газпрома, РАО ЕЭС, РЖД, — где своя физическая инфраструктура, не связанная с бэкбонами Интернета. Причем по причинам коммерческого характера эти сети не мониторят даже спецслужбы.

С.: Практически в каждом министерстве есть своя ведомственная сеть. И эта сеть всегда является объектом атак.

Естественно — потому что какой смысл ломиться на веб-сайт, к примеру, Газпрома, где заведомо нет никакой критической информации? Но тем не менее и на веб-сайты крупных компаний и других заметных организаций непрерывно идут атаки.

Я.: Совершенно верно. Например на веб-сайт президента РФ за одиннадцать месяцев текущего года было более ста тысяч кибератак. Причем в данном случае это не попытки дефейсинга или рассылки спама с этих серверов, тут другие типы атак. Но наш институт не занимается оперативными мерами борьбы против таких вещей, мы только даем рекомендации и ведем научные исследования. В том числе разрабатываем программы для мониторинга атак. Хотя большинство сотрудников в разное время вплотную занималось и практическими вопросами.

С.: Таксономия атак очень сложная. Сегодня по общепринятой международной классификации выделяют порядка шестисот видов кибератак, и эта цифра все время растет. Соответственно и программы регистрации атак, мониторинга непрерывно обновляются — точно так же, как антивирусные средства.

Существует у нас единый центр мониторинга кибератак?

С.: Единого центра нет — во всяком случае, открытого. По научным и образовательным сетям такая работа, насколько нам известно, ведется

только в Курчатовском институте под руководством Алексея Солдатова. Кибератаки на органы госвласти мониторят силовые структуры, в частности ФСБ и МВД. Министерства, крупные компании — например, Газпром или РАО ЕЭС, имеют собственные службы информационной безопасности. Разработкой программ и аппаратуры компании и министерства обычно не занимаются, используют то, что есть на рынке.

Я.: Другие страны стали раскрывать информацию о своих центрах мониторинга совсем недавно. Мы с Алексеем были в 2004 году на очень узкой конференции в Мюнхене, посвященной как раз этой проблеме. Там впервые рассказывалось о национальных центрах мониторинга, причем я был поражен тем, насколько подробно и открыто это делалось. Выступали начальник центра мониторинга кибератак МО США, директор центра мониторинга Великобритании, его коллега из Германии (там центр мониторинга — отдел бундесвера). И важнейшим вопросом был вопрос о международном сотрудничестве и обмене опытом. Потому что информационное пространство на самом деле едино. Оно не имеет границ! Защититься от атак в одиночку ни одна страна не может. Известный пример — веб-сайт ЦРУ два года назад был взломан некими «студентами из Томска». Но есть соглашения между ЦРУ и ФСБ о взаимодействии, поэтому людей в Томске быстро нашли. Суда не было, случай был не очень серьезный, главное, что система сотрудничества сработала. Но заставить ее работать очень трудно, в частности из за различий в национальных законодательствах.

Не кажется ли вам, что есть нечто парадоксальное в том, что теракт против той или иной инфраструктуры ударит по всему населению, по всему государству — а защищает ее не государство, а закрытая ведомственная служба?

Я.: Сейчас в Госдуме рассматривается проект закона, который будет регламентировать ответственность в этих вопросах. Все вопросы должны решаться на основе соглашения государства, бизнеса и гражданского общества. Эти соглашения и оформляются в виде законов. Государственные органы юридически контролируют процесс, а бизнес в данном случае должен обеспечивать функциональную составляющую мер безопасности.

С.: Противоречия нет еще и потому, что эти компании — крупнейшие экономические игроки, и им не интересно пускать кого бы то ни было в свои информационные потоки. Там масса конфиденциальной информации, которую они не хотели бы показывать госорганам. Но зато государство теперь жестко навязывает сертификацию средств защиты. Всевозможные «отраслевые стандарты» больше не будут использоваться. Такой ситуации, когда, к примеру, криптографические средства заказываются у некоей частной компании, не имеющей серьезной гослицензии, но близкой к ру-

ководству заказчика, больше не будет. Но надо помнить, что существует рынок средств защиты информации. И система сертификации, хочет того государство или нет, становится активнейшим инструментом игры на этом рынке. Тот, кто является лицензиатом соответствующих структур (ФСТЭК [Федеральная служба по техническому и экспортному контролю, занимается противодействием иностранным техническим разведкам], ФСБ), автоматически получает преференции на рынке, поскольку многие компании обязаны покупать сертифицированные средства. Следовательно, отделы по лицензированию и сертификации находятся на острие экономической борьбы. Именно поэтому было принято решение, что в сертифицированных средствах должны использоваться только ГОСТовские алгоритмы. А как их воплощать — это уже другое дело. Те, кто сертифицирует, будут только смотреть, правильно ли реализованы эти стандарты.

Ну а «импортные» средства защиты и/или мониторинга коммерсанты могут у себя поставить?

С.: Их невозможно лицензировать. То есть для внутрикорпоративного использования — ради бога. Для обмена с Центробанком и госорганами — будь любезен поставить сертифицированные средства.

В Германии в начале 2000-х государство рекомендовало бизнесу использовать для деловой переписки программу GPG (опенсорсный аналог знаменитой PGP).

С.: Наши стандарты на электронную цифровую подпись построены на алгоритме типа Эль Гамаля. Поэтому PGP, RSA и все, что вокруг них, у нас не лицензируется, насколько мне известно. Но там, где не нужна лицензия, — пожалуйста. Де-факто PGP сейчас почти стандарт для шифрования частной переписки в Интернете.

А опенсорсность дает преимущество в надежности? Ведь программу могут проверять все желающие.

С.: Чтобы аккуратно просмотреть такие коды, нужны огромные затраты, надо надолго занять группу высококлассных спецов. В Минатоме в начале 90-х изучали коды Microsoft Windows одной из тогдашних версий (они были предоставлены Microsoft в полном объеме), в связи с установкой специального ПО на предприятиях атомной отрасли по программе контроля за ядерными вооружениями. Аналогичная история была позже, в связи с использованием программ под Windows в госструктурах. Коды были открыты на каких-то сверхжестких условиях, смотреть можно было только в отдельном помещении, с дискетой не заходить, смотреть с экрана и т. п. — но тем не менее. В результате — отдельные куски проанализировали, ничего не нашли. Ну и что? Полностью все эти гигабайты невозможно проанализировать. То же самое и с опенсорсом.

У нас есть разработки своих защищенных операционных систем?

Я.: Леонид, что значит «у нас»? Все равно каждая фирма, организация доверяет только себе. Из-за того, что сегодня все демократично, понятие «у нас» лишается того смысла, который вы, я полагаю, в это слово вкладываете.

С.: Классический пример. Я вел переговоры с одним банком о проекте по оценке их инфобезопасности. Говорю: в нашем институте есть специалисты, которые могут провести так называемое «обследование безопасности информационных систем» (мы такие работы часто делаем, в том числе для коммерческих фирм). Объясним, где у вас дыры могут быть. Смотрю — нет реакции. Потом объясняют: «Алексей, приходи к нам в банк работать, и тогда ты это сделаешь. Но заказывать на стороне такое исследование мы не хотим, потому что придется раскрыть информацию, которую не хотим раскрывать. Мы доверяем только себе и своим сотрудникам». Это просто классический пример отношения к внешнему аудиту.

И в критических ИС то же самое?

С.: Естественно.

Я.: Я совсем по-простому скажу. Вторая сторона вопроса — не всегда даже крупный игрок заинтересован, чтобы у него не было дыр в ИБ.

Почему?

С.: Потому что иногда он думает: «Если ты придешь ко мне и сделаешь все как надо — как же я тогда буду воровать деньги?»

Раскрыться, чтобы защититься

С.: Пример с нестыковкой ведомств в Нью-Йорке, о котором мы говорили, показывает одну из самых больших опасностей, связанных с ИБ критических ИС. Эти ИС — огромные и очень сложные, но часто построены на сегментах, которые мало связаны друг с другом. Внутренние сети министерств и ведомств очень плохо совместимы, и это глобальная проблема. К счастью, этим всерьез занялись Минсвязи и Федеральное агентство по инфотехнологиям.

Я.: У нас когда-то пустили создание этих сетей на самотек, и каждый лепил, как мог. Но два года назад все это было проанализировано, и приняли единственно возможное решение — делать надстройку, через которую все будут общаться, то есть создать федеральный информационный центр для межведомственного взаимодействия. В этом году уже демонстрировался макет системы. Данные из Москвы передавались в центр другой организации, условно говоря — кто-то пришел в Москве в ГИБДД, и запрос об этом человеке, о машине идет по всем ведомствам. И по квартире,

кажется, был такой тестовый запрос. Все сработало более или менее нормально.

Где же берутся кадры для всех этих проектов? ИБ сегодня — это множество рабочих мест. ИБ — самая модная ИТ-специальность в любом вузе. Действительно тут есть большое поле деятельности или это просто мода?

Я.: Специальность и правда модная, но люди, которые закончили МГУ — ВМК, мехмат, не очень востребованы по этой линии. В основном нужны не разработчики, а те, кто будет эксплуатировать готовые системы.

С.: Не совсем согласен. Я знаю, что в коммерческих структурах, в банках на самом деле востребованы квалифицированные люди, которые могут разрабатывать и сопровождать именно построение системы ИБ в целом. Конечно, надо ее и наполнить — купить нужное железо, поставить нужные программы, но в первую очередь грамотно придумать концепцию системы. Если же говорить о науке — например, о криптографии, то в ней и в смежных вопросах ИБ сейчас огромное количество новых научных задач. Надо только учитывать сейчас степень востребованности науки в России вообще.

Я.: По поводу задач в более широком смысле слова — существует официально утвержденный в 2001 году список 114 приоритетных научных задач в области ИБ (показывает документ: «Научные и методологические проблемы информационной безопасности», сборник статей под ред. В. П. Шерстюка, М., МЦНМО, 2004).

Беру наугад. Задача 2.2.1.5 — «исследование проблем информационной безопасности общероссийской информационной структуры». Нужное дело, бесспорно. Но как может быть сразу 114 приоритетных задач? В каком смысле они приоритетные?

Я.: Это очень полезный список, здесь представлены все аспекты ИБ, от фундаментальных философских до математики, криптографии, стеганографии, и кончая кадровыми вопросами. Многое имеет отношение и к критически важным ИС.

Отлично. Но давайте в заключение обсудим простой житейский вопрос: с чего начать компании, которая хочет себя защитить?

С., *Я.* (*хором*): От чего?

От атаки по информационным каналам.

С.: Нет, так не ставится вопрос. Компания должна четко объяснить специалисту, от чего она хочет защититься. Все компании всегда произносят те же слова, что и вы сейчас! Тут и начинается работа специалиста, который конкретизирует — от кого защитить, что защитить.

Я.: Защита всегда конкретна. Нужно понять, какую информацию хотим сохранить, и самое главное — создать модель противника.

С.: Может быть такая постановка задачи: мне не страшно, что будут читать то, что я пишу, — но страшно, если там что нибудь изменят. Или так: если прочитают Петров и Сидоров, не страшно, а если мистер Джонс — страшно. Причем все они работают в моей компании.

Я.: Чтобы дать рецепт, нужно влезть в компанию. То есть если хочешь получить надежные рецепты — должен раскрыться. Вот это многих останавливает. Первый этап информационной защиты — твоя оценка того, кто тебе угрожает.

А у нас даже ИС этого не делают?

С.: Нет, конечно. Вместо этого они идут на большие расходы и создают собственные подразделения, куда и пытаются набрать лучших специалистов.

Вот это и есть ключевой тезис — о раскрытии. Очень серьезная проблема!

Я.: Ключевой тезис такой: у нас в стране не было и пока нет системы подготовки кадров, которые могли бы давать такие рекомендации. Остались только те, кто был воспитан еще... в давние времена. Поэтому во всех крупных структурах люди именно такие. Для этого нужно быть широко образованным человеком.

Такого образования уже нет?

Я.: Нет.

То есть — катастрофа?

Я.: Катастрофа. Мы в МГУ очень узкие специализации готовим. Людей широкого профиля, которые могут дать рекомендации по защите крупного объекта, никто нигде в России не готовит. За исключением закрытых структур, готовящих кадры для закрытых же структур. 120 вузов открыли специализацию по ИБ. Но по пальцам можно пересчитать вузы, которые готовят действительно хороших специалистов.

С.: Чтобы готовить специалистов, нужно самому быть специалистом и иметь большой опыт. А таких преподавателей, увы, немного.

Что можете порекомендовать — где лучше учиться по этому профилю?

Я.: Лучше всего — в ИКСИ (Институт криптографии, связи и информатики) академии ФСБ. Но он готовит специалистов только для военных и для себя. Далее — МИФИ (факультет ИБ), МГТУ им. Баумана (но там тематика несколько уже, с ориентацией на технические средства защиты). Потом — РГГУ, МИЭМ, Московский Университет связи, в МИРЭА есть хорошая кафедра. В послед ние годы резко вырос Самарский универси-

тет. Проблема образования каждый год обсуждается на всех уровнях — но пока ничего не сдвинулось с места.

А на Западе какие университеты сильнее всех по этой части?

С.: Там много очень сильных школ. МТИ, Цюрих (ETH), прекрасная школа — Бельгийский католический университет. Они открыты, но до определенного предела. Некоторые работы выполняют для своих спецструктур, кое что им не рекомендуют обсуждать на конференциях.

Значит, у нас такой уровень только у военных, а там и у гражданских?

Я.: Могу ответить так: мы опоздали на тридцать лет с четким разделением проблематики ИБ на открытую и закрытую. Когда у американцев в 1975 году появились Диффи и Хеллман — это было начало. После нескольких лет борьбы их отпустили «на волю», и пошло все это развиваться в университетах. Сначала был принцип добровольного цензурирования, с докладом в АНБ, но потихоньку все освободилось.

С.: А в России, уже после того, как Советский Союз рухнул, еще долго продолжали бороться против открытого крипто, и вообще открытости в ИБ. Само слово «криптография» было секретным.

Я.: Настоящий рывок к открытости у нас тоже произошел — но только пять лет назад, когда в МГУ состоялась международная конференция «Московский университет и развитие криптографии в России».

Часть VI

КРУГЛЫЙ СТОЛ «КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА»

Вступительное слово проректора МГУ им. М. В. Ломоносова В. А. Мамонтова

Уважаемые коллеги!

Тема нашего круглого стола «Комплексная безопасность критически важных объектов топливно-энергетического комплекса». Сегодня мы планируем всесторонне обсудить проблему обеспечения защищённости критически важных для национальной безопасности объектов инфраструктуры и населения страны от угроз техногенного, природного характера и террористических проявлений. К таким объектам несомненно относятся производственные объекты топливно-энергетического комплекса нашей страны.

Ознакомление с темами докладов и сообщений, заявленных на заседании «круглого стола», даёт возможность оценить сложность и многоплановость рассматриваемой проблемы. На наш взгляд, основными задачами при её решении являются следующие:

1. *Формирование перечня критически важных для национальной безопасности объектов и обоснование требований к способам и средствам их защиты от аварий и террористических проявлений.*
2. *Оценка природных и техногенных рисков и определение мер по их компенсации.*
3. *Обоснование комплекса технических средств и организационных мер по обеспечению требуемого уровня защищённости объекта от террористических проявлений.*
4. *Обеспечение готовности руководителей и персонала объектов к действиям в условиях возникновения чрезвычайных ситуаций, обусловленных авариями, стихийными бедствиями и террористическими проявлениями.*

С позиций университетской науки, первостепенное значение имеет разработка научно-методических вопросов обеспечения защищённости критически важных для национальной безопасности объектов.

Одной из проблем здесь является наличие и состояние нормативно-методических документов, регулирующих вопросы безопасности и противодействию терроризму. Мы надеемся, что содержание основных норматив-

ных документов в этой сфере станет одной из тем обсуждения на нашей встрече.

Значительный интерес представляет история становления научно-обоснованных методов оценки риска опасных производственных объектов, методические подходы для создания системы критериев отнесения промышленных объектов к критически важным, использование информационных технологий при управлении промышленной безопасностью.

Эти и другие вопросы заявлены сегодня для обсуждения. И последнее, комплексность и сложность задач, стоящих в этой сфере требует объединения усилий государства, бизнеса и науки в деле подготовки специалистов нового уровня, экспертов в области промышленной безопасности и противодействия терроризму. Эта задача может быть успешно решена при активном участии ведущих научно-педагогических школ Московского университета, объединения усилий ученых и специалистов-практиков.

Хочу пригласить к заинтересованной дискуссии и обмену мнениями по этим и другим актуальным вопросам. Мы рассчитываем, что в процессе сегодняшней работы нам удастся существенно расширить наши представления по решению проблемы обеспечения защищённости критически важных для национальной безопасности объектов инфраструктуры и населения страны от угроз техногенного, природного характера и террористических проявлений.

Перспективные технологии предотвращения несанкционированного доступа к трубопроводам

Б. Н. Епифанцев, К. С. Патронов

Очевидно, что на сегодняшний день экономика России опирается на экспорт углеводородного сырья. Повышение добычи и транспортировки нефти и газа являются приоритетными задачами правительства. Другой задачей государства является безотказное жизнеобеспечение крупных городов, которое в первую очередь зависит от непрерывного тепло и водоснабжения. Анализ показывает, что в случае системного подхода к планированию и целенаправленному проведению серий терактов и диверсий на трубопроводных системах различного назначения, Россия неминуемо столкнётся с тяжёлым экономическим и социальным кризисом.

На сегодняшний день охрана магистральных продуктопроводов представляет собой периодическое патрулирование вдоль трасс. Но такой способ не приносит результатов по причине их огромной протяжённости. Поэтому трубопроводы являются удобной мишенью для террористов, так как невозможно определить, когда и в каком месте может быть нанесён удар. А последствия от вывода из строя, например, магистральных водоводов водоканала или ТЭЦ могут быть катастрофическими для населения мегаполиса. Подрыв нефтегазопроводов чреват огромными экономическими и финансовыми потерями, как для отдельных компаний, так и для региона в целом.

Кроме того, на линейных участках магистральных трубопроводов ежегодно фиксируются сотни случаев незаконных подключений с целью хищения нефти и нефтепродуктов. Проводимые службами безопасности нефтегазотранспортных компаний мероприятия по предотвращению незаконного доступа к трубам третьих лиц не приносят положительного результата. Кражи продукта из трубы и диверсионные акты продолжаются и имеют положительную динамику.

Научные исследования в направлении решения описанных выше проблем привели к появлению новых перспективных технологий для предотвращения современных угроз безопасности трубопроводному транспорту. Анализ задачи создания технологии обнаружения «канала кражи» на

стадии подключения к магистральным трубопроводам приводит к выводу об отсутствии альтернатив акустическому виду контроля. Ориентируясь на принцип «распределённого датчика», «сторожевая» система контроля видится в виде совокупности акустических датчиков, установленных на поверхности продуктопровода на определённом расстоянии друг от друга и связанных с системой обнаружения «подготовительных работ к подключению» или «появления утечек продукта» посредством канала телемеханики. Система может быть дополнена каналом автоматического обнаружения моментов перехода оборудования перекачивающих станций в предаварийное состояние.

При обнаружении на трассе продуктопровода злоумышленника, устанавливающего устройство отбора продукта (врезку), «сторожевая» система, работающая в режиме реального времени, сначала на основе знаний об элементарных типовых сигналах (см. рис. 1) производит распознавание класса физического взаимодействия (удар, сверление, сварка). Затем производится локализация источника (определяется координата) акустического сигнала в оболочке трубы.

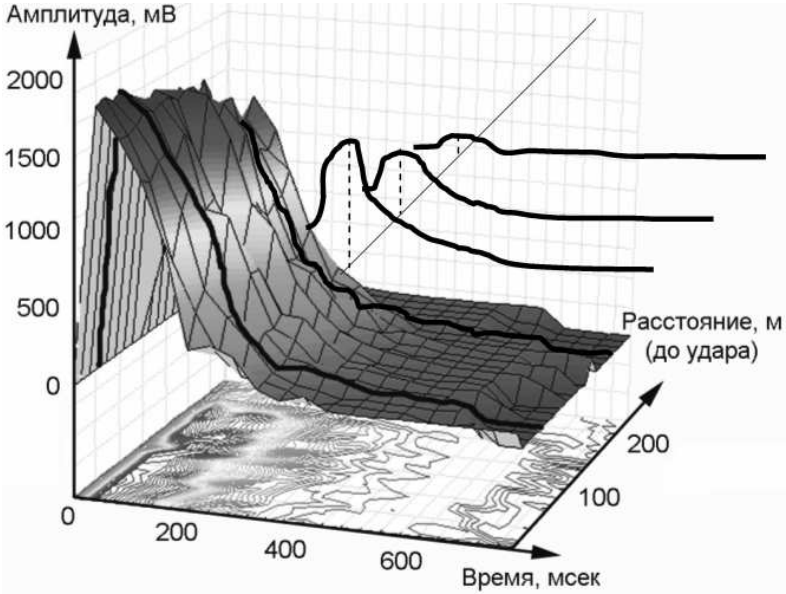


Рис. 1. 3-d поверхность, характеризующая затухание уровня эталонного ударного сигнала от расстояния

Особенности формирования акустических шумов в оболочках трубопроводов при их повреждении человеком с целью незаконного отбора продукта из трубы, а также математическая интерпретация возникающих при этом процессов и явлений позволили создать ряд эффективных алгоритмов для обнаружения и распознавания акустических сигналов «вторжения». Натурные эксперименты показывают, что такой подход к построению системы безопасности даёт положительные результаты и при быстром реагировании позволяет не допустить критического разрушения оболочки трубопровода и пресечь действия злоумышленников. Экономия финансовых затрат, предотвращение экологических катастроф и обеспечение стабильного снабжения потребителей нефтепродуктами — вот несколько практических выигрышей от принятия описанной концепции защиты трубопроводов.

При более углубленном анализе указанной задачи становится ясным, что избежать ложных решений в такой системе контроля невозможно (они могут быть и сымитированы злоумышленниками). Потребуется периодически прибегать к услугам, например, авиации для проверки достоверности решений. Используемый для этих целей визуальный метод оценки состояния трассы характеризуется высокой вероятностью «пропуска цели»: отводы продукта маскируются в видимом диапазоне волн, выход вытекающего продукта может произойти на значительном удалении от продуктопровода.

Усовершенствования системы «патрульного контроля» возможны на пути использования тепловизионных средств разведки. Тепловизионные приборы последнего поколения позволяют получить температурные изображения трассы пролегания продуктопроводов отличного качества. Но чтобы вести речь о технологии тепловизионной разведки рассматриваемого назначения, следует снять вопросы о формировании полезных сигналов и помех, а также изменении риска принимаемых решений во времени.

У злоумышленника достаточно времени, чтобы за время между осмотрами трассы подключиться к трубопроводу, проложить канал для отвода продукта и замаскировать его. Требуется продолжительное время появления оптического контраста в месте залегания отводной трубы (за счет подсыхания маскирующего дерна, более быстрого высыхания песчаного грунта над отводной трубой и т. д.). В то же время факт нарушения естественной плотности грунта неизбежно изменяет температурное поле подстилающей поверхности; на тепловом снимке регистрируется слабо контрастная полоса, формирующая практически в реальном масштабе времени вдоль полосы отвода продукта.

В тепловом диапазоне оптических излучений указанные «объекты» замаскировать невозможно, и нет технических проблем для их регистрации с помощью серийно выпускаемых приборов. Наряду с сигналами от «объектов» регистрируются тепловые флуктуации подстилающей поверхности,

обусловленные пространственной неоднородностью коэффициентов поглощения солнечной радиации и излучения земных покровов, а также изменением теплофизических параметров почво-грунтов в поле зрения регистрирующей аппаратуры.

Существуют в течение суток интервалы времени, когда дисперсия флуктуаций становится соизмеримой или превышает плотность потока излучения от места залегания «объекта». Однако известны методы повышения отношения сигнал/помеха на входе схемы принятия решений, основанные на подавлении пространственных частот флуктуаций, слабо выраженных в спектре искомых изображений объектов, регулируемом подсвете пролетаемой мощности, прогнозировании уровней сигнала и помех с введением спектральной фильтрации, многоспектральном представлении вектора признаков сигнала и помех. Применение первого из них (пространственной селекции объектов) оказывается достаточным, чтобы обеспечить высокие параметры по обнаружению. В этих условиях задача обнаружения сводится к автоматическому поиску в тепловизионных снимках «Т»-образных отводов от магистральной трубы или других заранее заданных эталонных объектов (пятна, разливы нефти и т. д.). Применение пространственной селекции тепловых изображений объектов на фоне типичных помех позволяет снять вопросы о неэффективности обнаружения мест несанкционированных подключений к трубопроводам и выхода вытекающего продукта на границу раздела «земля — атмосфера».

Таким образом, на сегодняшний день существуют теоретические и практические наработки, заблаговременное внедрение которых позволит заранее обеспечить безопасную эксплуатацию трубопроводного транспорта в РФ.

Этапы становления оценки риска опасных производственных объектов ОАО «Газпром»

А. А. Швыряев

История развития методологии риска в нашей стране насчитывает не более 20 лет. В начале эта методология применялась к объектам атомной энергетики, а с 90-х годов к объектам химической, нефтехимической и газовой промышленности. Значительный толчок развитию методологии дал закон «О безопасности», принятый в 1992 г. Безопасность в законе определяется как состояние защищенности жизненно важных интересов личности, общества и государства, эти интересы рассматриваются как совокупность потребностей, удовлетворение которых надежно обеспечивает их существование и возможность прогрессивного развития. Таким образом было признано существование источников риска и наличие определенной степени защищенности от них. Эта степень защищенности носит не абсолютный характер, а подразумевает некоторую защищенность, определение степени которой и является предметом анализа риска.

В 90-е годы основное внимание уделялось вопросам оценки риска для населения и персонала опасных производственных объектов (ОПО). Так оценка риска функционирования Астраханского ГПЗ в 1995 г. показала, что уровень потенциальной токсической опасности на месторождении не превышает 10^{-6} в год в 5-километровой зоне ГПЗ, что позволило в дальнейшем уменьшить зону повышенного риска с 8 км до 5 км и при этом снизить затраты на отселение местного населения. Проведенные работы по оценке риска проектов освоения Бованенковского месторождения, газопровода Ямал — Центр, конденсатопроводов позволили обобщить накопленный опыт в «Отраслевом руководстве по анализу и управлению риском, связанным с техногенным воздействием на человека и окружающую среду при сооружении и эксплуатации объектов добычи, транспорта, хранения и переработки углеводородного сырья с целью повышения их надежности и безопасности» в 1996 г.

Принятый в 1997 г. закон «О промышленной безопасности опасных производственных объектов» потребовал разработки декларации промышленной безопасности ОПО. При этом разработка декларации промышленной безопасности предполагает всестороннюю оценку риска аварии и свя-

занной с нею угрозы; анализ достаточности принятых мер по предупреждению аварий, по обеспечению готовности организаций к эксплуатации опасного производственного объекта в соответствии с требованиями промышленной безопасности, а также к локализации и ликвидации последствий аварии на опасном производственном объекте; разработку мероприятий, направленных на снижение масштаба последствий аварии и размера ущерба, нанесенного в случае аварии на опасном производственном объекте. Этот закон придал методологии риска основную роль в оценке промышленной безопасности.

В результате работ по декларированию ОПО газотранспортных предприятий ОАО «Газпром» были сформулированы обоснованные консервативные критерии по частоте возникновения аварий и их последствиям для человека и окружающей среды. Опыт этих работ нашел отражение в СТО РД Газпром 39-1.10-084-2003 «Методические указания по проведению анализа риска для опасных производственных объектов газотранспортных предприятий ОАО «Газпром»». Особо следует отметить, что при декларировании требуется не только оценить ожидаемые социальные потери, но и ожидаемый экономический ущерб. Пример этой оценки дан в табл. 1. При этом показатели ущерба ежегодно меняются в соответствие с законом «О бюджете» или при изменении соответствующих тарифов. Так наиболее значимо за последние 5 лет изменился ущерб, связанный с потерями газа. Поскольку, если до 2000 г. потери оценивались из внутренней цены для транспорта газа около 80 руб. за 1000 м^3, то в последнее время оценка производится с учетом затрат по транспортировке и экспортной составляющей цены газа, что составляет для центральных регионов свыше 1000 руб. за 1000 м^3.

С введением в действие приказа по МЧС РФ № 506 от 4.10.2004 «Об утверждении типового паспорта безопасности опасного объекта» в соответствии с решением Совета Безопасности РФ «О мерах по обеспечению защищенности критически важных для национальной безопасности объектов инфраструктуры и населения страны от угроз техногенного, природного характера и террористических проявлений» от ОПО ОАО «Газпром» требуется не только охарактеризовать социальные и экономические риски, но и дать их распределения в виде F/N и F/G-диаграмм, а также отразить готовность ОПО к чрезвычайным ситуациям и взаимодействию с антитеррористическими подразделениями.

Эти требования являются новыми в практике анализа риска ОПО и требуют своего обоснования и соответствующих методик оценки с учетом реальной специфики каждого объекта.

Стоит особо остановиться на необходимости создания системы комплексной безопасности. По сути промышленная безопасность принимается

Таблица 1. Ожидаемый экономический ущерб от аварий на 100 км МГ Ду 1400 мм в различных регионах РФ

Вид ежегодного ущерба	**Значение руб./год**	
	Тверская обл.	Ямало-Ненецкий АО
Ущерб владельцу		
Ущерб потери персонала	435	132
Ежегодные потери газа	396967	63611
Ежегодные затраты на восстановление трубопроводов	32667	9841
Ежегодные затраты на восстановление наземного оборудования ЛЧ МГ	40429	9469
Итого ущерб владельцу:	**470497**	**83052**
Ущерб третьим лицам		
Ущерб от гибели третьих лиц	3130	348
Ежегодный ущерб сельхозугодьям	2005	0
Ежегодный ущерб лесам	149300	13700
Ежегодный ущерб атмосфере	15529	2862
Ежегодный ущерб строениям	33	0
Ежегодный ущерб автотранспорту	47	7
Ежегодный ущерб подземным коммуникациям	24	6
Ежегодный ущерб ЛЭП	748	280
Итого ущерб третьим лицам:	**170816**	**17203**

только при условии, что сам проект будет приносить прибыль компании. Поэтому на этапе проектирования крайне важно оценить весь спектр рисков, возможных для проекта. К таким рискам следует отнести:

- производственно-технологические риски;
- финансово-экономические и организационные риски;
- эколого-правовые риски;
- политические риски;
- институциональные риски;
- конъюнктурно-сбытовые риски;
- ресурсные риски.

К сожалению, количественная оценка рисков этого перечня на сегодня невозможна, а методики качественной оценки во многом зависят от качества привлекаемых экспертов. Тем не менее, оценка этих рисков является на сегодня востребованной. Решение этих задач требует привлечения целого ряда специалистов: экономистов, юристов, физиков, химиков социологов, геологов и др.

Разработка моделей и методов управления безопасностью критически важных объектов топливно-энергетического комплекса

В. Н. Пожарский, В. В. Лесных, Е. А. Иванов

Россия располагает значительными запасами энергетических ресурсов и мощным топливно-энергетическим комплексом (ТЭК), который является базой развития экономики, фундаментом для проведения внутренней и внешней политики. От устойчивого развития и безопасности критически важных объектов (КВО) топливно-энергетического комплекса зависит энергоснабжение страны и, в целом, национальная безопасность России.

КВО ТЭК, в силу их большой значимости для страны и высокой потенциальной опасности, а также недостаточной защищенности, *обладают большой «привлекательностью» для террористов*, что подтверждается уже неоднократными террористическими акциями против этих объектов. Поэтому в условиях прогрессирующего физического и морального износа основного оборудования объектов ТЭК, сравнительно низкого уровня экологичности технологических процессов, возросшей частоты террористических акций на объектах, особенно остро стоит *проблема управления безопасностью КВО ТЭК в интересах устойчивого развития топливно-энергетического комплекса страны*.

Основная цель управления безопасностью — снижение риска эксплуатации объектов ТЭК до приемлемого (нормативного, допустимого) уровня. Управление безопасностью КВО ТЭК может осуществляться путем *снижения возможности* (*вероятности*) *реализации угроз безопасности КВО*.

Ключевым направлением парирования террористических угроз безопасности КВО ТЭК является оснащение этих объектов системами безопасности. При создании систем безопасности необходимо учесть ряд факторов, среди которых:

- разная системная значимость объектов;
- многообразие объектов по производственно-технологическому назначению;
- нахождение объектов в разных регионах России.

С целью дифференцирования требований к безопасности объектов и обеспечения единства подходов к организации охраны объектов определенной категории, а именно, определения состава и требуемой эффективности комплекса инженерных и технических средств охраны, численности подразделений физической охраны объектов, выполняется *категорирование объектов по степени потенциальной опасности и террористической уязвимости*.

Категорирование объекта проводится:

- по степени потенциальной опасности;
- по степени террористической уязвимости.

Категория объекта по степени его потенциальной опасности определяется социально-экономическими последствиями аварий на объекте и размерами зоны чрезвычайной ситуации. Прогнозируемые социально-экономические последствия характеризуются следующими показателями:

- количество пострадавших;
- количество людей, в отношении которых нарушены условия жизнедеятельности;
- материальный ущерб.

Устанавливается шесть категорий объектов по степени их потенциальной опасности.

Категория объекта по степени его террористической уязвимости определяется величиной риска возникновения чрезвычайной ситуации в результате террористических воздействий на объект. По степени террористической уязвимости устанавливается шесть категорий объектов.

Каждый объект характеризуется двумя категориями:

- категорией потенциальной опасности;
- категорией террористической уязвимости.

Показана взаимосвязь категорий потенциальной опасности и террористической уязвимости объекта.

Для решения задач управления безопасностью КВО ТЭК разработана взаимоувязанная совокупность методик:

- формирования характерных сценариев террористических воздействий;
- оценки вероятности реализации характерных сценариев террористических воздействий;

- оценки вероятности пресечения действий нарушителя системой охраны объекта;
- определения масштабов недопоставок продукции в результате выхода из строя КВО ТЭК;
- категорирования КВО ТЭК по степени потенциальной опасности;
- категорирования КВО ТЭК по степени террористической уязвимости.

Методика формирования характерных сценариев террористических воздействий

Сценарии террористических воздействий на объект формируют следующим образом:

1. Каждому разделу сценария ставят в соответствие множество, элементами которого, в свою очередь, могут быть другие множества. Такими множествами являются:

- множество критических элементов объекта;
- множество, характеризующее средства системы безопасности объекта, находящиеся на маршруте нарушителя к критическому элементу. Каждый элемент данного множества описывает типы используемых средств, их количество, расположение на генплане и т. п.;
- множество характеристик нарушителей;
- тактика преодоления персонала и технических средств охраны на периметре, в охраняемых зонах, зданиях и помещениях, искусственных и естественных препятствий на маршруте.

Дополнительными множествами характеристик, подлежащими включению в сценарий для его уточнения и детализации, являются множество возможных пособников и множество способов преодоления физических барьеров.

2. Произвольный сценарий террористических воздействий на объект представляет собой последовательность из n компонент, содержащих описание объекта, характеристику нарушителей и описание способов действия нарушителей. Первая компонента данной последовательности — элемент множества критических элементов объекта, вторая — элемент множества характеризующее средства системы безопасности объекта, находящиеся на маршруте нарушителя к критическому элементу и так далее, а последняя компонента — элемент множества способов преодоления физических барьеров.

3. Формирование характерных сценариев террористических воздействий на конкретный объект осуществляют в два этапа.

На первом этапе формируют множества качественных и количественных характеристик объекта, нарушителей и способов действия нарушителей.

На втором этапе выполняют синтез полного множества характерных сценариев террористических воздействий путем полного перебора (декартового произведения) всех возможных комбинаций элементов сформированных множеств.

Схема формирования характерных сценариев террористических воздействий приведена на рис. 1.

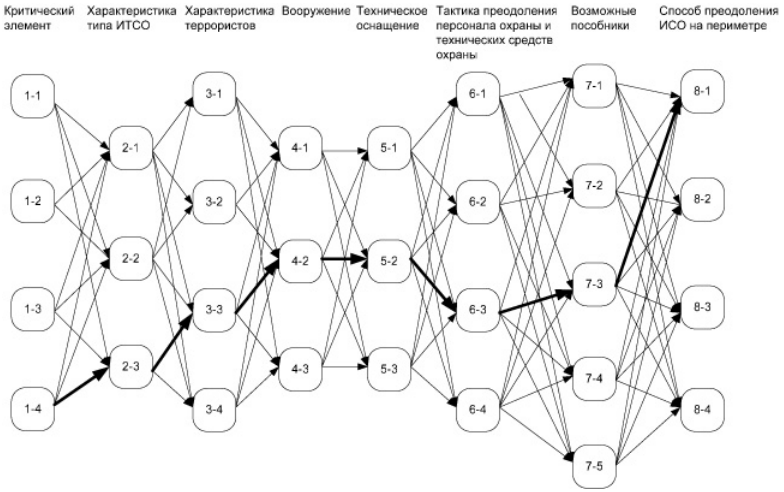


Рис. 1. Схема формирования сценариев террористических воздействий на объект

Методика оценки вероятности реализации характерных сценариев террористических воздействий

Для оценки вероятности реализации характерных сценариев террористического воздействия строятся логические схемы («деревья» событий). Структура «дерева» событий зависит от сценария террористического воздействия. «Дерево» событий строится для этапов: подготовка (планирование) акции; выдвижение на объект; проникновение на объект; подготовка взрывного устройства; подрыв взрывного устройства. Пример «дерева» событий для этапа *подготовки* террористических воздействий, с учетом

возможности обнаружения и уничтожения террориста (террористической группы) на данном этапе, показан на рис. 2.

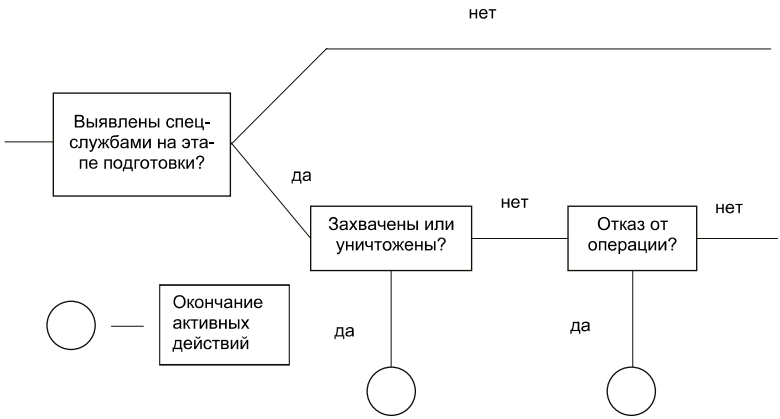


Рис. 2

Вероятность реализации террористической акции в целом зависит от вероятностей успешной реализации отдельных этапов. Оценка вероятности реализации этапов производится на основе «деревьев» событий соответствующих этапов. Вероятность реализации террористических воздействий на объект оценивается на основании вероятностей реализации всех этапов.

Методика оценки вероятности пресечения действий нарушителя системой охраны объекта

Область применения методики:

- оценка эффективности функционирования систем охраны объектов;
- формирование требований к составу ИТСО и САЗ объектов;
- обоснование технических решений создания (совершенствования) систем безопасности объектов;
- определение оптимальных схем действия персонала охраны объектов.

Принимается, что персонал охраны использует тактику блокирования критических элементов (уязвимых мест) объекта, то есть по сигналу «тревога», поступившему от периметральных или объектовых средств сигна-

лизации, персонал охраны прибывает и защищает критические элементы объекта.

Действия нарушителя считаются пресеченными, если у персонала охраны достаточно времени для блокирования критических элементов объекта.

Возможные маршруты нарушителей представляются в виде ориентированного графа (см. рис. 3). На этом рисунке

- вершина № 1 — начало пути нарушителя (любая точка на периметре — для внешнего нарушителя или внутри территории охраняемого объекта — для внутреннего нарушителя);
- вершины №№ 2, 3, ..., 6, ..., N — промежуточные точки маршрута (инженерные и технические средства охраны, естественные и искусственные препятствия);
- вершина № $N+1$ — уязвимый место объекта.

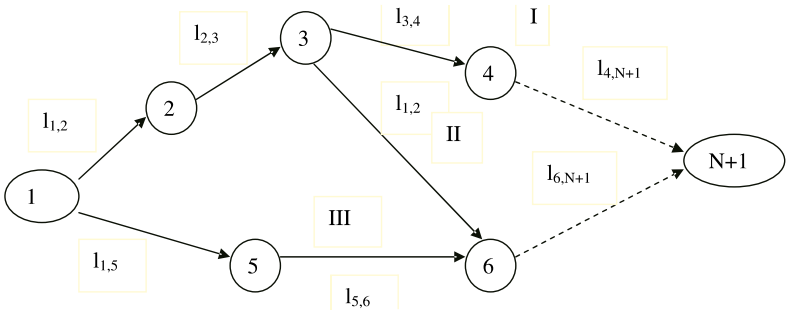


Рис. 3

Маршруты нарушителя:

I: 1 — 2 — 3 — 4 — ... — $N+1$ (длина маршрута $l_{1,2}+l_{2,3}+l_{3,4}+$ $+l_{4,N+1}$ м);

II: 1 — 2 — 3 — 6 — ... — $N+1$ (длина маршрута $l_{1,2}+l_{2,3}+l_{3,6}+$ $+l_{6,N+1}$ м);

III: 1 — 5 — 6 — ... — $N+1$ (длина маршрута $l_{1,5}+l_{5,6}+l_{6,N+1}$ м).

$l_{i,j}$ — расстояние между i-й и j-й смежными, то есть соединенными одной дугой, вершинами графа в м.

Для каждого маршрута оценивают интегральную вероятность обнаружения нарушителя. Маршрут, у которого величина «интегральная вероятность обнаружения нарушителя» минимальна, является критическим, а со-

ответствующая ему вероятность есть вероятность пресечения действий нарушителя системой охраны объекта. С критического пути начинается доработка системы охраны, если она не удовлетворяет требованиям Заказчика (технического задания).

По принципу сбалансированности система безопасности должна обеспечивать примерно одинаковую величину интегральной вероятности обнаружения нарушителя для всех путей, ведущих к наиболее критическому элементу защищаемого объекта.

Методика категорирования КВО ТЭК по степени потенциальной опасности

В качестве критерия отнесения объекта к одной из шести категорий потенциальной опасности принят максимальный масштаб чрезвычайных ситуаций, которые могут возникнуть в результате аварий (катастроф) на объекте.

Принимается, что:

- чрезвычайные ситуации на объектах первой категории потенциальной опасности могут приобрести трансграничный масштаб;
- чрезвычайные ситуации на объектах второй категории потенциальной опасности могут приобрести федеральный масштаб;
- чрезвычайные ситуации на объектах третьей категории потенциальной опасности могут приобрести региональный масштаб;
- чрезвычайные ситуации на объектах четвертой категории потенциальной опасности могут приобрести территориальный масштаб;
- чрезвычайные ситуации на объектах пятой категории потенциальной опасности могут приобрести местный масштаб;
- чрезвычайные ситуации на объектах шестой категории потенциальной опасности могут приобрести локальный масштаб.

Категорию потенциальной опасности объекта определяют с использованием нормативных значений социально-экономических показателей и размеров зоны чрезвычайной ситуации, введенных Постановлением Правительства Российской Федерации «О классификации чрезвычайных ситуаций природного и техногенного характера» от 13 сентября 1996 г. № 1094.

Значение показателя «материальный ущерб» определяют с учетом:

- прямых потерь предприятия;
- затрат на локализацию и ликвидацию аварии;
- социально-экономических потерь (затраты вследствие гибели и травматизма людей);

- косвенного ущерба;
- экологического ущерба;
- потерь от выбытия трудовых ресурсов в результате гибели людей или потери ими трудоспособности.

Методика категорирования КВО ТЭК по степени террористической уязвимости

Категорирование КВО ТЭК по степени террористической уязвимости выполняют следующим образом:

- Формируют характерные сценарии террористических воздействий на объект.
- Оценивают вероятности их реализации.
- Выполняют анализ уязвимости производственно-технологического процесса функционирования объекта и определяют критические элементы, террористические воздействия на которые могут привести к возникновению ЧС различных масштабов.
- Выполняют оценку возможности успешной реализации террористического воздействия на критические элементы объекта путем сопоставления опасного и возможного воздействий на группу критических элементов. Опасность воздействия выражается характеристикой специального снаряжения и вооружения террористов, необходимого для подрыва, поджога и т. п. критического элемента (группы элементов) объекта. Возможные воздействия определяются комиссией и с использованием методики формирования характерных сценариев террористических воздействий.
- Для каждого уязвимого места объекта оценивают:
    - эффективность функционирования системы охраны;
    - величины социально-экономических последствий террористических акций.
- Рассчитывают величины рисков возникновения чрезвычайной ситуации в результате террористических воздействий на уязвимые места объекта (по каждому характерному сценарию).
- Оценивают риск возникновения ЧС для объекта в целом.
- Каждому из полученных значений риска соответствует определенная категория террористической уязвимости объекта. Наиболее высокая из них является категорией террористической уязвимости объекта.

Возобновляемая энергетика для безопасности объектов ТЭК

И. И. Тюхов

Энергетическая безопасность — важнейшая проблема, обсуждаемая, как на самом высоком межгосударственном уровнем, так и на уровне конкретных производителей и потребителей энергии. Проблема обострилась в последнее время в связи с террористическими угрозами, возрастающими экологическими проблемами, пониманием ограниченности ископаемых ресурсов.

Достигнутые в последние годы успехи в развитии возобновляемых источников энергии (ВИЭ), связанные как со снижением стоимости производимой энергии, повышением эффективности преобразования, появлением новых и модернизации известных технологий привлекают все большее внимание общественности, научно-технического сообщества, энергетических компаний традиционного направления.

Многие зарубежные нефтяные компании диверсифицируют свою деятельность, вкладывая прибыль, получаемую от традиционого бизнеса, в новые технологии, связанные с ВИЭ тем самым, создавая для себя возможности включения в новый быстро растущий бизнес.

Перечислим основные проблемы традиционной энергетики, которые с ростом населения на земном шаре будут только усугубляться:

- экологические проблемы (выбросы парниковых газов, вредные и опасные загрязнения, кислотные дожди), которые создают высокую нагрузку на окружающую среду; заметим, что парниковый эффект часто связывают с проблемой глобального потепления (global warming) и, поскольку, в чистом виде тепловые выбросы традиционной энергетики трудно отнести основным факторам форсинга потепления по сравнению с потоком солнечного излучения, то задача о влиянии энергетики на современный климат оказывается очень сложной (рис. 1);
- глобальное потемнение (global dimming) — постепенное сокращение доли прямого солнечного излучения, приходящего на поверхность земли, наблюдаемое с начала регулярных наблюдений в 50-е годы;

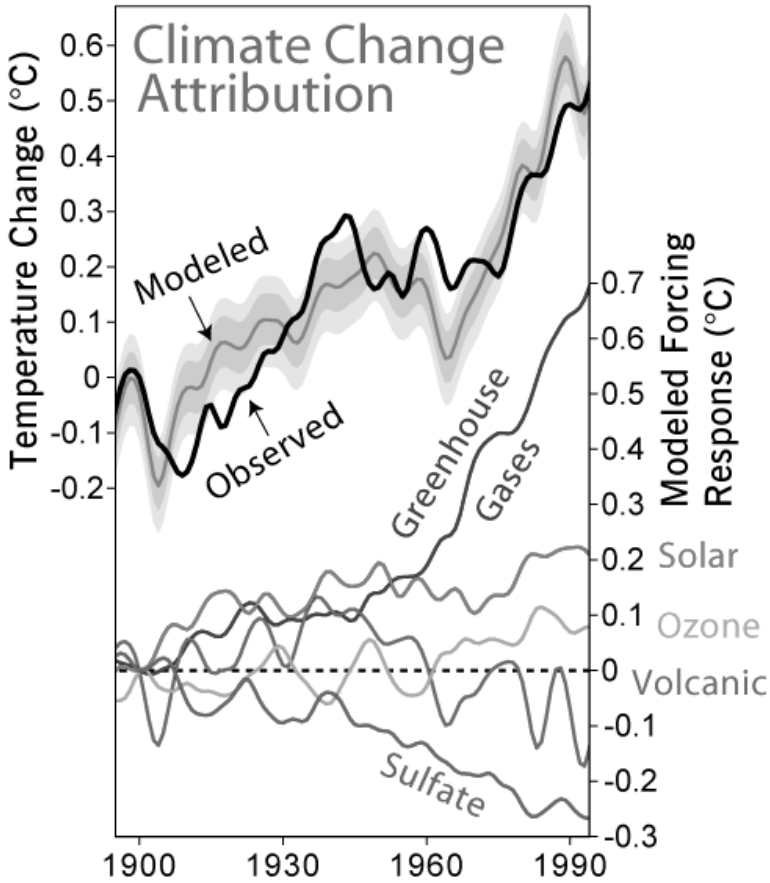


Рис. 1. Показано соответствие между моделью климата, описываемого при воздействии пяти форсингов (солнечная активность, парниковые газы, озоновый слой, сульфатный аэрозоль, вулканическая активность) с результатами наблюдений

эффект зависит от места наблюдения, но во всем мире он составляет порядка 4 % снижения в 1960–1990 гг. (см. ниже);

- освобождение запасенной в недрах Земли энергии нарушает естественный, природный баланс (это в полной мере относится и к атомной энергии, которую рекламируют как экологически чистую), что ведет к глобальному потеплению;

- высокие внешние затраты (затраты общества, например, на здоровье людей, пострадавших от выбросов в атмосферу и, которые не учитываются при определении цены на энергию);
- высокая централизация энергосистем и высокая концентрация энергетических носителей, приводящая к многократным потерям в случае техногенных, природных катастроф и террористических атак,
- принципиальная ограниченность ресурсов (исчерпаемость), при этом временные ресурсы зависят от нашей активности, в то время как солнце будет существовать около 4,5 млрд. лет;
- перекладывание проблем на будущие поколения (в частности, захоронение ядерных отходов);
- качественное ухудшение сырьевой базы (например, прирост запасов газа в 2–3 раза ниже уровня добычи);
- отдаление районов добычи энергии и сырья от районов их переработки и потребления;
- технологии ископаемых топлив подошли к физическому пределу эффективности, добыча и переработка будут только усложняться;
- снижение конкурентоспособности и даже невозможность обеспечить все удаленные регионы энергией.

Среди широко обсуждаемых научной общественностью проблем глобальных следует выделить новую проблему, упомянутую выше, — «глобальное потемнение» — эффект, обнаруженный недавно Джимом Хансеном (Jim Hansen, NASA's Goddard Institute for Space Science, NY) и другими исследователями. За последние два года стало ясным, что количество солнечной радиации, приходящей на земную поверхность, уменьшается из-за поглощения и рассеяния в атмосфере частицами (зола, сульфатные аэрозоли и др.), поступающими в атмосферу в результате человеческой деятельности. Частицы также способствуют более интенсивному образованию облачности. Это привело за последние годы к ослаблению ультрафиолетового излучения на поверхности земли примерно 20 % (по данным 100 метеорологических станций), и, следовательно, снижает эффективность преобразования солнечного света растениями. И если проблема глобального потепления, как проблема созданная человеком, оспаривается некоторыми учеными, верящими в то, что нынешнее потепление лишь часть естественно-природного цикла системы Земля — Солнце, то глобальное потемнение является еще одним сигналом, призывающим нас задуматься над будущим. В любом случае ясно, что воздействие человеческой деятельности на природу только усиливается.

Эксперты Международного совета ООН по изменению климата (Intergovernmental Panel on Climate Change, IPCC) подготовили четвертый

доклад, посвященный глобальному потеплению (февраль 2007). Они пришли к выводу, что основной причиной изменения климата на планете стала деятельность человека и что температура на Земле в этом столетии значительно возрастет. Документ объемом 1,6 тыс. страниц, над созданием которого работали более 600 специалистов из целого ряда стран, обнародован в Париже на экологическом форуме Climate Change 2007. Если доклад 2001 года называл деятельность человечества возможной (от 66 % до 90 %) причиной потепления, то теперь он дает минимум 90 % на то, что именно человек повинен в изменениях климата.

Традиционную энергетику с полным правом можно отнести к отрасли с растущей природоемкостью, имеющей ограниченный ресурс и требующей существенной перестройки уже в настоящее время.

Перечислим преимущества и необходимость интенсивного развития возобновляемой энергетики:

- неистощаемость ВИЭ в отличие от истощаемости ископаемых органических ресурсов;
- экологическая чистота, ВИЭ приносят минимальный ущерб окружающей среде;
- ВИЭ позволяют в большей мере использовать местные ресурсы, что существенно снижает потери на доставку энергии;
- ВИЭ способствуют развитию местной промышленности и соответствующей инфраструктуры;
- в удаленных регионах ВИЭ — единственно возможный и экономически эффективный способ получения энергии и исключения (или снижения) поставок дальнепривозного и сезонного топлива;
- многие ВИЭ позволяют использовать уже существующие электрические сети, обеспечивая закачку избыточной энергии в сеть (без использования аккумулирующих систем), снижая таким образом отрицательное влияние традиционной энергетики и используя уже созданную инфраструктуру;
- децентрализованный характер ВИЭ снижает риски техногенных катастроф, террористических атак, менее уязвимы с военной точки зрения; живучесть ВИЭ превосходит остальные энергетические системы;
- ВИЭ способствуют энергетической безопасности соответствующих регионов, стран, что приводит снижению политических конфликтов, борьбы за энергетические ресурсы;
- в развивающихся странах ВИЭ способствуют решению социальных проблем, проблем здравоохранения и образования, что, в конечном счете, положительно скажется на мировых проблемах в целом;

- все виды возобновляемой энергии, за исключением биомассы, имеют нулевую стоимость топлива, все виды возобновляемой энергии имеют низкую эксплуатационную стоимость; в то же время, возобновляемая энергетика требует высоких начальных затрат так, что финансовые риски и барьеры на пути возобновляемой энергетики (а также исследования и разработка возобновляемых источников) требуют дополнительных инвестиций;
- разработка децентрализованных энергетических систем на базе ВИЭ способствует решению как глобальных, так и местных экологических проблем (глобальное потепление и потемнение, кислотные дожди), за которые в большой степени ответственна традиционная энергетика.

Возобновляемая энергетика способствует энергосбережению. Каждый, кто покупает солнечную батарею, например, для организации резервного освещения, быстро осознает однозначную необходимость использования для создаваемой системы энергосберегающих ламп или высокоэффективных светодиодов. Заданный уровень сервиса при проектировании солнечно-энергетических установок существенно облегчается при использовании только энергоэффективных устройств. В то же время в быту и на работе энергосберегающие технологии используются недопустимо плохо, в то время как все экспертные оценки и проведенные на некоторых территориях расчеты показывают величину резерва энергосбережения до 40 % от существующего уровня потребления.

Рассмотрим несколько конкретных примеров, в частности, из области фотоэлектричества. Прямое преобразование солнечного излучения в электрическую энергию с помощью солнечных полупроводниковых модулей — это один из самых красивых и перспективных методов получения энергии. Ежегодные темпы прироста производства в мире солнечных элементов и модулей в течение последних десяти лет превышают 30 %. Заметим, что темпы роста могли бы быть и выше, если бы не ограничения, связанные с производством монокристаллического кремния. Россия с ее богатыми запасами чистого кварца и энергетическими ресурсами Сибири, могла бы стать лидером в производстве монокристаллического кремния, являющегося основным материалов для фотоэлектрической промышленности.

Уровень мощностей, генерируемых с помощью солнечных элементов, варьируется от микроватт до сотен МВт. Маломощные системы (рис. 2) используются для индивидуальной безопасности (индивидуальное освещение, связь, энергопитание портативных компьютеров и т. д.).

Солнечные электростанции мегаваттных мощностей используются для снижения пиковых нагрузок и получения энергии в районах, не охваченных централизованной энергосистемой.

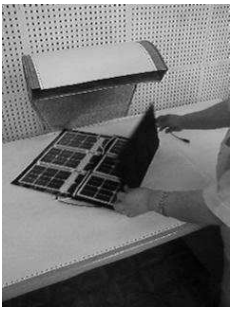


Рис. 2. Складываемая в 6 раз солнечная батарея производства ВИЭСХ (слева) и солнечные элементы, вмонтированные в палатку, производства США (справа)

Важную роль фотоэлектрические системы играют для модернизации электрических сетей. Одно из важных применений фотоэлектричества разработано для электрических сетей с системами SCADA. Начиная с 80-х гг. региональные энергосети за рубежом используют в ряде сетевых и автономных применений по причине их экономической эффективности. Растущий интерес к энергоэффективным и возобновляемым технологиям может помочь в решении ряда проблем энергетической инфраструктуры, делая ее более надежной и менее уязвимой. Физическая безопасность критически важного энергетического оборудования и, связанных с этим оборудованием сетей контроля и связи, уже обеспечивается в последние десятилетия эффективными по стоимости фотоэлектрическими системами (рис. 3). На-

Рис. 3. Система SCADA, работающая от фотоэлектрической батареи

пример, уже в течение долгого времени фотоэлектрические системы используются в удаленных релейных станциях для систем контроля и управления (SCADA) в сетевых и газовых кампаниях.

Фотоэлектрические системы успешно используются в телеметрии, метрологии, и многих других случаях, когда других источников электроэнергии нет, а строительство линии электропередачи слишком дорого. На рис. 4 приведена фотография системы для контроля за трубопроводами. Система работает надежнее и с точки зрения защиты от ударов молнии (соединенные с сетью системы повреждаются гораздо чаще).

Рис. 4. Контроль и мониторинг трубопроводов с помощью фотоэлектрической системы

Фотоэлектрические системы, модульные и децентрализованные, по сути, обеспечивают уникальные возможности генерации энергии, когда централизованные системы не работают. Рынок применения таких систем непрерывно расширяется и традиционные энергетические кампании, такие как, например, BP все больше средств вкладывают в новые энергетические технологии.

Проектирование комплексных систем обеспечения безопасности объектов нефтегазовой отрасли, критически важных для национальной безопасности по критериям риска

В. А. Мамонтов, Н. И. Бурдаков

Совместным Решением Совета безопасности России и Президиума Государственного совета Российской Федерации от 13 ноября 2006 года протокол № 14 «О мерах по обеспечению защищённости критически важных для национальной безопасности объектов инфраструктуры и населения страны от угроз техногенного, природного характера и террористических проявлений» выделен класс объектов, к которым необходимо предъявлять особые, повышенные требования к обеспечению безопасности. В него попадает большинство объектов топливно-энергетического комплекса.

Указанные требования, по сути, предусматривают реализацию на объектах топливно-энергетического комплекса широкого спектра мер по предупреждению возникновения чрезвычайных ситуации природного и техногенного характера, обеспечению готовности к ликвидации их последствий и защите от террористических проявлений. Рациональная совокупность подобных мер, внедрённых на объекте, образует интегрированную/комплексную систему обеспечения безопасности, которая должна не только компенсировать риски, обусловленные возможными авариями, стихийными бедствиями, но и обеспечивать требуемый уровень защищённости объекта от возможных террористических проявлений.

В настоящее время практически отсутствуют нормативные и методические требования, в соответствии с которыми организации должны осуществлять свою деятельность по предупреждению возникновения чрезвычайных ситуации природного и техногенного характера, обеспечению готовности к ликвидации их последствий и защите от террористических проявлений. Естественно отсутствуют и подобные требования к проектированию интегрированных систем обеспечения безопасности для объектов топливно-энергетического комплекса, критически важных для национальной безопасности.

В качестве основного действующего нормативного документа в этой области следует упомянуть приказ МЧС России от 4 ноября 2004 года № 506 (зарегистрирован в Минюсте России 22 декабря 2004 года, регистрационный номер 6218), которым вводилась в действие форма паспорта безопасности опасного объекта.

Паспорт безопасности, по замыслу его авторов, должен отражать степень безопасности объекта, в том числе и с учётом угрозы возможных террористических проявлений.

Однако для того, чтобы «паспорт безопасности» стал эффективным инструментом, необходима методология его составления, в которой должны иметься критерии, позволяющие ответить на следующие вопросы:

- является ли данный объект критически важным для национальной безопасности, и какие меры по предупреждению ЧС и защите от возможных террористических проявлений на нём должны быть реализованы;
- соответствует ли объект требованиям безопасности с учётом угрозы террористических проявлений.

В настоящее время однозначные ответы на подобные вопросы дать сложно. Поэтому необходимо *формирование федерального перечня объектов критически важных для национальной безопасности*.

При составлении паспорта безопасности, в соответствии с вышеупомянутым приказом МЧС России принимается, что объект соответствует требованиям безопасности, если для него имеется декларация безопасности опасного производственного объекта, получившая в установленном порядке положительное экспертное заключения. Однако, если речь идёт об учёте возможных террористических проявлений, то декларации безопасности для подобного вывода может оказаться недостаточно, так как при её подготовке, в рамках количественной оценки риска, часть сценариев возникновения и развития аварий не учитываются.

Поэтому, применительно к рассматриваемой задаче, методология оценки безопасности должна предусматривать анализ всего спектра возможных аварий и сценариев их развития, без учёта реальных значений частот их возникновения.

Другой важной проблемой является отсутствие методологии построения/проектирования интегрированных систем безопасности, в рамках которых обеспечивались бы требования к:

- охране объекта и физической защите его элементов;
- количеству и условиям размещения опасных веществ и материалов;

- размещению персонала, его перемещению по территории предприятия, как в режиме нормальной эксплуатации, так и при возникновении аварийных ситуаций;
- безопасной эксплуатации опасных производственных объектов и уровню соответствующих рисков;
- готовности персонала и специальных, в том числе аварийно-спасательных и пожарных подразделений к действиям при возникновении аварии или при совершении террористического акта.

На практике наиболее распространена ситуация, когда проектирование систем ведётся по критерию «эффект — затраты».

Если рассматривать только проблему обеспечения промышленной безопасности, то в качестве критерия эффективности можно использовать показатели риска. Однако учет угрозы возможных террористических проявлений потребует модификации данного критерия. Для этого предлагается сделать следующие допущения:

- на объекте планируется реализовать комплекс средств физической защиты, включая современные системы контроля периметра, ограждения, автоматизированные средства блокирования транспортных средств и т. д.;
- функционирование указанного комплекса технических средств совместно с соответствующими организационными мерами обеспечивает требуемый уровень защищённости объекта от террористических проявлений;
- сценарии возможных террористических проявлений совпадают с сценариями возникновения аварий за исключением событий и способа их инициирования;
- в качестве условной вероятностной меры реализуемости террористических проявлений используются частоты отказов соответствующих средств физической защиты.

Сделанные допущения позволяют применить для проектирования интегрированных систем обеспечения безопасности объектов метод барьерных диаграмм, достаточно широко используемый для оценки опасности или промышленных рисков. При этом в качестве барьеров рассматриваются предупредительные мероприятия, как по снижению риска аварий, так и по снижению риска реализации террористических проявлений.

Унифицированные проектные решения (УПР) по комплексам ИТСО и САЗ объектов ОАО «Газпром»

В. Б. Ляхов

Вступление

Цель разработки — сокращение сроков и оптимизация затрат на разработку ПКД.

Выполнение поставленной задачи может быть достигнуто при решении следующих задач:

1. Выбор из разрешенных к применению технических средств охраны и средств антитеррористической защиты устройств, позволяющих решить оптимальным образом задачи обеспечения безопасности объектов.

2. Разработать наиболее сложные и трудоемкие варианты размещения ТСО на периметре различной конфигурации, варианты размещения аппаратуры в контрольно-пропускных пунктах, караульных помещениях, участковых шкафах и аппаратных стойках.

3. Исключить рутинную работу и, как следствие, ошибки, связанные с человеческим фактором при создании проектных документов:

- рисование различных схем соединений в коммутационных устройствах (коробки, участковые, распределительные и другие шкафы), схем подключения ИТСО и САЗ;
- разработка спецификаций и т. д.

4. Разработка унифицированных конструкций и монтажных узлов высокой заводской готовности, включающие:

- конструкции сетчатых и решетчатых заграждений для периметров объектов и локальных зон;
- шкафы участковые, распределительные, щитки электропитания;

- комплекты конструкций ворот и калиток, и том числе сигнализационных;
- узлы крепления и установки в грунт, на заграждения, на стену ТСО различного принципа действия, стационарных и поворотных телевизионных камер;
- узлы металлических кабелепроводов с креплением к опорам заграждений, для установки на грунт;
- узлы заземлений;
- комплекты оборудования для пультовых КПП караульных помещений;
- узлы установки элементов тревожно-вызывной сигнализации.

Реализация поставленных задач

Рассматривается два варианта разработки УПР:

Консервативный — когда на основе проекта повторного применения путем «привязки» создается проект на конкретный объект.

Нами разработан проект повторного применения для объектов с размерами охраняемого рубежа до 250 м.

В эту категорию объектов попадают периметры крановых площадок, частично периметры газораспределительных станций и пунктов (ГРС,ГРП), замерных узлов и переходов газопровода через искусственные и естественные препятствия и другие объекты, периметр которых не превышает 250 м.

За основу принят двухрубежный принцип охраны. Первый рубеж — предварительный на основе сейсмического средства «Годограф-С» . Второй рубеж представлен в трех вариантах.

Вариант 1. Микроволновые датчики СМД-1,4П2.

Вариант 2. Проводноволновое средство «Газон-24»

Вариант 3. Вибрационное средство «Дельфин».

Выбор варианта исполнения определяется Техническим заданием и в зависимости от наличия , отсутствия или качества заграждения вокруг объекта. Проектом предусмотрено также:

- установка телевизионных камер;
- световая и звуковая сигнализация;
- громкоговорящая система оповещения;
- система передачи изображения и тревожных сообщений по радиоканалу.

Передача телевизионного изображения осуществляется с помощью системы WIMAX на расстояние до 50 км.

Система оповещения включается при срабатывании первого рубежа и транслирует заранее записанный текст предупреждения о запрете проникновения в запретную зону.

Выбор варианта, как уже указывалось, происходит путем «привязки» УПР. Инструкция по привязке так же приведена в УПР, где указаны все действия проектировщика для разработки реального проект — что необходимо сделать с каждым из составных частей УПР.

Динамический вариант

Мы попытались разработать УПР, которые впоследствии послужат основой для разработки САПР ТСО «Газпром».

Составными элементами УПР являются:

- автоматизированная расстановка сигнализационных датчиков и телевизионных камер на периметре;
- автоматизированное подписание расставленного оборудования;
- формирование схем соединения аппаратуры;
- составление спецификаций и смет.

Расстановка аппаратуры производится в соответствии с параметрами, заложенными в программу: допустимые разбросы длины охраняемого (или просматриваемого) участка, наличие на участке ворот или калиток, пересечение периметра трубопроводами или эстакадами. На воротах и калитках автоматически проектируется установка магнитоконтактного датчика. На воротах автоматически — телевизионная камера, на пересечениях периметра трубопроводом — однопозиционный датчик СМД-1,4-М2.

Автоматизированное подписание осуществляется с учетом наличия у средств обнаружения коммутационных элементов.

Формирование схем соединения аппаратуры производится с учетом выполнения условия — в одном участковом шкафу подключается 3 телевизионные камеры, 3 комплекта микроволновых датчика и один комплект вибрационного датчика. Расстановка участковых шкафов так же производится автоматически.

Программой учитывается длина линии сигнализации для аппаратуры типа «Рубеж-08». Если длина линии сигнализации превышает 1,5 км., в участковом шкафу устанавливается блок ретрансляции линии — БРЛ.

После выполнения операций по созданию проекта — автоматически формируется спецификация и смета.

Кроме того УПР формирует из каталога унифицированных нестандартизированных изделий альбом монтажных чертежей на выбранное оборудование.

Данный материал иллюстрируется проектом повторного применения на крановые площадки и видеороликом динамического варианта проектирования ТСО периметров объектов.

УПР находится в стадии разработки — еще много необходимо сделать для завершения разработки, пригодной к использованию проектными организациями.

Основные направления работ по оценке соответствия ИТСО и САЗ в системе добровольной сертификации ГАЗПРОМСЕРТ

И. А. Калайда

Система добровольной сертификации ГАЗПРОМСЕРТ создана ОАО «Газпром» приказом от 06 февраля 1999 г. № 10 в соответствии с законом Российской Федерации «О сертификации продукции и услуг» и зарегистрирована Госстандартом России (в настоящее время Федеральное агентство по техническому регулированию и метрологии), регистрационный № РОСС RU.3022.04ГО00 от 17 июля 2000 г. В связи с вступлением в силу (июль 2003 г.) Федерального закона № 184-ФЗ от 27 декабря 2002 г. «О техническом регулировании» и принятием Правительством Российской Федерации, федеральными органами исполнительной власти ряда нормативных правовых актов в его развитие, влияющих на деятельность Системы ГАЗПРОМСЕРТ, были внесены изменения как в структуру Системы, так и в документы, устанавливающие правила и процедуры деятельности участников Системы.

Система ГАЗПРОМСЕРТ создана для организации и проведения работ по добровольному подтверждению соответствия в форме добровольной сертификации:

- продукции и систем менеджмента дочерних обществ и организаций ОАО «Газпром»,
- продукции и услуг, приобретаемых ОАО «Газпром» для осуществления им своей деятельности,
- систем менеджмента качества на предприятиях-поставщиках продукции и услуг.

Основными целями системы являются:

- минимизация техногенного воздействия организаций и дочерних обществ ОАО «Газпром» на окружающую среду на основе совершенствования структуры производства, внедрения оборудования и технологий добычи, переработки, транспортирования, реализации и потребления продукции,

- повышение конкурентоспособности продукции, работ (услуг) организаций и дочерних обществ ОАО «Газпром» на российском и международном рынках,
- удостоверение соответствия продукции, работ (услуг) и систем менеджмента стандартам, условиям договоров, с учётом особенностей газовой промышленности,
- подтверждение функциональных показателей, а также показателей качества продукции, заявленных изготовителем (исполнителем).

Основные принципы добровольной сертификации в Системе:

- доступность информации о порядке осуществления добровольной сертификации для заинтересованных лиц;
- установление перечня форм и схем добровольной сертификации в отношении объектов, подлежащих сертификации в Системе ГАЗПРОМСЕРТ;
- установление согласованных с заявителем сроков осуществления добровольной сертификации и приемлемых затрат заявителя;
- недопустимость принуждения к осуществлению добровольной сертификации в Системе ГАЗПРОМСЕРТ;
- защита имущественных интересов заявителей, соблюдение коммерческой тайны в отношении сведений, полученных при осуществлении добровольной сертификации.

Основными типами ИТСО и САЗ, подлежащих сертификации в системе сертификации являются:

- технические средства охраны для периметра и открытых площадок;
- технические средства охраны для помещений;
- средства тревожной сигнализации;
- средства сбора и обработки информации;
- технические средства передачи тревожных сообщений;
- интегрированные системы безопасности;
- системы охранные телевизионные;
- системы контроля и управления доступом;
- средства обнаружения взрывчатых веществ.

Некоторые проблемы защиты подводных участков магистральных газопроводов и объектов газодобывающей и газотранспортной инфраструктуры прибрежного, шельфового и морского базирования

А. В. Чекер

Международный терроризм на море

Терроризм — очень серьезная проблема в настоящем и ещё более значительная угроза в будущем. С конца 60-х годов он приобрел поистине угрожающие масштабы:

- *за период с* 1970 *по* 1985 *г.*:
  - — в Европе совершено около 3000 терактов;
  - — в Латинской Америке — 1573;
  - — на Ближнем Востоке — 1330;
  - — в Северной Америке — 448;
- *за период с* 1986 *г. по наше время* рост количества терактов в различных регионах мира составил от 50 до 60 процентов.

Эксперты отмечают, что к концу XX века резко возросло количество террористических групп, специализирующихся на действиях в акваториях морей и океанов. Среди них:

- морская диверсионная группа организации «Тигры освобождения Тамил Илама»;
- морские боевые отряды ХАМАСа и «Исламского джихада», имеющие обученных боевых пловцов;
- морские диверсанты филиппинской террористической организации;
- группировка баскских сепаратистов (ЕТА);
- организация «Ирландская республиканская армия» (ИРА);

- колумбийские наркоструктуры;
- прочие экстремистские движения.

Против морских и береговых объектов террористы используют:

- *в подводной среде*:
  - — сверхмалые подводные лодки, оснащенные торпедами, ракетами, минами и подрывными зарядами;
  - — боевых пловцов-диверсантов с подводными транспортировщиками;
  - — человеко-торпеды;
  - — подводные роботы-манипуляторы;
- *над водой*:
  - — различные типы судов и скоростные универсальные катера, вооруженные подрывными зарядами, ракетами, торпедами и минами.

Наиболее привлекательными целями для террористов на море являются:

- суда с химически опасными веществами, углеводородами;
- суда с ядерными движительными установками;
- нефтяные/газовые терминалы, магистральные нефте/газопроводы; нефте/газодобывающие платформы;
- объекты прибрежной инфраструктуры, уничтожение которых приведет к серьезным экономическим и экологическим последствиям (порты, гидроэлектростанции, магистральные водопроводы и т. п.)

Рассматривая различные варианты действий нарушителей в морской/прибрежной зонах, можно сформулировать следующую базовую модель события-угрозы:

а) доставка в операционную зону исполнителей и оборудования с помощью транспортных средств;

б) доставка исполнителей и целевого оборудования к линейной части трубопровода;

в) проведение целевых работ;

г) возращение исполнителей к транспортным средствам;

д) уход из операционной зоны.

Описанную выше базовую модель события-угрозы будем использовать для формулирования требований к системе мониторинга зон дислокации объектов энергетической инфраструктуры.

Потенциальные зоны ответственности систем мониторинга элементов ТК в общем смысле характеризуются следующими особенностями:

1) большая протяженность (десятки, сотни километров);
2) большая площадь (десятки и сотни квадратных километров);
3) благоприятные условия для скрытного перемещения нарушителей;
4) широкий спектр природно-климатических условий, в которых могут располагаться элементы ТК;
5) открытость для перемещения транспортных средств и пешеходов/пловцов, что создает значительный маскирующий фон для событий угрозы.

При формулировании требований к системам контроля элементов ТК следует учесть следующие особенности потенциальных исполнителей угрозы элементам ТК:

1) высокая подготовленность и техническая квалификация;
2) высокая техническая оснащенность (как средствами для осуществления целевой функции, так и средствами для обнаружения и противодействия системам контроля);
3) потенциально высокая степень информированности о состоянии элемента ТК и эксплуатирующих его служб.

Суммируя вышеизложенное, можно сформулировать следующие базовые требования к системе контроля ТК:

1) обнаружение, сопровождение и классификация транспортных средств, используемых нарушителями в качестве средств доставки в операционную зону;
2) обнаружение, сопровождение и классификация биологических объектов (люди, крупные животные), используемых в качестве исполнителей целевой функции угрозы;
3) высокая степень достоверности принимаемых решений о наличии событий угрозы;
4) низкий уровень ложных тревог;
5) обеспечение достаточного для развертывания маневренных сил временного интервала с момента принятия решения о событии угрозы до ее реализации;
6) высокая степень скрытности функционирования системы;
7) высокая степень живучести системы;
8) мониторинг состояния элементов ТК;
9) учет сложившейся структуры системы эксплуатации и обслуживания элементов ТК;
10) простота эксплуатации системы.

Стационарная активная гидроакустическая система контроля подводной обстановки в зонах прокладки линейных частей морских магистральных газопроводов («Дельфин-МТ1-М»)

Назначение системы

Стационарная активная гидроакустическая система (САГАС) «Дельфин-МТ1-М» обеспечивает непрерывное выполнение следующих функций:

1) создание средствами системы на протяженных морских/шельфовых участках методом активной вертикальной гидролокации зоны контроля;
2) обнаружение подводных пловцов-диверсантов, средств их движения и крупных морских животных, способных нести боевой заряд в зоне контроля;
3) классификация обнаруженных объектов;
4) обнаружение методом шумопеленгования надводных судов, которые потенциально могут использоваться в качестве средств доставки нарушителей (исполнителей угроз) в операционную зону;
5) выделение событий соответствующих заданным моделям угроз;
6) оповещение об обнаруженных угрозах и событиях потребителей информации.

Система «Дельфин-МТ1-М» предназначена для контроля несанкционированного доступа к:

1) линейным частям подводных магистральных трубопроводов;
2) отдельно стоящим судам;
3) небольшим терминалам;
4) морским нефте/газодобывающим платформам;
5) водным переходам магистральных трубопроводов;
6) другим объектам прибрежной инфраструктуры.

Принцип действия системы

САГАС «Дельфин-МТ1-М» представляет собой набор линейных активных приемно-излучающих секций (ЛАПИС), устанавливаемых на дне в соответствии с заданной конфигурацией зоны ответственности системы и образующих с помощью линейных модулей связи, источников энергоснабжения и собственно подводного магистрального кабеля зону контроля (выносная часть (ВЧ)), и берегового поста обработки и наблюдения (береговая аппаратура (БА)).

Выносная часть содержит пассивную и активную части. Пассивная часть обеспечивает вынос активной приемо-излучающей части системы от поста обработки. Размер активной и пассивной части определяется конфигурацией зоны ответственности системы и ее удалением от поста обработки и наблюдения. Длина 1 ЛАПИС достигает до 1000 м. В состав активной выносной части одной системы «Дельфин-МТ1-М» могут входить до 100 ЛАПИС.

Каждая линейная активная приемно-излучающая секция представляет набор приемно-излучающих модулей (ПИМ) соединенных кабельной линией передачи информации.

Приемно-излучающие модули монтируется на кабеле через Δ м друг от друга. ПИМ работают в режиме вертикальной локации, создавая активную зону контроля шириной Ω. Излучение проводится в полосе ультразвуковых частот. Параметры Δ и Ω уточняются по результатам исследований гидролого-акустических характеристик района установки системы.

Приемно-излучающий модуль (ПИМ) предназначен для излучения и приема зондирующих сигналов. В состав модуля входит акустический преобразователь, работающий в режиме излучения и приема звуковых импульсов, предварительный усилитель с электронными устройствами защиты при излучении импульса.

Пост обработки и наблюдения (береговая аппаратура (БА)) включает в себя:

1) источник дистанционного питания;
2) прибор сопряжения ИВК с выносной частью;
3) информационный вычислительный комплекс (ИВК) обработки и отображения информации.

Источник дистанционного питания (ИП) предназначен для питания выносной части и береговой аппаратуры.

ИВК представляет собой набор компьютеров со средствами отображения информации и средствами передачи информации заданным потребителям.

Стационарная активная гидроакустическая система с большой дальностью действия («Дельфин-М2»)

Назначение системы

Стационарная активная гидроакустическая система (САГАС) «Дельфин-М2» обеспечивает непрерывное выполнение следующих функций:

1) создание средствами системы в режиме горизонтальной гидролокации на основе метода малолучевой томографии зоны с использованием развитых вертикальных излучающих и приемных антенн активной зоны контроля;

2) обнаружение подводных пловцов-диверсантов и крупных морских животных, способных нести боевой заряд, на расстоянии не менее 1,5 км, средств их движения на расстоянии не менее 5 км в зоне контроля;

3) классификация обнаруженных объектов;

4) сопровождение обнаруженных объектов;

5) оповещение об обнаруженных угрозах и событиях потребителей информации.

Система «Дельфин-М2» предназначена для защиты:

1) морских нефте/газодобывающих платформ;

2) заводов по производству сжиженного газа;

3) морских терминалов;

4) других объектов прибрежной/шельфовой/морской инфраструктуры.

Принцип действия системы

САГАС «Дельфин-М2» представляет собой набор гидролокаторов, образующих активную зону контроля. Каждый активный гидролокатор использует метод малолучевой томографии для создания зоны контроля. САГАС «Дельфин-МТ1-М» может создавать активную зону контроля с использованием до 12 гидролокаторов. Гидролокаторы через информационную магистраль связаны с постом обработки и наблюдения (береговая аппаратура (БА)). Гидролокаторы вместе с подводным волоконно-оптическим магистральным кабелем составляют выносную часть системы (ВЧ).

В функции приемно-излучающего комплекса гидролокатора входят:

1) излучение зондирующего сигнала;

2) прием сигнала, рассеянного объектом наблюдения;

3) предобработка первичной информации с последующей передачей данных на стационарный пост обработки и управления.

Гидролокатор работает в двух полосах частот, поэтому приемно-излучающий комплекс имеет:

1) излучающую высокочастотную вертикальную антенну;

2) излучающую низкочастотную вертикальную антенну;

3) приемную вертикальную антенну;

4) приемную донную антенну;

5) цифровую программируемую систему формирования сложных сигналов для генерации и приема, что позволяет осуществлять согласованные со средой импульсную подсветку и прием.

Специальными методами направление излучения антенн фокусируется с учетом акустических характеристик района дислокации системы.

Стационарная система мониторинга событий-угроз безопасности объектам газодобывающей и газотранспортной сети ОАО «Газпром» прибрежного (сухопутного) базирования с длиной периметра до 10 км («Кольцо»)

Назначение системы

Система «Кольцо» обеспечивает:

1) контроль наземных и подземных перемещений биологических объектов (люди, животные) в полосе до 40 метров от оси установки выносных антенн систем;
2) контроль наземных перемещений транспортных средства и низколетящих вертолетов в полосе до 500 метров от оси установки выносных антенн систем;
3) контроль проведения земляных работ в зоне ответственности систем.

Система «Кольцо» предназначена для мониторинга зон небольшой размерности с длиной до 10 км. К объектам с такой зоной контроля относятся большинство объектов нефте/газодобывающей инфрастуктуры (скважины, компрессорные станции, распределительные станции, станции катодной защиты) как прибрежного, так и сухопутного базирования.

Принцип действия системы

Система «Кольцо» состоит из:

- двух базовых модулей. Каждый базовый модуль имеет в своем составе:
  - — линейный модуль, состоящий из шестнадцати функционально независимых линейных секций, конструктивно объединенных одной кабельной линией связи общей протяженностью 5 км;
  - — кабельную линию передачи информации протяженностью до 2,5 км (при её необходимости);

- оборудование обработки информации;
- подсистему дистанционного питания линейного модуля и линии передачи информации;
- оборудования представления и регистрации информации.

Кроме того, в состав системы «Кольцо» по согласованию с Заказчиком могут быть дополнительно включены:

- подсистема независимого гарантированного электропитания;
- подсистема связи с внешними каналами и удаленными пунктами наблюдения.

Линейные модули и линия сбора и передачи информации заглублены в грунт на глубину, обеспечивающую их защиту от внешних воздействий.

Оборудование обработки информации и подсистемы дистанционного питания размещено в стационарном обслуживаемом пункте наблюдения. Все оборудование пункта наблюдения системы «Кольцо» размещается в одном девятнадцатидюймовом шкафу. Общая площадь, необходимая для размещения оборудования, не более 12 кв. м. Потребляемая мощность не более 5 кВт.

Контролируемые события возбуждают на поверхности земли сейсмоакустические колебания, которые регистрируются чувствительными датчиками. Сейсмоакустические сигналы от каждого датчика, преобразованные в электрические, по кабельной линии передаются в аппаратуру уплотнения и по оптоволоконной линии передачи информации поступают в оборудование подготовки и обработки данных.

Вычислительный комплекс производит обработку информации, поступающей индивидуально от каждого датчика системы. Сложные интеллектуальные адаптивные алгоритмы обработки информации позволяют не только выделить и зарегистрировать сигналы интересующих событий угроз на фоне природных и искусственных помех, но и классифицировать их, т. е. определить, к какому именно виду события угрозы они относятся. Для повышения эффективности работы системы проводится сезонная и региональная адаптация системы (алгоритмов обработки информации), позволяющая учесть климатические сезонные особенности данного региона и специфические особенности грунта в конкретном месте установки системы.

Результаты обработки представляются на монитор дежурного оператора в удобной для эффективного восприятия форме. По требованию Заказчика результаты обработки могут быть переданы без участия оператора в формализованном виде на любой удаленный пункт наблюдения по внешним каналам связи. Вся информация о зарегистрированных событиях угроз в зоне ответственности данной системы заносится в базу данных и хра-

нится определенное время, что позволяет использовать интеллектуальные процедуры прогнозирования возможного развития событий на ближайший оперативный период.

Для системы «ОБЗОР-периметр» возможны варианты по использованию дополнительных систем. Так, например, по согласованию с Заказчиком возможна установка вспомогательной системы видеонаблюдения, которая позволит при обнаружении факта наличия события-угрозы на периметре объекта включить систему видеонаблюдения на данный участок периметра и произвести дополнительную классификацию и регистрацию происходящих событий.

МАТЕРИАЛЫ ВТОРОЙ МЕЖДУНАРОДНОЙ НАУЧНОЙ КОНФЕРЕНЦИИ ПО ПРОБЛЕМАМ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ

Московский государственный университет им. М. В. Ломоносова,
25–26 октября 2006 г.

Подписано в печать 05.09.07 г. Формат 60×90 $^1/_{16}$.
Бумага офсетная. Печать офсетная. Печ. л. 41,5.
Тираж 500 экз. Заказ №

Издательство Московского центра непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. (495) 241-74-83.

Отпечатано с готовых диапозитивов в ППП «Типография “Наука”»
121099, Москва, Шубинский пер., 6

Книги издательства МЦНМО можно приобрести в магазине «Математическая книга»,
Большой Власьевский пер., д. 11. Тел. (495) 241–72–85. E-mail: biblio@mccme.ru
http://www.mccme.ru/publications/