Московский государственный университет
им. М. В. Ломоносова

Институт проблем информационной
безопасности МГУ

Академия криптографии Российской Федерации

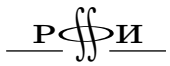
Материалы Третьей международной научной конференции по проблемам безопасности и противодействия терроризму

Московский государственный университет им. М. В. Ломоносова,
25—27 октября 2007 г.

Москва
Издательство МЦНМО
2008

ББК 32.81В6
М34

Организация и проведение Шестой общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2007) были поддержаны Федеральным агентством по науке и инновациям (Роснаука) и грантом РФФИ № 07-07-06047-г.



М34 **Материалы** Третьей международной научной конференции по проблемам безопасности и противодействия терроризму. Московский государственный университет им. М. В. Ломоносова. 25—27 октября 2007 г. — М.: МЦНМО, 2008. — 501 с.

Подписано в печать 09.06.2008 г. Формат $60 \times 90\ ^1/_{16}$. Бумага офсетная № 1. Печать офсетная. Печ. л. 31,5. Тираж 500 экз. Заказ № .

ISBN 978-5-94057-393-7

Оглавление

Общая информация о конференции

Мероприятия конференции:

- Шестая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-2007) по следующим тематическим направлениям:
  - математические проблемы информационной безопасности;
  - математическое и программное обеспечение безопасности компьютерных систем.
- Семинар-круглый стол «Интернационализация управления Интернетом».
- Семинар-круглый стол «Социально-психологические факторы развития терроризма».
- Семинар-круглый стол «Проблемы развития системы страхования риска „террористический акт“».
- Семинар-круглый стол «СМИ и терроризм: взаимоотношения, стратегия антитеррора».
- Первое заседание Научной Секции по безопасности информационных технологий Научного Совета при Постоянном Комитете Союзного государства.

Сопредседатели конференции:

- В. А. Садовничий — ректор МГУ им. М. В. Ломоносова;
- В. П. Шерстюк — помощник Секретаря Совета Безопасности РФ;
- С. М. Буравлев — заместитель Директора ФСБ России, президент Академии криптографии РФ.

Оргкомитет конференции:

- В. В. Белокуров — сопредседатель Оргкомитета, проректор МГУ;
- Н. В. Семин — сопредседатель Оргкомитета, проректор МГУ;
- В. В. Ященко — сопредседатель Оргкомитета, зам. директора ИПИБ МГУ;
- А. А. Стрельцов (аппарат Совета Безопасности РФ);
- В. Н. Сачков (Академия криптографии РФ);
- А. В. Сурин (факультет государственного управления МГУ);
- Ю. П. Зинченко (факультет психологии МГУ);
- Е. Л. Вартанова (факультет журналистики МГУ);
- В. Б. Алексеев (факультет ВМиК МГУ);
- В. А. Васенин (ИПИБ МГУ);
- Г. М. Кобельков (механико-математический факультет МГУ);
- И. Б. Котлобовский (экономический факультет МГУ);
- О. А. Логачёв (ИПИБ МГУ);
- А. А. Сальников (ИПИБ МГУ);
- В. В. Соколов (ИПИБ МГУ);
- А. В. Беляева (Фонд гражданских инициатив в политике Интернет);
- Р. Госенда (Университет штата Нью-Йорк, США);
- Ш. Кросс (Центр им. Джорджа К. Маршалла);
- Р. Рогозинский (Университет Кембриджа, Великобритания);
- Ю. В. Малинин (Академия информационных систем, Российская Федерация).

Программа конференции

Четверг, 25 октября 2007 г.

Зал конференций Интеллектуального Центра — Фундаментальной библиотеки МГУ им. М. В. Ломоносова

9.15—10.00. Регистрация участников

10.00—14.00. Пленарное заседание № 1

Открытие конференции

В. А. Садовничий (ректор МГУ им. М. В. Ломоносова). Стратегия развития науки и образования в России при построении информационного общества.

В. П. Шерстюк (Совет Безопасности Российской Федерации). Научные проблемы безопасности и противодействия терроризму.

11.30—12.00. Кофе-брейк

Е. П. Ильин (Национальный антитеррористический комитет). Национальный антитеррористический комитет — коллективный инструмент противодействия терроризму.

С. Г. Тер-Минасова (МГУ имени М.В.Ломоносова). Культурно-языковые проблемы безопасности в современном обществе.

А.-Н. З. Дибиров (Дагестанский государственный университет). Религиозно-политический экстремизм как идеология маргинальных слоев общества (на примере Республики Дагестан).

14.00—15.30. Обед

15.30—18.30 Пленарное заседание № 2

Т. Рассел (Университет Санта Клара, США). Роль государства в страховании риска терроризма.

H. Brandl (Infineon technologies AG and Trusted Computing Group). Trusted Computing: A Security Standard Based on Platform Integrity and Trust.

17.00—17.30. Кофе-брейк

Е. Л. Вартанова (МГУ им. М.В.Ломоносова). Терроризм и СМИ: симбиоз или противостояние? К вопросу о природе современных взаимоотношений.

В. Г. Кулаков, А. Б. Андреев, Г. А. Остапенко, В. И. Белоножкин, С. Ю. Соколова (Администрация Воронежской области). Информационная сущность и технологии терроризма.

17.30—18.30. Первое заседание Научной Секции по безопасности информационных технологий Научного Совета при Постоянном Комитете Союзного государства

Сопредседатели: А. Н. Курбацкий (Белорусский государственный университет), В. А. Васенин (МГУ им. М. В. Ломоносова).

18.30. Прием

Пятница, 26 октября 2007 г.

9.00—13.00. Секционные заседания и круглые столы (проводятся параллельно)

Семинар-круглый стол «Интернационализация управления Интернетом»

Место проведения: Главное здание МГУ, ауд. 1030.
Сопредседатели: А. А. Стрельцов (Совет Безопасности Российской Федерации), В. Марковский (ICANN).

Вопросы для обсуждения:

1. Принципы интернационализации административного управления системой доменов и адресами Интернет-протокола.
2. Принципы и механизмы интернационализации управления системой корневых серверов.
3. Принципы интернационализации управления разработкой и внедрением технических стандартов.
4. Принципы и механизмы перевода Интернета на многоязычный режим работы.
5. Основные угрозы безопасности функционирования и использования глобальной информационной инфраструктуры, оценка опасности их проявления.

6. Принципы и механизмы международного сотрудничества в обеспечении информационной безопасности, включая противодействие киберпреступности, кибертерроризму и кибервойнам.
7. Необходимость создания в ООН международной структуры по управлению Интернетом, в которую войдут все заинтересованные субъекты международных отношений по принципу справедливого представительства, отвечающего правилам, духу и традициям Организации объединенных наций.

В дискуссии принимают участие: А. А. Стрельцов (СБ РФ), В. Марковский, Д. Крейн (ICANN), А. Г. Романов, М. В. Якушев («.RU»), С. Гоэл (СУНИ), А. В. Крутских (МИД РФ), А. В. Фёдоров (МГИМО), А. Н. Курбацкий (БГУ), Е. С. Васильев (Мининформсвязи России), Е. К. Волчинская (аппарат ГД РФ), Т. А. Полякова (Минюст России), представители других заинтересованных организаций.

Математическое и программное обеспечение безопасности компьютерных систем

Место проведения: НИИ механики МГУ, Мичуринский просп., д. 1, кинозал.
Сопредседатели: В. А. Васенин (ИПИБ МГУ), Г. М. Кобельков (механико-математический факультет МГУ).

Доклады:

П. Д. Зегжда, Д. П. Зегжда, М. О. Калинин (Санкт-Петербургский государственный политехнический университет). Автоматическое обнаружение уязвимостей настроек безопасности в защищенных информационных системах с использованием логики предикатов.

К. А. Шапченко (ИПИБ МГУ). О ряде математических аспектов создания дистрибутивов защищенных систем на базе ядра Linux.

D. O. Rice, G. Wright (Loyola College in Maryland, USA). A Peer-to-Peer Network Security Pricing (PNSP) Model for Increased Network Resistance to Malicious Code Propagation.

П. Д. Зегжда, С. С. Корт, А. А. Немчанинов (Санкт-Петербургский государственный политехнический университет). Оценка эффективности работы системы обнаружения вторжений с учетом контекста.

В. Б. Савкин (НИИ механики МГУ). Эффективность, надежность и безопасность систем управления объектами критически важных инфраструктур.

П. Н. Девянин (ИПИБ МГУ). О разработке моделей безопасности информационных потоков в компьютерных системах с ролевым управлением доступом.

Семинар-круглый стол «Проблемы развития системы страхования риска „террористический акт“»

Место проведения: трансформируемый зал Интеллектуального центра — Фундаментальной библиотеки МГУ.
Председатель: И. Б. Котлобовский (экономический факультет МГУ).

Доклады:

J. E. Thomas (University of Missouri—Kansas City, School of Law, USA). The U.S. Model for Terrorism Insurance: Analysis of the U.S. Model.

И. Б. Котлобовский (экономический факультет МГУ). Методические основы страхования риска террористического акта».

В дискуссии принимают участие: представители Министерства финансов РФ, Федеральной службы страхового надзора, Министерства экономического развития и торговли РФ, Всероссийского Союза страховщиков, Государственной Думы Федерального Собрания РФ, Российского союза автостраховщиков, НИФИ при Министерстве финансов РФ, заведующие кафедрами, профессорско-преподавательский состав и аспиранты ведущих университетов г. Москвы, представители отечественных и зарубежных страховых компаний, других заинтересованных организаций.

14.30—18.30. Секционные заседания и круглые столы (проводятся параллельно)

Математические проблемы информационной безопасности

Место проведения: 2-й учебный корпус МГУ, факультет ВМиК, ауд. П-8А.
Сопредседатели: О. А. Логачёв (ИПИБ МГУ), В. Б. Алексеев (факультет ВМиК МГУ).

Доклады:

А. Я. Дорофеев (Академия криптографии РФ). Решение разреженных систем линейных уравнений при вычислении логарифмов в конечном простом поле.

М. А. Черепнёв (механико-математический факультет МГУ). Вариант блочного алгоритма типа Ланцоша решения систем линейных уравнений.

О. А. Логачёв (ИПИБ МГУ). Об одном классе совершенно уравновешенных булевых функций.

Б. А. Погорелов (Академия криптографии РФ), М. А. Пудовкина (МИФИ). Линейные структуры групп подстановок векторных пространств.

С. Н. Селезнёва (факультет ВМиК МГУ). О сложности нахождения некоторых свойств веса булевой функции, заданной полиномом.

С. А. Пометун (Физико-технический институт Национального технического университета Украины «Киевский политехнический институт»). Обобщенные корреляция и нелинейность высокого порядка булевых функций для описания вероятностных алгебраических атак.

Дополнительное заседание (Rump Session)

Л. В. Ковальчук (Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт»), В. Е. Федюкович (Киев). Двухраундовые протоколы демонстрации знания логарифмов.

Математическое и программное обеспечение безопасности компьютерных систем

Место проведения: НИИ механики МГУ, Мичуринский просп., д. 1, кинозал.
Сопредседатели: В. А. Васенин (ИПИБ МГУ), Г. М. Кобельков (механико-математический факультет МГУ).

Доклады:

D. O. Rice (Loyola College in Maryland, USA), Robert Garfinkel, Ram Gopal (University of Connecticut, USA). Confidentiality Via Camoflauge (CVC) POL and STAR—Protecting Numerical Data in Statistical Databases.

А. В. Уланов, И. В. Котенко (Санкт-Петербургский институт информатики и автоматизации РАН). Моделирование кооперативных механизмов защиты компьютерных сетей.

В. С. Заборовский, А. В. Силиненко (Государственный политехнический университет, ЦНИИ РТК, Санкт-Петербург). Логико-динамические аспекты моделирования процессов контентной фильтрации прикладных протоколов.

Н. И. Вьюкова, В. А. Галатенко, С. В. Самборский (НИИСИ РАН). Обобщение задачи конвейеризации циклов в С-компиляторе для отечественной аппаратно-программной информационно безопасной платформы Багет.

И. В. Котенко, В. В. Воронцов, А. В. Тишков, А. А. Чечулин, А. В. Уланов (Санкт-Петербургский институт информатики и автоматизации РАН). Исследование проактивных механизмов защиты от сетевых червей.

В. А. Галатенко, К. А. Костюхин, А. С. Малиновский, Н. В. Шмырев (НИИСИ РАН). Модели распределенных систем реального времени и методы их контроля.

Семинар-круглый стол «Социально-психологические факторы развития терроризма», подсекция «Противодействие идеологии терроризма»

Место проведения: Главное здание МГУ, ауд. 1030.
Председатель: А. В. Сурин (факультет государственного управления МГУ).

Вопросы для обсуждения:

1. Поддерживаете ли Вы тезис о том, что ведущим противоречием современности является «противостояние цивилизаций»: противостояние между западной цивилизацией, с одной стороны, и исламской цивилизацией — с другой. Не играет ли подобное противопоставление на руку религиозному, и в первую очередь, исламскому экстремизму в том смысле, что является идеологическим оправданием исламского терроризма?
2. Терроризм всегда имеет политическую или идеологическую «окраску», но при этом цели терроризма не всегда лежат на поверхности. Современный мир многолик, многоконфессионален. Можно ли утверждать, что терроризм является ответом на стремление построить однополярный мир? Снижение угрозы терроризма возможно лишь при переходе к концепции многополярного мира?
3. Как известно, терроризм не может и не должен ассоциироваться с какой-либо религией, национальностью, цивилизацией или этнической группой. В таком случае, что лежит в основе идеологии терроризма? Или есть много разных идеологических оснований терроризма?

4. Насколько опасно распространение идеологии терроризма? Какова роль межцивилизационного и межкультурного диалога в противодействии этой угрозе?
5. Насколько возможно плодотворное сотрудничество традиционных религий в борьбе с религиозным терроризмом и экстремизмом? Какие еще шаги можно предложить для развития такого сотрудничества?
6. Состав и структура террористических групп многообразны и различны, как по идеологии, так и по степени фанатизма, они имеют четкую иерархическую структуру, включающую в себя несколько уровней (от рядовых исполнителей до основных идеологов). Можно ли говорить о существовании «точки невозврата» в процессе формирования мировоззрения террориста? Насколько возможно представителя идеологической элиты терроризма убедить отказаться от идеологии терроризма? Или, после прохождения идеологической «точки невозврата» остается одно средство борьбы — физическое уничтожение?
7. Международные террористические организации, кроме иерархической структуры, имеют сетевой характер. Согласны ли Вы, что, в свою очередь, эффективная структура противодействия идеологии терроризма должна иметь сетевой характер? В чем это должно выражаться?
8. Согласны ли Вы с тем, что одной из главных целей государственной политики противостояния терроризму должно быть внедрение во все слои общества (и в первую очередь, в группы риска) антитеррористической идеологии? Какие для достижения этой цели можно предложить механизмы партнерства государства, бизнеса и гражданского общества?
9. Согласны ли Вы с тем, что революционаризм и экстремизм рождаются всегда в молодежной среде и поэтому необходимы особые «молодежные» мероприятия по противодействию идеологии терроризма?

В дискуссии принимают участие: А. В. Сурин (МГУ), А.-Н. З. Дибиров (Дагестанский государственный университет), Дж. Райдер (СУНИ), Л. Н. Панкова, П. А. Цыганков, Е. Н. Мощелков, Г. В. Иващенко, А. Е. Сувалов (МГУ), А. В. Фёдоров (МГИМО), представители других заинтересованных организаций.

Семинар-круглый стол «СМИ и терроризм: взаимоотношения, стратегия антитеррора»

Место проведения: факультет журналистики МГУ, ул. Моховая, д. 9, ауд. № 104.
Председатель: Е. Л. Вартанова (факультет журналистики МГУ).

15.30—16.30. Первое заседание

Доклады:

Е. Е. Пронина (факультет журналистики МГУ). СМИ в условиях террористической угрозы: медиапсихология против политтехнологии.

Н. Н. Литвинова. О роли государственного патернализма в деятельности СМИ в рамках построения системы противодействия терроризму.

С. Э. Некляев (факультет журналистики МГУ). Стратегии деятельности СМИ в контексте локальных войн и терроризма.

16.30—17.00. Кофе-брейк

17.00—18.00. Второе заседание

Доклады:

М. И. Макеенко (факультет журналистики МГУ). Борьба с терроризмом и свобода слова (опыт США).

М. В. Блинова (факультет журналистики МГУ). Японская практика борьбы с терроризмом в СМИ.

О. А. Бакулин (факультет журналистики МГУ). «Карикатурная война» в СМИ и проблемы информационной безопасности».

А. Ольшанский (факультет журналистики МГУ). Террористические акты в Лондоне 7 июля 2005 г. в освещении французской прессы.

Семинар-круглый стол «Социально-психологические факторы развития терроризма», подсекция «Психология терроризма»

Место проведения: факультет психологии МГУ, ул. Моховая, д. 11, стр. 5.
Председатель: Ю. П. Зинченко (факультет психологии МГУ).

Доклады:

Ю. П. Зинченко (факультет психологии МГУ). Психологический портрет терроризма: истоки терроризма как социальной формы идентичности.

Р. С. Шилко (факультет психологии МГУ). Методологические проблемы психологической подготовки специалистов по ведению переговоров для преодоления террористических актов.

Е. Ю. Лихачева, А. В. Зайкова (факультет психологии МГУ). Динамика восприятия фактора неопределенности в управлении экстремальными ситуациями в имитационной игре «Координация».

С. Н. Ениколопов, А. А. Мкртычян (факультет психологии МГУ). СМИ и психологические последствия терроризма.

Н. Н. Анисимова, И. Л. Бирагов (ВИПК МВД России), В. А. Минкин (ООО «Многопрофильное Предприятие „Элсис“»). Правовые вопросы применения системы виброизображения в качестве средства технического профайлинга.

О. В. Деснянская (факультет психологии МГУ). Профайлинг как метод выявления потенциально опасных пассажиров в целях авиационной безопасности.

Суббота, 27 октября 2007 г.

9.00—13.00. Секционные заседания и круглые столы (проводятся параллельно)

Математические проблемы информационной безопасности

Место проведения: 2-й учебный корпус МГУ, факультет ВМиК, ауд. П-8А.
Сопредседатели: О. А. Логачёв (ИПИБ МГУ), В. Б. Алексеев (факультет ВМиК МГУ).

Доклады:

В. А. Носов, А. Е. Панкратьев (механико-математический факультет МГУ). О функциональном задании латинских квадратов над абелевыми группами.

S. Kazmi, N. Ikram (National University of Science and Technology, Rawalpindi, Pakistan). S-Box Design Using Random Walk Based Algorithm.

G. Murtaza, N. Ikram (National University of Science and Technology, Rawalpindi, Pakistan). New Methods of Generating MDS Matrices.

А. Н. Ярмола (Белорусский государственный университет). Об обнаружении квазипериодов в бинарных последовательностях.

Ю. С. Харин, А. И. Петлицкий (Белорусский государственный университет). Идентификация двоичных последовательностей на основе искаженных цепей Маркова с частичными связями.

С. С. Коновалова, С. С. Титов (Уральский государственный университет путей сообщения). Построение $O(L)$- и $U(L)$-стойких шифров в конечных плоскостях.

А. В. Зырянов (ИПИБ МГУ). Использование стохастических зависимостей в видеоконтейнере формата MPEG для оценки его емкости.

Б. Б. Борисенко (ИПИБ МГУ). Построение адаптивных методов внедрения ЦВЗ в изображения с использованием контрастности.

Математическое и программное обеспечение безопасности компьютерных систем

Место проведения: НИИ механики МГУ, Мичуринский просп., д. 1, кинозал.
Сопредседатели: В. А. Васенин (ИПИБ МГУ), Г. М. Кобельков (механико-математический факультет МГУ)

Доклады:

К. К. Маркелов. Активный аудит: методы выявления аномальной активности.

В. Д. Недильниченко (ИБ ГСП «Чернобыльская АЭС»). Информационные угрозы в контексте противодействия терроризму.

Ю. Н. Гуркин (ФГУП ГНЦ РФ ИТЭФ). Обзор и анализ актуальных в сети Интернет атак.

И. С. Астапов, М. С. Дзыба, А. А. Коршунов (НИИ механики МГУ). Мониторинг функционирования компонентов компьютерных систем.

О. Д. Соколова (ИВМиМГ СО РАН), М. Н. Дмитриев (НГУ). Моделирование атаки „внедрение ложного агента“ на распределенные вычислительные системы.

А. С. Шундеев (НИИ механики МГУ), О. О. Андреев (ИПИБ МГУ). Подходы к созданию средств разграничения доступа в распределенных АИС.

С. Л. Коваленко (Санкт-Петербургский государственный политехнический университет). Безопасность клиентов в публичных беспроводных сетях.

Круглый стол «СМИ и терроризм: взаимоотношения, стратегия антитеррора»

Место проведения: факультет журналистики МГУ, ул. Моховая, д. 9, ауд. № 103.

Сопредседатели: Я. Н. Засурский, Е. Л. Вартанова (факультет журналистики МГУ).

Вопросы для обсуждения:

1. Глобализация информационных потоков и проблемы международного терроризма.
2. Освещение проблем терроризма в СМИ: как найти грань между свободой слова, социальной ответственностью и профессионализмом журналиста?
3. Перспективы саморегулирования журналистского сообщества как формы противостояния террористической угрозе.
4. Журналистская этика в условиях террористической опасности: как работать с источниками информации.
5. Журналист под угрозой: как сохранить жизнь, здоровье и профессионализм журналистов, освещающих проблемы терроризма.

К участию в дискуссии приглашены: журналисты Первого канала, канала «Россия», НТВ, столичных радиостанций, центральных московских газет и журналов, ведущих интернет-сайтов.

Международная научная школа «Булевы функции в криптологии и информационной безопасности» (Звенигород, 8—18 сентября 2007 г.)

Advanced Study Institute „Boolean Functions in Cryptology and Information Security“ (Zvenigorod, September 8–18, 2007)

Перечень лекций и докладов по темам:

1. Криптографические свойства булевых функций и отображений.
   - S. MAITRA (Applied Statistics Unit, India). Boolean Functions on Odd Number of Variables Having Nonlinearity Greater Than the Bent Concatenation Bound.
   - T. CUSICK (State Univeristy of New York, USA). Counting Balanced Boolean Functions with Bounded Degree.
   - V. B. ALEKSEEV (Faculty of Computational Mathematics and Cybernetics, Lomonosov University, Moscow). On Some Algebraic Algorithms for Recognition of Properties of Discrete Functions.

   - F. RODIER (Centre National de la Recherche Scientifique, France). Nonlinearity of Boolean Functions and Hyperelliptic Curves.
   - Y. ZHENG (University of North Carolina at Charlotte, USA). Balanced Nonlinear Boolean Functions.
   - O. A. LOGACHEV, A. A. SALNIKOV V. V. YASHCHENKO (Information Security Institute, Lomonosov University, Moscow). Geometry of Boolean Functions on Euclidean Sphere.
   - S. NIKOVA (Katholieke Universiteit, Leuven, Belgium). Generalized Monotone Cryptographic Properties of Boolean Functions.
   - P. STANICA (Naval Postgraduate School, USA). Remarks on Homogeneous Bent Boolean Functions Invariant under a Group of Permutations.
   - S. V. AGIEVICH (Belarusian State University, Republic of Belarus). Bent Rectangles.
   - G. KYUREGHYAN (Otto-von-Guericke University of Magdeburg, Germany). Monomial Bent Functions.
   - M. S. LOBANOV (Faculty of Mathematics and Mechanics, Lomonosov University, Moscow). Bounds between Algebraic Immunity and Nonlinearity.
   - I. ZVEREV (Faculty of Mathematics and Mechanics, Lomonosov University, Moscow). On the Structure of the Spectrum Support of Boolean Functions.
   - M. L. BURYAKOV (Faculty of Computational Mathematics and Cybernetics, Lomonosov University, Moscow). On Affinity Level of Boolean Functions.
2. Алгебраические и комбинаторные конструкции булевых функций и отображений с заданными криптографическими свойствами.
   - YU. V. TARANNIKOV (Faculty of Mathematics and Mechanics, Lomonosov University, Moscow). On Correlation Immune Functions.
   - V. A. NOSOV (Faculty of Mathematics and Mechanics, Lomonosov University, Moscow). Latin Squares in Boolean Parametrization.
   - A. BOTEV (Faculty of Mathematics and Mechanics, Lomonosov University, Moscow). On Properties of Correlation Immune Functions with High Nonlinearity.
   - V. KHALYAVIN (Faculty of Mathematics and Mechanics, Lomonosov University, Moscow). The Constructing of 3" Resilient Boolean Functions of 9 Variables with Nonlinearity 240.
   - J. WOLFMANN (Université du Sud Toulon, France). A Cyclic Code Approach of Bent Functions over $\mathbb{F}_2$ and $\mathbb{Z}_4$.

- S. G. SHIPUNOV (Faculty of Mathematics and Mechanics, Lomonosov University, Moscow). On Implementation of One Type of Recursive Constructions.

3. Булевы функции и отображения в криптосинтезе.
   - A. KLAPPER (The University of Kentucky, USA). Feedback with Carry Shift Registers and with Carry Transforms of Sequences and Boolean Functions.
   - P. WILD (University of London, United Kingdom). Stream Ciphers and Boolean Functions.
4. Классификация булевых функций.
   - PH. LANGEVIN (Université du Sud Toulon, France). The Classification of Boolean Forms of Degree 4 in 8 Variables.
   - YU. BORISSOV (Bulgarian Academy of Sciences, Bulgaria). Classification of the Cosets of RM(1, 7) in RM(3, 7).
5. Криптоанализ шифров.
   - V. S. ANASHIN (Information Security Institute, Lomonosov University, Moscow). Non" Archimedean Theory of T" Functions.
   - N. COURTOIS (University College of London, United Kingdom). New Frontiers in Symmetric Cryptanalysis.
   - M. MIHALJEVIĆ (Serbian Academy of Sciences and Arts, Serbia). Decimation Based Correlation and Algebraic Attacks and Design of Boolean Functions.
   - O. A. LOGACHEV, V. V. YASHCHENKO, M. P. DENISENKO (Information Security Institute, Lomonosov University, Moscow). Local Affinity of Boolean Mappings.
   - V. V. BAYEV (Faculty of Computational Mathematics and Cybernetics, Lomonosov University, Moscow). Review of Algorithms for Finding Annihilators of Boolean Functions.
6. Эффективные вычисления в конечных полях.
   - S. B. GASHKOV (Faculty of Mathematics and Mechanics, Lomonosov University, Moscow). Logical Circuits of Operations in Finite Fields and Their Applications in Cryptography.
   - I. SERGEEV (Faculty of Mathematics and Mechanics, Lomonosov University, Moscow). Implementation of Arithmetic in Finite Fields Using Logarithmic Depth Circuits.

Часть I

ПЛЕНАРНЫЕ ДОКЛАДЫ

Стратегия развития науки и образования в России при построении информационного общества

В. А. Садовничий

Глобализация, как необратимый процесс интеграции России в мировую экономическую систему, требует борьбы за такое место в политическом, экономическом и технологическом пространствах, которое может обеспечить процветание нашей страны.

Важным следствием процесса глобализации, представляющим вызов возможностям экономического развития России, стало обострение конкурентной среды, которое сопровождается технологическим давлением, проявляющимся в том, что страна, сделавшая рывок в использовании «прорывных технологий», получает возможность диктовать направления технологического развития другим странам, тем самым закрепляя за собой конкурентные преимущества.

Все это уже создало серьезные проблемы для российской промышленности и обусловило вытеснение нашей страны с рынков высокотехнологичной продукции.

Для характеристики места России в мировом технологическом пространстве приведу данные, в которых сравниваются наукоемкость и наукоотдача национальных экономик ряда стран (см. табл. 1).

Опыт развития отечественно научно-производственного комплекса состоит в том, что для повышения научно-технологического потенциала страны абсолютно необходима постановка со стороны государства масштабных научно-технологических проблем, требующих для их решения высочайшей концентрации интеллектуальных, финансовых и материальных ресурсов. Как правило, подобного рода проблемы связаны с задачами в области космических исследований, нанотехнологий, энергетики, транспорта, обороны, здравоохранения и особенно фармакологии. Примеров тому множество, начиная с программ освоения космоса, создания атомной бомбы, атомной энергетики, программ в области противоракетной обороны, проектов в области вычислительной техники и электроники и т. д. При этом, необходимость осуществления таких

Таблица 1

Страна	ВВП на одного занятого, тыс. долл.	Доля расходов на ИР в ВВП, %	Текущий индекс конкурентоспособности страны	Доля hitech продукции в товарном экспорте, %	Доля в мировом экспорте информационного оборудования, %
США	73,1	2,64	2	28,2	16,3
Китай	7,2	1,00	47	16,7	4,6
Германия	56,0	2,44	4	15,3	4,8
Франция	56,5	2,17	12	19,4	3,4
Россия	18,0	1,01	58	3,1	0,2

ИР — исследования и разработки.

программ и проектов определяется, как правило, не только рыночной конъюнктурой, но и логикой развития научно-технического прогресса.

Постановка каждой из подобных проблем во все времена становилась катализатором генерирования множества новых знаний и продвигало развитие отечественных технологий, как минимум, на одно или нескольких поколений. При этом на «вторичном уровне» всегда возникало множество технологий и проектов, порождающих рыночный спрос на них и стимулирующих создание новых технологических кластеров.

А прошедшие 90-е годы государство практически не ставило подобные проблемы и не создавало условия для их разрешения. Как следствие, отсутствие масштабных проектов привело к слабой востребованности научно-исследовательских и опытно-конструкторских разработок, в том числе и в таких ключевых направлениях, как лазерные технологии, оптоэлектроника, нано и биотехнологии и др., где у нас пока еще сохраняются приоритеты в фундаментальных разработках.

В этой связи хотелось бы сказать несколько слов о нанотехнологии. Как-то нобелевский лауреат физик Р. Фейтман сказал: «Если бы меня спросили, какая область науки может нам обеспечить прорыв в будущее, я бы назвал нанотехнологии».

Акт об исследованиях и развитии нанотехнологий в XXI веке, подписанный президентом Бушем в 2003 г., предлагает фронтальное решение проблем нанотехнологий как в фундаментальном, так и в прикладном направлениях, с выделением свыше тысячи направлений поиска. Объем бюджетного финансирования нанотехнологических исследований в США составляет свыше 1 млрд долларов/год.

Поэтому принципиально важно, что сейчас у нас в стране по указанию Президента принята мощная программа по нанотехнологиям. Важно, что она имеет такую сильную государственную поддержку, важно, что она принята в то время, когда практически все развитые страны мира считают у себя такие программы приоритетными. Это замечательный пример постановки государством крупной научно-технической задачи.

Важно теперь не упустить из виду другие крупные важные научные направления.

Одним из самых критических является отставание России в информационных технологиях, имеющее в последние 30 лет постоянно растущий характер. Сейчас стало ясным, что уровень развития стран в этой области будет определять в дальнейшем их геополитический статус и конкурентоспособность. Поэтому для России стратегически важным стала задача преодоления рывком отставания от развитых стран мира за относительно небольшой период времени. «Небольшой период» — в том числе, пока Россия еще не растеряла научный и интеллектуальный потенциал для такого рывка. Наличие этого потенциала является единственным условием абсолютного характера — в случае отсутствия этого потенциала его невозможно создать за обозримое время.

В своем вступительном слове на недавнем заседании президиума Государственного Совета России «Об информационных и коммуникационных технологиях в Российской Федерации» 16 февраля 2006 года в Нижнем Новгороде Президент В. В. Путин сказал: «Год назад, в Новосибирске, мы подробно говорили о создании технопарков. Сегодня мы уже рассмотрим комплекс вопросов, связанных с развитием новых технологий.

Общеизвестно, что страны, своевременно сделавшие на них ставку, не только успешно решили ряд внутренних проблем, но в целом сумели вывести свои экономики на самые передовые позиции.

По большому счету, это один из самых проверенных прогрессивных путей развития, перспективных и для нашей страны, заведомо обладающей здесь сильным стартовым капиталом, хорошими стартовыми возможностями. Речь идет, разумеется, о нашем интеллектуальном, инновационном и научно-техническом потенциале.

Однако любой потенциал становится материальной силой лишь при наличии для него благоприятных условий. Но и в этом смысле отрасль информационных технологий сегодня у нас можно считать наиболее подготовленной. Очевидно и то, что ее рост должен повлечь за собой развитие фундаментальной науки, а также целого ряда прикладных исследований в смежных отраслях».

Отставание в развитии информационно-коммуникационной инфраструктуры является проблемой первоочередной, если принимать про-

грамму прорывного развития в области информационных технологий. По данным, представленным специалистами Стэнфордского университета, которые анализировали пропускную способность и качество передачи данных по оптоволоконным линиям связи в разных странах, Россия экспоненциально отстает от развитых стран в развитии информационно-коммуникационной инфраструктуры. Эта общая ситуация программирует отставание России далеко на будущее. Причем не только в науке, но и, как следствие, в промышленности, финансовой сфере и сфере управления.

Информационное общество в мире в настоящее время претерпевает очередной качественный скачок в своем развитии — массовое вхождение «цифровых» технологий в повседневную жизнь человека, не только в область его профессиональных занятий, но и в быт, отдых. Даже в личную жизнь. Например, назревает переход от персональных компьютеров на существенно более дешевые (порядка 100 долларов) компьютерные устройства, которые позволят иметь доступ к самым разным информационным ресурсам в любом месте и в любой момент времени. Это предполагает другой, в том числе качественно, уровень развития информационно-коммуникационной инфраструктуры. Она должна стать всепроникающей, надежной, безопасной и простой для массового пользователя. К тому же эта инфраструктура должна отвечать широкому спектру пользовательских запросов, в том числе и в плане вычислений и работы с базами данных. Одним из ключевых направлений такого инновационного развития информационного общества является появление технологий ГРИД.

Инновационная технологическая концепция ГРИД, по сути, предполагает оптимизацию использования географически распределенных компьютерных ресурсов удаленными пользователями за счет создания постоянно работающих универсальных сервисов в сети Интернет. Кроме этого, грид технологии могут использоваться для создания принципиально нового качества в использовании распределенных компьютерных ресурсов.

Одним из примеров может служить обеспечение катастрофо устойчивого хранения данных через организацию реплицированных (2—3 копии) данных в распределенной системе дисковых или роботизированных хранилищ.

Другим примером может быть «мгновенная» мобилизация «неограниченных» вычислительных мощностей для нахождения наиболее оптимального или достоверного решения какой-то проблемы. Например, для нахождения наиболее оптимального решения экологических катастроф.

В качестве успешного применения грид инфраструктуры можно привести следующий пример. Летом 2005 года в грид инфраструктуре европейского проекта были мобилизованы огромные вычислительные ресурсы (на уровне Терафлота) для выбора нескольких наиболее подходящих кандидатов из миллионов вариантов белковых структур при разработке нового лекарства от малярии. Сразу после завершения этой задачи эти ресурсы были мобилизованы для выполнения другой прикладной задачи.

Концепция Грид возникла на базе впечатляющих успехов, прежде всего, в четырех направлениях:

1) резкого повышения производительности микропроцессоров массового производства — современный персональный компьютер сравним по производительности с суперкомпьютерами десятилетней давности;

2) появлением дешевых и быстрых линий связи — на уровне нескольких Гигабит/с;

3) феномена ИНТЕРНЕТ — глобализация обмена информацией;

4) развитие методов метакомпьютинга — научной дисциплины по организации массовых и сложноструктурированных вычислительных процессов.

В мире осуществляется несколько глобальных инфраструктурных грид проектов, среди которых можно отметить следующие:

- европейский проект создания глобальной грид инфраструктуры для обслуживания различных областей науки,
- американский проект с аналогичными целями,
- проект ЭлЭйЧСи Компьютинг Грид (этот проект ориентирован на физику высоких энергий), который базируется на первых двух на основе создания соответствующих интерфейсов для обеспечения интероперабельности между двумя разными грид инфраструктурами.

Единственным инфраструктурным проектом в России в области грид является РДИГ (Российский грид для интенсивных операций с данными), — создание российского сегмента глобальной грид инфраструктуры. (*В проекте участвуют восемь российских институтов — РНЦ КИ, МГУ, ОИЯИ, ИФВЭ, ИТЭФ, ИГМ РАН, ИМПБ РАН, ПИЯФ*). Финансирование осуществляется паритетно — из 6-й Рамочной программы ЕС и из российских источников в размере примерно 1 млн евро в год. Основная задача — построение первой в России пилотной грид инфраструктуры, получение опыта построения грид инфрастуктур и их эксплуатации. В плане приложений основной задачей сейчас является обработка и анализ данных экспериментов на крупнейшем ускорителе протонов и ионов — Большом адронном коллайдере (LHC — Large Hadron Collider), создаваемом в ЦЕРНе (Женева). В планах — распространение этой инфрастуктуры на другие науки — биологию, физику управляемого термоядерного синтеза, геофизику, нанотехнологии и др. Активное участие в этом инфор-

мационно-коммуникационном проекте позволит обеспечить российским ученым равноправный доступ к данным экспериментов на ускорителе LHC, а также даст уникальный опыт в развитии новейших технологий распределенных вычислений — гид технологий.

Современные суперкомпьютерные технологии являются одной из ключевых компонент информационной среды любого развитого государства. Создание национальных суперкомпьютерных центров, баз данных и систем, обеспечивающих распределенную корпоративную деятельность, развитие грид-технологий относится к факторам стратегического значения и входит в число важнейших приоритетов ведущих стран мира.

В нашей стране происходит сейчас быстрый рост суперкомпьютерных мощностей. При этом мы все же существенно отстаем от многих стран мира, где рост таких мощностей также происходит по экспоненциальному закону. Например, пиковая мощность супервычислителя РАН в 2005 году составила 9,5 Тфлопс, супервычислителя МГУ — 1,5 Тфлопс, а в Ливерморской лаборатории в США — 367 Тфлопс. Уже в этом году в Московском университете будет установлен супервычислитель мощностью около 60 Тфлопс.

Суперкомпьютерные мощности МГУ используются сейчас для проведения фундаментальных исследований по строению Земли, звезд и галактик, по прогнозированию изменений климата под действием различных факторов (например, увеличению содержания в атмосфере окиси углерода), по молекулярной генетике и биоинженерии, по моделированию новых лекарственных препаратов и по многим другим направлениям. Особенностью фундаментальных исследований, требующих высокопроизводительных вычислений, является то, что они, как правило, имеют непосредственный практический выход и дают толчок развитию новых технологий.

Дальнейшее развитие отечественных суперкомпьютерных мощностей позволит нам решать задачи стратегического значения. Например, в энергетике проектирование новых мощных гидротурбин методами компьютерного моделирования требует предельных суперкомпьютерных мощностей. Многие задачи, связанные с прогнозом последствий катастрофических явлений, требуют детального моделирования строения Земли. Одним из подходов к такому моделированию является «сейсмическая томография» (во многом аналогичная медицинской томографии). Она также требует огромных суперкомпьютерных мощностей.

Таким образом, современное информационное общество проходит ряд качественных скачков в своем развитии. В целом этот этап можно охарактеризовать как «оцифровывание всех» сфер деятельности человека.

Для того, чтобы Россия вошла в новейший процесс развития информационного общества, необходима программа прорывного развития

информационно-коммуникационной инфраструктуры в стране и ее эффективного встраивания в мировую инфраструктуру. Такая программа должна основываться на конкретных проектах, в том числе международных, с достижением определенного уровня качественных и количественных параметров развития инфраструктуры.

Одним из основных ресурсов экономики, основанной на знании, является кадровый потенциал науки. Россия прочно интегрирована в мировое пространство, но мы должны четко отдавать себе отчет в том, что ее роль и место в современном мире будут зависеть от того, сумеет ли она вернуться в число наиболее развитых государств. А один из признаков такого государства — забота о своих научных кадрах. Невнимание к этой проблеме может привести к необратимым последствиям. Потерю научных позиций нельзя восполнить за короткий срок даже при самых благоприятных экономических условиях, и тому есть немало примеров в мировой истории.

Вот почему так важно, чтобы позитивные процессы по сохранению и развитию кадрового потенциала научно-образовательной и научно-технической сферы, которые наметились у нас в последнее время, были поддержаны и продолжены.

Несмотря на то, что процесс лавинообразного сокращения научных кадров в пределах от 4,1 % до 15,9 % в год, характерный для 1990-х гг., к настоящему времени остановлен, общая тенденция снижения численности занятых исследованиями и разработками сохраняется. В последние годы, после кратковременного роста численности, наблюдавшегося в 1999 и 2000 гг. и составившегося соответственно 2,0 % и 1,8 %, опять происходит постепенное сокращение научных кадров в размере 0,2—2,2 % в год. По данным Росстата на начало 2005 г. в научных организациях России зафиксирована рекордно низкая численность работников — 839,3 тыс. человек, что составляет лишь 43,2 % по отношению к их числу в 1990 г.

За период с 1990 по 2004 гг. численность персонала, выполняющего исследования и разработки, в расчете на 10 тыс. занятых в российской экономике, снизилась в 2 раза, что свидетельствует о том, что наша страна идет в диссонанс с мировыми процессами в этой сфере. Это обстоятельство серьезно осложняет построение в России экономики, основанной на знаниях, обязательным условием которой является воспроизводство высококвалифицированной, мобильной рабочей силы, способной к исследовательской деятельности. Например, в США в последние два десятилетия численность лиц, занятых научной и инженерной деятельностью, росла быстрее, чем общая численность рабочей силы в гражданских отраслях экономики. Прогнозируется дальнейшее сохранение ее быстрого роста, как в абсолютном исчислении, так и относительно

всего рынка рабочей силы: как ожидается, к 2010 г. в США прирост числа занятых в сфере исследований и разработок в 3 раза превысит увеличение численности работников в других профессиях. Такая позитивная тенденция наблюдается и в странах Евросоюза, где растет доля занятых в наукоемких отраслях экономики.

На протяжении всех лет существования международной интеллектуальной миграции наша страна выступает в роли страны-донора. В последнее время процесс утечки умов все в большей степени затрагивает исследователей молодого возраста.

По имеющимся оценкам, сделанным на основе данных, разрабатывающихся МВД РФ до 2002 г., в 1990-х годах численность лиц, занятых в отрасли «Наука и научное обслуживание» и эмигрировавших из России, насчитывала порядка 1—2 тысяч человек в год. Таким образом, общая численность этой категории эмигрантов за период с 1990 по 2002 гг. составила примерно 211 тыс. чел. Вместе с тем, как показывают данные Росстата, масштабы выезда ученых на временной основе превышают размеры официального выезда в эмиграцию. Так, в 2002 г. их численность составила почти 3 тысячи или 0,7 % от общего числа российских исследователей. Большинство российских исследователей, выехавших на работу за границу, работают в ведущих странах мира.

Таким образом, для улучшения ситуации с кадровым потенциалом, обеспечения эффективности научно-образовательной деятельности, существенного повышения уровня и качества проводимых исследований необходимо:

во-первых, выстраивание эффективных механизмов регулирования трудовых отношений в научно-технической сфере, стимулирующих мобильность, инициативность, высокую ответственность за представляемые научные результаты;

во-вторых, совершенствование социальной поддержки в научно-технической сфере, включая создание внебюджетных пенсионных фондов федерального и регионального значения, развитие социальной инфраструктуры для работников науки и т. д.;

в-третьих, создание гибких механизмов, в том числе в рамках интеграционных процессов науки и высшего образования, обеспечивающих взаимодействие между поколениями и безболезненный выход из профессии для научных сотрудников, отработавших лучшую часть своего творческого потенциала, но способных быть весьма полезными в качестве преподавателей, консультантов и даже предпринимателей.

В этой ситуации особое значение приобретают меры государственной поддержки ученых. Она должна быть адресована всем возрастным категориям исследователей, включая их достойное пенсионное обеспечение.

Но острие внимания, конечно же, должно быть нацелено на молодых, поскольку именно молодежь является основным источником пополнения научных кадров.

Система образования — вот та область, где начинается воспроизводство научного потенциала. У нас есть хороший опыт отбора в вуз талантливой молодежи путем проведения олимпиад, творческих конкурсов, организации молодежных научных школ, конференций, создания школ-интернатов для одаренных старшеклассников. Эту работу надо расширять, тем более, что увеличивающееся социальное расслоение российского общества существенно сужает стартовые возможности молодежи, особенно из сельской местности, маленьких городов.

Следует сказать, что принимаемые Президентом РФ меры по поддержке молодых ученых, уже дают положительные результаты. Наметился, хотя еще и недостаточно интенсивный, процесс возвращения выехавших молодых ученых на работу за рубеж в Россию.

Очень важно эти тенденции закрепить.

Нельзя не заметить, что в системе российского образования за последнее десятилетие произошли существенные изменения. Вместе с тем все принимаемые меры по модернизации системы образования не привели пока к качественному улучшению дел.

По данным, приведенным на заседании Совета по науке, технологиям и образованию при Президенте РФ 21 октября 2005 года, доля средств, выделяемых на образование, растет несущественно. С 2001 года она не превышает 12 % от общего объема государственных расходов. В результате обеспеченность бюджетным финансированием образовательных учреждений составляет только 25—40 % от расчетной нормативной потребности.

Не в полной мере обеспечиваются конституционные гарантии бесплатности и доступности образования: фактическая доступность сокращается, а размер платы за дополнительные образовательные услуги постоянно растет.

Исследования качества образования, в том числе международные, выявили снижение фундаментальности среднего образования в нашей стране, недостаточность обеспечения современными методическими материалами, слабость материальной базы, неподготовленность большей части учителей.

Низка оснащенность образовательных учреждений современным учебным оборудованием, средствами информационных и коммуникационных технологий. Для большинства школ различных регионов, особенно сельских, выпускаемое учебное оборудование пока недоступно ввиду его высокой стоимости.

Но мало привлечь в науку талантливую молодежь. Надо, чтобы она была востребована в своей стране, чтобы у нее была возможность полноценно работать и получать как моральное, так и материальное удовлетворение от своего труда. И здесь чрезвычайно велика роль университетов. Именно университеты оказываются главным связующим звеном между новыми знаниями и их конкретным использованием на практике, что одновременно способствует повышению уровня профессионального образования. Эффективность этого процесса в большой степени зависит от интеграции высшей школы, академических и отраслевых структур науки, промышленности, бизнеса. Здесь особое значение приобретает развитие инновационной сферы науки и образования.

Говоря об образовании, необходимо особо выделить математическое образование, которое во многом задает уровень науки и в других областях. В нашей стране во все времена, начиная с Петра Первого, математическому образованию уделялось большое внимание. Напомню, в качестве примера, о специальном решении Политбюро ЦК КПСС и Совмина СССР в 80-е годы о поддержке математического образования.

В Московском университете и других университетах страны ведется широкая подготовка специалистов, бакалавров, магистров, аспирантов и докторантов по специальности «Прикладная математика и информатика» и «Информационные технологии», которая включает почти двадцать направлений этой науки. Однако в докладе я хотел бы сказать о новом направлении подготовки специалистов, которое появилось в последние годы.

В информационном обществе в деятельности государства как общественного института возникает новая задача — обеспечение целостности и безопасности информационного пространства, которая приобретает не меньшую значимость, чем традиционные задачи защиты территории и производственной базы.

Всеобщая компьютеризация основных сфер деятельности общества приводит к появлению широкого спектра нетрадиционных каналов утечки информации и несанкционированного доступа к ней. Последнее таит в себе реальную угрозу создания разветвленных систем несанкционированного контроля за информационными процессами и злоумышленного вмешательства в них. Это особо опасно в связи с тем, что техническая база информатизации в России практически целиком ориентирована на использование продукции зарубежных фирм, а достижения в области информационных технологий приводят к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне в виде информационных войн.

Важнейшим условием решения задач информационной безопасности является обеспечение и поддержание адекватного образовательного уровня общества как в общеобразовательном отношении, так и в специфических вопросах информационной безопасности.

Проблемы безопасности вообще, и информационной безопасности в частности, перестали сегодня быть областью исключительной компетенции специальных служб, они стали объектом внимания большой части общества, поэтому обеспечение национальных интересов в информационной сфере потребовало достаточного количества высококвалифицированных специалистов.

Система подготовки кадров в области информационной безопасности начала формироваться с начала 90-х годов. Этому способствовал целый ряд обстоятельств, в том числе: новые информационные и телекоммуникационные технологии, включая глобальные компьютерные сети; повсеместное использование этих технологий частными компаниями и гражданами, как следствие — большой интерес в негосударственном секторе к вопросам криптографии (например, криптография с открытым ключом) и компьютерной безопасности; происходившая одновременно реформа высшего образования в стране, позволившая ввести государственные образовательные стандарты высшего профессионального образования.

Сегодня образовательную деятельность в области информационной безопасности ведут около 80 вузов страны. Это не только реакция на спрос рынка в отношении таких специалистов, но и важная составляющая комплекса мероприятий государства по противодействию угрозам в информационной сфере. Этим обстоятельством определяются и содержание подготовки указанных специалистов, и особые требования, предъявляемые к образовательным учреждениям при организации такой подготовки.

Создание системы качественного образования явилось основой для решения проблемы кадрового обеспечения федеральных органов исполнительной власти, промышленно-хозяйственного комплекса страны и других структур специалистами в области информационной безопасности.

Большое значение для развития науки и образования в информационном обществе будет иметь реализация приоритетных национальных проектов в сфере образования, объявленных Президентом Российской Федерации В. В. Путиным.

Такие масштабные национальные проекты как «Стимулирование инновационных образовательных программ» и «Информатизация образования» будут способствовать развитию инициативы образовательных учреждений, поддержке участия гражданских институтов в управлении образованием, оптимизации структуры образовательной сети, привлечению дополнительных ресурсов в образование, повышению доступности каче-

ственного образования, распространению передовых технологий обучения.

В числе первостепенных задач они включают:

- стимулирование инновационных программ высшего профессионального и общего образования путем финансирования на конкурсной основе, в виде грантов, проектов развития около 50 вузов;
- информатизацию образования через создание системы электронных учебных ресурсов и соответствующей программно-технической инфраструктуры, а также через масштабное подключение школ к Интернету и оснащение их компьютерными классами.

В последние годы в мире стала проявляться тенденция рассматривать науку, а вместе с ней и образование, преимущественно в плане краткосрочной экономической целесообразности. При этом стремление к получению быстрой финансовой отдачи становится препятствием к развитию фундаментальных научных исследований, которые, однако, могут дать результаты, хотя и уступающие в скорости внедрения, но несоизмеримые как по своей экономической эффективности, так и по социальной значимости. Перенос рыночных механизмов в сферу науки и образования чреват стратегическими потерями, которые в перспективе могут оказаться более ощутимыми, чем сегодняшняя выгода.

Во время празднования 250-летия Московского университета ведущие мировые ученые и деятели образования приняли Московскую декларацию. Позволю себе процитировать ее главный вывод.

«Развитие современного общества, создание экономики, основанной на знаниях, во все возрастающей степени зависят от уровня науки и образования. Экономическое процветание, качество жизни, национальная безопасность определяются прогрессом науки и эффективностью использования результатов научно-исследовательской деятельности. Особое значение при этом имеют фундаментальные научные исследования, обеспечивающие прорыв к принципиально новым знаниям, на которых основаны революционные преобразования в производстве и в общественных отношениях.

Фундаментальная наука и образование — это основа устойчивого развития общества, в котором используются только мирные средства разрешения конфликтов, применяются экологически безопасные технологии и создаются условия для сближения народов при сохранении своеобразия национальных культур.

Именно фундаментальное знание становится условием и инструментом освоения частных предметных областей и решения конкретных задач. С этим связана особая роль фундаментальной науки в университетах, которые призваны готовить специалистов, способных выдвинуть и воспринять новые идеи, обеспечивающие технологии завтрашнего дня.

Необходимым условием успешного развития науки и образования является их полноценная государственная поддержка, включающая в себя решение вопросов финансирования, обновления научного оборудования, привлечения талантливой молодежи.

На нынешнем поколении лежит ответственность за сохранение и приумножение знаний, составляющих основу цивилизации. Будущее человечества создается уже сегодня, и определяется оно уровнем фундаментальной науки и образования».

Очень важно, что вопросы развития науки и образования являются приоритетными для руководства страны и регулярно обсуждаются на заседаниях Совета по науке, технологиям и образованию при Президенте Российской Федерации.

Поставленные Президентом задачи, создание системы национальных приоритетов ориентируют нас не на сиюминутные решения, а на обеспечение системных изменений, которые, будем надеяться, выведут российскую науку и образование на качественно новый уровень.

Научные проблемы безопасности и противодействия терроризму

В. П. Шерстюк

В современных условиях одной из наиболее опасных угроз безопасности многих стран мира, их территориальной целостности, правам и свободам граждан является терроризм в различных его формах.

Провоцируя недоверие и ненависть между социальными и этническими группами, порождая активизацию регионального сепаратизма, обострение национальных и конфессиональных противоречий, терроризм становится глобальной проблемой, представляющей серьезную угрозу для безопасности всего международного сообщества.

Террор как способ достижения политических целей насильственными средствами возник достаточно давно, одновременно с появлением государства, и прослеживается на всем протяжении истории цивилизации. Особенно интенсивно масштабы терроризма росли в XX веке, когда он вышел на международный уровень.

Как отмечает профессор Петрищев в статье «Антитеррористическая стратегия», «современный терроризм превратился не только в реальную угрозу национальной безопасности отдельных государств, но и приобрел планетарные масштабы, угрожая стабильности сложившихся международных отношений, поступательному эволюционному развитию всего международного сообщества. Фиксируется повсеместное сращивание терроризма с транснациональной преступностью, незаконным оборотом оружия и наркотиков».

Для нахождения эффективных путей предупреждения различных форм терроризма, а также правового обеспечения противодействия терроризму и религиозному экстремизму, правильному выбору средств и методов борьбы с ним важен комплексный социологический и политологический анализ этого сложнейшего социально-политического феномена, его глубокое теоретическое осмысление, изучение законодательного и правоприменительного опыта зарубежных государств.

Борьба с таким деструктивным явлением как терроризм может быть эффективной лишь в том случае, если она опирается на хорошее знание этого феномена, его природы, истоков, движущих сил, механизмов формирования и функционирования террористических структур, мотивации субъектов террористической деятельности, источников социальной, финансовой, материальной, военной, идеологической, агитационно-пропагандистской поддержки.

Действительно, любой ученый и даже просто грамотный человек скажет, что для целенаправленного воздействия на объект, процесс или явление нужно предварительно изучить его. Это особенно важно при воздействии на такой сложный и опасный феномен как современный терроризм. В противном случае разрабатываемые методы и способы противодействия этому явлению обречены на низкую эффективность, а в отдельных случаях могут даже серьезно осложнить обстановку.

Масштабы терроризма, его потенциальная опасность и трансграничный характер обусловливают значительную широту проблематики научных исследований вопросов антитеррористического противодействия, необходимость координации усилий по разработке методов противодействия терроризму ученых и специалистов различных государств мира и разных научных специальностей.

Только на базе глубоких научных исследований, наряду с разработкой мер антитеррористического противодействия, можно подойти к решению еще одной важнейшей задачи — создание общегосударственной системы мер профилактики терроризма, которая в настоящее время, к сожалению, в России отсутствует.

Обеспечение безопасности и противодействие терроризму является одним из важнейших приоритетов государственной деятельности. Среди восьми утвержденных президентом Российской федерации В. В. Путиным приоритетных направлений развития науки, технологий и техники в Российской Федерации «Безопасность и противодействие терроризму» поставлено на первое место.

Это направление по сути своей является междисциплинарным и межведомственным, поскольку предполагает проведение широкого спектра фундаментальных, поисковых и прикладных исследований, направленных на разработку технологий обеспечения безопасности населения и опасных объектов при террористических проявлениях.

Для организации исследований по данному направлению в МГУ им. М. В. Ломоносова по инициативе ректора создан Координационный совет, в состав которого вошли руководители 17 естественных и гуманитарных факультетов и научных подразделений Университета, ученые, преподаватели и студенты которых принимают участие в научных исследованиях и проектах по тематике приоритетного направления «Безопасность и противодействие терроризму». Наша, уже ставшая традиционной, конфе-

ренция — это тоже один из результатов деятельности Координационного совета МГУ по безопасности и противодействия терроризму.

В работе нашей конференции принимают участие математики, психологи, юристы, лингвисты, историки и другие ученые, проще сказать — представители всех сфер знаний, представленных в Московском университете, а также сотрудники правоохранительных органов и специальных служб.

Я хотел бы поприветствовать ученых и специалистов из 14 стран мира, изъявивших желание принять участие в работе конференции.

Третья международная научная конференция по проблемам безопасности и противодействия терроризму предполагает проведение дискуссий по широкому кругу научных проблем.

Это, прежде всего, гуманитарные проблемы, которые впервые столь широко представлены в программе конференции. Мы исходили из того, что комплекс социально-гуманитарных исследований, разработок и рекомендаций является серьезным ресурсом антитеррористической деятельности.

На секционных заседаниях и круглых столах будут рассмотрены:

- философско-политологические концепции взаимосвязей политических, социально-экономических, национально-религиозных и духовно-психологических причин, факторов и условий формирования и развития террора;
- психологические модели и критерии, позволяющие выделить признаки потенциальных террористов;
- концепция самоорганизации журналистского сообщества в целях регулирования распространения материалов, вызывающих неоправданные страхи;
- СМИ в условиях террористической угрозы;
- сетевые стратегии информационно-психологического противоборства;
- проблемы развития системы страхования риска «террористический акт», роль государства в страховании данного риска;
- модели глобальных процессов как одного из ресурсов развития терроризма.

Некоторые результаты исследований по этим направлениям ученых Московского университета вошли в научную монографию «Современный терроризм и борьба с ним: социально-гуманитарные измерения», которую получили все участники Конференции.

Хотел бы остановиться на работах по направлению «Безопасность и противодействие терроризму», выполненных в рамках федеральных целевых программ, объявленных Минобрнауки России.

В рамках этих программ под руководством аппарата Совета Безопасности Российской Федерации выполняются работы, развивающие 6 приоритетных технологических областей:

- системы оперативного и комплексного обнаружения металлов, взрывчатых веществ, радиоактивных и химических веществ, биологических агентов, психотропных веществ;
- робототехнические и кибернетические системы безопасности, в том числе мониторинга объектов и территорий и ликвидации последствий чрезвычайных ситуаций и террористических актов;
- аппаратура автоматической идентификации личности на основе индивидуальных биометрических и поведенческих признаков человека;
- диагностические экспресс-тесты от биологических и химических агентов, средства медицинской защиты, универсальные антидоты и вакцины;
- системы защиты информации и кибербезопасности, специальные системы интеграции и обработки информации для обнаружения предпосылок и предупреждения террористических проявлений;
- системы выявления и парирования угроз биологического и химического терроризма, в том числе современные технические средства индивидуальной и коллективной защиты, а также ликвидации последствий террористических актов с применением средств массового поражения.

Перечень данных областей объективно отражает современные мировые тенденции, а также учитывает особенности развития технологий безопасности гражданского и двойного назначения в России. Во всех шести приведенных технологических областях в России существуют сложившиеся научные школы, проводящие исследования на мировом, а в некоторых случаях — превышающем общемировой уровень.

Приведу всего лишь один пример. Государственным учреждением «Научно-производственный комплекс «Технологический центр» Московского государственного института электронной техники как головного исполнителя в кооперации с 8 научными, производственными и образовательными учреждениями (в числе которых и Московский университет) разработана уникальная комплексная технология и аппаратурные средства обнаружения и идентификации металлических предметов, взрывчатых и психотропных веществ, предназначенные для оснащения различных контрольно-пропускных пунктов, в том числе объектов транспорта. Комплекс включает модифицированные установки для обнаружения и идентификации взрывчатых и психотропных веществ на основе методов нейтронного радиационного анализа и ядерного квадрупольного резонанса, двухпроекционную рентгенотелевизионную установку, другие технические средства.

Если давать оценку аппаратуре по достигнутым параметрам обнаружения — ничего подобного в мире не существует.

Из шести перечисленных мною приоритетных технологических областей отдельно хотелось бы выделить одну, связанную с системами защиты информации и кибербезопасностью. Как отметил Президент Российской Федерации В. В. Путин на заседании Совета Безопасности 25 июля 2007 г., посвященном обсуждению Стратегии развития информационного общества в России, «глобализация открывает для нас не только новые возможности, но и создает определенные риски, и мы должны быть готовыми адекватно парировать такие потенциальные угрозы, как, например, кибертерроризм».

Противодействие угрозе кибертерроризма является одним из важных направлений деятельности государства и общества по активизации постиндустриального развития России, закрепленных в Стратегии развития информационного общества в России, проект которой был одобрен на заседании Совета Безопасности Российской Федерации и в настоящее время представлен на утверждение Президенту Российской Федерации.

Основная идея Стратегии заключается в том, чтобы попытаться, используя имеющийся политический и ресурсный потенциал российского общества придать процессу постиндустриального развития России новое качество.

Разработка проекта Стратегии осуществлялась межведомственной рабочей группой при аппарате Совета Безопасности при ведущей роли Мининформсвязи России и при поддержке Центра развития информационного общества, Института развития информационного общества, Российской Ассоциации электронных коммуникаций, МГУ им. М. В. Ломоносова, Фонда гражданских инициатив в Интернет и некоторых других организаций.

Стратегия призвана стать основой для подготовки и уточнения концептуальных, доктринальных, программных и иных документов, определяющих цели и направления деятельности органов государственной власти, а также принципы и механизмы их взаимодействия с гражданским обществом в области развития информационного общества в России.

В Стратегии определено, что цель формирования и развития информационного общества в Российской Федерации заключается в повышении качества жизни граждан, обеспечении конкурентоспособности России, развитии экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствовании системы государственного управления на основе использования информационных и телекоммуникационных технологий.

Изложены основные принципы деятельности по достижению данной цели, к числу наиболее важных из которых отнесены:

- партнерство государства, бизнеса и гражданского общества;
- свобода и равенство доступа к информации и знаниям;
- поддержка отечественных производителей продукции и услуг в сфере информационных и телекоммуникационных технологий;
- содействие развитию международного сотрудничества в сфере информационных и телекоммуникационных технологий;
- обеспечение национальной безопасности в информационной сфере.

Определены 8 основных решаемых задач, которые условно могут быть сгруппированы в четыре группы:

1) совершенствование информационной инфраструктуры;

2) расширение использования информационных и телекоммуникационных технологий в жизни общества;

3) повышение экономической и социальной эффективности внедрения информационных и телекоммуникационных технологий;

4) противодействие угрозам использования информационных и телекоммуникационных технологий для нанесения ущерба национальным интересам России.

Важным направлением научных исследований в области защиты информации, которое можно назвать классическим, является криптография и смежные математические проблемы информационной безопасности. Как вы помните, наша первая конференция в 2002 году называлась «Московский университет и развитие криптографии в России». Последние годы характеризовались массовым внедрением криптографических технологий даже в быт современного человека, у которого сейчас очень большой арсенал средств «интеллектуального окружения» для обработки и передачи информации. Соответственно возрастает и количество математических проблем, связанных с обоснованием информационной безопасности.

Значительное место криптографии и ее приложениям отводится и на настоящей конференции, в чем Вы можете убедиться, заглянув в Программу. Хотелось бы сделать лишь одно замечание.

В период с 8 по 18 сентября 2007 года в пансионате «Университетский» в г. Звенигороде в рамках конференции мы провели Международную научную школу «Булевы функции в криптологии и информационной безопасности». Фактически 8 сентября можно считать началом работы нашей конференции.

В заседаниях, семинарах и научных дискуссиях Международной школы приняли участие преподаватели, научные сотрудники, аспиранты и

студенты Института проблем информационной безопасности, механико-математического факультета и факультета вычислительной математики и кибернетики МГУ. В работе Школы приняли участие 15 зарубежных ученых, представляющие практически все мировые ведущие научные школы, работающие в области криптографии. Список докладов приведен в программе Конференции, которую вы получили. Труды Школы будут опубликованы через полгода.

В работе Школы принял участие известный бельгийский криптолог Барт Пренеель (Bart Preneel), вице-президент Международной ассоциации криптологических исследований (IACR), автор действующего американского стандарта шифрования, председатель конкурсной комиссии по разработке стандарта шифрования стран Евросоюза. 11 сентября с. г. профессор Пренеель прочитал на механико-математическом факультете в аудитории имени Колмогорова открытую публичную лекцию для студентов и преподавателей МГУ «Роль криптологии в информационном обществе».

Тематика Международной школы нам представляется весьма актуальной. Конечно, основоположник современной математической логики английский математик Джордж Буль когда 160 лет назад придумывал алгебру, которую сегодня называют булевой, не предполагал, что он возводит себе памятник. Но сегодня булева алгебра — это язык математики, криптографии, информационных технологий и отрадно, что участники международной школы выразили желание и готовность приложить совместные усилия по разработке перечня открытых проблем в области криптографических приложений булевых функций. Такой перечень позволит всем специалистам в этой области более четко понимать взаимоотношение разных задач и проблем, видеть возможные «точки прорыва», а также сфокусировать усилия молодых перспективных ученых на наиболее актуальных задачах.

На наш взгляд, достигнутые научные результаты Международной школы придадут дополнительный импульс развитию в Московском университете разделов математики, использующих аппарат теории булевых функций или связанных с приложениями в криптографии. Принято решение международные школы по криптографии проводить в Московском университете один раз в два года. Другим «классическим» направлением научных исследований, вынесенных на обсуждение нашей Конференции, является компьютерная безопасность или безопасность информационных технологий. Неуклонный рост масштабов и сфер применения информационных технологий приводит к адекватному росту новых вызовов и угроз.

Этой проблематике в Московском университете уделяется повышенное внимание, проводится широкий круг исследований.

Высокую оценку специалистов получило завершенное недавно фундаментальное исследование «Методы и средства противодействия компьютерному терроризму: механизмы, модели, сценарии, инструментальные средства и административно-правовые решения», выполненное в Московском университете под научным руководством ректора МГУ академика В. А. Садовничего и профессора Института проблем информационной безопасности МГУ В. А. Васенина.

В программу Конференции включено около 20 докладов по направлению «Математическое и программное обеспечение безопасности компьютерных систем».

Хотелось бы обратить Ваше внимание на то, что, наша конференция проходит в предверии Второго этапа Международного Форума по вопросам управления использованием Интернета, который состоится в ноябре с. г. в Бразилии. Считаем принципиально важным включение семинара «Интернационализация управления Интернетом» в проблематику нашей конференции.

На Всемирной встрече на высшем уровне по вопросам информационного общества, состоявшейся в 2003—2005 гг. в Женеве и Тунисе, совместными усилиями всех стран мира удалось выработать документы, отражающие общую точку зрения на те проблемы, с которыми столкнулось человечество в своем стремлении овладеть новыми информационными технологиями, использовать их потенциал для прогрессивного, устойчивого развития.

С учетом общей направленности настоящей конференции представляется важным отметить, что и в Женевской Декларации принципов и в Тунисском обязательстве, принятых, соответственно, на первом и втором этапах Всемирной встречи на высшем уровне в качестве важнейших условий построения открытого для всех информационного общества, в частности, закреплены повышение доверия и безопасности при использовании информационно-коммуникационных технологий. Международное сообщество признало «необходимость эффективного противодействия проблемам и угрозам, возникающим в результате использования ИКТ, в целях, которые несовместимы с задачами по поддержанию международной стабильности и безопасности и могут оказать негативное воздействие на целостность инфраструктуры в рамках отдельных государств в ущерб их безопасности». Оно признало также необходимость «предотвращать злоупотребление информационными ресурсами и технологиями в преступных и террористических целях и соблюдать права человека».

Представляется, что в нашей работе мы можем опираться на эти положения заключительных документов Всемирной встречи.

На первом этапе Форума в Афинах (2006 г.) мы пытались донести позицию России по вопросам управления Интернетом, выделив ряд приоритетных проблем:

1. Формирование международного механизма обеспечения безопасного, непрерывного и стабильного функционирования Интернета и других сетей ИКТ. При этом мы исходили из необходимости разработки при равноправном участии всех заинтересованных сторон и применения правительствами, частным сектором и гражданским обществом общих принципов, норм, правил и процедур принятия решений в данной области.

Активизация международного сотрудничества с целью укрепления безопасности функционирования Интернета, как представляется, также должна быть направлена на разработку необходимых правовых механизмов, обеспечивающих проведение расследования и уголовное преследование киберпреступности, включая киберпреступления, совершенные в рамках юрисдикции одной страны, но имеющим последствия в другой.

2. Разработка международным сообществом, частным сектором и гражданским обществом общих принципов, норм, правил и процедур принятия решений в области обеспечения защиты информации личного характера, неприкосновенности частной жизни и данных в целях обеспечения безопасного осуществления гражданами их прав и свобод в информационной сфере.

3. Разработка международных механизмов правоприменения для защиты прав потребителей при онлайновом приобретении товаров и услуг, а также активизации международного сотрудничества в целях обеспечения безопасного использования Интернета в интересах электронной коммерции, электронного бизнеса, защиты интеллектуальной собственности.

Управление в данной области необходимо в целях формирования единых правовых аспектов регулирования отношений, обеспечения одинаковых правил ведения дел, предупреждения возникновения разногласий, несогласованных решений.

Однако одним из выводов, которые можно сделать по результатам политических дискуссий, прошедших на первом заседании Форума в Афинах, заключается в том, что участникам встречи так и не удалось приступить к обсуждению, в соответствии с мандатом Форума, цитирую: «вопросов государственной политики, касающихся ключевых элементов управления использованием Интернет в целях содействия обеспечению жизнеспособности, эксплуатационной надежности, безопасности, стабильности и развития Интернет».

В связи с этим работа нашей конференции в некоторой мере могла бы содействовать формированию основы для начала такой дискуссии.

Как представляется, это будет способствовать прояснению позиций заинтересованных сторон по данной проблеме.

В заключении позвольте мне выразить твердую уверенность в том, что наша конференция будет способствовать укреплению сотрудничества ученых в деле обеспечения безопасности и противодействия терроризму.

Спасибо за внимание.

Национальный антитеррористический комитет — коллективный инструмент противодействия терроризму

Е. П. Ильин

Уважаемые участники конференции!

В конце XX — начале XXI века Российская Федерация, как и весь мир, пережила масштабные атаки со стороны международного и внутреннего терроризма.

Россия столкнулась с захватами школы в Беслане, здания «Норд-Оста» в столице, вооруженным нападением на Нальчик, взрывами домов в Москве, Буйнакске и Волгодонске, а также другими жестокими преступлениями террористического характера. Не менее масштабные теракты произошли и во многих зарубежных странах: в США — 11 сентября 2001 г. (атаки на здание Всемирного торгового центра и здание Пентагона, в результате которых погибли, соответственно, 2749 и 184 человека), в Испании — в марте 2004 г. (серия взрывов в пригородных электричках г. Мадрида, в результате которых погиб 191 и ранено более 1900 человек), Великобритании — в июле 2005 г. (серия взрывов в г. Лондоне, в результате которых погибли 56, ранены более 800 человек) и т. д. Отмечаются все более значимые теракты в Ираке и Афганистане (количество единовременных жертв зачастую превышает 100 человек).

Указанные террористические атаки — лишь наиболее заметные террористические проявления; в целом же их количество непрерывно увеличивается. О беспрецедентном росте терроризма свидетельствует и обобщенная статистика. Если в 2004 г., по данным Государственного департамента США, в мире было осуществлено 3100 терактов (в результате которых погибли, были ранены и похищены более 28 тыс. человек), то в 2005 г. эти цифры возросли до 11 тыс. террористических акций (вследствие которых пострадало более 74 тыс. человек), а в 2006 году — до 14 с половиной тысяч (погибло около 75 тыс. человек).

Несмотря на то, что терроризм в тех или иных формах существовал всегда, XX век (и преимущественно вторая половина) стал периодом

качественного его изменения. Из индивидуального (например, терроризма эсеров в последний период существования Российской Империи) терроризм трансформировался в массовый: главным объектом террора стала не только властная элита, но и все общество; основными средствами устрашения стали убийства не конкретных людей, а неопределенного, как можно более широкого, круга лиц.

Главной задачей террористов при этом становится осуществление масштабных разрушений, сопровождающихся как можно большим количеством человеческих жертв, с тем, чтобы достичь максимального резонанса в СМИ, спровоцировать напряженность в обществе и тем самым оказать давление на действия и политику государств.

Современный терроризм является динамично развивающейся системой. Происходит постоянное развитие форм и методов осуществления террористической деятельности, установление связей и обмен опытом между террористическими группировками, в том числе с использованием глобальной коммуникационной сети Интернет.

Анализ практики террористической деятельности, а также отечественного и зарубежного опыта контртеррористической работы способствовал росту в российском государстве понимания того, что основным методологическим принципом деятельности по линии антитеррора должно стать адекватное упреждающее развитие самой системы противодействия терроризму, а также системный подход к устранению данного явления.

После крупнейшего и наиболее циничного за всю российскую, да и мировую, историю акта терроризма, произошедшего в Беслане в начале сентября 2004 года, Президент Российской Федерации В. В. Путин, выступая 13 сентября 2004 г. на расширенном заседании Правительства России, подчеркнул, что борьба с терроризмом является общегосударственной задачей, для выполнения которой требуется «единство действий всей исполнительной вертикали».

В своем выступлении он определил одно из важнейших направлений ее решения: «Нам в целом нужна антикризисная система управления, рассчитанная на условия ведущейся против России террористической войны. Нужна полноценная система мер, адекватная обстановке и готовая отразить угрозу террора в любой ее форме. Нужны и соответствующие антикризисные планы действий, которые должны быть у Правительства страны, у министерств, у ведомств, у субъектов Российской Федерации и у местных властей... В целом ряде стран, столкнувшихся с террористической угрозой, уже давно созданы единые системы безопасности, ответственные за комплексное обеспечение внутренней безопасности и борьбу с терроризмом. И нам в России необходима такая же организационная работа и такая же организация работы национальной системы безопас-

ности, которая способна не только пресекать теракты и преодолевать их последствия, но и работать на предотвращение вылазок террористов, организуемых ими диверсий и техногенных катастроф».

Во исполнение подписанного в тот же день Указа Президента России № 1167 «О неотложных мерах по повышению эффективности борьбы с терроризмом» Федеральной службой безопасности Российской Федерации совместно с заинтересованными министерствами и ведомствами была разработана принципиально новая концепция контртеррористической деятельности государства.

Данная концепция воплотилась в созданной Федеральным законом от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» и Указом Президента России от 15 февраля 2006 г. № 116 «О мерах по противодействию терроризму» качественно новой системе противодействия терроризму. Эта система включила в себя самые современные подходы в части определения понятия «терроризм», понимания стратегии контртеррористической деятельности, установления порядка взаимодействия органов государственной власти в сфере противодействия терроризму и т. д.

Важнейшей новеллой новой концепции противодействия терроризму стало включение в состав определения понятия «терроризм» термина «идеология насилия», что фактически послужило законодательным и теоретическим обоснованием необходимости существования наряду с институтами борьбы с терроризмом институтов предупреждения и профилактики терроризма. Полагаем, что подобное понимание является наиболее объективным и современным, отражает действительную сущность терроризма на современном этапе и в перспективе могло бы лечь в основу общемирового подхода к выработке и трактовке единого для всех стран-участников антитеррористической коалиции определения понятия «терроризм».

В то же время необходимо отметить, что данная концепция противодействия терроризму возникла не на пустом месте: ее созданию предшествовал анализ многолетней практики функционирования в нашей стране системы борьбы с терроризмом.

Хотел бы заметить, что то понимание концепции противодействия терроризму, к которому пришло российское государство, в определенной мере кореллирует и с европейским пониманием данного вопроса. Так, Контртеррористическая стратегия Европейского Союза также предусматривает комплексный подход к противодействию терроризму и выделяет 4 основных его составляющих: Предотвращение (предотвращение вовлечения людей в террористическую деятельность путем воздействия на факторы и коренные причины терроризма в Европе и мире), Защита (защита людей и инфраструктуры, а также снижение уязвимости от атак, включая

усиленную защиту границ, транспорта, критически важных объектов), Преследование (преследование террористов и расследование терактов вне зависимости от границ; препятствование планированию, перемещению и коммуникации; уничтожение поддерживающих террористов сетей; пресечение финансирования и доступа к орудиям преступлений, а также правосудие в отношении террористов), Ответ (подготовка себя в духе солидарности, минимизация последствий террористических атак, улучшение возможностей по предотвращению последствий).

Основа российской общегосударственной системы противодействия терроризму в новом ее качестве начала складываться в 1996 году, когда по инициативе ФСБ России был издан Указ Президента Российской Федерации «О мерах по усилению борьбы с терроризмом».

В данном документе была впервые нормативно закреплена долго вынашиваемая идея межведомственного подхода к борьбе с терроризмом. Правительству России предписывалось определить порядок взаимодействия федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации при возникновении угрозы актов терроризма или при их совершении.

Также впервые данным Указом была обозначена необходимость создания единого координационного органа по организации взаимодействия федеральных органов исполнительной власти при проведении антитеррористической деятельности и пресечении актов терроризма.

В целях реализации положений Указа Президента Российской Федерации об обеспечении координации деятельности по борьбе с терроризмом, повышении эффективности проведения специальных операций в 1997 году была создана Межведомственная антитеррористическая комиссия Российской Федерации. Председателем комиссии стал по должности Директор ФСБ России.

Также был нормативно закреплен институт региональных антитеррористических комиссий (АТК), что позволило сформировать многоуровневую систему координации деятельности различных органов государственной власти в данной сфере.

Несмотря на то, что Межведомственная антитеррористическая комиссия Российской Федерации была призвана осуществлять свою работу на постоянной плановой основе (в частности, проводить заседания не реже одного раза в квартал), она не имела собственного постоянного рабочего органа, в связи с чем подготовка материалов к заседанию Комиссии и ее решений осуществлялись в основном представителями тех федеральных органов исполнительной власти, к ведению которых относились вопросы, выносимые на повестку дня. Определенную дополнительную нагрузку и оказание содействия в подготовке заседаний взяла на себя Федеральная

служба безопасности Российской Федерации, на которую возлагалось организационно-техническое и информационно-аналитическое обеспечение деятельности Комиссии.

Для непосредственного управления силами и средствами, привлекаемыми для проведения контртеррористических операций (КТО) и ликвидации последствий террористической деятельности, Комиссия образовывала из своих членов оперативный штаб (ОШ), деятельность которого носила, однако, ситуационный, а не системный характер, что, естественно, снижало эффективность проводимых КТО.

В 1998 году в связи с принятием Федерального закона «О борьбе с терроризмом» Межведомственная антитеррористическая комиссия Российской Федерации была упразднена, а вместо нее образована Федеральная антитеррористическая комиссия (ФАК).

Безусловно, принятие Федерального закона «О борьбе с терроризмом» стало важнейшим шагом на пути совершенствования системы борьбы с терроризмом. Принятие данного закона вывело правовое регулирование на качественно новый — законодательный — уровень, что позволило сформировать общегосударственную концепцию понимания борьбы с терроризмом, и, в соответствии с ней, создать новую организационную структуру. Была осуществлена попытка поднять статус Федеральной антитеррористической комиссии путем определения в качестве ее руководителя Председателя Правительства Российской Федерации.

Вместе с тем Федеральная антитеррористическая комиссия так же, как и Межведомственная антитеррористическая комиссия Российской Федерации, не смогла устранить отмеченных выше недостатков, так как по-прежнему не имела своего постоянно действующего аппарата, в связи с чем подготовка материалов к заседаниям Комиссии в основном возлагалась на представителей федеральных органов исполнительной власти, к ведению которых относились рассматриваемые вопросы повестки дня. Кроме того, данное обстоятельство объективно снижало организационное начало и уровень контроля за реализацией решений Комиссии.

Таким образом, несмотря на многие положительные черты новой системы борьбы с терроризмом, недостатки правового регулирования и организационного обеспечения в целом снижали эффективность ее функционирования. Так, деятельность региональных антитеррористических комиссий была слабо урегулирована нормативными правовыми актами и документами. Многие региональные АТК возглавлялись не руководителями субъектов Российской Федерации, а назначаемыми ими заместителями, зачастую не наделенных необходимыми властными полномочиями; не предусматривалось создание и функционирование постоянно действующих оперативных штабов по подготовке и проведению КТО и т. д.

В 2002 году, после захвата заложников в здании «Норд-Оста», было принято новое положение о Федеральной антитеррористической комиссии, которое, однако, принципиальных недостатков существовавшей на тот момент системы борьбы с терроризмом не устраняло.

В целом концепция антитеррористической деятельности государства, существовавшая в начале нового тысячелетия, по-прежнему нуждалась в совершенствовании, и трагические события в г. Беслане в начале сентября 2004 г. лишь обнажили многие недостатки в действовавшей в тот период системе борьбы с терроризмом.

Анализ проведения операции в Беслане и многих предшествующих ей контртеррористических операций показал, что наиболее крупными проблемными вопросами, характерными для всей системы борьбы с терроризмом, являлись:

- отсутствие системного подхода к формированию единой государственной стратегии антитеррористической деятельности и долгосрочных программ ее реализации;
- слабое нормативно-правовое регулирование основополагающих принципов функционирования системы противодействия терроризму, в том числе отсутствие заблаговременного, упреждающего планирования порядка действий группировок сил и средств при совершении диверсионно-террористических акций;
- несовершенство системы контроля и надзора за выполнением федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, их должностными лицами, юридическими лицами, общественными организациями, предпринимательскими кругами и отдельными гражданами установленных Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами и другими нормативными правовыми актами общеобязательных требований в сфере противодействия терроризму;
- неспособность существовавшего на межведомственном уровне механизма координации субъектов, осуществляющих борьбу с терроризмом, решать весь спектр возникающих в этой сфере задач;
- отсутствие слаженности в работе и единого управляющего центра;
- недостаточно четкое распределение задач и функций в сфере борьбы с терроризмом, отсутствие упреждающего начала в этой сфере;
- наличие параллелизма в работе правоохранительных органов в сфере борьбы с терроризмом;
- недостаточное ресурсное и научно-техническое обеспечение органов, осуществляющих борьбу с терроризмом.

Таким образом, как уже было отмечено ранее, в целях устранения существовавших недостатков и совершенствования государственного управления в области контртеррористической деятельности, в соответствии с Федеральным законом «О противодействии терроризму» и Указом Президента Российской Федерации «О мерах по противодействию терроризму», 10 марта 2006 года был образован Национальный антитеррористический комитет (далее — НАК, Комитет). Для организации планирования применения сил и средств федеральных органов исполнительной власти и их территориальных органов по борьбе с терроризмом, а также для управления контртеррористическими операциями в составе Комитета образован Федеральный оперативный штаб (далее — ФОШ, Штаб). В регионах, соответственно, были созданы антитеррористические комиссии (АТК) и оперативные штабы (ОШ) в субъектах Российской Федерации.

Таким образом, организационная составляющая сложившейся сегодня системы противодействия терроризму представлена в виде двух взаимосвязанных вертикалей структур, осуществляющих управление антитеррористическими мероприятиями в стране. Первую из них составляют структуры, осуществляющие координацию деятельности органов исполнительной власти по профилактике терроризма в Российской Федерации: НАК и АТК в субъектах Российской Федерации. Вторую вертикаль — структуры, осуществляющие управление мероприятиями по борьбе с терроризмом: ФОШ и ОШ в субъектах Российской Федерации.

Антитеррористические комиссии в субъектах Российской Федерации возглавляют руководители соответствующих субъектов, а оперативные штабы — руководители соответствующих территориальных органов безопасности. Таким образом достигается не только разграничение полномочий в сферах профилактики и борьбы с терроризмом, но и максимальная эффективность деятельности в рамках каждого из указанных направлений, поскольку руководитель субъекта Российской Федерации обладает наибольшим политическим влиянием и, соответственно, рычагами воздействия в своем регионе, а руководитель территориального органа безопасности владеет максимально широким спектром возможностей по линии борьбы с терроризмом и координации деятельности в этой сфере выделенных сил и средств правоохранительных органов и специальных служб.

В целом Национальный антитеррористический комитет, включив в себя представителей 17 государственных структур, министерств и ведомств (в том числе ФСБ, ФСО, МВД, МЧС, Минздравсоцразвития, Минтранс России, а также заместителя Руководителя Администрации Президента России, заместителя Председателя Государственной Думы Федерального Собрания Российской Федерации, заместителя Председателя Совета Федерации Федерального Собрания Российской Федерации и заместителя Председателя Правительства — руководителя аппарата Правительства) стал, действительно, коллективным инструментом противодействия терроризму, позволяя на практике осуществлять эффективную межведомственную координацию деятельности и совместное решение всех наиболее важных проблем в сфере противодействия терроризму.

Важным выводом из анализа работы предшественников НАКа — Межведомственной антитеррористической комиссии Российской Федерации и Федеральной антитеррористической комиссии стало понимание необходимости формирования действующего на постоянной основе аппарата Национального антитеррористического комитета.

В соответствии с Положением об аппарате Национального антитеррористического комитета аппаратом НАК осуществляется непрерывное информационное и методическое обеспечение антитеррористических комиссий и оперативных штабов в субъектах Российской Федерации, а также контроль за исполнением ими решений НАК и ФОШ по вопросам организации, координации и совершенствования деятельности территориальных органов федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и местного самоуправления в сфере противодействия терроризму.

К настоящему времени также впервые создана нормативная правовая база, регулирующая организацию контртеррористической деятельности не только на федеральном (деятельность НАК и ФОШ), но и на региональном уровнях (деятельность АТК и ОШ в субъектах Российской Федерации).

Положение об антитеррористических комиссиях в субъектах Российской Федерации было принято Национальным антитеррористическим комитетом 7 июля 2006 г. В соответствии с данным положением АТК в субъекте Российской Федерации является органом, осуществляющим координацию деятельности на территории субъекта Российской Федерации территориальных органов федеральных органов исполнительной власти, органов исполнительной власти субъекта Российской Федерации и органов местного самоуправления по профилактике терроризма, а также минимизации и ликвидации последствий его проявлений.

Для организационного и материально-технического обеспечения деятельности АТК в субъекте Российской Федерации высшим должностным лицом субъекта в составе органа исполнительной власти субъекта Российской Федерации определяется или создается вновь структурное подразделение — аппарат Комиссии, а также назначается должностное лицо, ответственное за организацию этой работы (руководитель аппарата АТК).

Так, например, в Москве в целях координации данной деятельности в Аппарате Мэра и Правительства создано Управление координации антитеррористической деятельности в городе Москве численностью 13 штатных единиц.

Деятельность оперативных штабов в отличие от антитеррористических комиссий в субъектах Российской Федерации не регулируется отдельным нормативным правовым актом, поскольку положения, регулирующие деятельность оперативных штабов в субъектах Российской Федерации, достаточно подробно раскрыты в Федеральном законе «О противодействии терроризму» и Указе Президента Российской Федерации «О мерах по противодействию терроризму».

Подводя итоги первых полутора лет функционирования новой системы противодействия терроризму, можно сделать вывод о правильности избранного государством подхода.

Так, за период существования НАК с марта 2006 г. пресечена деятельность более 130 бандглаварей и эмиссаров международных террористических организаций, предотвращено более 330 террористических актов, которые в основном планировались к осуществлению на территориях Дагестана, Ингушетии, Карачаево-Черкесской и Чеченской республик, Ставропольского края. За преступления, связанные с террористической и экстремистской деятельностью, осуждены 896 человек.

Наиболее ярко новый подход к противодействию терроризму, заключающийся в комплексном применении организационных, оперативных, информационных и иных мер, проявился при организации работы по профилактике терроризма в Чеченской Республике и в Южном федеральном округе в целом. После обращения в июле прошлого года Председателя НАК генерала армии Н. П. Патрушева к участникам бандформирований с предложением о добровольной сдаче властям и принятия Государственной Думой Федерального Собрания Российской Федерации соответствующего постановления об амнистии был реализован комплекс информационно-пропагандистских, оперативных и иных мероприятий. В результате проведенной в нашей стране и за рубежом работы с задействованием возможностей антитеррористических комиссий и оперативных штабов в субъектах Российской Федерации, СМИ, участием парламентариев, представителей духовенства, государственных институтов власти и общественности в период с 15 июля 2006 г. по 15 января 2007 г. были склонены к добровольной сдаче властям 546 боевиков. Этот процесс продолжается и в настоящее время, несмотря на то, что срок действия постановления об амнистии уже истек: по данным МВД Чеченской Республики, за 9 месяцев текущего года явились с повинной 127 человек.

К числу важнейших результатов работы Национального антитеррористического комитета следует также отнести реальное повышение эффективности действий всех ветвей власти в сфере борьбы с терроризмом. Так, в 2006 году практически вдвое, по сравнению с 2005 годом, сократилось число совершенных в России террористических актов (из них в Чеченской Республике — со 111 до 74, в Республике Дагестан — с 77 до 17)[1]. За период с января по сентябрь 2007 года количество терактов в Чеченской Республике также снизилось на 77 процентов (по сравнению с 2006 годом).

Безусловно, указанные позитивные сдвиги не следует объяснять только созданием и деятельностью НАК, однако существенный вклад в достижение таких показателей внесло, по оценке экспертов, безусловное улучшение координации и взаимодействия министерств и ведомств, руководители которых вошли в состав Национального антитеррористического комитета, Федерального оперативного штаба, АТК и ОШ в субъектах Российской Федерации.

По словам Президента Российской Федерации В. В. Путина, сказанным 18 октября 2007 г. в ходе прямого теле- и радиоэфира («Прямая линия с Президентом России»), Национальный антитеррористический комитет действует гораздо более эффективно, чем совокупность федеральных органов государственной власти в середине 90-х годов, свидетельством чему является последовательное сокращение количества террористических актов. В 2005 году их было зафиксировано около 250, в 2006 году — около 130, а за 8 месяцев текущего года — всего 25. Наряду с осуществлением координации предупредительно-профилактических и силовых действий соответствующих федеральных структур важнейшим направлением в деятельности Комитета было и остается совершенствование правовой основы противодействия терроризму.

В целях реализации положений Федерального закона «О противодействии терроризму» приняты постановления Правительства Российской Федерации от 11 ноября 2006 г. № 662 «Об источниках финансирования выплат денежного вознаграждения за содействие борьбе с терроризмом», от 12 января 2007 г. № 6 «Об утверждении Правил осуществления социальной реабилитации лиц, пострадавших в результате террористического акта, а также лиц, участвующих в борьбе с терроризмом» и от 6 июня 2007 г. № 352 «О мерах по реализации Федерального закона «О противодействии терроризму».

[1] Статистические сведения касаются деяний, предусмотренных в диспозициях ст. 205 (террористический акт) и ст. 277 (посягательство на жизнь государственного или общественного деятеля) Уголовного кодекса Российской Федерации.

В соответствии с указанным законом принято также Постановление Правительства Российской Федерации от 6 июня 2007 г. № 352, которым утверждены три очень значимых положения, регламентирующие порядок применения оружия и боевой техники Вооруженными Силами Российской Федерации для устранения угрозы террористического акта или его пресечения в воздушной среде, во внутренних водах, территориальном море, на континентальном шельфе Российской Федерации и подводной среде, а также при участии в проведении контртеррористической операции.

Кроме того, к настоящему времени Председателем НАК утверждены положения о Федеральном оперативном штабе, оперативном штабе в субъекте Российской Федерации и его аппарате, аппарате Национального антитеррористического комитета.

В результате скоординированных усилий всех заинтересованных министерств и ведомств в июне 2006 года решением Верховного Суда Российской Федерации признаны террористическими еще две международные организации — «Джунд аш-Шам» (Войско Великой Сирии) и «Исламский джихад — Джамаат моджахедов». Всего на территории Российской Федерации к настоящему времени запрещена деятельность 17 подобных структур, в том числе таких печально известных как «Аль-каида», «Хизб-ут-Тахрир», «Братья-мусульмане». Это серьезно усилило правовую основу для пресечения их противоправной деятельности в нашей стране.

Вносятся изменения в Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации», в части осуществления журналистской деятельности при проведении контртеррористической операции. При этом используются ранее одобренные журналистским сообществом принципы освещения подобных событий, закрепленные своего рода Кодексом (или Хартией) журналистов России после событий, связанных с захватом заложников в г. Москве.

Так, в целях недопущения вооружения террористов информацией о принимаемых участниками КТО мерах предполагается, что при проведении контртеррористической операции порядок сбора и получения информации журналистами определяется представителем оперативного штаба, осуществляющим управление операцией и несущим персональную ответственность за ее результаты и жизнь каждого заложника. Запрещается распространение сведений о тактике проведения операции, спецсредствах и иной информации, которая может поставить под угрозу жизнь и здоровье людей.

Как вы помните, печальный опыт недостаточно выверенного для кризисной ситуации исполнения журналистского долга был уже получен при проведении операции по освобождению заложников на Дубровке, когда освещение событий в некоторых СМИ позволяло террористам корректировать свои преступные деяния, ухудшать положение заложников и затруднять действия властей по их освобождению. Безусловно, при осуществлении этой работы следует учесть, что инструмент подобной регламентации очень тонок, поэтому предстоит еще неоднократно тщательно выверить предлагаемые проектом закона изменения, в том числе с учетом позиции журналистского сообщества и институтов гражданского общества.

Важнейшим направлением деятельности Национального антитеррористического комитета является совершенствование межведомственного взаимодействия.

В данной сфере особого внимания требуют вопросы разграничения правомочий и компетенции министерств и ведомств в сфере противодействия терроризму, определения задач и четкого порядка выделения и применения сил и средств различной ведомственной принадлежности при проведении совместных мероприятий по предупреждению и пресечению террористической деятельности.

От слаженности и согласованности действий всех взаимодействующих структур во многом зависит общий успех принимаемых антитеррористических мер. Именно в этом: упреждающем формировании и обучении привлекаемых сил и средств, их постоянной готовности к решению контртеррористических задач, и состоит одно из важнейших условий создания качественно новой системы противодействия терроризму.

Главной задачей оптимизации межведомственного взаимодействия является формирование единого межведомственного информационного пространства путем создания единых коммуникационных сетей между различными министерствами и ведомствами с тем, чтобы сделать обмен информацией более эффективным и оперативным.

Первые шаги в данном направлении уже сделаны, наглядным свидетельством чему является продемонстрированный накануне Президенту Российской Федерации В. В. Путину Единый банк данных по проблемам борьбы с терроризмом. Ее основу составляет единая информационно-коммутационная сеть, абонентами и поставщиками информации которой станут министерства и ведомства силового блока, а также Росфинмониторинг, Минобрнауки, Минпромэнерго и некоторые другие структуры.

Говоря о совершенствовании материально-технического обеспечения функционирования системы противодействия терроризму, следует указать, что в 2007 году завершаются мероприятия, предусмотренные федеральной целевой программой «Антитеррор (2005—2007 годы)». Предварительные результаты ее выполнения позволяют сделать вывод о том, что и в дальнейшем все наиболее важные проблемы противодействия

терроризму необходимо решать с использованием программно-целевого метода планирования. К настоящему времени разработана и внесена на утверждение в Правительство Российской Федерации концепция федеральной целевой программы «Антитеррор (2009—2012 годы)» объемом более 20 млрд рублей.

Характеризуя функционирование новой организационной структуры общегосударственной системы противодействия терроризму, об опыте которой, к слову говоря, очень позитивно отозвались средства массовой информации, прокомментировавшие Указ Президента страны о создании Государственного антинаркотического комитета как развитие «опыта НАК, показавшего свою эффективности в подавлении терроризма», необходимо отметить, что с марта 2006 года по настоящее время проведено 20 серьезных организационно-управленческих мероприятий: 10 заседаний НАК и 10 заседаний ФОШ.

На заседаниях НАК рассмотрены вопросы о проекте основ государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов; о разработке и внедрении единых типовых требований по антитеррористической защищенности потенциально опасных объектов, об антитеррористической защищенности объектов атомно-энергетического комплекса Российской Федерации, о профилактике террористических угроз и мерах по обеспечению безопасности населения на территории санаторно-курортных комплексов, о противодействии угрозе биотерроризма и мерах по обеспечению антитеррористической защищенности биологически опасных объектов на территории Российской Федерации и т. п. Не менее важные вопросы рассматривались и ФОШ.

В рамках международного сотрудничества федеральными органами исполнительной власти, представленными в НАК, в 2006—2007 годах обеспечено участие во всех наиболее значимых международных форумах, посвященных вопросам противодействия терроризму.

Россия стала первой страной, ратифицировавшей Конвенцию Совета Европы о предупреждении терроризма, в связи с чем внесен ряд изменений в нормативные правовые акты Российской Федерации. В частности, были определены полномочия органов государственной власти субъектов Российской Федерации и органов местного самоуправления в области профилактики терроризма, минимизации и ликвидации последствий его проявлений, что позволяет субъектам Российской Федерации самостоятельно планировать и осуществлять на местах антитеррористические мероприятия.

Международное сотрудничество в сфере противодействия терроризму установлено и в формате деятельности международных организаций и структур — ООН, «Группы восьми», ОБСЕ, Совета Европы, ОДКБ, СНГ, ШОС, АТЭС, Регионального форума по безопасности АСЕАН (АРФ), в рамках взаимоотношений России с авторитетными международными организациями — Евросоюзом, НАТО, АСЕАН, ОАГ, а также путем развития двусторонних отношений по линии международной антитеррористической коалиции.

Кроме того, расширяются возможности в сфере межгосударственного взаимодействия в связи с подписанием на июньском саммите ШОС соглашений «О порядке организации и проведения антитеррористических мероприятий на территориях государств-членов Шанхайской организации сотрудничества», «О сотрудничестве в области выявления и перекрытия каналов проникновения на территории членов Шанхайской организации сотрудничества лиц, причастных к террористической, сепаратистской и экстремистской деятельности», а также Программы сотрудничества в борьбе с терроризмом, сепаратизмом и экстремизмом на 2007—2009 годы.

Следует заметить, что деятельность Национального антитеррористического комитета и Российской Федерации в целом в сфере противодействия терроризму позитивно воспринимается многими зарубежными партнерами: ими признается приоритет Российской Федерации в этой сфере и эффективность нашей деятельности по многим составляющим этой работы. Так, например, в ежегодном докладе Государственного департамента США по террористической активности в мире в 2006 году изменение российского законодательства в рассматриваемой области и создание НАК отмечается как позитивный шаг, позволивший оздоровить ситуацию на Северном Кавказе и в других регионах Российской Федерации. В данном докладе, в частности, отмечается, что: «Во многом благодаря эффективной работе НАК, взявшего на себя координацию работы в этой сфере, впервые за 4 года в России не допущено масштабных терактов».

Вместе с тем, серьезные проблемы в сфере повышения эффективности международного сотрудничества продолжают иметь место. Ситуация в сфере борьбы мирового сообщества с международным терроризмом усугубляется, в частности, применением так называемой практики «двойных стандартов», которая мешает странам с различными приоритетами во внешнеполитической деятельности выработать единый подход к пониманию как самого феномена терроризма, так и к реализации конкретных совместных мер по противодействию данному явлению.

Основной причиной того, что до сих пор так и не удалось выработать признанного всем мировым сообществом определения международного

терроризма, были до недавнего времени острые политические разногласия государств, связанные прежде всего с различными подходами к оценке понятий национально-освободительной борьбы народов и ее взаимосвязь с международным терроризмом. Еще одной важной причиной неумения договориться является нежелание некоторых государств связывать себя твердыми обязательствами в области борьбы с международным терроризмом, а также намерениями получить в связи с этим определенные политические дивиденды.

Со своей стороны, Российская Федерация в целом и Национальный антитеррористический комитет в частности активно выступают за формирование единого подхода к противодействию терроризму во всем мире, являясь активным участником большинства уже существующих международных договоров и организаций. Значительным представляется вклад России в разработку и принятие 8 сентября 2006 г. Глобальной контртеррористической стратегии Организации Объединенных Наций, в рамках которой был закреплен план совместных усилий международного сообщества по отражению террористических угроз, а также целого ряда международных правовых актов в данной сфере.

Россия придает приоритетное значение универсализации участия государств в основных глобальных антитеррористических международно-правовых инструментах. Нашей страной подписаны и ратифицированы все 13 универсальных конвенций ООН в сфере противодействия терроризму.

Справочно: 24 *июля* 2007 *года Федеральным законом* № 201-*ФЗ ратифицирована последняя из указанных конвенций «О маркировке пластических взрывчатых веществ в целях их обнаружения»* (*от* 1 *марта* 1991 *г.*).

В целях развития международного сотрудничества и создания единого международного антитеррористического пространства при активном участии аппарата НАК был создан и представлен на VI Совещании руководителей спецслужб, органов безопасности и правоохранительных органов иностранных государств — партнеров ФСБ России Международный банк данных по противодействию терроризму (МБД).

Основной целью создания МБД является формирование единой межгосударственной информационной системы обеспечения антитеррористической деятельности.

Международный банк данных по противодействию терроризму наполняется информацией, предоставляемой специальными службами, органами безопасности и правоохранительными органами на добровольной основе, а также материалами из открытых источников. ФСБ России взяло на себя функцию разработки МБД, включая решение информационно-аналитических и лингвистических задач, а также обеспечение функционирования банка данных.

Основой Международного банка данных является структурированный информационный массив, в который правоохранительные органы и спецслужбы каждого из заинтересованных государств смогут предоставлять имеющуюся информацию по вопросам противодействия терроризму и, соответственно, использовать сведения, получаемые от партнеров в интересах проведения оперативно-розыскных, профилактических и организационных мероприятий.

В целом использование МБД позволит значительно сократить время получения интересующей информации в отношении лиц и организаций, подозреваемых в причастности к международной террористической деятельности, с большей эффективностью осуществлять мониторинг развития оперативной обстановки по линии противодействия терроризму, проводить работу по выявлению законспирированных схем и каналов финансирования международных террористических структур.

Безусловно, несмотря на то, что уже за первые полтора года своего существования Национальным антитеррористическим комитетом проделана значительная работа, многие направления его деятельности проходят еще стадию становления.

Мы считаем необходимым завершить работу по приведению в соответствие с Федеральным законом «О противодействии терроризму» и Указом Президента Российской Федерации «О мерах по противодействию терроризму» всех без исключения ведомственных нормативных правовых актов федеральных органов исполнительной власти — участников КТО, затрагивающих эту сферу, разработать единые требования по антитеррористической защищенности и паспортизации критически важных объектов, объектов повышенной опасности, жизнеобеспечения и мест массового пребывания граждан.

Предстоит законодательно регламентировать обязанности руководителей государственных и негосударственных предприятий, а также частных предпринимателей по антитеррористической защите указанных объектов, что, в свою очередь, позволит установить их персональную ответственность за нарушения антитеррористического законодательства. Представляется, что соответствующие изменения должны быть внесены и в Кодекс Российской Федерации об административных правонарушениях, Уголовный кодекс Российской Федерации и иные нормативные правовые акты.

Кроме того, требуют дополнительной правовой регламентации такие важные вопросы, как физическая защита ядерных материалов, производственных установок и пунктов их хранения, порядок возмещения вреда,

причиненного в результате террористического акта, социальная защита лиц, участвующих в борьбе с терроризмом, обустройство государственной границы и т. п.

Одним из важных направлений деятельности после захвата и убийства сотрудников российского посольства в Ираке, а также похищения российских специалистов в Нигерии является координация деятельности в этой сфере государственных структур и бизнеса за рубежом.

В целях защиты российских граждан и организаций за пределами Российской Федерации выработаны и находятся в стадии реализации предложения по созданию в МИД России Ситуационно-кризисного центра, на который будет возложено обеспечение ситуационного реагирования на угрозы проведения терактов. Для реализации неотложных действий, обеспечения своевременного информирования Ситуационно-кризисного центра и взаимодействия с местными властями выработано предложение о создании ситуационных групп во всех посольствах и консульствах Российской Федерации в зарубежных странах. В настоящее время, по данным МИД России, подобные группы уже созданы в более чем 150 странах. В эти структуры будут включены представители всех министерств и ведомств, в компетенцию которых входят вопросы обеспечения безопасности российских представительств за рубежом.

На сегодняшний день перед системой противодействия терроризму в Российской Федерации наиболее остро стоят следующие приоритетные задачи: предупреждение и пресечение террористических угроз в преддверии подготовки и проведения выборов в Государственную Думу Федерального Собрания и предстоящих выборов Президента Российской Федерации; повышение степени готовности сил и средств к пресечению террористических актов, ликвидации и минимизации их последствий; организация работы по противодействию и подрыву основ идеологии терроризма.

Принципиально важно отметить, что задача противодействия распространению идеологии терроризма рассматривается нами в качестве одной из приоритетнейших задач, стоящих перед Национальным антитеррористическим комитетом.

Наиболее проблемным вопросом в данной области является распространение указанной идеологии через сеть Интернет, поскольку в последние годы Интернет наиболее широко используется террористами как канал идеологического воздействия на объекты террористических устремлений и формирования выгодного террористам общественного мнения. Причины востребованности Интернета преступниками — легкий доступ к аудитории, обеспечение анонимной коммуникации, слабое регулирование этого вопроса на государственном уровне, глобальное распространение,

высокая скорость передачи информации, дешевизна и простота в использовании, мультимедийные возможности. Данный факт подтверждается, к примеру, ростом числа сайтов террористической направленности.

В настоящее время в сети Интернет поддерживается от 100 до 150 только русскоязычных сайтов, пропагандирующих идеи терроризма и экстремизма. Многие сайты специально и постоянно меняют свой электронный адрес.

В целом только ФСБ России в 2006—2007 гг. году выявила около 1300 фактов использования открытых телекоммуникационных сетей в экстремистских и террористических целях, около 100 из которых пресечено путем применения предусмотренных законодательством мер.

Для более широкого вовлечения гражданского общества в решение вопросов противодействия терроризму помимо активной антитеррористической пропагандистской деятельности ведется работа по созданию при НАК Координационно-экспертного совета и различных экспертных групп, к работе в которых планируется пригласить ведущих политических, общественных и религиозных деятелей, представителей бизнес-сообщества с тем, чтобы решать вопросы защиты наших граждан от террористических посягательств сообща.

Пользуясь присутствием иностранных коллег и партнеров по антитеррористической коалиции, хотелось бы сказать, что практика деятельности НАК, спецслужб и правоохранительных органов Российской Федерации убедительно свидетельствует о том, что в сфере непосредственной борьбы с терроризмом (именно борьбы, а не всего комплекса противодействия терроризму), в том числе на межгосударственном уровне, необходимо прежде всего работать над достижением межгосударственных договоренностей о решении данного вида антитеррористических задач преимущественно мерами, свойственными задачам и функциям спецслужб и правоохранительных органов, без применения военной силы и, соответственно, значительных воинских контингентов. Это позволит достичь главного — того, чтобы гражданское население испытывало как можно меньше неудобств, связанных с противостоянием государств и преступников в сфере борьбы с терроризмом. Антитеррористические меры в этом случае будут носить выверенный, преимущественно «точечный», характер, свойственный деятельности спецслужб.

Приоритет подобного способа решения задач пресечения террористической деятельности является наиболее приемлемым и актуальным как для Российской Федерации, так и для стран всего мира, активно борющихся с терроризмом. Негативные примеры Афганистана, Ирака и ряда других государств, где активно используются воинские континген-

ты, убедительно свидетельствуют о правильности российского подхода к решению антитеррористических задач.

В целом можно с уверенностью сказать, что в сфере противодействия терроризму Российская Федерация избрала наиболее верный путь. Именно консолидация усилий различных министерств и ведомств, а также гражданского общества является залогом победы в войне, которую, по справедливому замечанию Президента Российской Федерации В. В. Путина, международный терроризм объявил России.

Культурно-языковые проблемы безопасности в современном обществе

С. Г. Тер-Минасова

Сегодня на нашей конференции обсуждается наиважнейший вопрос о будущем человечества.

Именно так.

Будущее наше — так же, как и настоящее, и прошлое — напрямую связано со способностью к ОБЩЕНИЮ. Естественному человеческому общению. Вдумайтесь в слова: че-ло-ве-че-ско-му, ес-тес-твен-но-му! Данному нам, человекам, изначально, природой или Богом. Благодаря ОБЩЕНИЮ стало возможным развитие *человека разумного*, homo sapiens. **Общение правит миром, жизнью людей и определяет наше будущее.** А главное средство общения людей — это по-прежнему **язык**.

Язык — первое и главное средство познания мира — и внешнего, и внутреннего — (когнитивная функция языка). Знание, накопленное в процессе познания — развивается и передается — во всех сферах жизни, деятельности и, соответственно науки — тоже почти исключительно с помощью *языка* — в процессе *общения*

Современная эпоха, ее направление и развитие, обусловлена внезапными, стремительно ускоряющимися и умножающимися, неслыханными, небывалыми достижениями научно-технического прогресса, о которых не могли мечтать даже фантасты. Все эти величайшие открытия человеческого гения направлены на одно: облегчение, улучшение — оптимизацию — жизни и общения людей.

Телевидение, мобильные телефоны, Интернет дают возможность людям общаться, преодолевая и время, и пространство.

И снова сразу же замаячила впереди Вавилонская башня — возможность вместе, всей планетой, строить, растить, покупать-продавать, обучать и т. д. и т. п.

И замелькали новые вывески: Глобальная Деревня, Соединенные Штаты Земли, Глобализация...

Идея сама по себе такая же хорошая, как все остальные мечты человечества — от Земли Обетованной до Светлого Будущего Коммунизма и Американской Мечты.

В Глобальной Деревне все население планеты живет вместе, мирно, дружно, **безопасно**. Поскольку размеры Земли с изобретением сверхскоростных средств передвижения и коммуникаций очень сильно уменьшились, все осознали, что тридесятых царств уже нет, у нас одна общая — не такая уж огромная — планета и надо за ней всем вместе ухаживать.

Мы живем вместе, работаем вместе, объединяем достижения, таланты, умы. Вместе боремся за жизнь и безопасность как самой планеты, так и всех населяющих ее людей.

И глобализация — это взаимодействие и взаимозависимость всех людей и всех стран. Выражаясь нашей доброй старой лексикой — это мир и дружба между народами, потому что для всех людей жить безопасно — это, в первую очередь, жить в мире. Кто же может против этого возражать? Откуда взялись антиглобалисты?

Увы! Глобализация — явление противоречивое. Иначе говоря — диалектичное. А диалектика, борьба и единство противоположностей — это условие прогресса. Жаль, конечно, что прогресс, развитие человечества невозможны без конфликтов, без борьбы, жаль, что этот прогресс покупается кровью, несчастиями и жизнями миллионов людей.

Очень кратко: «за» и «против» глобализации.

«За» — это главная идея глобализации: мир, дружба, сотрудничество, объединение усилий всех народов по обеспечению безопасности. Международная промышленность, торговля, научная деятельность, сельское хозяйство, образование, здравоохранение, охрана окружающей среды, борьба с преступностью, борьба с терроризмом, международный туризм, спорт и т. д. и т. п.

Многое уже происходит.

«Против», во-первых, не получающиеся, искаженные и извращенные «за». Зло всегда активнее и организованнее Добра. Используя технические достижения, объединились террористы всего мира, преступные группировки, торговцы наркотиками. Их объединенные усилия гораздо эффективнее объединенных усилий полиции, Интерпола, борцов с терроризмом, наркотиками и т. п. Рост экономики, вызванный глобализацией, только увеличил пропасть между горсткой богатейших людей планеты и миллиардами (да, да!) бедных и беднейших людей. (меня потрясли цифры 2002 года: состояние 200 богатейших людей мира превышает совокупный доход 40 %, или 2,4 миллиарда, жителей планеты. Сейчас, значит разрыв еще больше...)

И, наконец, во-вторых и «в-главных» «против» — человеческий фактор: языки, культуры, цивилизации. Национальная самобытность, национальный язык и национальная культура — под угрозой поглощения, нивелирования, уничтожения.

Именно они препятствуют объединению людей. Без глобального языка (а язык неотделим от культуры) и, значит, глобальной культуры не может быть глобального сообщества и нет возможности построить новую Вавилонскую башню, то есть Глобальное Мировое Сообщество.

Отсутствие глобального языка тормозит объединение человечества для решения общечеловеческих проблем, в том числе и проблем безопасности.

Введение единого глобального языка (английского, как сейчас, или какого-то другого в будущем) привлекает возможностью решить многие проблемы: облегчить международное общение, сократить огромные финансовые расходы международных организаций, компаний, концернов на переводчиков — письменных и устных, способствовать обмену информацией и, следовательно, ускорению и улучшению научно-технического прогресса, торговли, бизнеса.

Единый язык освободил бы и армии преподавателей иностранных языков, и легионы их учащихся.

О едином языке мечтали поэты.

«Века все смелют,
дни пройдут.
Людская речь
В один поток сольется,
Историк, сочиняя труд,
Над нашей рознью улыбнется.»

(Сергей Есенин)

Борьба **за языковое господство** — и одновременно против него — разгорается всё сильнее: за языком стоит идеология, культура, система ценностей и, наконец, власть.

О «триумфальном шествии» английского языка по планете вообще и в нашей стране в частности много говорить не имеет смысла — настолько это очевидно и общеизвестно.

2 миллиарда человек говорит на английском языке — родном, втором или иностранном.

Официальный язык — единственный или наряду с другими более чем в 75 странах.

80 % компьютерной информации хранится в английском варианте.

85 % международных телефонных звонков — на английском языке.

Угонщик самолета в аэропорту Внуково потребовал 2 миллиона долларов, карты Франции и Турции и... англоговорящий экипаж.

Английский язык как иностранный в школах России одержал «сокрушительную» победу: 70 % учащихся (а в больших городах — 85 %)

выбрали именно английский язык в качестве иностранного. Цифра растет каждый день.

На повестке дня — введение английского языка как обязательного первого иностранного языка в российский школах. (Сравнение в Японии — то же самое: кампания по введению английского языка как обязательного в начальной школе).

Из многих причин, обусловивших явное превосходство английского языка в роли глобального, или мирового, главные — две:

1. Экономическое, политическое, культурное господство Америки и предшествующее этому геополитическое доминирование Британской империи.
2. Пришествие Его Величества — Интернета.

По поводу первой причины — только одно замечание: во многих странах (например — во Франции) «глобализацию» называют «американизацией».

Сейчас проблема американизации особенно обострилась, но первыми о ней стали говорить британцы в самом начале XX века. В 1901 г. британский писатель William Stead опубликовал книгу «Американизация мира» (The Americanization of the World)

В 1912 г. Б. Шоу писал: главное из того, чему я стал свидетелем на протяжении моей жизни — это американизация.

Глобальная культура воспринимается как американская культура, потому что глобальный язык — это английский (скорее — американский) язык.

Что касается Интернета, то с его пришествием роль английского языка еще более укрепилась, он стал глобальным языком «электронной глобальной деревни»: компьютерная терминология — практически полностью английская. Широкое и быстрое распространение Интернета имеет огромное влияние на развитие международного общения — влияние весьма и весьма противоречивое и по сути, и по последствиям.

Действительно, с одной стороны, Интернет ведет к «глобальной деревне», к некоему космополитическому обществу, к всемирной сети (world wide web), к великой **интер**национальной **интер**нетной семье, где национальные особенности культуры, менталитета, видения мира — мировоззрения, идеологии стираются, размываются и могут как бы перестать существовать вовсе.

В Интернете Интернациональное довлеет над Национальным.

Однако «мировая паутина» воспринимается многими и как «геополитическое орудие Запада»... право на голос (и самое главное, право на язык) есть у Запада, право на слушание — у всех остальных.

Александр Дугин «Континент в мировой паутине».

С другой стороны, противоположная тенденция — интерактивность, общедоступность, демократичность в самом полном смысле слова, предоставление **каждому** человеку возможности выразить себя, свое мнение, отношение и таким образом **участвовать** на равных правах.

В отличие от средств массовой информации, обрушивающих на индивидуума-реципиента свои сообщения-воздействия, где человек, личность — лишь **объект** их деятельности, Интернет вовлекает в общение всех участников, они одновременно **и субъект и объект** действия, каждый из них может выразить свое индивидуальное мнение и найти единомышленников из огромной всемирной, глобальной, интернетной семьи.

Иными словами, таким образом отражается одно из основных противоречий человеческого общества: противоречия между равенством и индивидуальностью, т. е. разнообразием (diversity). Люди рождаются **равными** и должны иметь равные права, но люди рождаются **разными** и стремятся сохранить свою индивидуальность, неповторимость, особенность. То же относится к нациям, языкам и культурам. Включают ли права человека право на язык?

Сейчас стала очевидной глубина и серьезность (возможно — неразрешимость) проблемы глобального языка.

Роль английского языка как «глобального» и сам язык оцениваются в самых разных языковых выражениях: начиная от «уникальный», «легко усваиваемый», «самый влиятельный и самый могущественный» до: «катастрофический», «евроцентристский», «языковой империализм» и даже «языковой фашизм». Paul Delaney: Английский язык — такой же убийца языков, как Интернет — убийца культур.

Очень важный вопрос — какой/что за английский язык стал/становится глобальным? Языком международного общения стал не великий и могучий английский язык, опирающийся на великую английскую литературу, философию, технические достижения мирового уровня. Глобальный английский язык — это некий «английский как иностранный», — это упрощенный, прагмалингвистический вариант языка учебников по английскому для иностранцев.

А теперь — следующий, еще более страшный вывод. Продвижение глобального языка, разумеется, обозначает продвижение некой глобальной культуры. Иначе говоря, глобальный язык навязывает миру глобальную культуру. И это не культурный потенциал великого английского языка, это дистиллированная, стереотипная упрощенная «англоязычная культура как иностранная».

Картина складывается очень нерадостная: убийство языков, разрушение культур. Американцы сопротивляются: наша культура сложилась из

многих культур, мол — многонациональная, уникальная страна и наша культура — уникальная, многонациональная, универсальная. Это — будущее мира и нечего плакать о разрушении «local eccentricities» — неких местных чудачествах.

Итак, поскольку язык и культура неразделимо спаяны, и каждый язык несет в себе весьма значительный культурно-идеологический заряд, продвижение и доминирование одного языка — в настоящее время английского — в качестве средства общения между народами мира неизбежно приводит к тому, что вместе с языком проникает чужая культура и идеология. Иными словами, всему миру навязываются англо-американские традиции, системы ценностей, образ жизни, менталитет, мировоззрение — то есть все то, что составляет нравственную основу нации. Часто этот заимствованный с языком культурно-идеологический заряд входит в противоречие с местной национальной культурой. При этом тайные силы культуры действуют постепенно, незаметно и поэтому гораздо более эффективно, чем любые способы открытого воздействия.

Мой любимый пример — простое невинное устойчивое английское словосочетание *poor but honest — бедный, но честный*. В сказках это определение всегда обозначает положительного героя. А теперь представьте себе начало русской сказки: *Жил-был бедный, но честный рыбак*. Все бы хорошо, если бы не *но*. Всего-то один союз, но за ним чуждое и неприемлемое, шокирующее мировоззрение, отношение к людям, какая-то странная мораль: ведь это *но* подразумевает, что все бедные нечестные, а вот этот рыбак, по исключению, оказался честным.

В наших историях логично было бы *богатый, но честный*, поскольку в нашем сознании, в нашей культуре богатство честным путем нажить нельзя, и такого даже в сказках, ни по какому исключению, представить невозможно.

Слушает, значит, англоязычный ребенок (или — изучающий английский язык) и в сознание его проникает заложенная в устойчивом обороте мысль: бедные — нечестные.

И еще один любимый пример — из области орфографии: в английском языке *I — я* — пишется всегда (!) с большой буквы. Представляете, если бы мы писали *Я* всегда так, как пишут *I*: «*Встречу Я вас, Иван Иванович, у входа в парк*». Я (любимый) — с большой буквы, а вы, Иван Иванович, с маленькой. Совсем другой народ бы получился.

Значит, вместе с глобальным языком формируется глобальная культура. В нынешней ситуации это англо-американская или просто американская, поскольку американцы как представители единственной в мире супердержавы активны во всех сферах жизни, и именно американский вариант английского языка стал самым востребованным и самым проникающим — и через политику, и через науку, и через компьютерные языки, и через песни и фильмы.

Получается, что во многом именно благодаря *языку*, несущему в себе огромный заряд культуры, идеологии, системы ценностей, образа жизни, отношений между людьми и очень много всего «человеческого», то есть гуманитарного, всемирное сообщество, глобальная деревня вместе с общечеловеческой, всепланетной безопасностью превращается в «американскую деревню». Эта тенденция к однополярному миру, вполне возможно, *провоцирует терроризм*, который, на мой взгляд, *не* верно относить на счет только исламского экстремизма. Конфликты языков и культур в современном обществе настолько обострились, что С. Хантингтон, политолог Гарвардского университета, предсказал III Мировую войну как войну культур и цивилизаций.

Роль языков и культур в современном обществе так же противоречива, как и само общество. Языки и культуры это не только и не просто барьеры, разделяющие людей со времен Вавилонской башни, это одновременно и *щиты*, охраняющие национальную культуру и идентичность народов.

Об этом моя последняя книга с значащим названием «Война и мир».

Подведем итоги.

1. Английский язык — это главный язык международного общения. Он получил этот статус по вполне определенным социально-историческим причинам. Он ни в чем не виноват. Он не купил это положение, не достал по знакомству. Так сложилась его история. Его нельзя «снять с должности», повысить или понизить в статусе. Это определяет ход истории человечества.

2. Будущее английского языка как глобального неизвестно. Можно (и нужно) делать предположения, но предсказать его судьбу невозможно.

Он может распасться на варианты, которые станут отдельными языками (как русский, белорусский, украинский). На это нужно время.

Он может быть вытеснен другим языком. Например, китайским... Это может произойти гораздо быстрее.

Могут получить статус глобальных, наравне с английским, другие языки.

3. Конечно, преподавание языка означает продвижение заложенной в нем культуры народа — носителя этого языка. Ничего плохого в знакомстве с другой культурой нет. Это только полезно, это расширяет горизонты, обогащает родную культуру, тем более что за английским языком стоит великая культура. Плохо, если это насильно навязывается или приводит к раболепному подражанию. Но это крайности.

4. Хорошо, что народы осознали угрозу этих крайностей. Это полезно и учителям, и учащимся. Сам факт, что вопросы «вины и ответственности» встали между людьми, — тоже факт отрадный: все заинтересованные стороны будут осторожнее, тактичнее, корректнее. Реальной угрозы вытеснения других языков нет. Но осознавать опасность и быть начеку — полезно.

5. Замечательный и неожиданный парадокс: перспектива глобализации и вторжения глобального языка и культуры заставила все народы встрепенуться, очнуться, *осознать* свою национальную самобытность, глубже оценить свою культуру и свой язык и начать о них заботиться. Однако с точки зрения безопасности всего человечества, обостряется конфликт между *международной*, всепланетной безопасностью и безопасностью *национальной*. И здесь, как это ни странно покажется представителям главных направлений нашей жизни — энергетикам, физикам, химикам, экономистам, финансистам и т. д. — важнейшую роль в качестве боюсь что главного препятствия играет этот самый человеческий (не — технический, не — естественный) фактор: язык как средство общения и неразрывно в ним связанная культура, то есть образ жизни, образ мысли, ви́дения мира и поведения. И у каждого народа — это *национальное*, *своё*, *родное*.

6. Еще один важный и неожиданный результат глобальных процессов — это осознание необходимости изучать иностранные языки и учиться межкультурной коммуникации, учиться если не уважать, то хотя бы быть терпимыми к другим культурам, научиться диалогу культур.

В замечательной статье, написанной Даниэлем Бернаром и Гансом-Фридрихом фон Плётцем (Daniel Bernard, Hans-Frienrich von Ploetz) послами Франции и Германии в Великобритании, говорится: «Learning one or more foreign languages is the true way of becoming „global“» (изучение одного или более иностранных языков – это и есть настоящий способ стать «глобальными»)[1].

Вот оно, прекрасное будущее английского языка: стать стимулом для изучения новых иностранных языков. Хотелось бы остановиться на этой мажорной ноте, но не на конференции о проблемах безопасности.

7. Нет сомнения, что для безопасности человечества принцип «поли» эффективнее, чем принцип «моно»: многополярный мир прочнее однополярного, многопартийная система правления, многоязычный Интернет, наконец, многоязычный мир — трудно, но нужно.

[1] The Spectator. February 17, 2001.

8. Разумеется, угроз безопасности много — геополитических, экономических и других. Но не нужно забывать об очень человеческом факторе — языке и культуре. Язык обманчиво доступен всем. Он как дыхание. О нем забывают, пока не начнут задыхаться. Memento lingua!

Религиозно-политический экстремизм как идеология маргинальных слоев общества (на примере Республики Дагестан)

А.-Н. З. Дибиров

Если определять в общем виде экстремизм, то это крайнее отклонение от нормы, как в идеологии, так и на практике. *Норма* в нашем контексте — это *толерантность* в мировоззренческих вопросах и *компромиссность* в практической политике, и как следствие, формирование политического устройства общества, чьи законы не противоречат основным принципам и ценностям каждой религии, каждого этноса, каждой социальной группы. Стремление изменить такое политическое устройство в чью-нибудь пользу, опираясь на действующие в обществе законы, можно назвать *радикализмом*. То же самое с использованием внеправовых форм и методов уже является *экстремизмом*. Стремление сохранить имеющиеся в политическом устройстве выгоды в чью то пользу, опираясь на действующие в обществе нормы и законы, мы называем *консерватизмом*. То же самое с использованием внеправовых форм и методов является *реакцией*. Когда экстремизм и реакция соединяются, мы получаем *терроризм*. Как один из наиболее распространенных видов современного экстремизма, *религиозно-политический экстремизм* также имеет своим основным содержанием внеправовую политическую практику, отвергающая компромиссные пути решения общественных проблем, но при этом *основана эта практика на идеях исключительности той или иной религии*. *Идеология* религиозно-политического экстремизма — это обоснование политического устройства общества, легитимированного исключительно ценностями одной религии. Формой легитимации такого политического устройства выступает политический режим, в котором террор в отношении инакомыслия возводится в ранг справедливости. При этом нет большего заблуждения, чем считать, что корни экстремизма находятся в самой религии. Многочисленные исследователи уже давно подметили, что истинно верующие люди, будь то мусульмане или христиане, более терпимы к инаковости, к светским законам и к иному вероисповеданию, нежели сомневающиеся или неверующие, что

религиозное население политически более лояльно, чем нерелигиозное. В этой связи можно вспомнить известное высказывание Карла Ясперса: «Вера может быть бесконечно многообразной по своему содержанию, однако общим для верующих является глубокая серьезность в понимании необходимой справедливости и законности условий и процессов в человеческом обществе. Лишь верующие люди способны на величие в смирении, лишь они надежны в нравственном аспекте своей политической деятельности»[1].

В основе идеологии современного религиозно-политического экстремизма лежит радикальный фундаментализм. Фундаментализм — это движение против современности, проявление неадекватной реакции на культурные изменения в современных обществах. Фундаментализм бывает не только религиозный. Например, западный либерализм в его американской неоконсервативной трактовке все больше приобретает сегодня черты фундаментализма. Выражается он, прежде всего, в абсолютизации ценностей американского общества, навязыванию их, порой насильственному, всему остальному человечеству, не учитывая при этом культурно-цивилизационные особенности современного мира. Целый ряд исследователей приходят сегодня к выводу о том, что религиозный фундаментализм пришел на смену коммунизму как призрак, преследующий западное сознание. Идеология фундаментализма неизбежно рождает экстремистскую практику борьбы с современностью. И очевидно, что реакционность фундаментализма в соединении с экстремизмом неизбежно вырождается в терроризм. Другими словами, главным оружием борьбы радикального фундаментализма с современностью становится религиозно-политический экстремизм в его крайнем проявлении — терроризме.

И в этом смысле религиозно-политический экстремизм на дагестанской почве мало чем отличается от его других форм и проявлений.

Корни религиозно-политического экстремизма лежат не за пределами нашей республики, а внутри нее. Религиозно-политический экстремизм проистекает, прежде всего, из *ограниченности экономического*, *социального*, *политического и духовного пространства республики для реализации человеческого потенциала*. Ограниченность *экономического пространства* выражается в том, что до сих пор в республике не сформирована конкурентоспособная экономика, для которой были бы востребованы современно мыслящие менеджеры и высококвалифицированные специалисты. Традиционное отходничество, характерное для республики, превратилось в бегство бизнесменов и капиталов в другие

[1] *Kolin Ясперс К.* Истоки истории и ее цель // Антология мировой политической мысли: В 5 т. Т. 2. М.: 1997. С. 277—278.

регионы, иногда вывозятся целые производства, созданные трудом не одного поколения дагестанцев. Причем убегают наиболее способные и талантливые, их же место зачастую замещают временщики, для которых республика лишь средство быстрой наживы. Ограниченность *социального пространства* выражается в том, что произошедшие необратимые изменения в социальной структуре дагестанского общества, в силу того, что они абсолютно не учитываются в реальной политике государства, стали фактором социальной нестабильности и массовой маргинализации населения республики. Формально Дагестан сельская республика, фактически же сегодня в городах республики живет подавляющее большинство населения республики. За последние 15—17 лет население городов удвоилось, а кое-где и утроилось. Одновременно происходит опустынивание горных районов. Выходцев из одного горного селения в Махачкале в 80-е годы проживало около 15 семей, сегодня же проживает около 250 семей. И это касается многих горных аулов. Одновременно в городах стремительно растет численность молодежи, особенно той, которая не имеет перспектив достойного трудоустройства и жизни. Массовая миграция уже сегодня ставит вопросы о перспективах в решении проблемы так называемых исконных этнических земель на равнине и возникающих на этой почве территориальных конфликтов, питающие во многом экстремистские настроения в обществе. В республике реально существует и экономическое, политическое и психосоциальное давление крупных этносов на более мелкие, которое также безусловно питает экстремизм. Ограниченность *политического пространства* выражается в закрытости политической элиты республики. Она слабо обновляется, она коррумпирована донельзя, внутри процветает кумовство, клановость, а многие ее представители тесно связаны с мафиозными структурами. Межэтническая на поверхности, национально-эгоистическая по сущности борьба за бюрократические должности в условиях полупатриархальной политической культуры приводит к патернализму, клиентелизму и продажности в государственных структурах по худшим образцам восточного байства и лакейского холуйства. В силу этого административно-управленческая и правоохранительная системы в Дагестане стали во многом даже объектами ненависти населения республики. Управленческие отношения в республике носят во многом «вотчинный» характер, что делает их неспособными решать свои имманентные задачи. С этим же связанно постоянное клановое противодействие свободному функционированию общественных институтов политики, права, средств массовой информации. У нас по большому счету отсутствует система обратной связи между государством и гражданским обществом. Общество, лишенное возможности воздействий на госаппарат, становится опытным

полигоном безответственно «хозяйствующих» чиновников. При этом идет постоянное доминирование бюрократического произвола, игнорирование юридических норм и законов должностными лицами государства. Они по существу не несут ответственности за результаты своих управленческих решений. Закрытость политической элиты, особенно характерная для традиционных обществ Востока, у нас выражена не так ярко, как, скажем, в ряде мусульманских государств, в силу достаточно длительного влияния русско-европейской культуры. Тем ни менее она рождает на стыках элит феномен «лишних людей», сублимирующих протестные настроения населения в экстремистскую идеологию. Закрытость политических элит приводит к тому, что огромные массы людей достаточно успешных и образованных оказываются вне этой элиты, чувствуют себя лишними в собственной стране. А из истории нашей страны мы уже знаем, что именно феномен лишних людей родил народничество и российский революционаризм в их самых крайних формах. Сегодня в республике сформировалась большая прослойка людей, особенно молодежи, обладающая как определенным уровнем образования и достатка, так и мобильностью, чьи социальные запросы все время нарастают. Но закостеневшая политическая и социальная структура, консервирующая традиционные модели обновления политических и экономических элит, закрывают этим людям процесс нормального естественного вхождения в эти элиты. Закрытость элит, отсутствие возможности вхождения в эти элиты для людей, имеющих для этого достаточный потенциал, стремительный рост массы таких людей, вызывает естественный протест и желание найти виноватых.

Ограниченность *духовного пространства* проявляется в том, что оно сегодня в республике расколото. С одной стороны крайняя исламизация образа жизни и духовности части населения, а с другой — крайняя вестернизация другой части населения. Обе эти крайности находятся в глубоком противоречии с традиционным образом жизни и ценностями дагестанского народа. Можно даже сказать, что национальная идентичность Дагестана находится в расколотом состоянии. Раскол этот проходит сегодня по линии противопоставления *исламской и русско-европейской культуры*. Первый вопрос, который возникает здесь, это вопрос о том, *является ли нашей идентичностью ислам*, *являемся ли мы частью исламской цивилизации*. Притом, что большинство населения республики относит себя к мусульманам, положительный ответ на этот вопрос не очевиден. На мой взгляд, необходимо отличать религию как духовное достояние человека от религии как образа жизни. В большинстве арабских стран ислам это не просто религия, а это образ жизни. Именно как образ жизни был изначально воспринят ислам аравийскими племенами в VII веке. Произошло это, потому что принятие ислама знаменовало для

них переход от варварства к цивилизации. Из исторических источников мы знаем о дикости и варварских обычаях, которые господствовали на Аравийском полуострове до принятия ислама. Ислам коренным образом изменил жизнь этих племен. Ислам дал не только веру в Аллаха и пророчество Мухаммеда, ислам дал им государственность, законы, нормы морали и нравственности. Другими словами ислам как бы перечеркнул всю их прошлую историю, нравы, обычаи и быт. В результате ислам утвердился здесь не просто как религия, а как образ жизни, полностью подчиняющийся религиозным нормам и требованиям. Сегодня к мусульманам причисляют себя сотни миллионов людей, не являющиеся арабами. Стал ли для них как для арабов ислам не только религией, но и образом жизни? Можно с уверенностью сказать, что в большинстве случаев нет. Там где до прихода ислама общество уже находилось не на уровне варварства, а на каком-то этапе определенной цивилизации, ислам либо видоизменялся, либо оставался лишь духовным достоянием общества. Это произошло в Индонезии, на Индостанском полуострове, в тюркских и других странах. В Иране и Азербайджане ислам принял форму шиизма. Народы Дагестана приняли ислам тогда, когда они уже находились в своем развитии на этапе цивилизации. Наши народы имели уже свою государственность, действовали политические нормы и законы, многие из них даже имели монотеистическую религию — христианство, иудаизм или буддизм. Безусловно, столкновение разных цивилизаций не происходит безболезненно. Религиозное знамя освободительной борьбы народов Дагестана под предводительством великого Шамиля во многом являло собой отражение этой борьбы. Мы понесли громадные жертвы в ходе этой борьбы. Тем ни менее, дагестанская государственность сохранила светский характер, ислам не стал нашим образом жизни, а лишь стержнем нашей нравственности. Сохранение светского характера Дагестана возможно на пути возрождения религиозной культуры, которая была исторически присуща дагестанскому обществу, а также широкое вовлечение дагестанской молодежи к активной экономической жизни. Поиск веры — это, прежде всего, поиск смысла жизни, и чтобы этот поиск не принимал крайние формы, необходимо наполнить саму жизнь многими смыслами.

Кризис нашей идентичности вызван также тем, что ислам как образ жизни противопоставляется многими адептами мусульманской культуры такой важной составляющей нашей идентичности, как *русско-европейская культура*. Ставится вопрос даже о том, *является ли вообще русско-европейская культура частью нашей идентичности*? Безусловно, мы испытываем и испытывали огромное влияние русско-европейской культуры, для многих дагестанцев ценности этой культуры гораздо бли-

же ценностей арабо-мусульманской культуры. И вряд ли может быть по-другому. Русская культура, русская литература, музыка, кино, театр и определяемый во многом ими образ жизни стали неотъемлемой частью нашей действительности и нашей духовности. Русский язык является не только официальным языком республики, но он действительно воспринят всеми народами республики как язык межнационального общения, как язык, на котором народы Дагестана общаются друг с другом в быту, на работе, в общественно-политической деятельности и т. д. Я, аварец, знаком с творчеством даргинца О. Батырая, кумыка И. Казака, лезгина С. Стальского через русский язык. Стихи аварца Расула Гамзатова стали достоянием других народов республики тоже благодаря русскому языку. Первая дагестанская опера звучала на русском языке, русский язык прославил на весь мир Расула Гамзатова, на русском языке написана Конституция республики, русская культура входит как важнейшая часть в общую культуру народов Дагестана. На мой взгляд, идентичность народов Дагестана сегодня естественным образом вплетена в общероссийскую через сочетание глубоко укоренившейся русско-европейской культуры и соответствующего образа жизни с духовно-нравственными основами ислама. Двойственная природа национальной идентичности народов России особенно ярко выражена именно в Дагестане. В развернувшейся сегодня в научном сообществе дискуссии о соотношении русскости и российскости иногда забывается, что российскости без русскости нет. Русскость это некий стандарт, связывающий воедино народы России. Русскость включает в себя не только тех, кто относит себя к этническим русским, но это и русский язык, которым владеет практически все население страны, это русская культура и культура народов России, во многом сформировавшаяся именно на основе русского языка. Русскость, с одной стороны, это максимальный простор для развития языков и культуры народов России, а с другой, это признание того, что проживая в культурном пространстве русского народа, представители других народов России обязаны знать русский язык, принимать нормы поведения, принятые в русской среде. Русскость — это отражение двойственной природы национальной идентичности нерусского населения России. С одной стороны, они являются русскими как носители русского языка и культуры, а с другой — представителями отдельного народа как носители языка и культуры этого народа. Русскость — это отражение реального существенного доминирования культурного, а не религиозного, гражданского или языкового принципа идентификации населения России.

Так, в общем, охарактеризовал бы я общие условия, в которых рождается религиозно-политический экстремизм в республике. В то же время,

на мой взгляд, дагестанский политический экстремизм и терроризм имеют ряд особенностей.

Первое. Основную массу террористических групп составляет дагестанская молодежь. Высокая рождаемость в условиях экономического кризиса привела к тому, что процент молодежи в составе населения республики стал критическим. Известно, что революционаризм и экстремизм рождаются всегда в молодежной среде. Между процентом молодежи в составе населения и политическим влиянием радикальных политических групп и партий в обществе существует прямо пропорциональная связь. Прежде всего, дагестанская молодежь стала жертвой экономического кризиса, по ней сильнее всего ударила безработица. И все это на фоне кричащего богатства новодагестанцев. При этом главное богатство накапливалось не в руках предпринимателей и бизнесменов, а в руках государственных чиновников. Это не может не возмущать чувство справедливости, которое особенно обостренно в молодежной среде. На этом фоне, подпитываемом, кроме того, материальным неблагополучием, социальной безысходностью и отсутствием обозримых перспектив, естественная активность молодежи принимает крайние агрессивные формы.

Второе. Объектами террора в республике выступают чаще всего не гражданское население и гражданские объекты, а государственные структуры и представители органов охраны правопорядка. В какой-то степени изменение характера объекта террора связано с попыткой легитимизировать в глазах общественности сам терроризм. Мягко говоря, правоохранительные структуры в республике не пользуются уважением. Скорее они являются объектом ненависти подавляющего большинства населения республики. Нераскрытые многочисленные убийства политических и общественных деятелей, заказные уголовные дела, необоснованные аресты ни в чем неповинных людей в целях вымогательства и шантажа, непрофессионализм в обеспечении безопасности людей, многочисленные скандалы внутри самой правоохранительной системы — все это не может прибавлять авторитета всей этой системе. И в глазах многих людей террористические акты против органов МВД и его работников воспринимаются как акты возмездия за то беззаконие, которое возведено в ранг государственной правоохранительной практики в республике. По сути, правоохранительная система в республике под личиной защиты государственных интересов опустилась до уровня уголовно-мафиозного террора против собственного населения, где во главу угла поставлены корыстные интересы милицейской верхушки.

Третье. Политические цели терроризма в республике имеют под собой религиозную идейную основу. Об этом написано очень много, а сказано еще больше. То, что ислам не только восстановил, но и очень

сильно укрепил свои традиционно сильные позиции в республике, не подлежит сомнению. В то же время следует учитывать, что семьдесят лет атеистического прошлого не прошли без следа в сознании людей и политической культуре общества. Утеряна, прежде всего, высокая религиозная культура, которая формируется поколениями истинно верующих. Для любого новообращенного религия предстает в силу этого, прежде всего не со стороны своей глубокой духовно-нравственной сущности, а со стороны обрядности, внешних форм и ритуалов. Содержание подменяется формой, сущность явлением, а кажимое принимается за действительное. Недоучившаяся или малоучившаяся молодежь (а такой именно она приходит в наши вузы и уходит из них) вот эти верхушки принимает за корни, рождая нетерпимость к другим взглядам и мнениям, фанатично следуя не принципам, а энтузиазизму. Религиозный фанатизм — это особая форма безверия, безверия в общество, в себя и свое окружение. Но это и другая сторона безверия в Бога. Фанатично верующий безмерно боится собственного сомнения, боится рассуждать в вере, потому что подсознательно боится за истинность своей веры.

Четвертое. Важной особенностью дагестанского терроризма является то, что в нем слабо присутствует антироссийская риторика. Если не считать дежурных лозунгов, подхваченных у чеченских террористов, российская тема не является здесь доминирующей. Причина этого заключается в том, что терроризм дагестанский имеет, прежде всего, чисто дагестанские корни. Экономическое, социальное, политическое и духовное состояние современного и прошлого дагестанского общества — вот причина, вот мишень терроризма в республике. Другими словами, это такой фон в глазах террористов, который делает пока несущественными факторы, связанные с российским присутствием.

Пятое. Если по своему составу террористические группы в республике в основном молодежные, то их социальную базу образуют в основном маргинальные слои. Маргинал, как известно, это человек, который потерял один социальный статус, но еще не приобрел другой. Дагестан — это по сути общество маргиналов. Такое положение является следствием стремительного роста городов за счет оттока значительной массы людей из горных районов. Любой человек, переселившийся из села или аула в город, автоматически горожанином не становится. Потому что обычаи и нормы сельского жителя существенно отличаются от норм городской жизни. Адаптация к этим нормам процесс длительный и во многом болезненный. Человек длительное время находится в этом двойственном положении — то ли селянин, то ли горожанин. Вот этот двойственный, межеумочный социальный статус порождает шараханье от одной крайности к другой. Поиск стабильности проходит через пробы

и ошибки. Такой человек с большей вероятностью принимает ложные ценности за истинные, второстепенное за главное, видимое за суть. Ваххабизм — главное идейное оружие террористов — по сути представляет собой маргинальную идеологию с религиозной риторикой. Маргинальные слои, оторванные от действительной национальной почвы, с ослабленной генетической памятью, живущие больше мифами о предках и истории собственного народа, они склонны воспринимать в гипертрофированном виде даже маленькие проблемы, возникающие на национальной и религиозной основе, или же интерпретировать многие общественные проблемы сквозь призму национализма и экстремизма.

Шестое. Основная масса населения республики довольно равнодушно относится к ходу борьбы с терроризмом. Люди не воспринимают эту борьбу как свою. Причина этого кроется в характере политического режима в республике, сформировавшегося за последние пятнадцать лет. Нелегитимная власть является наиболее существенным фактором дестабилизации ситуации в условиях нашей республики. Национальные, религиозные и культурные различия никогда и нигде не были сами по себе причиной национализма и религиозно-политического экстремизма, если, конечно исключить случаи этнократии и ксенофобии. Это относится и к ускоренной суверенизации союзных республик СССР в 1991 году, и к чеченским событиям, и к всплескам национализма в ряде автономий России в 90-е годы. Причина здесь была чисто политическая — резкое падение авторитета центральной власти, ее низкая легитимность. Национально-освободительное движение под руководством Имама Шамиля также возникло не на волне национальной ненависти к русским, а в силу делегитимизации власти традиционных правителей дагестанских народов. Легитимность политической власти — это действительно тот кудесник, который постоянно воспроизводит стабильность и эффективное развитие общественного организма. Введение поста президента и избрание нового главы республики пока существенных изменений в легитимизацию власти в республике не внесли. Политический режим республики — это режим, где правит чиновничья олигархия, опирающаяся не только на свой многолетний опыт и нажитое богатство, но и легитимирующая свою власть неким подобием плебисцитарной демократии. Пока государственные должности не перестанут быть синекурами для министров, глав администраций, руководителей различных федеральных и республиканских служб, до тех пор власть в глазах основной массы населения республики не будет иметь легитимного статуса. И до тех пор народ будет равнодушно взирать на борьбу государства с терроризмом.

Седьмое. Дагестанский терроризм включен не только в региональную террористическую сеть, но и имеет устойчивые связи с международным

терроризмом. Безусловно, современный мир является свидетелем рождения своего рода террористического интернационала. Рождающийся в западных обществах современный этнопролетариат вряд ли оставит и эти общества за пределами особых форм терроризма. Недавние молодежные бунты на парижских улицах вряд дают кому-либо усомниться в этом.

Восьмое. Возможно, дагестанский терроризм имеет серьезные источники самофинансирования, а не только финансовые подпитки из-за рубежа. Если вспомнить Карамахи и Чабанмахи, то там действовало достаточно много предприимчивых людей, имевших собственный и неплохой бизнес.

Безусловно, необходимо насилию террористов противопоставлять насилие. Но на сегодня в силу непрофессионализма исполнителей насилие в отношении террористов малоэффективно, высокозатратно, сопряжено с большими человеческими жертвами. Нетрадиционные методы борьбы, используемые террористами, вряд ли позволят в должной мере (менее затратно) реагировать на них и впредь.

Демографическая ситуациия в республике на сегодня также не дает оснований для прогноза в отношении уменьшения процента молодежи в составе населения. Дело даже не в численности, это не беда. Беда в том, что на сегодня республика не может предложить эффективное приложение сил молодого поколения. Высокий процент безработицы сохранится даже при очень высоких темпах экономического роста в ближайшие годы. Возможно, реализация национального проекта «Дороги» для республики как-то позволит решить эту проблему, если, конечно, такой проект будет принят.

Без крупномасштабных инвестиций в горные районы мы также не сможем переломить ситуацию с маргинализацией населения республики.

Для эффективной борьбы с терроризмом необходимо осознание того, что *терроризм для современных обществ — это естественное явление*, *такое же*, *как уголовная преступность*. Терроризм, так же как и преступность вырастает из самого общества и развивается вместе сообществом. Возможно, что его полное искоренение и невозможно, он может быть лишь локализован.

Исходя из этого, и необходимо строить стратегию борьбы терроризмом. Прежде всего, наверное, необходимо понять, что терроризм сам по себе из бедности и нищеты не вырастает. В мире немало бедных и нищих, немало эксплуатируемых, немало оскорбленных и униженных. Но не все из них становятся террористами. Террористы выходят из тех, кому объяснили, что он и беден, и нищ, и эксплуатируется, что постоянно оскорбляется его национальное или религиозное самолюбие. Для понимания этого террорист должен иметь определенный уровень образования,

доступа к достижениям современной цивилизации. Важнейшей причиной терроризма является не просто наличие экономических и социальных условий, а, прежде всего, объяснение и доказательство этих условий, показ виновников.

Поэтому в методах борьбы с терроризмом на первое место я бы поставил поиск адекватных средств идеологического и психологического воздействия на социальную базу терроризма. В этом направлении на полную мощь должны работать и средства массовой информации, и мечети и церкви, и школы и вузы. Со стороны государства и общества должны выдвигаться веские аргументы *объяснения и доказательства* бесчеловечной природы терроризма и его идеологии. Почему бы, например, не доводить до сознания каждого верующего последствия ваххабитского восстания в Аравии в XVIII веке. В ходе восстания ваххабиты разгромили ряд аравийских городов, изуродовали священный камень Каабы, а в Медине осквернили могилу пророка Мухаммеда. Это ли не объяснение вероотступнической природы ваххабизма?

Другими словами в обществе должна быть выработана *антитеррористическая идеология*, которая всеми доступными средствами должна доводиться до всех групп риска.

На сегодня это наиболее эффективное средство долговременного противостояния терроризму в республике. Но антитеррористическая идеология никогда не найдет добросовестных служителей в лице граждан республики, если не будет изменен характер легитимации политической власти в республике.

Современные террористические движения используют сегодня тактику «ожидания» с целью выиграть время для подрыва легитимности государств. Терроризм стремится сохранить свой потенциал, выжидая очередного кризиса легитимности в каком-либо из регионов, представляющих для нее интерес. Это же в полной мере относится и к дагестанскому терроризму.

Для нормальной эволюции политического режима в республике в сторону большей легитимности, на мой взгляд, необходимы *три* условия.

Первое. Средства массовой информации в республике должны быть свободными, не должно быть авторитарного давления на издателей, журналистов, не должно быть ангажированных изданий, или эти издания должны в полный голос сообщать о своей ангажированности. СМИ должны стать трибуной свободных дискуссий и критики, без каких бы то ни было заповедных зон. Средства массовой информации — это наиболее мощное и эффективное средство борьбы против главного бича нашей государственности — коррупции. У нас же пока с коррупцией борются сами коррупционеры. А такая борьба рождает лишь новую коррупцию, но

в неизмеримо больших масштабах. Свободные СМИ, поднимая больные проблемы общества, дают надежду людям, что эти проблемы будут решаться, что о них знают. Почему рождается внесистемная оппозиция? Потому, что внутри системы у инакомыслящего нет возможности выражения своего мнения, правила системы не позволяют ему этого. Так было в республике до сих пор. Поэтому необходимо изменить эти правила. И начать следует со средств массовой информации.

Второе. В современных обществах ключевую роль в обеспечении справедливости играют суды. В легитимации государственной власти в республике роль судей и всей судейской системы играет ключевую роль. Сегодня у человека нет иной возможности и нет иной инстанции, к которой он может апеллировать в поисках справедливости и законности. Справедливым может быть только независимый суд, вот такая независимость должна обеспечиваться и охраняться.

Третье. Сегодня мы имеем уникальный шанс создать из ключевого института нашей государственности — института президентства — орган, обладающий высшей легитимной силой. Сегодня наша республика один из немногих регионов России, где у власти находится некоррумпированный глава. Это дает возможность строить этот институт как образ высшей власти, как власть в «белых одеждах», чьи аппеляции к обществу должны встречать понимание и согласие, потому что воспринимаются обществом не только как законные, но и как справедливые. Легитимная власть президента должна опираться на развитые структуры гражданского общества, прежде всего на современную партийно-политическую систему, которая аккумулировала бы не только провластные ориентации населения, но и реальные оппозиционные настроения. Сильная внутрисистемная оппозиция вполне в состоянии в условиях республики преодолеть внесистемное, внеправовое, экстремистское оппозиционирование, которое существует сегодня.

Таким образом, дагестанское общество через создание антитеррористической идеологии и формирование легитимного политического режима, сможет, на мой взгляд, если и не искоренить полностью терроризм, то, по крайней мере, локализовать его возможности и сузить социальную базу.

Trusted Computing: A Security Standard Based on Platform Integrity and Trust

H. Brandl

Introduction

One of the as yet unresolved problems of widely used security applications is to protect the hardware platform against attacks on its integrity or modification of the security software. Within the PC area typical incidents and attacks are well known and are endangering PCs for home banking, but also on servers within companies and other organizations which are used for sensible data, like personal, billing, e-commerce and others. Current approaches for solving this problem purely at the software level are by their very principle unpromising. As has since been amply confirmed from experience and security trends in the smart card world, a trusted and tamperproof security basis cannot be implemented using software-based solutions alone.

1. The Trusted Computing Group

Major companies in the PC sector have therefore joined forces and begun working to solve this problem with the aid of a new hardware approach and the creation of an associated industry standard. In 1999 Compaq, Hewlett-Packard, IBM, Intel und Microsoft established the Trusted Computing Platform Group (TCG) [4]. The aim was to create Trusted Clients (e.g., PCs, but also PDAs or mobile telephones) in order to make important applications such as networks, communications and e-commerce much more trustworthy. This standard was also to be kept as open as possible in order to inform the technical and interested public in good time and to create confidence. The emerging Trusted Computing (TC) Standard employs a secure hardware structure whose main component, the Trusted Platform Module (TPM), is specified as an LSI security chip. This Standard is largely based on recent years' experience with high-security smart cards and their applications, important parts of whose architecture and security characteristics have been consistently adopted. Similarly to the way in which

we use the smart card's cryptographic mechanisms to protect sensitive and confidential personal data as well as critical processes in a security environment, these functions can also be used in the TPM to ensure not only the integrity of a platform but also to protect its user data.

To restate clearly: The TCG Standard provides authentication and accreditation *of the platform*, *not of the user*.

1.1. Standardisation: Activities of the TCG

The TCG has since agreed eight important specifications packages and continues its work within dedicated working groups:

- Trusted Platform Module (TPM), as the basic standard document.
- TCG TPM Software Stack Specifications(TSS), as API to the hosting system.
- PC Client, for PC Specific Implementation Specifications.
- Server, for enhancing security on server engines.
- Infrastructure, for secure architectural framework.
- Mobile, for trusted mobile phone and communication devices.
- Storage, for trusted and secure storage devices like disk drives.
- Trusted Network Connect, as an extension of the existing secure transport protocols for additional trust and identity information.

1.2. Security aspects in the TCG Specification

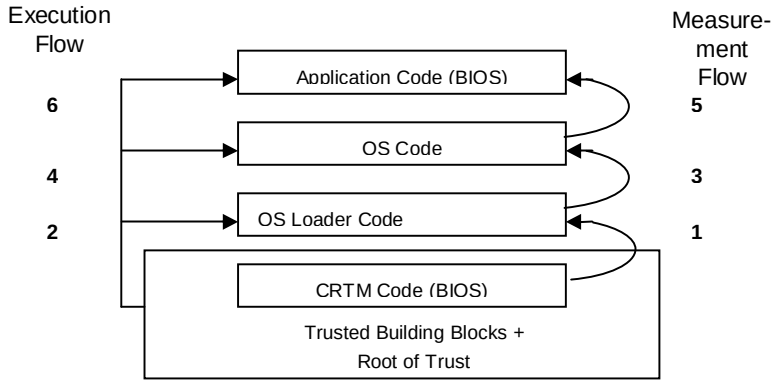


Рис. 1. Structure of the „chain of trust"

The generic TCG approach is producing a new security paradigma for trusted system structures: Whereas until now security was to be achieved by means of additional levels of encryption or antivirus software, TCG begins

at the very lowest level of the platform, and here right from the start of the booting operation of such a system with a certified hardware security chip, the TPM, being trusted a priori. At system startup an uninterrupted „chain of trust“ extends from this lowest layer up to the applications. As soon as the lower level in each case has a stable security reference, the next layer can be supported on it. Each of these domains is built upon the preceding one and can therefore expect every transaction, internal link and device connection to be trusted, reliable, secure and protected. Right at the start a check is performed to ascertain whether the signature (and therefore the constellation) of the platform components has changed, i.e., whether one of the components (disk storage, LAN connection, etc.) has been modified or even removed or replaced. Similar checking mechanisms supported by the TPM then successively verify, e.g., the correctness of the BIOS, of the boot block and of the booting process itself, as well as the next higher layers at startup of the operating system. This means that a compromised platform can also be securely identified by others and data exchange can be restricted to the appropriate extent. Trusted computing systems can create the conditions whereby for the first time modern, networked platform structures can also be significantly refined from the point of view of security and mutual trust.

2. Trusted Platform and the Trusted Platform Module (TPM)

2.1. TPM: hardware, software, functionality

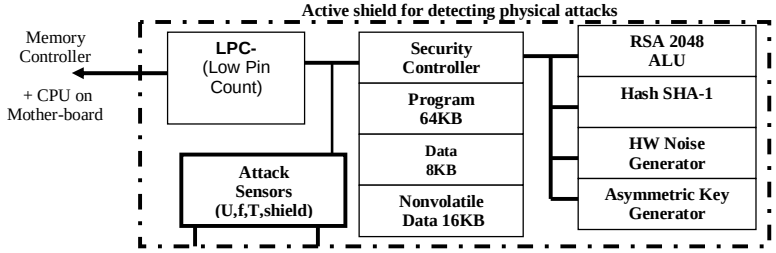


Рис. 2. Block diagram of Trusted Platform Module (TPM)

In accordance with the TCG architecture, the TPM provides the security functions requiring particular protection and which are therefore also implemented in a secure hardware environment. The TPM is designed as a passive part. It has no means of actively influencing program execution

of the central processor or the boot operation. It only receives control and status measuring data from the central processor which it processes, stores and reads out again from its secure structure, and feeds these results back to the central processor. Only access to particular data (such as key material) is made dependent by the TPM itself on the presentation of appropriate authentication patterns. The main security functions handled by the TPM are:

- *Protection of key material*. The various key classes are stored in a protected manner in the TPM. The access method is selected according to key type (TPM-bound, migratable, signature, identity, binding keys).
- *System authentication*. Authentication and validation of the platform to third parties.
- *Communication of the system's security status* (*attestation*). Trusted communication of the security–relevant (platform–user–defined) configuration.
- *File sealing*. Binding of data to the system configuration and signing of the data when storing with the hash value of the configuration. Access to the data is then only possible if the configuration remains unchanged.
- *Secure saving of configuration changes* in the Platform Configuration Registers (PCR). Status changes are detected, safeguarded by the SHA-1 hash algorithm.
- Protection against attacks on the integrity of the TPM, particularly against physical attacks.
- Inexpensive implementation in order to allow widespread use.
- Compliance with global export control regulations in order not to restrict international trade with TC platforms (PCs).

Skilful system design allows implementation with a minimal amount of cryptographic and security hardware in the TPM:

- Specialized crypto arithmetic unit for rapid computation of RSA cryptography up to 2048 bits.
- Fast hardware hash unit with the SHA-1 algorithm for measuring the data structures
- Internal processor with the appropriate hardware for computing the critical functions (e.g., RSA with the secret key part) on a trusted basis in a secure environment.
- Nonvolatile memory (EEPROM) to retain the data even if the operating voltage is off
- Sensors and internal security structures (e.g., active screen over the top wiring layer of the chip) in order to detect physical attacks and counteract them.

Extensive internal firmware implements the interface protocol checks and administers the various security sensors and reacts appropriately to detected physical tampering or alterations to the chip or its environment.

3. The Trusted Computing Software Stack (TSS) for the Host

Like any other hardware element, the TPM requires a special driver and service provider interface in order to enable it to be addressed from the operating system. This Trusted Platform Support Service (TSS) constitutes a security API which provides the TPM functions for the relevant operating system. TSS handles the following functions:

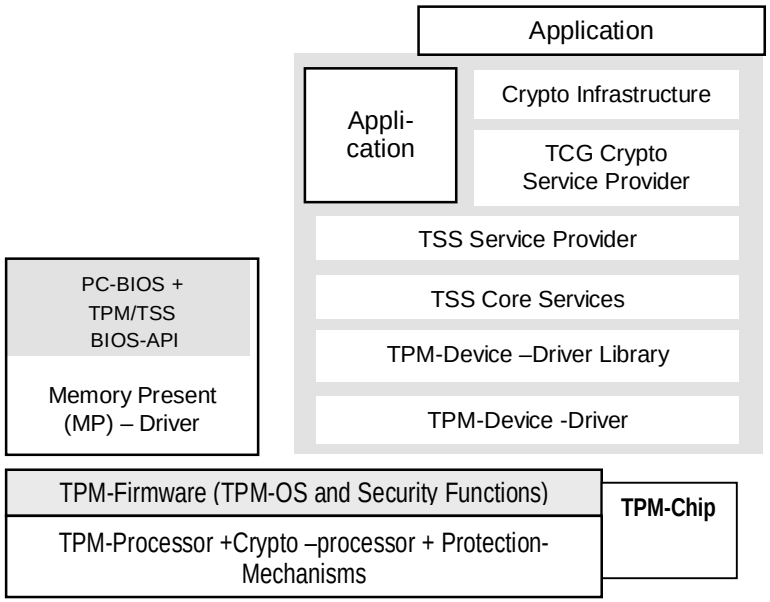


Рис. 3. Trusted Platform Support Services (TSS)

- Coordination and management of multiple accesses to the TPM.
- Converting the abstract API commands to the data stream for the TPM.
- A Cache Manager securely stores the data exceeding the memory area on the external mass storage, thereby providing a storage capacity for keys and security data which is limited only by the size of the disk storage.

3.1. Cryptographic interfaces of the TSS

Since the TSS, as an API, makes its security functions available to the operating system, it seems reasonable to provide this interface also for other security applications via an adaptation module, thereby enabling in particular secure storage and signature services of the TPM to be made available to the normal applications and the security level of these standard applications to be significantly increased. Two usual implementations currently exist:

- Microsoft Cryptographic Service Provider (MS-CSP).
- PKCS#11.

3.2. Secure PC-Type platforms: Trust oriented processor architecture

As has already emerged from the deliberations concerning the implementation of trusted digital signatures, in addition to making the platform secure, for the other critical parts of a computer trusted functionality is also required. Therefore the two major PC chipset manufacturers AMD and Intel are beginning for incorporating the relevant security functions into their chip sets.

4. Secure Key and Data Hierarchy

4.1. Key and certificate chain of the TPM protects integrity of data

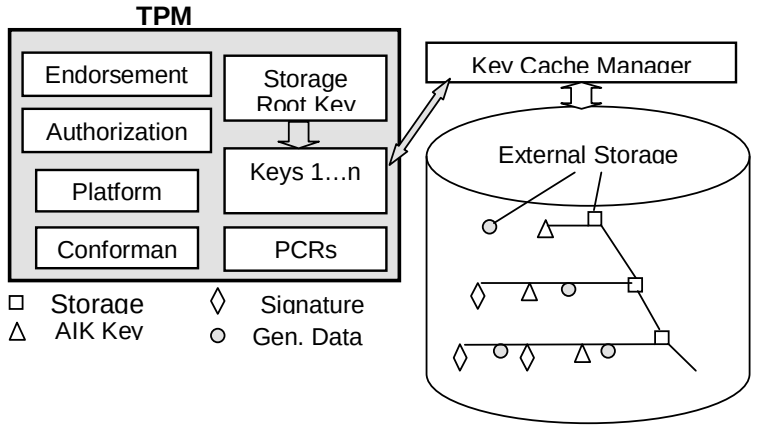


Рис. 4. Certificate chain

Additional confidence in the correctness of the platform is created using further cryptographic certificates which are likewise stored in the TPM:

- The *Endorsement Certificate* is based on the Endorsement Key pair (EK) and is uniquely generated for every TPM at production. It confirms that a TPM originates from a trusted source and can therefore be used for verification of TC based certificate chains.
- The *Storage Certificate* is generated at the „Take ownership procedure“ and during initialisation by the first user. It is the root certificate for all the users data structures.

All the stored keys and critical data material is integrated into a certificate tree hierarchy, where every item is digitally signed. Any unallowed modification or manipulation of data can so easily be detected. The TCG standard does not differentiate much between different data elements like external keys or internal storage certificate. This method allows a very flexible and comfortable implementation of standard security protocols on different objects.

4.2. Operating systems and applications

Contrary to the assumption in some publications, the TCG standard is not bound to any operating system. It essentially governs trusted hardware platforms and consequently contains no requirements towards the operating system.

On the other hand, it is only an operating system on a TCG hardware platform that can make flexible trusted computing possible. Secure operating systems for TC platforms are mainly designed for separated compartments and domains.

5. Fields of Applications

Although the TCG began its activities with PC security in mind, the idea of the secure platform is transferable to other devices and applications:

- PDAs and smart phones.
- Mobile communication applications.
- Communication (WLAN security, network remote access...).
- Digital rights management.

6. Further reading

- The entire Specification, concepts and architectural considerations of the TCG can be openly found on the TCG web site [4]. Currently there is a considerable size of a total of 2700 pages.

- The basic objectives and principles are described in „TCG Design Principles“ [5]. It is recommended that at least this overview document of the TCG be worked through directly.
- Security experts from HP who were involved in the Specification have written the book on TC [3]: TCPA Design Philosophies and Concepts. This book is the best introduction to the TCG philosophy, is well explained and is best related to applications.

Литература

[1] Infineon Technologies AG: TPM Produkt Information: `http://www.infineon.com/TPM`.
[2] EU sponsored TC research project: Open Trusted Computing; targeting mainly for trusted Operating Systems based on Linux: `https://www.OpenTC.net`.
[3] S. Pearson (ed.). Trusted Computing Platforms: TCPA Technology in Context. Prentice Hall PTR2003.
[4] Trusted Computing Group Website: `http://www.trustedcomputinggroup.org`.
[5] TCG Design principles: `https://www.trustedcomputinggroup.org/specs/TPM/mainP1DPrev103.zip`.

Терроризм и СМИ: симбиоз или противостояние? К вопросу о природе современных взаимоотношений

Е. Л. Вартанова

Терроризм, несомненно, относится к числу наиболее сложных проблем, с которыми столкнулся современный мир. Очевидно, что в борьбе против него усилий одних лишь правоохранительных и правительственных органов не достаточно. СМИ являются мощнейшим инструментом формирования общественного мнения и обязаны сыграть в этом процессе важную роль. Однако задача перед ними стоит отнюдь непростая — найти баланс между свободой слова и безопасностью человека и общества, правом общества и его граждан на информацию и гражданской ответственностью СМИ. Составными частями последней в демократическом обществе являются такие часто противоречащие друг другу элементы, как:

- предоставление гражданам объективной и сбалансированной своевременной информации;
- предоставление основным политическим силам и движениям доступа к СМИ;
- обеспечение плюрализма и разнообразия в содержании СМИ;
- использование разнообразных источников информации;
- подотчетность обществу;
- защита общества от паники;
- сохранение эмоционального и морального спокойствия аудитории.

Влияние, оказываемое СМИ на общественное мнение, в современном обществе можно назвать ключевым. Особенностью современного терроризма является использование информационного воздействия как важного элемента манипуляции сознанием и поведением людей, при активном использовании глобальных коммуникаций. Действия террористов рассчитаны не только на нанесение материального ущерба и угрозу жизни людей, но и на информационно-психологический шок, воздействие которого на большие массы людей создает благоприятную обстановку для достижения террористами своих целей. Террористы учитывают возможности информационной эпохи, связанной с существованием глобальных СМИ, а также ориентированность рыночных масс-медиа не негативные сенсации, способные собирать значительные аудитории. В результате появляется излишне детализированное освещение «террористических сенсаций», способных с помощью определенных комментариев к происходящим событиям эффективно влиять на общественное мнение в любой стране мира.

Воздействие террористов на СМИ становится еще более массированным, глубоким и эффективным, если они находятся «в руках» профессионалов, владеющих пером и словом, умело сочетающих в процессе контакта со своей аудиторией рациональную и эмоциональную составляющие преподносимой информации. Сегодня СМИ являются главным инструментом политического влияния в современном обществе. Их способность быть эффективным средством влияния на общественный климат давно подмечена и максимально используется силами, пытающимися достичь своих целей насильственным и нелегитимным путем.

Анализируя материалы российских масс-медиа по проблеме терроризма, можно заметить опасное разногласие их в вопросах, касающихся общей безопасности, отчужденность и даже враждебность многих СМИ по отношению к государству, правоохранительным и силовым органам в условиях опасности международного терроризма. Невозможность консолидации власти, СМИ и общества в чрезвычайных обстоятельствах стала одной из центральных проблем информационной безопасности в России. Именно поэтому сегодня становится необходимым рассматривать информационную безопасность самым широким образом, не только вводя в это понятие безопасность электронных сетей, связи банков данных, но и обязательно 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.

Как уже отмечалось, современный терроризм немыслим без СМИ. Многие зарубежные исследователи отмечают, что терроризм сегодня имеет симбиотическую связь со СМИ. И задача широко понимаемой нами информационной безопасности — не преградить информации о терроре доступ в СМИ, не ввести цензуру или ограничить свободу слова, а разорвать именно эту симбиотическую связь, без которой террористы не смогут вызывать страх у широкой аудитории. Нельзя согласиться с утверждением о том, что само развитие современных СМИ породило современный терроризм в его нынешнем виде. Напротив, террористы на протяжении всей истории существования этого явления стремились использовать существующие каналы масс-медиа для распространения сво-

их взглядов и информации о своей деятельности. Более того, террористы преследовали целью не только добиться распространения информации о своих деяниях, но и пытались получить у СМИ признания легитимности или моральности своих действий для того, чтобы завербовать сторонников и новых участников.

Французский социолог М. Вивиорка, осмысливая связи СМИ и террора, выделил 4 типа отношений между ними. Первый он обозначил как *полное равнодушие*, причем в этом случае именно террористы не считают нужным запугивать население или пропагандировать свои действия. Второй тип отношений, названный *относительным равнодушием*, предполагает, что террористы не стремятся попасть в заголовки новостей или на первые полосы массовых СМИ, но происходит это потому, что они опираются на собственные медиаканалы для объяснения своей точки зрения. К таким каналам могут относиться проплаченные газеты, некоммерческое вещание из подконтрольных террористам политических или религиозных центров, сайты в интернете. Однако все эти СМИ носят характер альтернативных и не адресуются широкой аудитории. Третий тип отношений — *медиаориентированные стратегии* — направлены на то, чтобы создать террористам максимальное присутствие в СМИ. Террористы в данном случае прибегают к инструментальному использованию СМИ, что стало основной современной формой терроризации широкого населения. Четвертая форма отношений была определена как «*тотальный разрыв*», и это значит, что террористы относятся к медиаорганизациям, редакторам и журналистам СМИ как к врагам, которых надо наказывать и уничтожать. В этом случае сами журналисты становятся объектами воздействия террористов.

Вовлечение СМИ как социального института и журналистов как профессионалов и граждан в сферу влияния экстремистов происходит под воздействием определенных обстоятельств. Причем в обоих случаях они несколько различны. Можно выделить несколько основных факторов вовлечения журналистов в сферу влияния террористических группировок. Это:

- отсутствие в обществе ясных представлений о национальных интересах, его дезинтеграция и дезориентация, проявляющиеся в отсутствии внутренних этических принципов, потерях перспектив и социального оптимизма;
- отсутствие общих и разделяемых всеми журналистами правил профессиональной деятельности, в том числе и при освещении терактов и деятельности террористических групп, преобладание узкокорпоративных интересов над общенациональными, что является следствием отсутствия системы принципов профессиональной деятельности, профессиональных стандартов и норм, а также отсутствие понимания и критериев оценки вреда, наносимого национальным интересам;
- корпоративная зависимость и незащищенность журналиста от работодателя (страх остаться без работы, власть редактора, собственника издания, групповое давление);
- внутренние причины: психологическая некомпетентность, непонимание собственных психических процессов (неконтролируемая эмпатия, сочувствие «угнетенным»), неспособность к эмоциональному самоконтролю и саморегуляции («стокгольмский синдром»), недостаточно развитые способности логического мышления, неструктурированная, диффузная система ценностей (тщеславие, стремление играть влиятельную роль, желание получить эксклюзив любой ценой и т. д.);
- физическая и правовая незащищенность журналиста (страх мести со стороны экстремистов, лоббистских группировок);
- принадлежность к группам с экстремистской и маргинальной ориентацией (этническим, социальным, референтным).

Деструктивные последствия деятельности СМИ могут стать результатом их вовлечения в сферу интересов террористических группировок, которые стремятся превратить СМИ в инструмент собственного продвижения. Сами СМИ могут вовлекаться в сферу влияния террористических группировок по многим причинам. В их числе наиболее важную роль играют размытая система представлений о содержании национальных интересов; лоббирование интересов групп или политических партий; неограниченная власть главного редактора или владельца СМИ; непрозрачность источников финансирования изданий и программ; отсутствие контроля над СМИ со стороны гражданского общества.

Остановимся подробней на каналах распространения контента террористической направленности. К ним могут быть в принципе отнесены все СМИ, правда, формы взаимодействия создателей контента и самих каналов существенно различаются.

Во взаимодействии с *традиционными печатными СМИ* можно выделить следующие особенности. Самым простым для террористических группировок является издание пропагандистской книжной продукции. В условиях удешевления и децентрализации издательского бизнеса, появления современной множительной техники такая деятельность легко осуществляется самими террористическими группировками. Однако реальную трудность представляет широкое распространение такой продукции, поскольку оно запрещено в конституциях практически всех стран.

Использование террористическими группировками периодической печати предполагает публикацию журналистских материалов — как новост-

ных, так и аналитических — в газетах и журналах. Вполне логичным в этой связи выглядит создание партийных изданий или собственных органов террористических группировок, а также сотрудничество с печатными СМИ, принадлежащими «сочувствующим». Правда, часто такая деятельность часто имеет гипотетический характер: при запрете самих террористических организаций возможности для такой «партийной» журналистики исчезают, и СМИ, «отлученные» от своих идеологов, прекращают свою деятельность.

Более сложная ситуация возникает при освещении проблемы терроризма общеполитическими — непартийными, независимыми — печатными СМИ, создание которых в большинстве стран мира не контролируется государством и его правоохранительными структурами. В этом случае мы видим непосредственное взаимодействие журналистов и источников, находящихся в руках или в связи с террористами, на основе чего журналисты и создают свои материалы. Именно здесь возникает первый узел проблем, связанных с пособничеством терроризму. В условиях актуальности террористических угроз материалы независимой прессы на тему терроризма могут оказывать весьма неоднозначное воздействие на аудиторию, которая пребывает в уверенности, что пресса во всех случаях нейтрально, непредвзято и объективно освещает проблемы терроризма. В большинстве случае так и происходит, однако встречаются и примеры того, как террористы манипулируют журналистами для дальнейшей манипуляции аудиторией.

Важнейший для современной журналистики принцип объективности обязывает журналистов представлять позиции всех упоминающихся в материале сторон. Проявлением этого же принципа во многих журналистских культурах является нейтральность в изложении материала, нежелательность высказывания собственного отношения к происходящему. С другой стороны, и сам этот принцип таит определенные «подводные камни»: журналист может подробно излагать позицию террориста, мотивируя это необходимостью ответного слова «другой» стороны. Он также может, пренебрегая принципом нейтральности, создавать позитивный образ террористов. Играя на естественной в условиях рынка конкуренции СМИ за сенсацию или на противоречиях внутри медиасообщества, террористические группировки умудряются получить доступ к массовой аудитории через практику «вброса»\утечки сенсаций, подкупа или идеологической «обработки» журналистов, декларирующих принципы объективности и нейтральности.

Здесь мы уже сталкиваемся с проблемами журналистского профессионализма, журналистской этики и ответственности журналистов, что должно решаться на уровне журналистского сообщества, но при обязательном участии гражданского общества.

В более жесткие условия террористы попадают при взаимодействии с *аналоговым радио- и телевещанием*. «Старые» электронные СМИ существуют по-прежнему в условиях редкости частот вещания, следовательно, они попадают в сферу особого внимания государственных органов. Создание террористами собственных радио- и телестанций невозможно, так как в большинстве стран аналоговое вещание лицензируется государственными органами. Для трансляции передач иностранных телеканалов на массовую аудиторию в большинстве стран созданы определенные барьеры, преодолеть которые оказывается довольно сложно. Такая ситуация на зарубежных телерынках характерна для катарского канала «Аль-Джазира», предоставляющего право обращения к телезрителям лидерам исламистских террористических организаций. У канала существуют очень серьезные сложности и с вещанием на территории США, и с созданием англоязычной версии, которую заранее отказываются транслировать практически все крупные вещатели и даже кабельные телесети. Однако попадание интервью или телеобращений террористических деятелей международного масштаба в эфир крупных каналов все-таки возможно по упомянутым выше причинам — коммерциализации СМИ, стандартам профессиональной объективности, просто по человеческим симпатиям.

Теоретически возможность проникновения материалов террористической направленности в *рекламные материалы* СМИ значительно выше, чем в журналистские материалы: как правило, журналисты не принимают участие в создании текста рекламы, оставляя его на усмотрение рекламных отделов или рекламных агентств. Вероятность публикации террористических материалов на полосах рекламы, таким образом, выше, чем на полосах редакционных, однако во многих странах мира кодексы рекламных ассоциаций запрещают публикацию материалов, нарушающих законодательство или нравственные, этические и культурные нормы страны. Несмотря на то, что размещение рекламы в СМИ преследует откровенный коммерческий интерес, осознание рекламными сообществами многих зарубежных стран недопустимости определенного типа содержания стимулирует появление кодексов рекламной деятельности. А если, как говорят японские рекламисты, «покупатель — это божество», то и содержания, оскорбляющего или травматизирующего покупателя, реклама допускать не может. Это уже вопрос экономический.

Мы видим, что как в редакционных, так и рекламных материалах СМИ важнейшую роль при публикации материалов террористической направленности играет наличие или отсутствие определенных «филь-

тров». Они присутствуют как на уровне самих редакций (критерии профессиональной деятельности журналистов, кодексы их поведения, информационные приоритеты СМИ), так и на уровне «сырьевых» поставщиков медиаиндустрии — информационных агентств. На этом уровне мы сталкиваемся с необходимостью анализа принципов отбора информационного «сырья» для журналистов, а также факторов, определяющих формирование «повестки дня» для традиционных СМИ.

Ситуация радикально меняется, если мы обратимся к новой области современного медиапространства — к сектору интерактивных онлайновых СМИ.

Благодаря компьютерным технологиям и телекоммуникационной инфраструктуре доступ террористов к СМИ существенно упростился. Создать материал террористической направленности и сделать его одновременно доступным миллионам людей во всем мире сегодня не сложно. Цифровые СМИ, не попадающие под прежние жесткие формы государственного контроля, в руках террористов становятся новым пластичным и эффективным инструментом воздействия на глобальное общественное мнение.

Кабельное или спутниковое телевидение, не подлежащее государственному регулированию, усиливает вероятность того, что материалы террористического содержания могут транслироваться этими каналами. Исходя из западного опыта, появление «контента террористической направленности» возможно в эфире отдельных каналов в рамках реализации концепции равного доступа.

Интернет-ресурсы представляют практически неограниченные возможности для пропагандистской и информационной деятельности, для распространения текстовых и мультимедийных материалов, для создания и трансляции сигнала онлайновых радиостанций или даже видеоканалов, для электронной коммерции и коммуникации, как через собственные ресурсы организаций, так и через сайты или блоги отдельных членов сетевого сообщества, сочувствующих экстремистам. Онлайновые представительства крупных СМИ также несколько более свободны в обращении к специфической тематике, чем офлайновые редакции, и могут размещать собственные материалы, полученные текстовые и мультимедийные файлы, а также давать ссылки на ресурсы радикальных и террористических организаций или связанных с ними групп и отдельных активистов.

Возможности электронной коммуникации позволяют проводить структурные изменениях в террористических группах, обеспечивая отказ от обязательной иерархической структуры, переход к сетевому децентрализованному построению организации и делегированию многих функций, в

том числе, и пропагандистских, и популяризаторских — на индивидуальный уровень.

Впрочем, отсутствие ограничений в законодательстве многих стран периодически компенсируется инициативами или законодательных органов, или провайдеров доступа к сети, которые могут блокировать тот или иной ресурс. Подобные действия могут предприниматься как в отношении откровенно террористических ресурсов, так и заподозренных в сочувствии группам экстремистов. Например, временные сайты, которые создаются после каждого крупного теракта, в США быстро блокируются властями, в чьих руках сосредоточенно управление доменными адресами Интернета. А Европейская ассоциация провайдеров доступа в качестве важнейшей меры саморегулирования считает лишение доступа в Сети тех производителей контента, которые нарушают закон или общественные порядок и нравственность.

Совершенно очевидно, что для обуздания терроризма усилий одних лишь правительственных и правоохранительных органов не достаточно. СМИ являются мощнейшим инструментом формирования общественного мнения и могут сыграть в этом процессе важную роль. С их помощью можно либо создать атмосферу полного неприятия обществом любых форм насилия и убийства гражданских лиц, либо вызвать понимание и сочувствие к террористам и применяемым ими методам. Анализируя материалы российских СМИ по проблеме терроризма, можно заметить, очевидное разногласие СМИ по вопросам, касающимся общей безопасности, а также отчужденность и даже враждебность многих СМИ по отношению к государству, правоохранительным и силовым органам в ситуации террористической угрозы.

Часто создается впечатление, что СМИ забывают о своей социальной ответственности в обществе, хотя они, несомненно, должны работать для развития правового просвещения людей, выполнять образовательную и воспитательную функцию. В процессе противодействия терроризму конструктивная позиция СМИ не менее важна, чем действия антикриминальных и антитеррористических силовых структур. СМИ должны стать одним из эффективных каналов деятельности институтов гражданского общества, донося до властей независимое экспертное мнение по вопросам борьбы с терроризмом.

Найти тонкую грань, между свободой слова и безопасностью человека и общества, правом на информацию и гражданской ответственностью — это сложная задача, решить которую можно, лишь объединив интеллектуальный потенциал гражданского общества, практиков и теоретиков СМИ и профессионалов силового блока. В поиске баланса между соблюдением свободы слова и необходимостью борьбы с терроризмом мно-

гие международные организации — ООН, ЮНЕСКО, Совет Европы — в своих документах сходятся в том, что ограничения свободы слова и информации в рамках кампаний по противодействию терроризму недопустимы, так как это нарушает одну из фундаментальных свобод человека, которую стараются низвергнуть террористы. Свобода слова рассматривается как основной ресурс для борьбы с экстремизмом и терроризмом, однако при соблюдении важнейшего профессионального принципа — социальной ответственности СМИ перед гражданским обществом. В то же время некоторые документы ограничиваются достаточно расплывчатыми формулировками в отношении пределов допустимых ограничений. Это связано с различными политическими культурами в разных странах, что не позволяет выработать универсальных механизмов гарантирования свободы слова и условий соблюдения социальной ответственности.

Каждая страна должна найти свои решения, опираясь на свои традиции в сфере масс-медиа и свободы слова, в области взаимодействия государства — гражданского общества — СМИ. С другой стороны, очевидно, что необходимые решения всегда лежат в сфере информационной политики, и набор «действующих сил» во всех национальных контекстах остается одним и тем же. В современных условиях информационная политика не может вырабатываться только при участии официальных структур. К ее выработке, наряду с государством, законодательными структурами и органами исполнительной власти, необходимо привлекать профессиональные организации медиасферы — журналистов, издателей, вещателей, распространителей, писателей, кинематографистов, деятелей музыкальной культуры, а также широкую аудиторию, представителей и организации гражданского общества, организации потребителей.

Как показывает опыт развитых демократий, внутренний самоконтроль журналистского сообщества помогает существенно упростить и удешевить необходимый внешний контроль со стороны государства. Но вместе с тем внутренний контроль только дополняет единственную возможную форму внешнего контроля — контроля со стороны гражданского общества, то есть сами читателей, слушателей, зрителей и пользователей. Именно этот контроль призван осуществлять обратную связь общества со СМИ. Сегодня в российских условиях только развивающееся гражданское общество — в сотрудничестве с государством и профессионалами антитеррористических структур — должно инициировать создание механизма и рычагов 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.

Информационная сущность и технологии терроризма

В. Г. Кулаков, А. Б. Андреев, Г. А. Остапенко, В. И. Белоножкин, С. Ю. Соколова

По мнению авторов, терроризм как явление имеет преимущественно информационный характер (по целям, технологиям и основным последствиям). С учетом этого, дадим рабочие определения понятиям данной предметной области, акцентирующие внимание на информационных аспектах терроризма:

- *терроризм* — направление достижения политико-идеологических целей, основанное на применении насилия в целях изменения общественного сознания;
- *террор* — методология применения насилия в целях устрашения населения;
- *террористическая деятельность* — совокупность технологий и действий, реализуемых в процессе подготовки, совершения и использования результатов терактов;
- *террористический акт* — устрашающее информационно-управляющее воздействие на сознание населения и носителей властных полномочий.

На взгляд авторов, главные причины существования терроризма лежат в идеологической и психологической плоскостях. С одной стороны, это существование фанатично настроенных носителей идей, оправдывающих достижение целей любыми средствами (радикализм) и пренебрежение к человеческой жизни (антигуманизм). С другой стороны, присущие людям страхи и стадный инстинкт. К предпосылкам терроризма следует отнести любые условия и процессы, способствующие его существованию и развитию.

Типовыми локальными целями террористических структур (ТС) являются:

- принятие нужного (выгодного) решения органами власти;
- дискредитация органов власти;
- запугивание населения;

- освобождение соратников из заключения;
- финансирование дальнейшей борьбы.

ТС на разных этапах и направлениях своей деятельности используют различные технологии, среди которых наиболее значимыми с точки зрения рассматриваемой темы являются:

- технологии подготовки и совершения террористических актов;
- технологии воздействия на сознание;
- организационные и коммуникационные технологии.

Элементы технологических схем, разрабатываемых и применяемых ТС, как правило, взаимосвязаны и синхронизированы между собой в процессе подготовки и совершения теракта. Объективно технологии совершения терактов коррелируют со способами совершения насильственных преступлений и ведения войны. Однако, они разрабатываются (выбираются), исходя из локальных целей террористических структур, которые, в свою очередь, задают требуемый тип информационно-управляющего воздействия и, соответственно, характер и масштабы последствий теракта. Выбор конкретных технологий и средств нападения определяется террористическими структурами также, исходя из возможностей их добывания, вероятности успешного использования и степени готовности антитеррористических систем к их отражению.

Специфика современного этапа развития терроризма заключается в использовании нетрадиционных средств нападения, например, осуществления компьютерных атак на критически важные информационно-управляющие системы с учетом их повсеместного распространения, а также объективных возможностей нанесения скрытного и удаленного воздействия. В то же время, у кибератак имеются недостатки по сравнению с физическими, поскольку подготовить и осуществить результативную атаку на сложную информационную систему значительно труднее. Следует также констатировать, что на данный момент не имеется достоверной информации о совершении компьютерных атак на критически важные ИТКС с террористическими целями и серьезными негативными последствиями.

Используемые террористическими структурами информационно-управляющие воздействия можно сгруппировать следующим образом:

- провоцирование властей на неадекватные (приводящие к дискредитации) действия необычностью теракта, большими масштабами ущерба, невыполнимыми требованиями и т. п.;
- оказание давления в нужном направлении на органы власти угрозой возможных негативных последствий;

- изменение общественного сознания в направлениях эскалации страхов, психологического шока, ощущения нестабильности, недовольства властями и т. п.

К технологиям воздействия на сознание можно отнести:

- технологии пропаганды терроризма;
- технологии прямого устрашающего воздействия на массовое сознание;
- технологии вербовки участников и сторонников;
- технологии планирования эффективных сценариев терактов.

В основе современных технологий пропаганды терроризма лежит прямое или опосредованное использование средств массовой информации (СМИ). Подавляющее большинство СМИ в настоящее время не предоставляет свои страницы или эфир террористам с учетом общественного мнения и законодательства своих стран. Однако, в государствах с фундаменталистскими, левыми и гипертрофированно либеральными режимами такие СМИ всегда находятся («Аль-Джазира» и т. д.), а остальные их в обязательном порядке цитируют. Прямое использование СМИ в настоящее время реализуется, как правило, в глобальной сети Интернет, где в этом качестве выступают сайты ТС. Сеть Интернет является идеальной средой для деятельности террористов, поскольку доступ к ней крайне легок, потенциальная аудитория огромна, там легко обеспечить анонимность пользователей, она никем не управляется и не контролируется.

К обсуждаемым в последнее время возможным террористическим технологиям относятся также акции по непосредственному оказанию устрашающего воздействия на массовое сознание (без реализации классического теракта) с помощью информационного оружия и социальных технологий. Так, на террористические сайтах публикуются дезинформационные сообщения, новости, вызывающие панику и ощущение безнадежности у населения, фото- и видеоматериалы, внушающие ужас, например, казни заложников. «Аль Каида» периодически публикует на своих сайтах угрозы и предупреждения о готовящихся террористических атаках. Технологии вербовки участников и сторонников терроризма используют приемы манипуляции сознанием, скрытно превращающими субъекта в объект управления.

Технологии планирования сценариев терактов направлены на достижение максимального информационно-психологического эффекта от их проведения и базируются на хорошем знании социальной психологии и массовых коммуникаций. Ролевые функции террористов здесь пересекаются с ролевыми функциями сценаристов и режиссеров голливудских блокбастеров, просчитывающих наиболее коммерчески успешные

сюжеты. Об этом свидетельствуют результаты моделирования сценариев наиболее резонансных терактов последних лет.

Рассмотрим, например, террористическую атаку (ТА) на небоскребы ВТЦ в Нью-Йорке 11 сентября 2001 года. Главное отличие этого теракта от предыдущих представляется в качественно ином уровне организации и формирования целостного замысла с прогнозируемыми (но неочевидными на стадии реализации) последствиями. Информационный «успех» операции был многократно усилен работой СМИ, которые на протяжении нескольких месяцев работали на террористов, дестабилизируя социальную ситуацию и разрушая доверие к государственным институтам.

Анализируя события 11 сентября 2001 года, можно с большой вероятностью реконструировать причины, по которым террористы выбрали именно такой сценарий проведения теракта. Замысел этой ТА состоял, видимо, в уничтожении наиболее значимых символов США, что должно было вызвать шок, деморализацию и дезорганизацию американской нации и мировой общественности. Выбор объектов атаки, вероятно, осуществлялся путем анализа символов Америки по критериям получения максимального информационного возмущения, наибольшей доступности объекта и максимальной вероятности успеха его атаки доступными средствами. Все цели избранные для проведения терактов являются символами могущества государства, современного миропорядка и системы ценностей современной цивилизации:

- здание Пентагона — символ военного могущества США и военного противостояния «антицивилизационным устремлениям»;
- здания ВТЦ — символ экономического доминирования США и международного экономического регулирования.

В качестве инструмента атаки, были использованы самолеты гражданской авиации с учетом:

- непроработанности мер противодействия;
- планируемых масштабов последствий;
- высокой зрелищности и эмоциональной насыщенности;
- оптимальной скорости сближения объектов для проведения съемок.

Двухактная композиция теракта также стала оптимальной для обеспечения максимального присутствия прессы на месте происшествия.

В процессе обеспечения своей деятельности и подготовки терактов ТС также активно применяют различные нестандартные организационные и коммуникационные технологии. К организационным технологиям относятся формы и методы управления, взаимодействия, финансирования, расширения зон влияния и состава участников и т. п. Важной разновидностью организационных технологий является информационное обеспечение деятельности ТС, многие из которых создали в Интернете базы разведывательных данных, собранных из открытых и закрытых источников, которые они используют при подготовке терактов, выполнении текущих организационных задач и обеспечении собственной безопасности. Через интернет-сайты собираются пожертвования для ТС, привлекаются новые члены. Существуют сайты, выполняющие учебно-методические функции, на которых террористов обучают проводить хакерские атаки, изготавливать взрывные устройства и т. д. ТС активно используют при подготовке и координации терактов передачу зашифрованных посланий и приказов посредством электронной почты, интернет-чатов и форумов.

Итак, эскалация применения террора как метода решения политических проблем с одновременной технологизацией террористической деятельности на фоне ускоренной информатизации цивилизации и усиления ее технологической зависимости, представляет очень серьезную проблему, актуальность которой будет только возрастать по мере развития и распространения информационно-коммуникационных технологий.

Системная актуализация проблемы информационной безопасности личности

А. Н. Курбацкий

Мы слишком привыкли к сочетанию «защита информации» — оно становится все популярней, становится обыденным. Становится все привычней сочетание защита информации в глобальных информационных сетях. Еще десять—пятнадцать лет назад им пользовались в основном профессионалы в сфере информационных технологий и смежных областей, сейчас это общеупотребляемое сочетание. Но, пожалуй, все острее становится проблема — «защита *от* информации в глобальных информационных сетях», или защита от средств массовой информации (СМИ), как в настоящее время основного инструмента формирования общественного мнения. При прогнозировании и формировании общественного мнения по международной системе мониторинга глобальных информационных сетей необходимо учитывать эти аспекты.

Когда мы говорим «проинформирован — значит защищен», то предполагаем разумность и достоверность информации. Если это не обеспечивать, то и мониторинг естественно не будет пользоваться доверием. Но вот с обеспечением этих свойств в глобальных информационных сетях как раз становится все больше и больше проблем.

Попробуем сегментировать проблему в зависимости от различных контекстов. Следует учитывать, что по отношению к Интернету есть две категории: пользователи и не пользователи — приверженцы традиционных источников информации (бумажные СМИ, традиционное телевидение, радио и т. д.). Первая категория быстро увеличивается, вторая сокращается, но не так быстро как прогнозировалось, например, в 90-е годы прошлого века. Говоря об источниках информации в глобальных сетях, следует различать два понятия: СМИ в Интернете и сетевые СМИ.

Угрозы и опасности в глобальных информационных сетях (и соответственно обеспечение защиты, информационной безопасности) следует рассматривать:

- для личности;
- для общества;
- для государства.

Постоянно нужно держать в фокусе внимания все три категории. Анализ требует в каждом конкретном случае придания весовых коэффициентов всем трем категориям. Часто смещение акцентов в сторону государства, может привести к недооценке опасности для личности или общества, смещение в сторону личности, может привести к недооценке опасности для государства и т. д.

Информационную безопасность невозможно рассматривать независимо от безопасности в политической, экономической, военной, экологической, гуманитарной сферах.

Среди пользователей глобальных информационных систем особо нужно выделить молодое поколение. Его представители с одной стороны еще активно формируются в личность, становятся активными членами общества, с другой стороны могут в массовом порядке активно воздействовать на государство. Раньше эти процессы были гораздо более медленными, и главное детерминированными как со стороны государства, так и во многих случаях и со стороны общества. Сейчас же этот детерминизм быстро разрушается, государство и общество сталкиваются с большими трудностями. В существенной степени такими ускорителями возможностей молодого поколения явились глобальные сети. Всегда ли этот процесс ускорения позитивен большой вопрос. Более ранняя активизация требует получения опыта принятия решений на основе получаемой информации, большей ответственности за последствия принятых решений — а этого опыта как раз и не хватает. Общество и государство оказались практически не готовы к таким процессам.

У молодого поколения активно формируется зависимость от Интернета. Но как любой социальный феномен, он имеет колоссальные негативные аспекты. Прежде всего, формируется так называемая виртуальная реальность, то есть реальность, которой нет в жизни, потому у многих рождается искаженное представление о мире. Некоторые перестают адекватно воспринимать реальный мир, в котором живут и уходят в виртуальный мир от реальных проблем.

Молодежь все больше времени проводит за компьютером, предпочитая виртуальный мир реальному и в существенной степени худший виртуальный мир, создаваемый агрессивными компьютерными играми. «Живые картинки» с экранов телевизоров и компьютерных мониторов практически совпадают. Убийство и насилие становится нормой жизни.

Существование зависимости от виртуального мира, аналогичной наркотической, пока еще вызывает сомнения у многих ученых и специалистов, но несомненно то, что количество молодежи, увлекающихся нахождением в виртуальной реальности растет катастрофически быстро. Человек, находясь длительное время в такой среде, переносит ее законы

на реальный мир: начинает чувствовать себя более уязвимым. Многие психологи подтверждают, что игры, где присутствует насилие, формируют агрессивность в сознании человека. При этом такая агрессивность может проявиться не сразу, а постепенно накапливаясь, через некоторый временной промежуток, иногда и достаточно длительный. Взрослый человек сегодня пока еще способен более-менее четко разделять виртуальные и реальные миры. Но дети, которые еще не в достаточной степени получили представление об окружающем их реальном мире, такую способность сейчас приобретают все меньше. Начинается подмена нравственности. И действия в виртуальном мире переносятся в реальность. И тогда — убийства в школьной среде, необъяснимые самоубийства и так далее. Практически даже стадии формирования компьютерной (виртуальной) зависимости схожи со стадиями «привязки» к наркотику. Современный терроризм — это распределенная *система сетевого типа*. Этим в существенной степени обусловлена и трудность борьбы с терроризмом, поскольку сетевые системы невозможно уничтожить «точечными ударами»: они способны к самовосстановлению. Здесь напрашивается аналогия с сетевым принципом многих популярных агрессивных компьютерных игр.

Ранее на секциях семинара много говорилось о проблеме терроризма. Террористические организации пытаются навязать обществу новую модель регулирования экономической и политической жизни, в которой информационное и физическое *насилие* над личностью становится основным *методом управления* обществом и его институтами. Методология информационного противоборства освоена террористическими организациями в мере, достаточной для внесения масштабных и долговременных корректив в параметры процесса общественного развития не только одного государства, но и всего международного сообщества. И все это сопровождается «живыми картинками в СМИ». Даже Збигнев Бжезинский в своей статье в «Los Angeles Times» от 11 октября 2005 года пишет «Террористами не рождаются, а становятся — под воздействием конкретных событий, личного опыта, представлений, фобий, национальных мифов, исторической памяти, религиозного фанатизма и сознательного «промывания мозгов». Ими становятся под влиянием телевизионной „картинки“...». А молодой человек видит эти картинки в Интернете постоянно.

Последствия сегодняшних упущений в образовании и воспитании могут проявиться гораздо раньше, чем мы думаем.

К большому сожалению, зачастую информационные технологии в образовании внедряются лишь для того, чтобы шагать в ногу со временем, а не для решения тщательно спланированных образовательных задач. Во многих случаях те, кто занимается компьютеризацией школьного обучения, тратят слишком много сил и средств на само компьютерное оборудование и подключение к Интернету, уделяя слишком мало внимания профессиональной подготовке и поддержке тех же учителей. И скучные занятия в школах заменяются внешкольными игровыми, массово низкого качества.

Практически мы пока не имеем массового формирования молодежной культуры на основе применения информационных и коммуникационных технологий, которая способствовала бы применению в реальной жизни знаний и навыков, полученных молодежью в виртуальной среде.

К сожалению, решение этих задач в обществе возлагают часто только на одну систему образования. Но этого явно недостаточно. Нужен более масштабный общественный контроль через самые разные институты гражданского общества — общенациональные общественные организации, религиозные институты, родительские и преподавательские сообщества, политические партии и молодежные организации. Нужно эффективное правовое регулирование, т. е. государственное вмешательство в регулирование деятельности глобальных информационных сетей. Здесь уже имеется огромный опыт и выработаны разные подходы. Почти все правительства поощряют саморегулирование и политику фильтрации материалов конечными потребителями. Практически все государства жестко ограничивают и наказывают за распространение в Интернете детской порнографии и за возбуждение расовой ненависти. Причем, важно то, что в ряде случаев особо и изобретать нового не нужно. Нужно эффективнее, масштабнее использовать накопленный накоплен достаточно большой опыт по защите как взрослых, так и детей от вредного контента. Например, в США, власти считают эффективным широкое использование индивидуальных систем защиты — контентной фильтрации. Контентная фильтрация обычно основана на использовании методов блокирования доступа к веб-сайтам. Пользователям либо позволяется посещать определенный набор IP-адресов («контроль по типу включения»), либо для них заводится определенный набор IP-адресов с заблокированным доступом («контроль по типу исключения»). Следует отметить, контентная фильтрация отличается от контентного анализа, который представляет собой динамический анализ контента и блокировании доступа к веб-страницам, которые содержат информацию, определяемую по определенным критериям. В 2001 году в США вступил в силу акт, обязывающий школы и библиотеки, получающие госдотации, устанавливать системы контентной фильтрации.

В Европе Интернет регулируется союзным законодательством и национальными нормами. В целом, там используется подход, подобный американскому.

1 марта 2007 года № 265 утверждена программа «Комплексная информатизация системы образования Республики Беларусь на 2007—2010 годы».

Если предыдущая программа была ориентирована главным образом на создание инфраструктуры информатизации, то главная задача новой программы — это содержательное наполнение созданной инфраструктуры, ее дальнейшее развитие и совершенствование на качественно новом уровне.

Основные направления программы следующие.

1. Разработка и внедрение национальных информационных образовательных ресурсов, электронных средств обучения, отраслевых автоматизированных систем управления.
2. Интеграция учреждений образования и государственных органов управления образованием в единую образовательную сеть.

Особое внимание будет направлено на развитие доступа учреждений образования в сеть Интернет. Необходимо обеспечить возможность качественного доступа, в первую очередь в корпоративную информационную сеть системы образования внутри Республики Беларусь. Вместе с тем, доступ в сеть Интернет должен быть организованным и контролируемым. В частности в программе предусмотрен комплекс мероприятий по контролю за использованием информационных ресурсов.

Решение этой задачи в рамках программы обеспечивается за счет:

1. Создания интегрированной системы национальных информационных ресурсов образовательного назначения, фильтрации и зеркалирования наиболее востребованных информационных ресурсов образовательного назначения Интернета, организации эффективного поиска информационных ресурсов образовательного назначения, в том числе за счет каталогизации професионально-ориентированных учебных ресурсов и ссылок на них.
2. Разработки и внедрения специализированного программного обеспечения (например, контент-контроля, отслеживание в режиме реального времени в локальной сети учреждения образования потоки информации, не относящиеся к учебно-воспитательному процессу, обеспечивающего идентификацию пользователя, работающего с информационными ресурсами и т. п.).
3. Разработки нормативных документов, инструкций и правил, регламентирующих работу в корпоративной сети (например, внесение соответствующего регламентирующего пункта в Правила внутреннего распорядка учреждения образования или разработка Правил функционирования сети учреждения образования).
4. Проведения организационных мероприятий с пользователями информационных ресурсов: педагогами, учащимися, студентами (например, заключение договоров, регламентирующих порядок работы, права и обязанности пользователей).

Глобальные информационные сети становятся универсальной инфраструктурой для формирования новых общественных, социальных структур, которые существенно могут влиять на все три категории — государство, общество, личность. Интернет максимально децентрализует возможности социального проектирования, удешевляет коммуникационные возможности. Интересно в этом плане соотношение иерархии и сети. В определенном смысле можно сказать, что любой социальный организм самоорганизуется двумя возможными способами — в иерархию и в сеть. Эти два способа и не существуют один без другого и, так или иначе, взаимно переходят друг в друга. Зачастую одной из целей существования сети является превращение в иерархию — просто цель может быть отдалена во времени (замаскирована). И сеть, и иерархия являются способом распределения капитала среди участников сети. Капитал имеется ввиду в широком смысле — и экономический, и политический, и капитал знаний, и капитал культуры и т. д.

Особый интерес представляют социальные сети, которые могут быть своего рода надстройкой над государством и возможно станут сильным информационным механизмом модернизации общества, государства, что собственно уже и подтверждается. Обычно выделяют пять основных характеристик сети: независимость членов сети; множественность лидеров; объединяющая цель; добровольность связей; множественность уровней взаимодействия.

Впервые громко заявив о себе в начале 2000-х годов, сейчас социальные сети переживают настоящий бум. Сегодня социальные сети обзавелись целым рядом возможностей, выводящих их на принципиально новый уровень. Теперь при общении в Интернете все чаще задается не вопрос, «в какой стране живешь?», а «в какой социальной сети общаешься?»

Журналисты взяли несколько интервью у подростков, которые «живут» в онлайновых социальных сетях. Они объясняют, что воспринимают Интернет-страницу неотрывно от своей личности. Твоя страница — это и есть ты. Сегодня в социальных сетях десятки миллионов пользователей пишут о том, что их волнует, делятся новостями и впечатлениями, общаются и спорят, находят бизнес-партнеров и сотрудников, обмениваются ссылками, фотографиями, песнями и видеороликами, знакомятся. Социальные сети можно рассматривать как СМИ нового поколения.

Но сайты социальных сетей могут открыть хакерам «черный ход» в корпоративные сети; угроза растет, поскольку всё больше взрослых приобщаются к новым веяниям интернета, говорится в докладе, представленном CA (бывшая Computer Associates) и Национальным альянсом кибербезопасности США (NCSA).

«Мы уже видели случаи, когда хакеры использовали возможности веб-сайтов сообществ», — пишет в анонсе доклада исполнительный директор NCSA Рон Тексериа. Помимо риска для бизнеса, взрослые участники социальных сетей подвергают риску свои реквизиты, говорит Сэм Карри, вице-президент CA по управлению угрозами. Он сравнивает хакеров с террористами, которые тоже ищут людные места для своей деятельности.

По данным доклада, 47 % пользователей социальных сетей относятся к возрастной группе от 18 до 34, а 53 % — старше 35. Практически половина — 46 % — выходит в социальные сети из офисов.

Хотя 57 % осознают опасность стать жертвой киберпреступников, они продолжают рассказывать о себе то, что может подвергнуть их риску. Например, 74 % сообщают свой почтовый адрес, имя, дату рождения и иногда даже номер социального страхования. 83 % пользователей социальных сетей загружали файлы из профилей других участников.

Что же касается защиты детей, то 51 % родителей не интересуются, включены ли в профилях детей ограничения, обеспечивающие контакты только со своей возрастной группой. 36 % родителей вообще не интересуются тем, что делают их дети в социальных сетях.

Проблема молодого поколения и виртуального мира крайне актуальна, поскольку время смены поколений очень скоротечно, и мы часто ошибаемся в оценках тех или иных общественных явлений из-за недооценки скоротечности и запаздываем в своих перспективных прогнозах.

В частности не следует недооценивать глобального влияния Интернета на молодое поколение в неанглоязычных государствах, особенно если их государственность только формируется вместе с формированием национальных элит. Здесь оно может вступать в явный или/и неявный конфликт с национальными интересами. В молодых государствах национальные элиты, если только это элиты, а не кланы, формируются в первую очередь на основе молодого поколения. На сегодняшний день Интернет является основным средством глобализации, но глобализации массово воспринимаемой как американизации. К сожалению, происходит массовое пропагандирование, навязывание населению (в первую очередь молодежи) других стран «американского образа жизни», весьма далекого от реального, однако преподносимого как общепринятого в США. По крайней мере, так все широко воспринимается во многих государствах, особенно национальными элитами. Очевидно, что национальные информационные ресурсы не способны конкурировать с глобальными Интернет-ресурсами — они заведомо обречены на поражение, особенно по мере воздействия на молодое поколение. Может происходить быстрое разрушение многих основ национальной культуры, традиций, их подмена неким универсальным виртуальным «суррогатом», который даже не соответствует американским (западным) реалиям. Причем этот процесс достаточно скоротечен, хотя и не всегда явно заметен в силу своей перманентности (как и любой воспитательный процесс). Отсюда и одна из основных причин формирования систем контент-фильтрации Интернета на государственном уровне в ряде государств, как защитной реакции. Можно с вероятностью близкой к единице прогнозировать, что такие защитные тенденции в мировом масштабе будут только нарастать.

С этими процессами непосредственно связана проблема интернационализации управления Интернетом. В 2005 году Китай, Россия, Бразилия, ЮАР, Норвегия, Швейцария, Саудовская Аравия и ряд других стран предложили кардинально изменить принципы управления Интернетом. Одним из предлагаемых вариантов решения — создание специального органа управления при ООН. Такой шаг мог бы в существенной мере уменьшить дискредитацию глобализации, в целом как прогрессивного, полезного мирового процесса, если не сводить его к американизации. США пока такой шаг не поддержали, хотя в стратегическом плане он может быть полезен и США.

Часть II

СЕКЦИЯ «МАТЕМАТИЧЕСКИЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Решение разреженных систем линейных уравнений при вычислении логарифмов в конечном простом поле

А. Я. Дорофеев

Современные алгоритмы дискретного логарифмирования в конечном простом поле GF(p), применявшиеся при проведении рекордных вычислений [1, 2, 3, 4, 5, 6, 7], распадаются на несколько этапов, из которых наибольшую трудоемкость имеют этап формирования разреженной системы линейных уравнений методом просеивания (решета) и этап решения этой системы в поле вычетов по модулю $(p-1)/2$.

Так как этап формирования системы распараллеливается на большое число изолированных вычислительных ветвей, каждая из которых имеет малую вычислительную сложность, то формирование системы можно выполнить в какой-либо общедоступной распределенной вычислительной среде, коммутируемой, например, по сети Internet. При этом будет получено ускорение вычислений приблизительно равное числу используемых вычислительных узлов.

Этап решения системы уравнений является тем «узким местом», которое определяет размерность задачи логарифмирования, поддающейся решению на современной вычислительной технике за приемлемое время [1]. Это связано с тем, что при решении системы необходимо в цикле выполнять процедуру умножения вектора на разреженную матрицу большой размерности. При распараллеливании указанной процедуры данные, расположенные в различных процессорах, взаимодействуют между собой в основном цикле алгоритма, что приводит к необходимости использовать дорогостоящую многопроцессорную вычислительную технику с высокоскоростной сетью межпроцессорной коммутации. При этом эффективность вычислений существенно снижается за счет накладных расходов на пересылку данных между процессорами и синхронизацию вычислений.

В настоящее время при решении разреженных систем, возникающих при вычислении дискретных логарифмов, используют, как правило, алгоритм Ланцоша [7, 8, 9]. Было замечено, что время решения системы можно существенно сократить, если предварительно исключить из

системы часть неизвестных методом Гаусса, а для определения оставшихся неизвестных воспользоваться методом Ланцоша. Для сокращения времени алгоритма Ланцоша неизвестные следует исключать так, чтобы минимизировать число ненулевых элементов, добавленных в матрицу системы — этот метод получил название структурированного гауссова исключения [8, 10, 11], [12, с. 280].

Алгоритм Ланцоша вычисляет в произвольном поле K решение линейной системы $Ax = b$, где A — симметричная $n \times n$-матрица, b — ненулевой n-вектор. Алгоритм состоит в следующем.

1. Вычислить

$$w_0 = b, \quad v_1 = Aw_0, \quad w_1 = v_1 - w_0\frac{(v_1,\, v_1)}{(w_0,\, v_1)}, \quad x_0 = w_0\frac{(w_0,\, b)}{(w_0,\, v_1)}. \tag{1}$$

2. При $i \geqslant 1$ в цикле выполнить

$$v_{i+1} = Aw_i, \quad w_{i+1} = v_{i+1} - w_i\frac{(v_{i+1},\, v_{i+1})}{(w_i,\, v_{i+1})} - w_{i-1}\frac{(w_i,\, v_{i+1})}{(w_{i-1},\, v_i)}, \tag{2}$$

$$x_i = x_{i-1} + w_i\frac{(w_i,\, b)}{(w_i,\, v_{i+1})}. \tag{3}$$

3. Алгоритм заканчивает работу как только $(w_k, Aw_k) = 0$ для некоторого $k \leqslant n$. Если $w_k = 0$, то система имеет решение

$$x = x_{k-1} = \sum_{i=0}^{k-1}\frac{(w_i,\, b)}{(w_i,\, Aw_i)}w_i;$$

если $w_k \neq 0$, то алгоритм не находит решения [13].

При вычислении матрицы решений $X = \left(x^{(0)}x^{(1)}\ldots x^{(s-1)}\right)$ системы $AX = B$ для $n \times s$-матрицы $B = \left(b^{(0)}b^{(1)}\ldots b^{(s-1)}\right)$,

$b^{(j)} \in \operatorname{span}(A^0b,\, A^1b,\, \ldots,\quad A^{n-1}b), \quad 1 \leqslant j \leqslant s-1, \quad b^{(0)} = b, \quad b \neq 0$

следует на шагах (1) и (3) алгоритма Ланцоша вычислять:

$$x_0^{(j)} = w_0\frac{(w_0,\, b^{(j)})}{(w_0,\, v_1)}, \quad x_i^{(j)} = x_{i-1}^{(j)} + w_i\frac{(w_i,\, b^{(j)})}{(w_i,\, v_{i+1})}, \quad 0 \leqslant j \leqslant s-1.$$

Если матрица A не является симметричной, то система приводится к виду $A^TAX = A^TB$. Для однородной системы $AX = 0$ выполняется разбиение $A = (A'A'')$ и решается система $A'X' = -A''$.

Пусть матрица A имеет δ ненулевых элементов, пусть c_1 — трудоемкость аддитивной операции в K, c_2 — трудоемкость мультипликативной операции в K, тогда трудоемкость алгоритма Ланцоша составляет

$$2n\delta c_1 + n^2((s+2)2(c_1 + c_2) + c_2).$$

Алгоритм Ланцоша был запрограммирован на языке C в среде параллельного программирования MPI (Message Passing Interface) [14]. При программировании коммутационных операций был реализован асинхронный режим обмена, что позволило совместить во времени коммутационные и вычислительные операции.

Структурированный алгоритм Гаусса представляет собой версию алгоритма Гаусса, в которой минимизируется число ненулевых элементов, добавляемых в матрицу системы при ее приведении к треугольному виду. Алгоритм состоит в следующем.

Для матрицы $A = (a_{ij})$ выполнить:

1. Выбрать t столбцов с минимальным числом ненулевых элементов и объявить их активными.
2. Для каждого $a_{ij} = \pm 1$ в активных столбцах вычислить вес Марковица — величину $(r_i - 2)(c_j - 2)$, где r_i — число ненулевых элементов в строке i, c_j — число ненулевых элементов в столбце j.
3. Найти элемент $a_{ij}^* = \pm 1$ для которого достигается минимальное значение веса Марковица. Используя a_{ij}^* как ведущий элемент, выполнить гауссово исключение. Удалить строку i и столбец j.
4. Если все активные столбцы удалены, перейти к шагу 1, иначе перейти к шагу 2.

Структурированный алгоритм Гаусса был запрограммирован на языке C. Для организации быстрого доступа к элементам матрицы $A = (a_{ij})$ в порядке увеличения их весов Марковица применялось сбалансированное двоичное AVL-дерево [15, с. 492]. Для экономного использования оперативной памяти при выполнении гауссова исключения был разработан оригинальный алгоритм дефрагментации памяти.

Алгоритм Ланцоша и структурированный алгоритм Гаусса были совместно апробированы при решении разреженных систем, возникших при вычислении дискретных логарифмов для рекордных модулей, размера 100 и 135 десятичных знаков (задачи DL100 и DL135) [16]. Для указанных модулей Д. В. Матюхин и Д. М. Дыгин на основе разработанного ими оригинального алгоритма решета числового поля сформировали разреженные системы линейных уравнений. Для сокращения времени решения разреженных систем их матрицы были сжаты с использованием структурированного алгоритма Гаусса. Полученные после сжатия системы были решены методом Ланцоша.

Замеры времени решения систем выполнены для кластера «twin1», установленного в НИВЦ МГУ (`http://parallel.ru/cluster/twin1-config.html`). Кластер содержит узлы (2 × Opteron 285/2,6 GHz/16 GB RAM), связанные коммутационной сетью InfiniBand 10 Gbit/sec (4x).

Таблица 1

	$S_2^{(100)}$	$S_1^{(100)}$	$S_0^{(100)}$	$S^{(100)}$
rows	56000	66000	76000	365976
columns	55000	65000	75000	314142
$\neq 0$	93682986	26995360	15013788	6832588
$\neq 0$/rows	1672.910	409.020	197.549	18.669
density	$3.041 \cdot 10^{-2}$	$6.292 \cdot 10^{-3}$	$2.633 \cdot 10^{-3}$	$5.943 \cdot 10^{-5}$
± 1	86280564	25292212	14028263	6365244
± 1/rows	1540.724	383.215	184.582	17.392
$\pm 1/\neq 0$	0.920	0.936	0.934	0.931
time	38.398	7.451	4.011	—

Таблица 2

	$S_2^{(135)}$	$S_1^{(135)}$	$S_0^{(135)}$	$S^{(135)}$
rows	501000	565000	629000	2739345
columns	500000	564000	628000	2541033
$\neq 0$	730414017	323188542	195954354	57250340
$\neq 0$/rows	1457.912	572.015	311.533	20.899
density	$2.915 \cdot 10^{-3}$	$1.014 \cdot 10^{-3}$	$4.960 \cdot 10^{-4}$	$8.224 \cdot 10^{-6}$
± 1	695243804	307608541	185703456	52724736
± 1/rows	1387.712	544.439	295.236	19.247
$\pm 1/\neq 0$	0.951	0.951	0.947	0.920
time	364.554	233.296	194.077	—

Для задач DL100 и DL135 характеристики разреженных систем представлены соответственно в таблицах 1 и 2. Системы $S^{(100)}$ и $S^{(135)}$ сформированы в результате работы алгоритма решета числового поля. Системы $S_2^{(100)}$, $S_1^{(100)}$, $S_0^{(100)}$ и $S_2^{(135)}$, $S_1^{(135)}$, $S_0^{(135)}$ получены соответственно в результате сжатия систем $S^{(100)}$ и $S^{(135)}$ методом структурированного гауссова исключения.

Строки rows и columns указывают размерность матрицы системы; строки $\neq 0$ и ± 1 указывают число ненулевых элементов в матрице и число

Таблица 3

	$S_2^{(100)}$	$S_1^{(100)}$	$S_0^{(100)}$	$S^{(100)}$
2	172.875	73.881	62.588	584.243
4	97.721	42.571	37.337	354.814
8	56.659	27.466	24.047	237.389
16	30.088	15.941	15.814	158.221
20	29.842	15.164	15.356	160.909
24	25.543	14.528	15.244	155.154
32	21.032	11.527	12.753	128.980
40	15.442	10.950	13.042	124.333
48	16.591	10.083	14.727	141.826
56	16.401	9.410	13.230	142.896
64	15.911	9.635	13.501	154.179
72	14.285	10.010	15.239	145.545
80	14.370	11.027	13.819	144.806
88	12.771	11.451	12.712	134.041

Таблица 4

	$S_2^{(135)}$	$S_1^{(135)}$	$S_0^{(135)}$	$S^{(135)}$
4	11030.228	6047.812	4993.901	—
8	5997.731	3609.905	2854.421	18935.576
16	2799.032	1909.069	1677.021	12604.821
20	2346.157	1543.673	1411.289	11772.120
24	1938.673	1381.343	1253.580	11354.710
32	1485.232	1115.026	1058.837	10019.291
40	1281.431	997.849	997.102	9096.558
48	1121.114	894.404	915.280	9431.957
56	1070.212	836.118	909.966	8949.339
64	980.959	792.155	875.916	9006.267
72	892.904	752.872	846.570	8641.488
80	847.694	736.812	847.430	8365.086
88	832.054	693.795	801.985	8959.942

Таблица 5

	DL100		DL135	
P	$T(P)$	$E(P)$	$T(P)$	$E(P)$
4	42.571	1.000	6047.812	1.000
8	27.466	0.774	3609.905	0.837
16	15.941	0.667	1909.069	0.791
20	15.164	0.561	1543.673	0.783
24	14.528	0.488	1381.343	0.729
32	11.527	0.461	1115.026	0.677
40	10.950	0.388	997.849	0.606
48	10.083	0.351	894.404	0.563
56	9.410	0.323	836.118	0.516
64	9.635	0.276	792.155	0.477
72	10.010	0.236	752.872	0.446
80	11.027	0.193	736.812	0.410
88	11.451	0.168	693.795	0.396

элементов, равных $+1$ или -1; строки $\neq 0$/rows и ± 1/rows указывают среднее число ненулевых элементов и элементов равных ± 1 в одной строке матрицы; строка density указывает отношение числа ненулевых элементов к общему числу элементов матрицы; строка $\pm 1/\neq 0$ указывает отношение числа элементов матрицы равных ± 1 к общему числу ненулевых элементов; в строке time указано время (в минутах) сжатия системы методом структурированного гауссова исключения на одном процессоре кластера.

Из таблиц видно, что почти все элементы матриц систем равны $+1$ или -1. Остальные ненулевые элементы матриц представляют собой небольшие целые числа, каждое из которых целиком умещается в одну 32-разрядную ячейку памяти.

В таблицах 3 и 4 для задач DL100 и DL135 указаны (в часах) полученные в результате замеров оценки времен решения систем методом Ланцоша в зависимости от числа используемых вычислительных ядер.

Системы решаются в поле вычетов по модулю $(p-1)/2$, где p — модуль логарифмирования. Для хранения одного элемента указанного поля вычетов в задачах DL100 и DL135 используются соответственно 11 и 14 32-разрядных ячеек памяти.

Из оценок, представленных в таблицах 3 и 4 видно, что для задач DL100 и DL135 минимальные времена решения систем методом Ланцоша достигаются на системах $S_1^{(100)}$ и $S_1^{(135)}$.

В таблице 5 указаны (в часах) времена решения систем для задач DL100 и DL135 вместе с соответствующими оценками эффективности распараллеливания.

Из полученных оценок видно, что времена сжатия матриц систем методом Гаусса пренебрежимо малы по сравнению со временами решения систем методом Ланцоша. Вместе с тем, за счет предварительного сжатия матриц удается более чем на порядок сократить времена решения систем.

Литература

[1] *Odlyzko A. M.* Discrete logarithms: the past and future // Designs, Codes and Cryptography. 2000. Vol. 19. № 2. P. 129—145.

[2] *LaMacchia B. A.*, *Odlyzko A. M.* Computation of discrete logarithms in prime fields // Designs, Codes and Cryptography. 1991. Vol. 1. № 1. P. 47—62.

[3] *Weber D.* On the computation of discrete logarithms in finite prime fields. Ph. D. Thesis. 1997. 111 p.

[4] *Denny T. F.* Lösen großer dünnbesetztr Gleichungssysteme uber endlichen Primkörpern. Ph. D. Thesis. 1997. 137 p.

[5] *Joux A.*, *Lercier R.* Discrete logarithms in GF(p) // `http://listserv.nodak.edu/archives/nmbrthry.html`. 17.04.2001. 4 p.

[6] *Joux A.*, *Lercier R.* Improvements to the general number field sieve for discrete logarithmes in prime fields. A comparison with the gaussian integer method // Mathematics of Computation. 2002. Vol. 72, № 242. P. 953—967.

[7] *Joux A.*, *Lercier R.* Discrete logarithms in GF(p)—130 digits // `http://listserv.nodak.edu/archives/nmbrthry.html`. 18.06.2005. 4 p.

[8] *LaMacchia B. A.*, *Odlyzko A. M.* Solving large sparse linear systems over finit fields // Lecture notes in computer science. 1991. Vol. 537. P. 109—133.

[9] *Lanczos C.* Solutions of systems of linear equations by minimized iterations // J. Res. Nat. Bureu of Standards. 1952. Vol. 49. P. 33—53.

[10] *Odlyzko A. M.* Discrete logarithms in finite fields and their cryptographic significance // Lecture Notes in Computer Sciences. 1984. Vol. 209. P. 224—316.

[11] *Pomerance C.*, *Smith J. W.* Reduction of huge, sparse matrices over finit fields via created catastrophes // Experimental Mathematics. 1992. Vol. 1, N 2. P. 89—94.

[12] *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М.: 2003, 325 с.

[13] *Дорофеев А. Я.* Вычисление логарифмов в конечном простом поле методом линейного решета // Труды по дискретной математике. 2002. Т. 5. С. 29—50.

[14] *Корнеев В. Д.* Параллельное программирование в MPI. М.: 2003, 303 с.
[15] *Кнут Д. Е.* Искусство программирования. Т. 3. Сортировка и поиск. М.: Вильямс, 2000. 822 с.
[16] *Dorofeev A. Ya.*, *Dygin D. M.*, *Matyukhin D. V.* Discrete logarithms in GF(p)—135 digits // International Scientific Conference „Diophante and analytic problems in number theory“ dedicated to the 100th birthday of A. O. Gelfond. Abstracts. Moscow, 2007. P. 14—15. `http://listserv.nodak.edu/archives/nmbrthry.html`. 22.12.2006.

Вариант блочного алгоритма типа Ланцоша решения систем линейных уравнений

М. А. Черепнёв

Пусть требуется решить систему линейных уравнений

$$Ax = b, \quad A \in \mathbb{F}(N \times N), \quad b \in \mathbb{F}(N \times n), \tag{1}$$

где A — симметричная матрица, $\mathbb{F}$ — поле из двух элементов, а n, $n \leqslant N$ — длина машинного слова (в дальнейшем будем считать, что $n = 64$).

Для $R(\lambda) \in \mathbb{F}(n \times n)[\lambda]$, $n \in \mathbb{N}$, обозначим через R_i коэффициент при λ^i, то есть $R(\lambda) = \sum\limits_{i=0}^{\deg R(\lambda)} R_i \lambda^i$. Пусть так же

$$R(A, B) = \sum_{i=0}^{\deg R(\lambda)} A^i B R_i,$$

где $B \in \mathbb{F}(N \times n)$. Обозначим $W(B) \in \mathbb{F}(N \times n')$, $n' \leqslant n$ — подсовокупность вектор-столбцов матрицы B такую, что матрица $(W(B))^t A W(B)$ невырождена. Эта подсовокупность может быть построена при помощи алгоритма из пункта 8 работы [1]. Пусть далее O_n, I_n — соответственно нулевая и единичная матрицы из $\mathbb{F}(n \times n)$.

Рассмотрим случайную матрицу $B \in \mathbb{F}(N \times n)$, $n \leqslant N$. Пусть

$$\alpha = \sum_{i=0}^{2L+1} \alpha_i \lambda^{-i}, \quad \alpha_i = B^t A^i B. \tag{2}$$

Определим скалярное произведение двух многочленов степени не выше L: $(\varphi(\lambda), \psi(\lambda)) \in \mathbb{F}(n \times n)$ как коэффициент при λ^{-1} в произведении $\varphi(\lambda)^t \alpha \psi(\lambda)$. Обозначим $(C, D) = C^t A D \in \mathbb{F}(n \times n)$ матрицу A-скалярных произведений вектор-столбцов матриц C, $D \in \mathbb{F}(N \times n)$. Из этого определения и симметричности матрицы A следует в частности, что $(C, D) = (D, C)^t$.

Лемма 1. $(\varphi(A, B), \psi(A, B)) = (\varphi(\lambda), \psi(\lambda))$.

Доказательство. Согласно введённых определений правая и левая часть линейны по φ, ψ, поэтому достаточно доказать лемму при $\varphi = \lambda^i$,

$\psi = \lambda^j$, i, $j \in \mathbb{N} \cup \{0\}$. В этом случае правая часть равна $B^t A^{i+j+1} B$, а левая

$$(A^i B)^t A A^j B,$$

что ввиду симметричности матрицы A, одно и то же. Лемма доказана. □

Будем обозначать $\mathbf{W}$ линейное пространство над $\mathbb{F}$ столбцов матрицы W.

Теорема 1. *Пусть матрица $W \in \mathbb{F}(N \times M)$ такова, что A-скалярное произведение на $\mathbf{W}$ невырождено, то есть*

$$W^t A W \text{ — невырожденная матрица}, \tag{3}$$

а $u \in \mathbb{F}(N \times n)$. Тогда существует единственный блок $w \in \mathbb{F}(N \times n)$, $\mathbf{w} \subset \mathbf{W}$, для которого

$$W^t A(u - w) = 0. \tag{4}$$

При этом

$$w = W(W^t A W)^{-1} W^t A u. \tag{5}$$

Доказательство. Существование. Пусть w определён формулой (5), тогда $W^t A(u - w) = W^t A u - W^t A u = 0$.

Единственность. Пусть выполнено равенство (4). Поскольку $\mathbf{w} \in \mathbf{W}$, то $w = Wc$ для некоторого $c \in \mathbb{F}(N \times n)$, откуда

$$W^t A u = W^t A W c,$$

или

$$c = (W^t A W)^{-1} W^t A u,$$

то есть выполнено равенство (5). Теорема доказана. □

Будем в дальнейшем называть w из теоремы 1 A-ортогональной проекцией блока u на линейное пространство $\mathbf{W}$.

Если теперь предположить, что x — решение уравнения (1), то его A-ортогональная проекция на любое подпространство $\mathbf{W}$, базис которого, записанный по столбцам, образует матрицу W, удовлетворяющую условию (3), может быть вычислена однозначно по формуле

$$w = W(W^t A W)^{-1} W^t b. \tag{6}$$

Если же $\mathbf{x} \subset \mathbf{W}$, то в $\mathbf{W}$ оно единственно и определяется формулой (6).

Теорема 2. *Пусть имеется набор попарно A-ортогональных подпространств $\mathbf{W}_i$, $i = 0, 1, \ldots, m-1$, в $\mathbb{F}^N$, A-скалярное произведение на которых невырождено. Пусть так же матрица A переводит сумму этих подпространств $\mathbf{W}$ в себя, и $\mathbf{b} \subset \mathbf{W}$. Тогда решение системы (1) в $\mathbf{W}$ единственно и задаётся формулой*

$$x = \sum_{i=0}^{m-1} W_i ({W_i}^t A W_i)^{-1} {W_i}^t b. \tag{7}$$

Доказательство. Как показано в теореме 1, при выполнении условий теоремы формула (7) однозначно определяет A-ортогональную проекцию решения системы (1) на пространство $\mathbf{W}$. Для окончательного доказательства осталось показать, что формула (7) задаёт решение системы (1). Действительно, легко понять, что для $j = 0, 1, \ldots, m-1$ ${W_j}^t A x = {W_j}^t b$, откуда пространство столбцов матрицы

$${W_j}^t A(Ax - b) = {W_j}^t A^t (Ax - b) = (A W_j)^t (Ax - b)$$

лежит в пространстве столбцов матрицы $W^t(Ax - b) = 0$, поэтому блок $Ax - b$ A-ортогонален всему пространству $\mathbf{W}$. Кроме того, так как по условию $b \in \mathbf{W}$, и $A\mathbf{W} \subseteq \mathbf{W}$, то пространство столбцов матрицы $Ax - b$ лежит в $\mathbf{W}$ откуда, ввиду невырожденности A-скалярного произведения на $\mathbf{W}$, имеем $Ax - b = 0$. Теорема доказана. □

Пусть имеются последовательные матричные приближения

$$\begin{gathered}
\alpha(\lambda) Q^{(t-1)}(\lambda) - P^{(t-1)}(\lambda) = \sum_{i=t}^{\frac{N}{n}} \tau_i \lambda^{-i}, \quad \tau_t \neq O_n, \\
\alpha(\lambda) Q^{(t)}(\lambda) - P^{(t)}(\lambda) = \sum_{i=t+1}^{\frac{N}{n}} \rho_i \lambda^{-i}, \quad \rho_{t+1} \neq O_n, \\
\deg Q^{(s)}(\lambda) \leqslant s, \quad \deg P^{(s)}(\lambda) \leqslant s, \quad s \in \{t-1, t\}.
\end{gathered} \tag{8}$$

Здесь λ — переменная, а $Q^{(s)}(\lambda)$, $P^{(s)}(\lambda) \in \mathbb{F}(n \times n)[\lambda]$, τ_i, $\rho_i \in \mathbb{F}(n \times n)$. $Q^{(s)}(\lambda)$, $P^{(s)}(\lambda)$ — матричные многочлены. $Q^{(-1)} = 0_n$, $P^{(-1)} = I_n$, $Q^{(0)} = I_n$, $P^{(0)} = \alpha_0$.

Заметим, что при любых j, $t : 0 \leqslant j \leqslant t$

$$(Q^{(j)}(A, B),\ Q^{(t+1)}(A, B)) = O_n,$$

так как коэффициент при λ^{-1} в ряде

$$\left(Q^{(j)}(\lambda)\right)^t \alpha(\lambda) Q^{(t+1)}(\lambda) = \left(Q^{(j)}(\lambda)\right)^t \left(\sum_{i=t+2}^{\frac{N}{n}} \gamma_i \lambda^{-i} \right)$$

равен нулю. Поэтому столбцы матриц $Q^{(i)}(A, B)$ лежат в попарно A-ортогональных подпространствах. Для выполнения условий теоремы 2 сумма этих размеров должна быть приблизительно равна N. Обозначим $W_t = W(Q^{(t)}(A, B))$. Ожидаемый размер (ранг) матрицы (W_t, W_t) лишь чуть меньше n. Значит число матричных приближений при решении невырожденной системы линейных уравнений (1) приблизительно равно $\frac{N}{n}$. В случае вырожденной системы следует заменить N на $\operatorname{rang} A$.

Рассмотрим задачу построения следующего $(t+1)$-го приближения с аналогичными оценками на степень.

Вычислим ранг матрицы ρ_{t+1}: $\operatorname{rang}\rho_{t+1} := n - k$.

Если $k = 0$, вычислим $\nu_1 := -{\rho_{t+1}}^{-1}\tau_t$, $\nu_0 := -{\rho_{t+1}}^{-1}(\tau_{t+1} + \rho_{t+2}\nu_1)$ и найдём следующее приближение по формуле $\lambda Q^{(t)}\nu_1 + Q^{(t)}\nu_0 + Q^{(t-1)}$.

Иначе нужно выбрать $\overline{z}_i$, $i = 1, \ldots, n-k$ линейно независимые строки матрицы ρ_{t+1}. Выбрать строки $\overline{z}_i$, $i = n-k+1, \ldots, n$, которые дополняют набор рассматриваемых строк до базиса $\mathbb{F}^n$, обозначим $z \in \mathbb{F}(k \times n)$ матрицу, составленную из этих дополнительных строк. Обозначим $\overline{y}_i$, $i = 1, \ldots, k$, базис пространства решений системы $\overline{y}\rho_{t+1} = \overline{0}$, запишем его по строкам и соответствующую матрицу обозначим $y \in \mathbb{F}(k \times n)$.

Для этого последовательно сверху вниз строки матрицы ρ_{t+1} проверяются на линейную зависимость с предыдущими. В случае независимости всё остаётся без изменения. В случае зависимости выписывается очередное решение $\overline{y}_i$. В конечном итоге строится матрица $З \in \mathbb{F}(n-k \times n)$ выбора линейно независимых строк из матрицы ρ_{t+1}. Получим

$$З\rho_{t+1} = \begin{pmatrix} I_{n-k} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \overline{z}_1 \\ \vdots \\ \overline{z}_n \end{pmatrix}.$$

Вычислим $\rho \in \mathbb{F}(n \times n)$, $\delta \in \mathbb{F}(n \times k)$ такие, что $\rho_{t+2} = \rho\rho_{t+1} + \delta z$. Для этого необходимо разложить строки матрицы ρ_{t+2} по базису $\overline{z}_i$, $i = 1, \ldots, n$.

Вычислим $\overline{u}_i$, $i = 1, \ldots, l$; $l \leqslant k$, базис пространства решений системы $\overline{u}y\delta z = \overline{0}$, соответствующую матрицу обозначим $u \in \mathbb{F}(l \times n)$. Максимальный набор линейно независимых строк матрицы $y\delta z$ обозначим $Дy\delta z$, $Д \in \mathbb{F}(k-l \times k)$.

Определим значение оператора $s \in \mathbb{F}(n \times n)$ нулями на следующих $k+l$ вектор-строках:

$$\begin{cases} y\tau_t s = 0 \\ uy(\tau_{t+1} + \rho\tau_t)s = 0 \end{cases}$$

Допустим, что значение k невелико и эта система непротиворечива. Дополним рассматриваемые $k+l$ вектор-строк до базиса $t_1, \ldots, t_n$ всего пространства. Соответствующую матрицу из дополняемых $n-(k+l)$ строк обозначим t. Далее мы доопределим значение оператора s на остальных элементах этого базиса, после чего, обратив матрицу t, найдем матрицу s. Также в дальнейшем находятся и матрицы ν_0, ν_1.

Определим значение оператора $\nu_1 \in \mathbb{F}(n \times n)$ на следующих вектор-строках через соответствующие значения оператора s:

$$\begin{cases} -З\tau_t s = З\rho_{t+1}\nu_1 \\ -Дy(\tau_{t+1} + \rho\tau_t)s = Дy\delta z\nu_1 \end{cases}$$

Определим значение оператора $\nu_0 \in \mathbb{F}(n \times n)$ на следующих вектор-строках через соответствующие значения оператора s и ν_1: $-З(\tau_{t+1}s + \rho_{t+2}\nu_1) = З\rho_{t+1}\nu_0$.

Переобозначим матрицу z, заменив её на матрицу, в которой первые $k-l$ строк равны $Дy\delta z$, а последние l, которые будем обозначать z_l, дополняют их до базиса пространства, порождённого вектор-строками $\overline{z}_i$, $i = n-k+1, \ldots, n$.

Оставшиеся значения операторов s, ν_0, ν_1 определим из условия максимальности ранга над $\mathbb{F}$ матрицы будущего приближения в виде

$$\lambda Q^{(t)}\nu_1 + Q^(t)\nu_0 + Q^{(t-1)}s.$$

Для этого сначала максимизируем ранг матрицы, являющейся её свободным членом:

$$Q_0^{(t)}\nu_0 + Q_0^{(t-1)}s, \tag{9}$$

а затем ранг оставшихся столбцов матрицы-коэффициента при λ:

$$Q_0^{(t)}\nu_1 + Q_1^{(t)}\nu_0 + Q_1^{(t-1)}s. \tag{10}$$

Разложим строки матрицы $Q_0^{(t)}$ по базису, состоящему из $\overline{z}_i$, $i = 1, \ldots$ $\ldots, n-k$, и строк матрицы z, а $Q_0^{(t-1)}$ — по базису t_i. Подставим в (9) и получим для некоторых $Q \in \mathbb{F}(n \times n)$, $\Phi \in \mathbb{F}(n \times k)$, $Ш \in \mathbb{F}(n \times n-(k+l))$ следующую матрицу:

$$Q + \Phi z\nu_0 + Шts. \tag{11}$$

Найдём невырожденные матрицы $\alpha \in \mathbb{F}(n \times n)$, $\beta \in \mathbb{F}(n-(k+l) \times n-(k+l))$, $\gamma \in \mathbb{F}(l \times l)$ такие, что для некоторых целых неотрицательных ε, ε' для матриц $\alpha Q = \widetilde{Q}$, $\alpha\Phi\gamma = \widetilde{\Phi}$, $\alpha Ш\beta = \widetilde{Ш}$ имеются следующие пред-

ставления:

$$\widetilde{\text{Ш}} = \begin{pmatrix} I_{n-(k+l)-\varepsilon} & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{F}(n \times n - (k+l)),$$

$$\widetilde{\Phi} = \begin{pmatrix} * & * & \}n-(k+l)-\varepsilon \\ I_{k-\varepsilon'} & 0 & \\ 0 & 0 & \end{pmatrix} \in \mathbb{F}(n \times k),$$

Умножив матрицу (11) слева на α и, сделав подстановку $z\nu_0 = \gamma\gamma^{-1}z\nu_0$, $ts = \beta\beta^{-1}ts$, получим матрицу $\widetilde{Q} + \widetilde{\Phi}\gamma^{-1}z\nu_0 + \widetilde{\text{Ш}}\beta^{-1}ts$. Для получения максимального ранга этой матрицы приравняем её первые $n-l-\varepsilon-\varepsilon'$ строк к строкам единичной матрицы с теми же номерами. Теперь, двигаясь снизу вверх находим $k-\varepsilon'$ первых строк матрицы $\gamma^{-1}z\nu_0$, затем $n-(k+l)-\varepsilon$ первых строк матрицы $\beta^{-1}ts$ выражаются через ε' строк матрицы $\gamma^{-1}z\nu_0$. В результате матрица (9) будет полностью определена, а её ранг будет равен $n-l'$, где $l' \leqslant l+\varepsilon+\varepsilon'$, при этом остались неопределёнными последние ε' строк матрицы $\gamma^{-1}z\nu_0$, которые обозначим $z_{\varepsilon'}$ и последние ε строк матрицы $\beta^{-1}ts$, которые обозначим t_ε. Их и l последних строк матрицы $z\nu_1$ мы будем выбирать максимизируя ранг совокупности тех столбцов матрицы (10), которые остаются после отбрасывания столбцов с номерами некоторой максимальной линейно независимой совокупности столбцов матрицы $Q_0^{(t)}\nu_0 + Q_0^{(t-1)}s$. Умножим слева матрицу (10) на α, а затем на невырожденную матрицу α', приводящую последние l' столбцов матрицы (9) к нижнетреугольному виду.

Пусть $\widetilde{\nu}_1$, $\widetilde{\nu}_0$, $\widetilde{s}$ — последние l' столбцов матриц соответственно ν_1, ν_0, s. Аналогично предыдущему, представим последние l' столбцов матрицы (10), умноженной слева на $\alpha'\alpha$, в виде:

$$Q' + \Phi'_1 z_l \widetilde{\nu}_1 + \Phi'_2 z_{\varepsilon'} \widetilde{\nu}_0 + \text{Ш}' t_\varepsilon \widetilde{s} \in \mathbb{F}(n \times l').$$

Аналогично тому, как это было сделано раньше, находим невырожденные матрицы $\widetilde{\alpha}$, $\widetilde{\beta}$, $\widetilde{\gamma}$, $\widetilde{\delta}$, для которых при некоторых целых неотрицательных $\widetilde{\varepsilon}''$, $\widetilde{\varepsilon}'$, $\widetilde{\varepsilon}$:

$$\widetilde{\alpha}\Phi'_1\widetilde{\beta} = \begin{pmatrix} I_{l-\widetilde{\varepsilon}''} & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{F}(n \times l), \quad \widetilde{\alpha}\Phi'_2\widetilde{\delta} = \begin{pmatrix} * & * & \}l-\widetilde{\varepsilon}'' \\ I_{\varepsilon'-\widetilde{\varepsilon}'} & 0 & \\ 0 & 0 & \end{pmatrix} \in \mathbb{F}(n \times \varepsilon'),$$

$$\widetilde{\alpha}\text{Ш}'\widetilde{\gamma} = \begin{pmatrix} * & * & \}l-\widetilde{\varepsilon}''+\varepsilon'-\widetilde{\varepsilon}' \\ I_{\varepsilon-\widetilde{\varepsilon}} & 0 & \\ 0 & 0 & \end{pmatrix} \in \mathbb{F}(n \times \varepsilon).$$

Приравнивая к соответствующим строкам единичной матрицы, как и раньше последовательно находим первые $\varepsilon - \widetilde{\varepsilon}$ строк матрицы $\widetilde{\gamma}^{-1}t_\varepsilon\widetilde{s}$, затем первые $\varepsilon' - \widetilde{\varepsilon}'$ строк матрицы $\widetilde{\delta}^{-1}z_{\varepsilon'}\widetilde{\nu}_0$ выражаем через $\widetilde{\varepsilon}$ последних строк матрицы $\widetilde{\gamma}^{-1}t_\varepsilon\widetilde{s}$. Затем первые $l - \widetilde{\varepsilon}''$ строк матрицы $z_l\widetilde{\nu}_1$ выражаем через них же и $\widetilde{\varepsilon}'$ последних строк матрицы $\widetilde{\delta}^{-1}z_{\varepsilon'}\widetilde{\nu}_0$.

Продолжив далее аналогично для коэффициентов при λ в степенях больше первой, определим остальные строки, в противном случае определим их произвольно. В результате матрица (10) будет полностью определена и ранг матрицы $\lambda Q^{(t)}\nu_1 + Q^{(t)}\nu_0 + Q^{(t-1)}s$ над полем $\mathbb{F}$ будет не меньше $n - \widetilde{\varepsilon}'' - \widetilde{\varepsilon}' - \widetilde{\varepsilon}$.

Поскольку число необходимых шагов приблизительно равно $\frac{N}{n}$, то для того, чтобы доказать оценку на количество операций в нашем алгоритме в виде $O\left(\frac{dN^2}{n}\right)$ достаточно оценить количество операций для одного шага в $O(dN)$ то есть столько же по порядку сколько требуется для умножения на матрицу A. Поскольку

$$Q^{(t+1)}(\lambda) = Q^{(t)}(\lambda)b_{t+1}(\lambda) + Q^{(t-1)}(\lambda)s = \\ = \lambda Q^{(t)}(\lambda)\nu_1 + Q^{(t)}(\lambda)\nu_0 + Q^{(t-1)}(\lambda)s,$$

это будет следовать из равенств

$$Q^{(t+1)}(A, B) = AQ^{(t)}(A, B)\nu_1 + Q^{(t)}(A, B)\nu_0 + Q^{(t-1)}(A, B)s.$$

Также как и в алгоритме Монтгомери здесь только одна сложная операция умножения на матрицу A, но на одно слагаемое меньше, чем в соответствующей формуле Монтгомери. Ещё около $\frac{N}{n}$ умножений на матрицу A потребуется для вычисления всех необходимых α_i в равенстве (7), отметим, что эти вычисления могут быть проделаны параллельно остальной части алгоритма. Количество элементов α_i, которые нужно хранить для вычисления первых элементов в правых частях равенств (8) на шаге t не превосходит $t+1$, а количество блочных операций для этих вычислений во всём алгоритме будет $O\left(\left(\frac{N}{n}\right)^2\right)$.

Литература

[1] *Montgomery P. L.* A Block Lanczos Algorithm for Finding Dependencies over GF(2). Advances in Cryptology—EuroCrypt'95. L. C. Guillou and J.-J. Quisquater, editors. Berlin: Springer-Verlag, 1995. (Lect. Notes in Comp. Sci.; Vol. 921.) P. 106—120.

[2] B. A. LaMacchia, A. M. Odlyzko. Solving large sparse linear systems over finite fields. Advances in Cryptology—Crypto'95. (Lect. Notes in Comp. Sci.; Vol. 537.) P. 109—133.

[3] W. Eberly, E. Kaltofen. On randomized Lanczos algorithms. Proc. of the 1997 International Symposium on Symbolic Algebraic Computation. ACM Press, 1997. P. 176—183.

Об одном классе совершенно уравновешенных булевых функций

О. А. Логачёв

Аннотация

В работе предлагается новый способ построения совершенно уравновешенных булевых функций из $\mathcal{F}_n$, нелинейных по крайним переменным при $n \geqslant 5$.

Ключевые слова: булева функция, функция дефекта нуль, совершенно уравновешенная функция.

1. Введение

Одним из важных вопросов анализа криптографических примитивов, построенных на основе регистров сдвига и булевых функций, является вопрос о способности этого криптографического примитива породить произвольную {0, 1}-последовательность любой конечной длины. В работе [1] для кодирующего устройства с конечной памятью без обратной связи описан класс булевых функций, позволяющих обеспечить для кодирующего устройства указанное выше свойство. Описание не является конструктивным. В [1] разработана также техника построения функций из этого класса нелинейных по первой и последней переменным. В настоящей работе предлагается новый способ построения таких функций.

2. Основные определения и обозначения

Пусть $\mathbb{F}_2$ — поле Галуа из двух элементов, $\mathrm{V}_n = \mathbb{F}_2^n$ — пространство наборов-столбцов длины $n \in \mathbb{N}$ ($\mathbb{N}$ — множество натуральных чисел) над полем $\mathbb{F}_2$. Будем обозначать через $\mathcal{F}_n$ множество булевых функций от n

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант № 07-01-00154).

переменных $\{x_1, x_2, \ldots, x_n\}$. Пусть $m \in \mathbb{N}$. Рассмотрим систему булевых уравнений вида:

$$f(x_s, x_{s+1}, \ldots, x_{s+n-1}) = y_s, \quad s = 1, 2, \ldots, m. \tag{1}$$

Легко видеть, что система (1) описывает функционирование в течение m тактов кодирующего устройства (см. [2]), построенного с помощью регистра сдвига с m ячейками двоичной памяти и булевой функции f.

Обозначим для $f \in \mathcal{F}_n$ через f_n^* отображение из V_{m+n-1} в V_m вида

$$f_m^*(x_1, x_2, \ldots, x_{m+n-1}) = (f(x_1, \ldots, x_n), f(x_2, \ldots, x_{n+1}), \ldots, f(x_m, \ldots, x_{m+n-1}))^\top. \tag{2}$$

Для булевой функции f введем понятие дефекта, определив для произвольного $m \in \mathbb{N}$ множество

$$J(f, m) = \{y \in \mathrm{V}_m \mid \forall\, x \in \mathrm{V}_{m+n-1}\ f_m^*(x) \neq y\} \tag{3}$$

и

$$\mathrm{Def}_m(f) = \#J(f, m). \tag{4}$$

Определение 1 ([1]). Булева функция $f \in \mathcal{F}_n$ называется функцией дефекта нуль, если $\mathrm{Def}_m(f) = 0$ для любого $m \in \mathbb{N}$.

Легко видеть (см. [1]), что если функция линейна хотя бы по одной из крайних переменных, то она является функцией дефекта нуль. Обозначим множество функций из $\mathcal{F}_n$, линейных по первой переменной, $\mathcal{L}_n$, а множество функций из $\mathcal{F}_n$, линейных по последней переменной, $\mathcal{R}_n$.

Определение 2 ([1]). Булева функция $f \in \mathcal{F}_n$ называется совершенно уравновешнной, если соотношение

$$\#(f_m^*)^{-1}(y) = 2^{n-1}$$

выполняется для любого $m \in \mathbb{N}$ и любого $y \in \mathrm{V}_m$ ($\#M$ — мощность множества M).

Из определения 2 при $m = 1$ нетрудно заметить, что совершенно уравновешенная функция является уравновешенной (т. е. вес f равен 2^{n-1}). Следовательно, относительная доля совершенно уравновешенных булевых функций в $\mathcal{F}_n$ стремится к нулю при $n \to \infty$.

3. Предварительные результаты

Теорема 1 ([1]). *Булева функция $f \in \mathcal{F}_n$ является функцией дефекта нуль тогда и только тогда, когда она совершенно уравновешена.*

Множество совершенно уравновешенных функций (т. е. функций дефекта нуль) из $\mathcal{F}_n$ обозначим $\mathcal{E}_n$. Особый интерес представляют функции из $\mathcal{E}_n \setminus (\mathcal{L}_n \cup \mathcal{R}_n)$, существенно зависящие от переменных x_1 и x_n. В работе [1] была разработана техника (алгоритмического характера), позволившая строить такие функции.

Пример 1 ([1]). Функция из $\mathcal{F}_4$ вида

$$f(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_2 \oplus x_3 \oplus x_1x_2x_4 \oplus x_2x_4 \oplus 1$$

является совершенно уравновешенной функцией из $\mathcal{E}_4$ ($\oplus$ — сложение по mod 2).

В работе [1] также был получен ряд верхних оценок для m, соответствующих непустым множествам $J(f, m)$, при выполнении некоторых условий относительно функции f. Заинтересованного читателя отсылаем к этой работе.

Необходимо также отметить преобразования множества $\mathcal{F}_n$, оставляющие инвариантным множество $\mathcal{E}_n$ (см. [1]):

1) $\gamma_0\colon\ f(x_1, \ldots, x_n) \to f(x_1, \ldots, x_n) \oplus 1$;
2) $\gamma_1\colon\ f(x_1, \ldots, x_n) \to f(x_1 \oplus 1, \ldots, x_n \oplus 1)$;
3) $\gamma_2\colon\ f(x_1, \ldots, x_n) \to f(x_n, \ldots, x_1)$.

Определенный интерес представляют условия равномерности распределения правых частей системы уравнений (1) при условии равномерности распределения случайного вектора $X_m = (x_1, \ldots, x_{m+n-1})^\top$.

Теорема 2 ([3]). *Пусть $\{X_m = (x_1, \ldots, x_{m+n-1})^\top\}_{m=1}^\infty$ — последовательность случайных векторов с распределением*

$$\Pr\{X_m = (a_1, \ldots, a_{m+n-1})^\top\} = 2^{-(m+n-1)}$$

для любых $(a_1, \ldots, a_{m+n-1})^\top \in V_{m+n-1}$.

Случайный вектор $Y_m = f_m^*(X_m)$ распределен равномерно для любого $m \in \mathbb{N}$ тогда и только тогда, когда f совершенно уравновешенная функция.

4. Основной результат

Для пары натуральных чисел k, l рассмотрим отображение $\Xi_{k,l}$ из $\mathcal{F}_k \times \mathcal{F}_l$ в $\mathcal{F}_{k+l-1}$ вида

$$\Xi_{k,l}(f, g) = f[g] = h \in \mathcal{F}_{k+l-1}, \quad f \in \mathcal{F}_k,\ g \in \mathcal{F}_l,$$

где

$$h(x_1, \ldots, x_{k+l-1}) = f[g](x_1, \ldots, x_{k+l-1}) = f(g(x_1, \ldots, x_k), g(x_2, \ldots, x_{k+1}), \ldots, g(x_k, \ldots, x_{k+l-1})).$$

Для этой конструкции справедливо следующее утверждение.

Теорема 3. *Пусть $f \in \mathcal{F}_k$, $g \in \mathcal{F}_l$. Функция $h = f[g] \in \mathcal{F}_{k+l-1}$ совершенно уравновешена тогда и только тогда, когда функции f и g совершенно уравновешены.*

Доказательство. *Достаточность*. Пусть функции f и g совершенно уравновешены и m — произвольное натуральное число. Тогда для любого набора $z = (z_1, \ldots, z_m)^\top \in \mathrm{V}_m$ имеем $\#(f_m^*)^{-1}(z) = 2^{k-1}$. В свою очередь, для любого вектора $y = (y_1, \ldots, y_{m+k-1})^\top \in (f_m^*)^{-1}(z)$ выполнено равенство $\#(g_{m+k-1}^*)^{-1}(y) = 2^{l-1}$. Следовательно, имеем

$$\#(h_m^*)^{-1}(z) = \#(f[g]_m^*)^{-1}(z) = \sum_{y \in \#(f_m^*)^{-1}(z)} \#(g_{m+k-1}^*)^{-1}(y) = 2^{k+l-2} = 2^{(k+l-1)-1},$$

для любого $m \in \mathbb{N}$ и любого $z \in \mathrm{V}_m$, т. е. функция $h \in \mathcal{F}_{k+l-1}$ совершенно уравновешена.

Необходимость. Пусть $h = f[g]$ совершенно уравновешенная функция. Предположим, что функция f не является совершенно уравновешенной. Тогда в соответствии с утверждением теоремы 1 f не является функцией дефекта нуль и существует натуральное m и набор $z = (z_1, \ldots, z_m)^\top \in \mathrm{V}_m$ такие, что $z \in J(f, m)$. Но тогда $z \in J(f[g], m)$, т. е. $f[g]$ не является функцией дефекта нуль (это по теореме 1 равносильно тому, что $f[g]$ не является совершенно уравновешенной). Получаем противоречие. Следовательно, f — совершенно уравновешенная функция.

Предположим теперь, что функция g не является совершенно уравновешенной. Тогда найдется натуральное r и такой набор $y^* = (y_1^*, \ldots, y_r^*) \in \mathrm{V}_r$, что $\#(g_r^*)^{-1}(y^*) = 2^{l-1} + \alpha$, где $0 < \alpha \leqslant 2^{l-1}$. На основе y^* построим множество $M_{r,t}$ $(t = 1, 2, \ldots)$ наборов длины $r(t+1) + (l-1)t$ вида

$$y = (y_1^*, \ldots, y_r^*; y_{r+1}, \ldots, y_{l+r-1}; y_1^*, \ldots, y_r^*; \ldots; y_1^*, \ldots, y_r^*; y_{tr+(t-1)(l-1)}, \ldots, y_{tr+t(l-1)}; y_1^*, \ldots, y_r^*),$$

где значения двоичных переменных, не помеченных звездочкой, — произвольны. Тогда $\#M_{r,t} = (2^{l-1})^t$. Легко видеть, что если $\left(g_{r(t+1)+(l-1)t}^*\right)^{-1}(y) \neq \emptyset$, $y \in M_{r,t}$, то

$$\left(g_{r(t+1)+(l-1)t}^*\right)^{-1}(y) \subseteq \underbrace{(g_r^*)^{-1}(y^*) \times \ldots \times (g_r^*)^{-1}(y^*)}_{t+1}.$$

С другой стороны, справедливо включение

$$g_{r(t+1)+(l-1)t}^* \left(\underbrace{(g_r^*)^{-1}(y^*) \times \ldots \times (g_r^*)^{-1}(y^*)}_{t+1} \right) \subseteq M_{r,t}.$$

Обозначим через μ_k среднее число наборов из множества

$$\underbrace{(g_r^*)^{-1}(y^*) \times \ldots \times (g_r^*)^{-1}(y^*)}_{t+1},$$

приходящихся на один набор из множества $M_{r,t}$:

$$\mu_t = \frac{2^{l-1} + \alpha)^{t+1}}{(2^{l-1})^t} = 2^{l-1}\left(1 + \frac{\alpha}{2^{l-1}}\right)^{t+1}.$$

Поскольку $\left(1 + \alpha/2^{l-1}\right) > 1$, то существует такое натуральное t_0, что $\mu_{t_0} > 2^{(k+l-1)-1}$. Следовательно, существует набор $y \in M_{r,t_0}$ такой, что

$$\#\left(g_{r(t_0+1)+(l-1)t_0}^*\right)^{-1}(y) > 2^{(k+l-1)-1}. \tag{5}$$

Пусть $z = f_{r(t_0+1)+(l-1)t_0-k+1}^*(y)$. Тогда согласно (5)

$$\#\left(f[g]_{(t_0+1)(r+l-1)-k+1}^*\right)^{-1}(z) > 2^{(k+l-1)-1},$$

т. е. функция $f[g]$ не является сильно уравновешенной. Получаем противоречие. □

Утверждение теоремы 3 позволяет строить булевы функции, не входящие в классы $\mathcal{L}_n$ и $\mathcal{R}_n$.

Пример 2. Пусть

$$f(x_1, x_2, x_3) = x_1 + x_2x_3 \in \mathcal{L}_3, \qquad g(x_1, x_2, x_3) = x_1x_2 \oplus x_3 \in \mathcal{R}_3.$$

Тогда

$$h(x_1, x_2, x_3, x_4, x_5) = f(g(x_1, x_2, x_3), g((x_2, x_3, x_4), g(x_3, x_4, x_5)) = x_1x_2 \oplus x_3 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_3x_4 \oplus x_4x_5 \notin \mathcal{L}_5 \cup \mathcal{R}_5.$$

Литература

[1] *Сумароков С. Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств. Обозрение прикладной и промышленной математики. Т. 1, вып. 1. 1994. С. 33—55.

[2] *Preparata F. P.* Convolutional transformations of binary sequences: Boolean functions and their resynchronizing properties. IEEE Trans. Electron. Comput. Vol. 15, № 6. 1966. P. 398—909.

[3] *Логачёв О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

Линейные структуры групп подстановок векторных пространств

Б. А. Погорелов, М. А. Пудовкина

1. Введение

Понятие линейной структуры отображения, в частности, отображения, реализуемого блочным шифром, рассматривалось в работах [1, 2, 3] и др. В работах [1, 4] отмечается, что наличие нетривиальной линейной структуры является слабостью такого отображения, в частности, позволяет строить фактор-системы для данной шифрсистемы с тем, чтобы применять метод гомоморфизмов в явном виде. Кроме того, наличие линейной структуры у отображения означает существование дифференциальной разности с вероятностью единица, что позволяет использовать метод дифференциального криптоанализа. Также метод линейного криптоанализа состоит в аппроксимации произвольного отображения линейным (аффинным), т. е. подмножеством отображений с линейной структурой. С другой стороны, расстояние булевой функции до линейной структуры является одним из критериев нелинейности функции [3]. Некоторые свойства отображений с линейными структурами приведены, например, в [5]. Таким образом, характеризация отображений, обладающих линейными структурами, и самих структур важна для синтеза и анализа шифров. При этом естественно возникает задача аппроксимации криптографического отображения отображением с линейной структурой.

В данной работе на групповом языке описаны все подстановки (биективные отображения) векторных пространств над полем характеристики два, обладающие линейной структурой. Также описан алгоритм аппроксимации произвольной подстановки подстановками с линейной структурой.

Будем придерживаться следующих обозначений: N_0 — множество натуральных чисел с нулем, $m \in N_0$, $m \geqslant 2$, $F \in \{\mathrm{GF}(2^m), V_m(2)\}$, $\overline{a, b} = a, a+1, \ldots, b$, $a < b$, $S(X)$ — симметрическая группа подстановок на

Работа выполнена при поддержке гранта Президента РФ НШ № 8564.2006.10.

множестве X, $\pi, \sigma \in S(F)$, $d(\pi, \sigma) = |\{\alpha \in F | \alpha^\pi \neq \alpha^\sigma\}|$, $\vec{0}$ — нулевой элемент F, $F^* = F \setminus \vec{0}$. Всюду ниже поле $\mathrm{GF}(2^m)$ рассматривается как m-мерное векторное пространство над $\mathrm{GF}(2)$.

Напомним (см., например, [5]), что отображение $\pi \in S(F)$ обладает линейной структурой, если в F существует $\alpha \neq \vec{0}$ такой, что $\beta^\pi + (\beta+\alpha)^\pi = \gamma_\alpha$ для любого $\beta \in F$, где $\gamma_\alpha \in F^*$ — произвольный фиксированный элемент. Такой вектор α называется линейным транслятором отображения π.

Пусть

$$\Pi_{\alpha,\gamma} = \{\pi \in S(F) \mid \beta^\pi + (\beta+\alpha)^\pi = \gamma \quad \forall \beta \in F\}, \quad \alpha, \gamma \in F^*;$$
$$\Pi_{W,W} = \{\pi \in S(F) \mid \beta^\pi + (\beta+\alpha)^\pi \in W \quad \forall \beta \in F \ \forall \alpha \in W\},$$

где W — подпространство F. Отметим, что $\Pi_{W,W} = \Pi_{\alpha,\alpha}$, если $W = \{\vec{0}, \alpha\}$.

2. Группа подстановок с линейной структурой

Приведем сначала описание множества $\Pi_{W,W}$ для произвольного подпространства $W \leqslant F$.

Теорема 1. *Для любого подпространства $W \leqslant F$, $\dim W = t \in \{\overline{1, m}\}$, множество $\Pi_{W,W}$ является импримитивной группой из $S(F)$ с системой импримитивности $\{\beta + W \mid \beta \in F\}$. Группа $\Pi_{W,W}$ подобна группе $S_{2^t} \wr S_{2^{m-t}}$.*

Доказательство. Покажем, что $\Pi_{W,W}$ является группой. Если $\pi_1, \pi_2 \in \Pi_{W,W}$, то из равенств

$$\beta^{\pi_1\pi_2} + (\beta + W)^{\pi_1\pi_2} = \beta^{\pi_1\pi_2} + (\beta^{\pi_1} + W)^{\pi_2} = \beta^{\pi_1\pi_2} + \beta^{\pi_1\pi_2} + W = W$$

для любого $\beta \in F$ следует, что $\pi_1\pi_2 \in \Pi_{W,W}$. Очевидно, что $e \in \Pi_{W,W}$. Осталось доказать, что $\pi^{-1} \in \Pi_{W,W}$ для любой подстановки $\pi \in \Pi_{W,W}$. Если это не так, то существует $\gamma \in F$, $\alpha \in W$ и подстановка $\pi \in \Pi_{W,W}$ такие, что $\gamma^{\pi^{-1}} + (\gamma+\alpha)^{\pi^{-1}} \notin W$. Положим $\beta = \gamma^{\pi^{-1}}$. Тогда из равенства

$$\gamma^{\pi^{-1}} + (\gamma+\alpha)^{\pi^{-1}} = (\beta^\pi)^{\pi^{-1}} + (\beta^\pi + \alpha)^{\pi^{-1}} =$$
$$= (\beta^\pi)^{\pi^{-1}} + (\beta + \alpha')^{\pi\pi^{-1}} = \alpha' \in W,$$

получаем противоречие с предположением, что $\gamma^{\pi^{-1}} + (\gamma+\alpha)^{\pi^{-1}} \notin W$. Значит $\Pi_{W,W}$ — группа. Для любой подстановки $\pi \in \Pi_{W,W}$ равенство $(\beta + W)^\pi = \beta^\pi + W$ эквивалентно тому, что $\pi\colon \beta + W \to \beta^\pi + W$ для каждого $\beta \in F$. Группа, порождаемая всеми такими подстановками, является импримитивной с системой импримитивности $\{\beta + W \mid \beta \in F\}$ и совпадает с группой $S_{2^t} \wr S_{2^{m-t}}$. □

Из теоремы 1 следует, что для любого $\alpha \in F^*$ группа $\Pi_{\alpha,\alpha}$ задается системой импримитивности $\{\{\beta,\ \beta+\alpha\} \mid \beta \in F\}$ и подобна группе $S_2 \wr S_{2^{m-1}}$.

Теорема 2. *Для любого подмножества* $\{\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k\} \subseteq F^*$, $k \in \{\overline{1,\ 2^m}\}$, $\dim\langle\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k\rangle = t \geqslant 1$, *имеет место равенство*

$$\bigcap_{i=1}^{k} \Pi_{\alpha_i,\alpha_i} = \underbrace{S_2 \wr \ldots \wr S_2}_{t} \wr S_{2^{m-t}}.$$

Покажем, что множество $\Pi_{\alpha,\gamma}$ является правым смежным классы группы $S(F)$ по подгруппе $S_2 \wr S_{2^{m-1}}$.

Теорема 3. *Пусть* $\alpha,\ \gamma \in F^*$, *и группа* $S_2 \wr S_{2^{m-1}}$ *имеет систему импримитивности* $\{\{\beta,\ \beta+\alpha\} \mid \beta \in F\}$. *Пусть также* h *— произвольное биективное линейное отображение из* $\Pi_{\alpha,\gamma}$. *Тогда* $\Pi_{\alpha,\gamma} = \Pi_{\alpha,\alpha}h = (S_2 \wr S_{2^{m-1}})h$.

Доказательство. Очевидно, что $\Pi_{\alpha,\gamma} \cap \Pi_{\alpha,\alpha} = \emptyset$ при $\alpha \neq \gamma$. Если подстановка $s \in \Pi_{\alpha,\gamma}$ и $g \in (\Pi_{\alpha,\alpha})s$, то выполняется равенство

$$(\beta+\alpha)^g = (\beta+\alpha)^{\pi s} = (\beta^\pi+\alpha)^s = \beta^{\pi s} + \gamma,$$

где $g = \pi s$ для некоторой подстановки $\pi \in \Pi_{\alpha,\alpha}$. Кроме того, если $s \in \Pi_{\alpha,\gamma}$, то $s^{-1} \in \Pi_{\gamma,\alpha}$, т. к. равенство $(\beta+\alpha)^s = \beta^s + \gamma$ влечет $(\theta+\gamma)^{s^{-1}} = \theta^{s^{-1}} + \alpha$, где $\theta = \beta^s$.

Для любых подстановок $s_1,\ s_2 \in \Pi_{\alpha,\gamma}$ из справедливости равенства

$$(\beta+\alpha)^{s_1 s_2^{-1}} = (\beta^{s_1}+\gamma)^{s_2^{-1}} = \beta^{s_1 s_2^{-1}} + \alpha$$

следует, что $s_1 s_2^{-1} \in \Pi_{\alpha,\alpha}$. Таким образом, $\Pi_{\alpha,\gamma} = \Pi_{\alpha,\alpha}h$. Из теоремы 1 следует, что $\Pi_{\alpha,\alpha} = S_2 \wr S_{2^{m-1}}$. Значит $\Pi_{\alpha,\gamma} = (S_2 \wr S_{2^{m-1}})h$. □

Следствие 1. *Пусть* $\alpha,\ \gamma \in F^*$, *и группа* $S_2 \wr S_{2^{m-1}}$ *имеет систему импримитивности* $\{\{\beta,\ \beta+\gamma\} \mid \beta \in F\}$. *Пусть также* h *— произвольное биективное линейное отображение из* $\Pi_{\alpha,\gamma}$. *Тогда* $\Pi_{\alpha,\gamma} = h\Pi_{\gamma,\gamma} = h(S_2 \wr S_{2^{m-1}})$.

Доказательство аналогично доказательству теоремы 3.

Найдем величину $|\Pi_{\alpha,\gamma}|$.

Утверждение 1. *Пусть* $\alpha,\ \gamma \in F^*$. *Тогда* $|\Pi_{\alpha,\gamma}| = 2^{2^{m-1}} \cdot (2^{m-1}!)$. *Число подстановок из* $S(F)$, *обладающих линейным транслятором* α, *равно* $(2^m-1) \cdot 2^{2^{m-1}} \cdot (2^{m-1}!)$.

Доказательство. Известно (см., например, [6]) равенство $|S_2 \wr S_{2^{m-1}}| = 2^{2^{m-1}} \cdot (2^{m-1}!)$. Из теорем 1, 3 следует, что $|\Pi_{\alpha,\alpha}| = |\Pi_{\alpha,\gamma}| = |S_2 \wr S_{2^{m-1}}| = 2^{2^{m-1}} \cdot (2^{m-1}!)$. Таким образом, число подстановок с линейным транслятором α равно

$$\sum_{\gamma \in F \setminus 0} |\Pi_{\alpha,\gamma}| = (2^m-1) \cdot |\Pi_{\alpha,\alpha}|. \quad \square$$

3. Аппроксимация произвольной подстановки подстановками с линейной структурой

Пусть $A_{\gamma,\epsilon}(s) = \{\alpha \in F \mid \alpha^s + (\alpha+\gamma)^s = \epsilon\}$ для произвольных $\gamma,\ \epsilon \in F^*$. Для подпространства $A \leqslant F$ обозначим через $\tau_\epsilon(A)$, $\epsilon \in F^*$, произвольное разбиение множества A на два подмножества $\dot{A}$ и $\dot{A}+\epsilon$. Очевидно, что такое разбиение всегда существует.

Приведем алгоритм аппроксимации произвольной подстановки $s \in S(F)$ подстановкой из множества $\Pi_{\gamma,\epsilon}$.

Алгоритм 1 (Алгоритм аппроксимации подстановки $s \in S(F)$ подстановкой из множества $\Pi_{\gamma,\epsilon}$). Вход: подстановка $s \in S(F)$.

1. Для каждого $\alpha \in A_{\gamma,\epsilon}(s)$ полагаем $\alpha^\pi = \alpha^s$.
2. Полагаем $\widetilde{A} = A_{\gamma,\epsilon}(s)$, $B = A_{\gamma,\epsilon}(s)$, $B_{\gamma,\epsilon}(s) = \{\alpha^s \mid \alpha \in A_{\gamma,\epsilon}(s)\}$.
3. Пока $F \setminus B \neq \emptyset$ выполняем:
   (a) выбираем произвольный элемент $\beta \in F \setminus B$;
   (b) вычисляем $\theta_\beta \in F$ такой, что $\theta_\beta = (\beta^s+\epsilon)^{s^{-1}}$;
   (c) полагаем $\beta^\pi = \beta^s$, $(\beta+\gamma)^\pi = \beta^s + \epsilon$;
   (d) полагаем $\widetilde{A} := \widetilde{A} \cup \beta$, $B := B \cup \{\beta,\ \theta_\beta,\ \beta+\gamma\}$, $B_{\gamma,\epsilon}(s) := B_{\gamma,\epsilon}(s) \cup \cup \{\beta^s,\ \beta^s+\epsilon\}$.
4. Полагаем $\overline{A} = \widetilde{A} \cup (\widetilde{A}+\gamma)$.
5. Формируем произвольное разбиение $\tau_\gamma(F \setminus \overline{A})$ множества $F \setminus \overline{A}$ на два подмножества $\widehat{A}_{\gamma,\epsilon}(s)$, $\widehat{A}_{\gamma,\epsilon}(s)+\gamma$.
6. Формируем произвольное разбиение $\tau_\epsilon(F \setminus B_{\gamma,\epsilon}(s))$ множества $F \setminus B_{\gamma,\epsilon}(s)$ на два подмножества $\widehat{B}_{\gamma,\epsilon}(s)$, $\widehat{B}_{\gamma,\epsilon}(s)+\epsilon$.
7. Формируем произвольное взаимно однозначное соответствие ψ: $\widehat{A}_{\gamma,\epsilon}(s) \to \widehat{B}_{\gamma,\epsilon}(s)$.
8. Для каждого $\alpha \in \widehat{A}_{\gamma,\epsilon}(s)$ полагаем $\alpha^\pi = \psi(\alpha)$, $(\alpha+\gamma)^\pi = \psi(\alpha)+\epsilon$.

Выход: подстановка $\pi \in \Pi_{\gamma,\epsilon}$, являющаяся аппроксимацией подстановки s. Кроме того,

$$d(\pi,\ s) = 2^m - a_{\gamma,\epsilon}(s),$$

где $a_{\gamma,\epsilon}(s) = |\widetilde{A}|$.

Трудоемкость алгоритма равна $T_A^{(1)} = 7 \cdot (a_{\gamma,\epsilon}(s) - |A_{\gamma,\epsilon}(s)|) + 2 \cdot 2^m$ и не превосходит $9 \cdot 2^m$ э. о.

Если $a_{\gamma,\epsilon}(s) \neq |A_{\gamma,\epsilon}(s)|$, то выполняется неравенство $|A_{\gamma,\epsilon}(s)| + 1 \leqslant a_{\gamma,\epsilon}(s)$. Также $a_{\gamma,\epsilon}(s) \leqslant 2^{m-1}$ при $A_{\gamma,\epsilon}(s) = \emptyset$.

Для доказательства корректности алгоритма достаточно показать, что он генерирует подстановку π из множества $\Pi_{\gamma,\epsilon}$.

Лемма 1. *Для любых γ, $\epsilon \in F^*$, алгоритм 1 аппроксимации подстановки $s \in S(F)$ генерирует подстановку $\pi \in \Pi_{\gamma,\epsilon}$.*

Обозначим через $\Pi\left(\widetilde{A}_{\gamma,\epsilon}(s)\right)$ множество подстановок, аппроксимирующих подстановку s, получающихся из алгоритма 1 при всех разбиениях $\tau_\gamma\left(F \setminus \overline{A}\right)$, $\tau_\epsilon(F \setminus B_{\gamma,\epsilon}(s))$ и взаимно однозначных соответствиях $\psi\colon \widehat{A}_{\gamma,\epsilon}(s) \to \widehat{B}_{\gamma,\epsilon}(s)$.

Утверждение 2. *Для произвольных γ, $\epsilon \in F^*$ и произвольных подстановок $s \in S(F)$ и $\pi \in \Pi(\widetilde{A}_{\gamma,\epsilon}(s))$ выполняется равенство*

$$d(\pi, s) = 2^m - a_{\gamma,\epsilon}(s).$$

Пусть $\Pi = \bigcup_{\gamma,\epsilon \in F \setminus 0} \Pi_{\gamma,\epsilon}$. Приведем алгоритм аппроксимации подстановки $s \in S(F)$ подстановками, обладающими линейной структурой, т. е. множеством Π.

Алгоритм 2 (Алгоритм аппроксимации подстановки $s \in S(F)$ подстановками с линейной структурой). Вход: подстановка $s \in S(F)$.

1. Вычисляем $a_{\gamma,\epsilon}(s)$ и $\pi_{s,\gamma,\epsilon} \in \Pi_{\gamma,\epsilon}$ для всех $\epsilon \in F^*$.
2. Находим такие $\epsilon \in F^*$, для которых значение $2^m - a_{\gamma,\epsilon}(s)$ минимально и полагаем $\pi = \pi_{s,\gamma,\epsilon}$.

Выход: подстановка $\pi \in \Pi$, аппроксимирующая подстановку s.

Расстояние между подстановкой $\pi \in \Pi$, аппроксимирующей s и найденной алгоритмом 2, и подстановкой s удовлетворяет неравенству

$$d(\pi, s) \leqslant \min\{2^m - a_{\gamma,\epsilon}(s) \mid \gamma, \epsilon \in F^*\}.$$

Из алгоритма 1 следует, что трудоемкость алгоритма 2 удовлетворяет соотношениям

$$T_A^{(2)} = \left(7 \sum_{\gamma \in F \setminus \vec{0}} (a_{\gamma,\epsilon}(s) - |A_{\gamma,\epsilon}(s)|) + 2^{m+1}\right)(2^m - 1) \leqslant 9 \cdot 2^{2m} \text{ э. о.}$$

Отметим, что аппроксимация подстановки s из множества $\Pi_{\gamma,\gamma}$, $\gamma \in F^*$, эквивалентна ее аппроксимации подстановками из группы изометрий метрики

$$\mu_\gamma^{(1)}(\alpha, \beta) = \begin{cases} 0, & \text{если } \alpha = \beta, \\ 1, & \text{если } \alpha + \beta \neq \gamma, \\ 2, & \text{если } \alpha + \beta = \gamma. \end{cases}$$

Литература

[1] *Chaum D.*, *Evertse J. H.* Cryptanalysis of DES with a reduced number of rounds sequences of linear factors in block ciphers // Crypto'85. Springer-Verlag, 1985.

[2] *Evertse J. H.* Linear structures in block ciphers // EUROCRYPT'87. Springer-Verlag, 1987.

[3] *Meier W.*, *Staffelbach O.* Nonlinearity criteria for cryptographic functions // EUROCRYPT'89. Springer-Verlag, 1989.

[4] *Варфоломеев А. А.*, *Жуков А. Е.*, *Мельников А. Б.*, *Устюжанин Д. Д.* Блочные криптосистемы. Основные свойства и методы анализа стойкости. М.: МИФИ, 1998.

[5] *Логачев О. А.*, *Сальников А. А.*, *Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

[6] *Погорелов Б. А.* Основы теории групп подстановок. Ч. 1: Общие вопросы. М., 1986. 316 с.

О сложности нахождения некоторых свойств веса булевой функции, заданной полиномом

С. Н. Селезнева

Аннотация

Весом булевой функции называется число векторов, на которых она равна единице.

В настоящей заметке доказано, что по полиному (по mod 2) булевой функции f от n переменных можно найти остаток от деления ее веса на 2^k, $k = 2, 3, \ldots$, со сложностью $O(n \cdot l^k)$, где l — число слагаемых в полиноме.

1. Введение

Пусть $F_2 = \{0, 1\}$, V_n — множество всех векторов с n коодинатами из F_2. *Булевой функцией* от n переменных называется отображение $f^n\colon V_n \to F_2$, $n = 0, 1, 2, \ldots$. Множество всех булевых функций от переменных $x_1, \ldots, x_n$ обозначим через $\mathcal{F}_n$.

Булевы функции можно задавать полиномами (по mod 2). Произведение вида $x_{i_1} \cdot \cdots \cdot x_{i_r}$, где $x_{i_p} \neq x_{i_q}$ при $p \neq q$, назовем *мономом ранга* r. По определению будем считать 1 вырожденным мономом ранга 0. Сумма вида $M_1 \oplus \cdots \oplus M_l$, где M_i — попарно различные мономы, называется *полиномом*. При этом число l называют *длиной* полинома, *степенью* полинома называют максимальный из рангов его слагаемых. Будем считать 0 вырожденным полиномом с длиной и степенью, равными 0.

Теорема 1 ([1]). *Каждая булева функция из $\mathcal{F}_n$ может быть однозначно задана полиномом* (*по* mod 2).

В соответствии с теоремой 1 для булевой функции $f(\tilde{x})$ определим ее *степень* $\deg(f)$ как степень задающего ее полинома.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант № 06-01-00438).

Введем также некоторые обозначения. Буквой с тильдой наверху будем обозначать векторы из n соответствующих координат.

Так $\tilde{x} = (x_1, \ldots, x_n)$, $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$.

Через $\tilde{x}^{\tilde{\alpha}}$ будем обозначать моном $x_1^{\alpha_1} \cdot \cdots \cdot x_n^{\alpha_n}$, где

$$x^\alpha = \begin{cases} x, & \text{если } \alpha = 1, \\ 1, & \text{если } \alpha = 0, \end{cases} \qquad \alpha \in \{0, 1\}.$$

Многие важные криптографические свойства булевых функций определяются через ее вес. Для булевой функции f из $\mathcal{F}_n$ ее *весом* $\mathrm{wt}(f)$ называется число векторов из V_n, на которых она равна 1.

Интересна следующая задача: можно ли, зная полином Жегалкина булевой функции, «достаточно быстро» найти либо ее вес, либо некоторые свойства ее веса? Под словосочетанием «достаточно быстро» будем понимать существование алгоритма, решающего задачу за полиномиальное от числа мономов в полиноме шагов.

В книге [2] авторами было отмечено, что по полиному булевой функции довольно легко можно определить, делится ли ее вес на 2.

Теорема 2 ([2]). *Пусть $f(\tilde{x}) \in \mathcal{F}_n$. Тогда* $\mathrm{wt}(f) \equiv 0 \pmod 2$, *если и только если* $\deg(f) < n$.

А также была предложена следующая задача (как нерешенная): «Можно ли выделить множество мономов булевой функции, которое будет „отвечать“ за делимость веса булевой функции на 2^k, $k = 2, 3, \ldots$?»

В настоящей заметке предлагается некоторое решение похожей задачи: «С какой алгоритмической сложностью можно найти остаток от деления на 2^k, $k = 2, 3, \ldots$, веса булевой функции, зная ее полином?». Ниже будет доказано, что со сложностью $O(n \cdot l^k)$, где n — число переменных функции, а l — длина полинома.

2. О задании булевых функций полиномами над кольцом целых чисел

Для решения поставленной задачи мы расширим модель, а именно, рассмотрим задание булевых функций полиномами над кольцом целых чисел. Такое расширение модели можно найти в [3].

Пусть Z — кольцо целых чисел с операциями сложения $+$ и умножения $\cdot$ и $Z[\tilde{x}]$ — кольцо полиномов над кольцом Z. Рассмотрим множество $Z^b[\tilde{x}]$, содержащее все полиномы из $Z[\tilde{x}]$, в которых степень каждой переменной не выше 1.

Пусть $f(\tilde{x}) \in \mathcal{F}_n$. Будем говорить, что полином $p(\tilde{x})$ из $Z^b[\tilde{x}]$ задает функцию $f(\tilde{x})$, если на множестве V_n значения полинома $p(\tilde{x})$ и функции $f(\tilde{x})$ совпадают.

В [3] доказано, что каждую функцию из $\mathcal{F}_n$ можно однозначно задать полиномом из $Z^b[\tilde{x}]$.

Теорема 3 ([3]). *Пусть* $f(\tilde{x}) = M_1 \oplus \cdots \oplus M_l$. *Тогда*

$$f(\tilde{x}) = \sum_{s=1}^{l} \sum_{1 \leqslant i_1 < \cdots < i_s \leqslant l} (-1)^{s-1} \cdot 2^{s-1} \cdot M_{i_1} \cdot \ldots \cdot M_{i_s}.$$

В теореме 3 утверждается, что полином из $Z^b[\tilde{x}]$ для булевой функции $f(\tilde{x})$ по ее полиному по mod 2 можно получить так: составить формальную сумму из всех мономов ее полинома, всех попарных произведений мономов ее полинома с коэффициентами -2, всех произведений мономов ее полинома по три с коэффициентами 2^2, и т. д., и наконец, произведения всех мономов ее полинома с коэффициентом $(-1)^{l-1} \cdot 2^{l-1}$; произвести упрощения в полученных слагаемых по правилу $x \cdot x = x$; а потом привести подобные слагаемые.

3. О сложности нахождения по полиному булевой функции некоторых ее свойств

Заметим, что вес булевой функции — это сумма ее значений на всех векторах. В следующей теореме описывается, как найти сумму значений булевой функции на всех векторах через коэффициенты полинома из $Z^b[\tilde{x}]$, ее задающего.

На множестве V_n определим *отношение частичного порядка*: $\tilde{\alpha} \preceq \tilde{\beta}$, если $\alpha_i \leqslant \beta_i$ для всех $i = 1, \ldots, n$, и $\tilde{\alpha} \prec \beta$, если $\tilde{\alpha} \preceq \tilde{\beta}$, $\tilde{\alpha} \neq \tilde{\beta}$.

Для вектора $\tilde{\alpha}$ из V_n его *весом* $|\tilde{\alpha}|$ назовем число его единичных координат.

Теорема 4 ([3]). *Пусть функция* $f(\tilde{x})$ *из* $\mathcal{F}_n$ *задается полиномом* $p(\tilde{x})$ *из* $Z^b[\tilde{x}]$ *и пусть* $c(\tilde{\alpha})$, $\tilde{\alpha} \in V_n$, *есть коэффициент в нем при мономе* $\tilde{x}^{\tilde{\alpha}}$. *Тогда*

$$\mathrm{wt}(f) = \sum_{\tilde{\beta} \in V_n} f(\tilde{\beta}) = \sum_{\tilde{\gamma} \in V_n} c(\tilde{\gamma}) \cdot 2^{n-|\tilde{\gamma}|}.$$

Перечисленные свойства позволяют построить эффективный алгоритм, который по полиному булевой функции находит остаток от деления ее веса на степень двойки.

Мы не будем вводить формальную модель алгоритма. Будем считать, что на вход некоторой процедуры подается запись полинома (по mod 2) булевой функции $M_1 \oplus \cdots \oplus M_l$. Под сложностью алгоритма на данном входе будем понимать число битовых операций, которые выполняются процедурой для получения ответа.

Теорема 5. *Пусть* k *— заданное число. Существует алгоритм, который по полиному* (*по* mod 2) $P_f = M_1 \oplus \cdots \oplus M_l$ *булевой функции* $f(\tilde{x}) \in \mathcal{F}_n$ *находит остаток от деления ее веса на* 2^k *со сложностью* $O(n \cdot l^k)$.

Доказательство. Опишем требуемый алгоритм. Он будет опираться на теоремы 3 и 4.

В начале работы алгоритма текущая сумма (остаток от деления веса функции на 2^k) равна нулю.

Шаг 1. Рассматриваем последовательно все мономы полинома P_f. Пусть очередной моном есть M ранга r. Если $r \geqslant n - k + 1$, то к текущей сумме добавляем слагаемое 2^{n-r}.

Шаг 2. Рассматриваем все попарные произведения мономов полинома P_f, проводя упрощения по правилу $x \cdot x = x$. Пусть M — очередной полученный таким образом моном ранга r. Если $r \geqslant n - k + 2$, то к текущей сумме добавляем слагаемое $(-2) \cdot 2^{n-r}$.

Шаг 3. Рассматриваем все произведения мономов полинома P_f по три, проводя упрощения по правилу $x \cdot x = x$. Пусть M — очередной полученный таким образом моном ранга r. Если $r \geqslant n - k + 3$, то к текущей сумме добавляем слагаемое $2^2 \cdot 2^{n-r}$.

И так далее до шага k.

Шаг k. Рассматриваем все произведения мономов полинома P_f по k, проводя упрощения по правилу $x \cdot x = x$. Пусть M — очередной полученный таким образом моном ранга r. Если $r = n$, то к текущей сумме добавляем слагаемое 2^{k-1}.

При каждом изменении текущую сумму следует приводить по mod 2^k. В конце работы алгоритма в текущей сумме останется остаток от деления веса булевой функции f, заданной полиномом по mod 2 P_f, на 2^k.

Сложность предложенного алгоритма будет $O(n \cdot l^k)$.

Корректность алгоритма определяется теоремами 3 и 4 со следующими замечаниями:

1) нам достаточно построить все возможные произведения мономов полинома P_f по s при $s \leqslant k$, так как в произведениях мономов полинома P_f по s при $s > k$ коэффициент при них будет иметь вид $a \cdot 2^k$, a — некоторое целое число, то есть 0 по mod 2^k (по теореме 3);

2) получемые новые мономы можно рассматривать до ранга r при $r \geqslant n - k + 1$, так как числовой множитель при новых мономах ранга r

при $r < n - k + 1$ имеет вид $b \cdot 2^k$, b — некоторое целое число, то есть 0 по mod 2^k (по теореме 4).

Теорема 5 доказана. □

Литература

[1] *Жегалкин И. И.* Арифметизация символической логики // Матем. сб. 1928. Т. 35, вып. 3—4.

[2] *Логачёв О. А.*, *Сальников А. А.*, *Ященко В. В.* Булевы функции в теории кодировании и криптологии. М.: МЦНМО, 2004.

[3] *Carlet C.*, *Guillot Ph.* A new representation of Boolean function. Technical report INRIA Project CODES. 1999. P. 1—14.

Обобщенные корреляция и нелинейность высокого порядка булевых функций для описания вероятностных алгебраических атак

С. А. Пометун

Аннотация

Алгебраические атаки — новое интересное направление в криптоанализе. Впервые алгебраические атаки были предложены в 2003 г. в [1], где было дано несколько возможных сценариев атаки. С тех пор исследователями большое внимание было уделено детерминированным сценариям атаки. В этой работе изучаются вероятностные сценарии алгебраической атаки. С этой целью были введены такие понятия булевых функций, как условная корреляция и частичная нелинейность высокого порядка. (усл. корр. определяется как

$$C(g, f \mid f = a) := \Pr(g = f \mid f = a) - \Pr(g \neq f \mid f = a)).$$

Было показано, что как детерминированные, так и вероятностные сценарии атаки могут рассматриваться как одна атака — корреляционная атака высокого порядка, в которой используется условная корреляция вместо обычной. Дан простой критерий уязвимости булевой функции к обоим типам атак в терминах условной корреляции или же частичной нелинейности высокого порядка. Соответственно расширено понятие алгебраического иммунитета булевой функции.

Существуют функции, очень сильно уязвимые к вероятностному сценарию атаки. Вычисления показали, что если бы функция с очень низкой частичной нелинейностью второго порядка использовалась, например, в таком шифраторе как SFINKS [2], то простая вероятностная алгебраическая атака потребовала бы всего лишь 2^{42} операций и около 32 Kb гаммы. Вопрос о связи между нижней границей частичной нелинейности высокого порядка и алгебраическим иммунитетом функции пока остался открытым.

Ключевые слова: шифратор, алгебраическая атака, булева функция, алгебраический иммунитет, условная корреляция, частичная нелинейность высокого порядка.

Введение

Алгебраические атаки — относительно новое и интересное поле для исследований. Впервые они были предложены в 2003 г. [1], где были успешно применены к некоторым потоковым шифраторам, основанным на регистрах сдвига с линейной обратной связью (РСЛОС). На протяжении нескольких лет был написан ряд работ не эту тему, алгебраические атаки были более или менее успешно применены к потоковым шифраторам (основанным на РСЛОС), с памятью, с несколькими выходами, к шифратору E0 (Bluetooth), к блоковым шифраторам [1, 5, 2, 8, 9, 10, 11]. В работе [1] в целом предлагается два типа атаки: детерминированный, и вероятностный. Однако перечисленные выше работы [1, 5, 2, 8, 9, 10, 11] имеют дело лишь детерминированными сценариями. И это действительно дало ряд хороших с практической точки зрения результатов.

С другой стороны есть другой тип криптоаналитических атак — так называемая корреляционная атака высокого порядка [5]. Эта атака как раз дает уравнения, истинные лишь с определенной вероятностью. При этом примечательно, что работа [1] является логическим продолжением работы [5].

В данной работе исследуются вероятностные сценарии алгебраической атаки. Показано, что детерминированные и вероятностные сценарии могут быть представлены как одна атака — как раз корреляционная атака высокого порядка, но использующая условную корреляцию вместо обычной. Детерминированные сценарии являются частным случаем, когда точность аппроксимации равна единице. Также сделаны определенные шаги в исследовании вероятностных сценариев (вероятностной алгебраической атаки). В частности дан четкий критерий уязвимости функции к атаке, показано существование сильно уязвимых функций, дан пример расчета сложности простого варианта атаки.

Структура статьи. Первый раздел содержит краткое описание основной идеи статьи. Во втором разделе получены основные результаты по унификации описания сценариев алгебраической атаки. В третьем разделе вводится и рассматривается частичная нелинейность высокого порядка булевых функций. В четвертом разделе приводится пример класса функций, уязвимых к вероятностной алгебраической атаке, и дается оценка сложности атаки, в случае, если бы одна из таких функций использовалась в шифраторе SFINKS. Наконец последний раздел содержит замечания и подбивает итоги.

1. Основная идея — кратко

Основная идея алгебраической атаки состоит в понижении степени уравнений, описывающих функционирование шифратора, где неизвестными являются биты ключа. Уравнения задаются как функция от некоторой линейной комбинации ключа. Понижение степени производится путем домножения функции на другую, специально подобранную функцию. Например, $f(x) = a \;\Rightarrow\; f(x)\,g(x) = a\,g(x)$. В этой работе предлагается другой взгляд на этот же прием: $f(x) = a \;\Rightarrow\; h(x) = a$, где $h(x)$ имеет более низкую степень. Очевидно, $h(x)$ совпадает с $f(x)$ на подмножестве аргументов, где $f(x) = a$. Следовательно, условная корреляция между $h(x)$ и $f(x)$ равна $C(h,\, f \mid f = a) = 1$. Функции $h(x)$, такие что $C(h,\, f \mid f = a) \geqslant 1 - \epsilon$, — это как раз те функции, которые получаются при применении вероятностного сценария, предложенного Куртуа в [Cou03]. В соответствии с условной корреляцией вводится понятие частичной нелинейности r-го порядка функции $f(x)$ — это (удвоенное) расстояние от $f(x)$ до класса функций степени не выше r, которое считается на подмножестве аргументов, где $f(x) = a$. Очевидно, что это существенно усиливает уже известную корреляционную атаку высокого порядка.

2. Условная корреляция

В этом разделе вводится понятие условной корреляции и аппроксимаций булевых функций в терминах этой корреляции. Показано, что аннигиляторы булевых функций можно представить как частный случай таких аппроксимаций. Также с помощью введенной корреляции, возможно впервые, исследованы вероятностные сценарии алгебраической атаки, введенные в [1].

Определение 3. Обозначим через B_n множество булевых функций $f\colon \mathrm{GF}(2)^n \to \mathrm{GF}(2)$, $n \geqslant 0$. Введем множества $1_f = \{x \in \mathrm{GF}(2)^n \mid f(x) = 1\}$ и $0_f = \{x \in \mathrm{GF}(2)^n \mid f(x) = 0\}$ аргументов, на которых функция принимает значение 1 и 0 соответственно.

Определение 4. Обозначим через $|f|$ количество аргументов, на которых функция не равняется нулю (вес булевой функции $f \in B_n$): $|f| := |1_f|$. Также введем понятие частичного веса на подмножестве X, $|f|_X := |1_f \cap X|$, $X \subset \mathrm{GF}(2)^n$.

Определение 5. Пусть $f,\ g \in B_n$ — булевы функции. Корреляцией между f и g называют разность вероятностей совпадения и несовпадения f и g: $C(f,\ g) := \Pr(f = g) - \Pr(f \neq g) = |f + g + 1|/2^n - |f + g|/2^n$.

Определение 6. Аннигилятором функции $f \in B_n$ называют произвольную функцию $h \in B_n$, такую, что $f \cdot h \equiv 0$. Множество всех анни-

гиляторов f обозначим $\mathrm{An}(f) := \{h \in B_n | f \cdot h \equiv 0\}$ Функция h является аннигилятором f тогда и только тогда, когда $1_f \subset 0_h$ [13].

Определение 7. Алгебраическим иммунитетом $\mathrm{AI}(f)$ функции $f \in B_n$ называют минимальную степень аннигилятора среди всех ненулевых аннигиляторов f и $f+1$: $\mathrm{AI}(f) := \min\{\deg(h) | h \in \mathrm{An}(f) \cup \mathrm{An}(f+1)\}$.

Под степенью функции $h \in B_n$ понимается степень многочлена Жегалкина, которым представляется h. Чем ниже алгебраический иммунитет функции, тем более она уязвима к алгебраическим атакам.

Введем новое понятие — условную корреляцию булевых функций:

Определение 8. f, $g \in B_n$ — булевы функции, $a \in \mathrm{GF}(2)$. Условной корреляцией между функциями f и g при условии $f = a$ назовем такую величину:

$$\begin{aligned} C(g, f \mid f = a) &:= \Pr(g = f \mid f = a) - \Pr(g \neq f \mid f = a) \\ &= \Pr(g = a \mid f = a) - \Pr(g \neq a \mid f = a) \\ &= \frac{|a_g \cap a_f|}{|a_f|} - \frac{|\overline{a}_g \cap a_f|}{|a_f|} = \frac{|a_g|_{a_f} - |\overline{a}_g|_{a_f}}{|a_f|}, \end{aligned} \tag{1}$$

где $\overline{a} = a + 1 \in \mathrm{GF}(2)$ при равновероятной f: $|a_f| = 2^{n-1}$. Если $a_f = \emptyset$, то $C(g, f \mid f = a) := 1 \ \forall\, g \in B_n$.

Фактически было введено две корреляции — на подмножестве аргументов функции f $0_f \subset \mathrm{GF}(2)^n$, где f равняется нулю, и на подмножестве аргументов $1_f \subset \mathrm{GF}(2)^n$, где f равняется единице. Их можно также обозначать $C_0(g, f)$ и $C_1(g, f)$. Например, если имеет место равенство $C_0(g, f) = 1$, то это означает, что f и g совпадают на множестве нулей f (более точно, обе функции там равны нулю), или другими словами, имеет место импликация $f = 0 \ \Rightarrow \ g = 0$.

Лемма 1. *Пусть f, $h \in B_n$, f — равновероятна, $a \in \mathrm{GF}(2)$, $C_a(h, f) = 1 - \epsilon$. Тогда количество несовпадений значений функций h и f на множестве аргументов, где $f(x) = a$ равняется $|h + f|_{a_f} = \epsilon 2^{n-2}$.*

Доказательство.

$$\begin{aligned} C_a(h, f) &= \Pr(h = f \mid f = a) - \Pr(h \neq f \mid f = a) \\ &= 1 - 2\Pr(h \neq f \mid f = a) = 1 - 2\frac{|h+f|_{a_f}}{|a_f|} = 1 - 2\frac{|h+f|_{a_f}}{2^{n-1}} \\ &= 1 - 2^{-n+2}|h+f|_{a_f} = 1 - \epsilon \ \Rightarrow \ |h+f|_{a_f} = \epsilon 2^{n-2}. \end{aligned}$$

□

Пусть задано две булевы функции f, $g \in B_n$, $a \in \mathrm{GF}(2)$, и их корреляция при условии $f = a$ равняется $C_a(g, f) = 1 - \epsilon$. Функцию g можно назвать аппроксимацией (приближением) функции f в терминах корреляции C_a с точностью $1 - \epsilon$. Аппроксимацию с точностью 1 будем называть точной.

Определение 9. Пусть $f \in B_n$, $a \in \mathrm{GF}(2)$. Обозначим через $R_a(f, \epsilon) := \{g \in B_n \mid C(g, f \mid f = a) \geqslant 1 - \epsilon\}$ множество всех приближений в терминах C_a функции f с точностью не меньше, чем $1 - \epsilon$. Также будем обозначать $R(f, \epsilon) := R_0(f, \epsilon) \cup R_1(f, \epsilon)$.

Пусть $G \subset B_n$, $h \in B_n$. Будем обозначать $G + g := \{g + h \mid g \in G\}$.

Утверждение 1. *Пусть $f \in B_n$. Существует простая биекция между множествами аннигиляторов $\mathrm{An}(f)$, $\mathrm{An}(f+1) \subset B_n$ и множествами $R_1(f, 0)$, $R_0(f, 0) \subset B_n$ точных аппроксимаций f в терминах условной корреляции. Более точно*, $\mathrm{An}(f) = R_1(f, 0) + 1$, $\mathrm{An}(f+1) = R_0(f, 0)$.

Доказательство. 1. $\mathrm{An}(f) = R_1(f, 0) + 1$:

$$\begin{aligned} h \in \mathrm{An}(f) &\Leftrightarrow [f \cdot h \equiv 0] \Leftrightarrow [\forall\, x : f(x) = 1 \ \Rightarrow \ h(x) = 0] \\ &\Leftrightarrow [\forall\, x : f(x) = 1 \ \Rightarrow \ h(x) + 1 = 1] \\ \Leftrightarrow [\Pr(h + 1 = 1 \mid f = 1) = 1] &\Leftrightarrow [C(h+1, f \mid f = 1) = 1] \\ &\Leftrightarrow [h + 1 \in R_1(f, 0)] \Leftrightarrow h \in R_1(f, 0) + 1. \end{aligned}$$

2. $\mathrm{An}(f+1) = R_0(f, 0)$ — аналогично. □

Следствие 1. $\mathrm{An}(f + a + 1) = R_a(f, 0) + a$.

Следствие 2. $\min\{\deg(h) | h \in \mathrm{An}(f + a + 1)\} = \min\{\deg(h) | h \in R_a(f, 0)\}$.

Итак, алгебраический иммунитет можно задать и через точные аппроксимации:

$$\begin{aligned} \mathrm{AI}(f) &= \min(\deg(h) \mid h \in \mathrm{An}(f) \cup \mathrm{An}(f+1)\} = \\ &= \min(\deg(h) \mid h \in R_1(f, 0) \cup R_0(f, 0)\} = \\ &= \min\{\deg(h) \mid h \in R(f, 0)\}. \end{aligned} \tag{2}$$

Теперь основную идею алгебраической атаки — понижение степени функции f — можно видеть более прозрачно. Пусть h — функция низкой степени, и $h \in R_a(f, 0)$ для некоторого $a \in \mathrm{GF}(2)$. Тогда:

$$\begin{aligned} h \in R_a(f, 0) &\Leftrightarrow [C_a(h, f) = 1] \\ \Leftrightarrow [\Pr(h = a \mid f = a) = 1] &\Leftrightarrow [f = a \ \Rightarrow \ h = a]. \end{aligned} \tag{3}$$

Т. е. уравнение $f(x) = a$ заменяется уравнением $h(x) = a$. То же самое можно было видеть и с аннигиляторами:

$$f \cdot h \equiv 0 \Leftrightarrow [f = 1 \ \Rightarrow \ h = 0],\ (f+1)h \equiv 0 \Leftrightarrow [f = 0 \ \Rightarrow \ h = 0]. \tag{4}$$

Но введенное описание допускает простое обобщение на случаи неточных приближений, т. е. случаи, когда $h \in R_a(f, \epsilon)$, где $\epsilon > 0$ —

маленькое, но не нулевое число. Тогда будет иметь место:

$$\begin{gathered} h \in R_a(f,\,\epsilon) \Leftrightarrow [C_a(h,\,f) \geqslant 1-\epsilon] \\ \Leftrightarrow [\Pr(h=a \mid f=a) - \Pr(h\neq a \mid f=a) \geqslant 1-\epsilon] \\ \Leftrightarrow [2\Pr(h=a \mid f=a) - 1 \geqslant 1-\epsilon] \\ \Leftrightarrow [\Pr(h=a \mid f=a) \geqslant 1-\epsilon/2] \\ \Leftrightarrow [f=a \;\Rightarrow\; h=a,\;\; \Pr \geqslant 1-\epsilon/2]. \end{gathered} \tag{5}$$

Оказывается, что именно так описывается вероятностный сценарий S4 алгебраической атаки, теоретическую возможность которого показал Куртуа [1]. Напомним в целом этот сценарий. Уравнение $f(x)=a$, степень которого нужно понизить, умножается на функцию g. Полученное уравнение $[f(x)g(x)=a\,g(x)] \equiv [t(x)=0]$ (которое уже имеет более низкую степень, чем исходное) с высокой точностью приближается уравнением $h(x)=0$ еще более низкой степени. Целью являются нахождения функции h, — хотя уравнения вида $h(x)=0$ и будут ошибочны с небольшой вероятностью ϵ, их низкая степень дает какую-то надежду на возможность их решения. Известно [3], что функция t является аннигилятором $f+a+1$. (действительно, $[f(x)g(x)=a\,g(x)] \Leftrightarrow [(f+a)g=0]$, но $(f+a+1)(f+a)g \equiv 0$, т. е. $(f+a)g$ есть аннигилятор $(f+a+1)$). Поскольку $\mathrm{An}(f+a+1)+a=R_a(f,\,0)$, то $t+a$ является точным приближением f в терминах C_a, т. е. $C(t+a,\,f \mid f=a)=1$. Для простоты мы заменим функции $t+a$ и $h+a$ на t и h (фактически это означает, что уравнение $t(x)=a$ приближается уравнением $h(x)=a$). Корреляция между t и h от этого не изменится. Теперь сформулируем

Утверждение 2. *Пусть*

1) $f,\, h,\, t \in B_n$, f — *равновероятна*;
2) $C(t,\,f \mid f=a)=1$;
3) $C(h,\,t)=1-\epsilon$.

Тогда $h \in R_a(f,\,2\epsilon)$. *Более точно* $1-2\epsilon \leqslant C_a(h,\,f) \leqslant 1$ *и при условии* $\epsilon \leqslant 1$ *оба равенства достижимы.*

Доказательство. Из условия 3 вытекает, что $0 \leqslant |h+t|_{0_f} \leqslant \epsilon 2^{n-1}$ и $0 \leqslant |h+t|_{1_f} \leqslant \epsilon 2^{n-1}$. Действительно, $C(h,\,t)=1-2\Pr(h\neq t)=1-2(|h+t|/2^n)=1-\epsilon \;\Rightarrow\; |h+t|=\epsilon 2^{n-1}$, но $|h+t|=|h+t|_{0_f}+|h+t|_{1_f}$, откуда и вытекают необходимые неравенства. Если f — равновероятна и $\epsilon \leqslant 1$, то по отдельности $|h+t|_{0_f}$ и $|h+t|_{1_f}$ могут принимать значения от 0 до $\epsilon 2^{n-1}$ включительно. Условную корреляцию $C_a(h,\,f)$ можно выразить через количество точек несовпадений функций h и f на множестве

a-значений f:

$$\begin{aligned} C_a(h,\,f) &= \Pr(h=f \mid f=a) - \Pr(h\neq f \mid f=a) \\ &= 1-2\Pr(h\neq f \mid f=a) = 1-2\frac{|h+f|_{a_f}}{|a_f|} = 1-\frac{|h+f|_{a_f}}{2^{n-2}}. \end{aligned}$$

В силу условия 2 утверждения

$$C_a(h,\,f) = 1-\frac{|h+f|_{a_f}}{2^{n-2}} = 1-\frac{|h+t|_{a_f}}{2^{n-2}} = 1-2^{-n+2}|h+t|_{a_f}.$$

Теперь, с учетом выведенных выше неравенств имеем

$$1-2\epsilon \leqslant 1-2^{-n+2}|h+t|_{a_f} = C_a(h,\,f) \leqslant 1,$$

что и требовалось доказать. □

Итак, сценарий S4 сводится к поиску аппроксимаций в терминах условной корреляции.

Чтобы численно описать наименьшую степень среди функций $h \in R_a(f,\,2\epsilon)$, можно расширить понятие алгебраического иммунитета:

$$\begin{aligned} \mathrm{AI}(f,\,\epsilon) &= \min\{\deg(h) \mid h \in R_1(f,\,2\epsilon) \cup R_0(f,\,2\epsilon)\} = \\ &= \min\{\deg(h) \mid h \in R(f,\,2\epsilon)\}. \end{aligned} \tag{6}$$

Это расширение согласуется с уже существующим определением алгебраического иммунитета:

$$\begin{aligned} \mathrm{AI}(f,\,0) &= \min\{\deg(h) \mid h \in R(f,\,0)\} = \\ &= \min\{\deg(h) \mid h \in R_0(f,\,0) \cup R_1(f,\,0)\} = \\ &= \min\{\deg(h) \mid h \in \mathrm{An}(f+1) \cup \{\mathrm{An}(f)+1\}\} = \\ &= \min\{\deg(h) \mid h \in \mathrm{An}(f+1) \cup \mathrm{An}(f)\} = \mathrm{AI}(f), \end{aligned}$$

$\mathrm{AI}(f,\,\epsilon)$ является минимальной степенью уравнений, которые можно написать для функции f с вероятностью ошибки не больше, чем ϵ. С ростом ϵ $\mathrm{AI}(f,\,\epsilon)$ уменьшается единичными скачками.

Таким образом, мы доказали, что аппроксимация в терминах условной корреляции одновременно описывает детерминированные и вероятностные сценарии алгебраической атаки, предложенные в [1].

3. Частичная нелинейность высокого порядка булевых функций

Вероятностная алгебраическая атака является корреляционной атакой высокого порядка, использующей введенную выше корреляцию. Для обычной корреляционной атаки высокого порядка важнейшим параметром является нелинейность высокого порядка булевой функции [5], [6].

Нелинейность r-го порядка функции f можно задать также через корреляцию соотношением:

$$\mathrm{nl}_r(f) = 2^{n-1}(1 - \max\{C(h,\ f) \mid \deg(h) \leqslant r\}). \qquad (7)$$

В данной работе предлагается обобщение этого понятия — вводится частичная нелинейность r-го порядка:

$$\mathrm{nlp}_r(f) = 2^{n-1}(1 - \max\{C_0(h,\ f),\ C_1(h,\ f) \mid \deg(h) \leqslant r\}). \qquad (8)$$

Если обычная нелинейность r-го порядка показывает минимальное расстояние от f до класса функций степени не выше r, то частичная нелинейность дает удвоенное минимальное расстояние от f до этого же класса на подмножестве аргументов, где $f(x) = 0$ либо $f(x) = 1$. Автором доказан ряд утверждений о частичной нелинейности для равновероятной функции f:

1. Функции с низкой частичной нелинейностью так точно (в смысле вероятности истинности уравнений) уязвимы к вероятностной алгебраической атаке, как функции с обычной нелинейностью уязвимы к корреляционной атаке высокого порядка (у функции, построенной в предыдущем разделе, частичная нелинейность второго порядка $\mathrm{nlp}_2(f) = 2$).
2. $\forall\, r \geqslant 2\ \ \mathrm{nlp}_r(f) \leqslant \mathrm{nl}_r(f)$ (как правило, $\mathrm{nlp}_r(f)$ существенно меньше, чем $\mathrm{nl}_r(f)$, это показывает, что вероятностная алгебраическая атака эффективней, чем корреляционная атака высокого порядка).
3. $\mathrm{nlp}_{\mathrm{AI}(f)}(f) = 0$ (это значит, что алгебраическая атака — частный (детерминированный) случай вероятностной алгебраической атаки).
4. $\mathrm{nlp}_1(f) = \mathrm{nl}_1(f) \equiv \mathrm{nl}(f)$ (вытекает из того, что $C_0(g,\ f) = C_1(g,\ f) = C(g,\ f)$ для линейных g. Данное равенство показывает, что в случае аппроксимации линейными функциями (обычная корреляционная атака) частичная нелинейность не дает преимуществ. Это объясняет, почему алгебраические атаки «работают» только начиная со степени аппроксимаций $r = 2$).

Ясно, что частичная нелинейность является существенным усилением обычной.

4. Простой пример вероятностной алгебраической атаки и оценка ее сложности

Таким образом, получен критерий стойкости усложняющей функции f шифратора к вероятностной алгебраической атаке: не должно существовать достаточно точных низкостепенных аппроксимаций f в терминах условной корреляции C_0 или C_1; или же функция f должна иметь достаточно высокую частичную нелинейность второго, третьего и т. д. порядков; или, еще другими словами, алгебраический иммунитет функции $\mathrm{AI}(f,\ \epsilon)$ должен быть достаточно высоким для очень маленьких ϵ. (эти критерии включают в себя и детерминированный случай атаки). Можно также показать существование функций, сильно уязвимых к вероятностной алгебраической атаке. Например, пусть $f \in B_n$ — булева функция, и

$$f(x) = x_1x_2 + x_1x_2 \ldots x_n + h(x)(x_1x_2 + 1) \qquad (9)$$

где $h \in B_n$ — произвольная функция, обеспечивающая равновероятность f Можно доказать, что такие функции точно существуют для $n \geqslant 2$ и что $\mathrm{nlp}_{0,2}(f) = 2$ ($C_0(g,\ f) = 1 - 1/2^{n-2}$, где $g(x) = x_1x_2$). Опишем вариант возможной атаки. Предположим, такая функция используется как фильтрующая функция линейного регистра сдвига длиной 256 битов и количеством точек съема $n = 17$ (именно такие параметры имеет шифратор SFINKS [4]). Поскольку $\mathrm{nlp}_{0,2}(f) = 2$ и $C_0(g,\ f) = 1 - 1/2^{n-2}$ для $g(x) = x_1x_2$, то уравнения вида $f(x) = 0$ можно заменить уравнениями второй степени $x_1x_2 = 0$, причем они будет выполняться с вероятностью $1/2^{n-1}$ (для всех 2^{n-1} аргументов, на которых $f(x) = 0$, кроме $x = x_1,\ x_2,\ \ldots,\ x_n = 1,\ 1,\ \ldots,\ 1$). $256 \cdot 257/2 \approx 2^{15}$ истинных уравнений хватило бы для решения полученной квадратичной системы методом линеаризации. Так как вероятность ложности одного уравнения равна $1/2^{n-1} = 1/2^{16}$, то набор истинных уравнений удастся подобрать почти с первого раза. Сложность атаки при наличии $2^{15} = 32$ Kb гаммы составила бы около $(2^{15})^{\log_2 7} \approx 2^{42}$ операций.

5. Замечания и выводы

Вычислительные эксперименты по нахождению уязвимых функций показали интересный факт: если частичная нелинейность второго порядка булевой функции $f \in B_n$ равняется $\mathrm{nlp}_2(f) = 2$, то ее алгебраический иммунитет $\mathrm{AI}(f) \leqslant 3$ (нам не удалось найти такую f, что $\mathrm{nlp}_2(f) = 2$ и $\mathrm{AI}(f) = 4$ для $n = 8$). Конечно, должна существовать связь между алгебраическим иммунитетом функции и ее минимальной частичной нелинейностью высокого порядка. По крайней мере, аналогичная связь между алгебраическим иммунитетом и нижней границей обычной нелинейностью высокого порядка исследовалась в работах [7] и [12]. Можно предположить, что высокого алгебраического иммунитета будет достаточно, чтобы предотвратить существование эффективной вероятностной алгебраической атаки. Этот вопрос пока что остается открытым.

Однако для функций с очень маленькой частичной нелинейностью второго порядка (как в приведенном выше примере), вероятностная алгебраическая атака все же эффективней, чем эксплуатирующая низкий алгебраический иммунитет детерминированная.

Итак, в работе исследовались алгебраические атаки. Были введены понятия условной корреляции и частичной нелинейности булевых функций, также расширено понятия алгебраического иммунитета. Это дало возможность унифицировать описание детерминированных и вероятностных сценариев алгебраических атак, предложенных в [1], при этом вероятностные сценарии исследовались впервые. Был дан простой критерий уязвимости впечатлительности функции к вероятностному сценарию атаки в терминах условной корреляции и частичной нелинейности высокого порядка. Также показано существование функций, сильно уязвимых к вероятностному сценарию атаки, и что для некоторых усложняющих функций такой сценарий является наиболее эффективным.

Литература

[1] *Courtois N.*, *Meier W.* Algebraic Attacks on Stream Ciphers with Linear Feedback. Eurocrypt 2003, Warsaw, Poland, Springer, LNCS 2656. P. 345–359. An extended version is available at `http://www.minrank. org/toyolili.pdf`.

[2] *Nicolas T.* Courtois. Cryptanalysis of Sfinks. `http://eprint.iacr.org/2005/243`.

[3] *Meier W.*, *Pasalic E.*, *Carlet C.* Algebraic attacks and decomposition of Boolean functions. Eurocrypt 2004. Springer, LNCS 3027. 2004. P. 474–491.

[4] *Braeken A.*, *Lano J.*, *Mentens N.*, *Preneel B.*, *Verbauwhede Ingrid.* Sfinks specification and source code. April 2005. Available on ECRYPT Stream Cipher Project page `http://www.ecrypt.eu.org/stream/sfinks.html`.

[5] *Courtois N.* Higher Order Correlation Attacks, XL Algorithm and Cryptanalysis of Toyocrypt. `http://eprint.iacr.org/2002/087`.

[6] *Carlet C.* On the higher order nonlinearities of algebraic immune Boolean functions. CRYPTO 2006, Springer, LNCS 4117, 2006. P. 584–601.

[7] *Kolokotronis N.*, *Limniotis K.*, *Kalouptsidis N.* Best Quadratic Approximations of Cubic Boolean Functions. `http://eprint.iacr.org/ 2007/037`.

[8] *Courtois N.* Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. Crypto 2003. Springer, LNCS 2729. P. 177–194.

[9] *Armknecht F.* A Linearization Attack on the Bluetooth Key Stream Generator. Available at `http://eprint.iacr.org/2002/191`. 13 December 2002.

[10] *Armknecht F.*, *Krause M.* Algebraic attacks on Combiners with Memory. Crypto 2003, Springer, LNCS 2729, 2003. P. 162–176.

[11] *Courtois N.* Algebraic Attacks on Combiners with Memory and Several Outputs. Cryptology ePrint Archive, Report 2003/125, 2003. `http://eprint.iacr.org/2003/125`.

[12] *Carlet C.* A lower bound on the higher order nonlinearity of algebraic immune functions. `http://eprint.iacr.org/2005/469`.

[13] *Armknecht F.* On the Existence of Low"=Degree Equations for Algebraic Attacks. `http://eprint.iacr.org/2004/185`.

О функциональном задании латинских квадратов над абелевыми группами

В. А. Носов, А. Е. Панкратьев

Латинские квадраты представляют собой важный объект для криптографии и защиты информации. Согласно теории Шеннона [1], шифры, основанные на латинских квадратах, являются так называемыми совершенными шифрами. Для практического использования представляют интерес функциональные способы задания больших латинских квадратов, где элемент квадрата определяется с помощью функции от номера строки и номера столбца. При этом нет необходимости хранить в памяти шифрующего устройства весь квадрат целиком; достаточно только задать соответствующую функцию.

Напомним, что латинским квадратом L порядка k называется матрица размера $k \times k$, заполненная элементами некоторого множества Ω, $|\Omega| = k$, таким образом, что в каждой ее строке и в каждом столбце все элементы различны [2]. Примером латинского квадрата является таблица Кэли произвольной конечной группы. В коммутативном случае при аддитивной записи операции, латинский квадрат задается формулой $L(x, y) = x + y$, где $L(x, y)$ — элемент квадрата, стоящий на пересечении строки и столбца с «номерами» x и y, соответственно, $x, y \in \Omega = \mathbb{Z}_k$, и сложение понимается как сложение по модулю k. В данной работе изучаются свойства функций $f(x, y)\colon \Omega \times \Omega \to \Omega$, задающих латинские квадраты при помощи формулы $L(x, y) = x + y + f(x, y)$ в том случае, когда Ω является абелевой группой.

Рассмотрим прямое произведение нескольких (n) копий конечной абелевой группы G:

$$H = G^n = \underbrace{G \times G \times \cdots \times G}_{n}. \tag{1}$$

Над группой H зададим латинский квадрат L порядка $|H| = |G|^n$ следующим образом. Сначала «проиндексируем» строки и столбцы квадрата L элементами группы H. Пусть $x = (x_1, x_2, \ldots, x_n)$ и $y = (y_1, y_2, \ldots, y_n)$ суть элементы группы H. Элемент $L(x, y) = (z_1, z_2, \ldots, z_n)$ квадрата L, находящийся на пересечении строки x и столбца y, определим формулами

$$\begin{aligned} z_1 &= x_1 + y_1 + f_1(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) \\ z_2 &= x_2 + y_2 + f_2(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ z_n &= x_n + y_n + f_n(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)). \end{aligned} \tag{2}$$

Здесь $p_1, p_2, \ldots, p_n$ — функции $G \times G \to G$; $f_1, f_2, \ldots, f_n$ являются функциями $G^n \to G$.

Будем говорить, что функции $f_1, f_2, \ldots, f_n$ от переменных $p_1, p_2, \ldots, p_n$ образуют *правильное* семейство [3, 4, 5], если для любых различных наборов $p' = (p'_1, p'_2, \ldots, p'_n)$ и $p'' = (p''_1, p''_2, \ldots, p''_n)$ найдется индекс α, $1 \leqslant \alpha \leqslant n$, такой, что $p'_\alpha \neq p''_\alpha$ и $f_\alpha(p') = f_\alpha(p'')$.

Теорема 1 ([5]). *Формулы* (2) *определяют латинский квадрат для любых функций* $p_1, p_2, \ldots, p_n$ *тогда и только тогда, когда семейство функций* $\{f_1, f_2, \ldots, f_n\}$ *является правильным.*

Замечание 1. Теорема 1 позволяет при помощи любого правильного семейства функций $\{f_1, f_2, \ldots, f_n\}$ получать различные латинские квадраты, варьируя систему функций-параметров $p_1, p_1, \ldots, p_n$. Нетрудно также видеть, что систему параметров можно выбрать $|H|^{n|H|}$ способами.

Понятие правильности семейства функций тесно связано с понятием регулярности, т. е. со свойством семейства функций осуществлять биективное отображение на множестве всех входных наборов.

Теорема 2 ([5]). *Функции* $f_1, f_2, \ldots, f_n$ *образуют правильное семейство тогда и только тогда, когда для любого набора функций* $\psi_1, \psi_2, \ldots, \psi_n$ (*здесь* $\psi_i\colon G \to G$) *семейство функций* $\{x_1 + \psi_1(f_1(x)), x_2 + \psi_2(f_2(x)), \ldots, x_n + \psi_n(f_n(x))\}$ *является регулярным.*

Таким образом, теорема 2 позволяет проверять правильность семейства функций путем применения критериев регулярности к ассоциированным семействам функций. Для случая $G = \mathbb{Z}_p$, где p — простое, существуют критерии регулярности, основанные на изучении свойств определенных полиномов.

Для широкого класса функций проверку правильности семейства $F = \{f_1, f_2, \ldots, f_n\}$ можно свести к проверке отсутствия циклов в ориентированном *графе существенной зависимости* $G_F = (V, E)$ семейства F, который определяется на множестве вершин $V = \{1, 2, \ldots, n\}$ по правилу

$$(i, j) \in E \Leftrightarrow f_j \text{ существенно зависит от } x_i.$$

Для фиксированного элемента $g \in G$ функцию $f(x_1, \ldots, x_n)$ вида $G^n \to G$ назовем g-функцией, если для любой переменной x_i, от которой она зависит существенным образом, выполнено условие

$$f(g, \ldots, g, x_i, g, \ldots, g) \neq \text{const}.$$

Заметим, что константы являются g-функциями для любого $g \in G$.

Замечание 2. Можно показать, что при $|G| \to \infty$, $|G|/n \to \infty$, доля g-функций среди всех функций n переменных стремится к 1.

Теорема 3. *Семейство g-функций $F = \{f_1, f_2, \ldots, f_n\}$ правильно в том и только том случае, если его граф существенной зависимости G_F не содержит циклов.*

С другой стороны, за рамками широкого класса g-функций существуют правильные семейства с богатой цикловой структурой в графе существенной зависимости.

Будем говорить, что функции f и g вида $G^n \to G$ *ортогональны*, если для любого $x \in G^n$ либо $f(x) = 0$ либо $g(x) = 0$.

Лемма 1. *Пусть семейство $F = \{f_1, f_2, \ldots, f_n\}$ попарно ортогональных функций таково, что для любого i, $1 \leqslant i \leqslant n$, функция f_i не зависит от x_i существенным образом. Тогда семейство F является правильным.*

Приведем пример семейства $F = \{f_1, f_2, \ldots, f_n\}$ попарно ортогональных функций, удовлетворяющего условию леммы и такого, что граф существенной зависимости G_F является полным (разумеется, за исключением петель (i, i)).

Возьмем произвольное собственное подмножество $L \subset H$, $\emptyset \neq L \neq H$, и рассмотрим соответствующую характеристическую функцию вместе с ее отрицанием:

$$L(x) = \begin{cases} 1, & x \in L, \\ 0, & x \notin L; \end{cases} \qquad \overline{L}(x) = \begin{cases} 0, & x \in L, \\ 1, & x \notin L. \end{cases}$$

Определим семейство функций $F = \{f_1, f_2, \ldots, f_n\}$ формулами

$$\begin{aligned} f_1 &= \overline{L}(x_2)L(x_3)\cdots L(x_{n-1})L(x_n)\,g_1 \\ f_2 &= \overline{L}(x_3)L(x_4)\cdots L(x_n)L(x_1)\,g_2 \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ f_n &= \overline{L}(x_1)L(x_2)\cdots L(x_{n-2})L(x_{n-1})\,g_n. \end{aligned}$$

Здесь $g_1, g_2, \ldots, g_n$ суть произвольные элементы группы G, а коэффициенты перед ними суть произведения характеристических функций.

Нетрудно видеть, что полученное семейство $F = \{f_1, f_2, \ldots, f_n\}$, являющееся правильным в силу леммы, имеет полный граф существенной зависимости G_F.

В итоге, для любого фиксированного числа переменных доля функций, для которых правильность семейств равносильна отсутствию циклов в графах существенной зависимости, стремится к 1 с ростом порядка группы. С другой стороны, приведено простое достаточное условие построения правильных семейств функций, графы которых имеют богатую цикловую структуру.

Таким образом, в работе предложен способ построения параметрических семейств больших латинских квадратов, зависящих от большого числа параметров (ключей). Применение таких семейств в системах защиты информации позволит существенно повысить уровень информационной безопасности.

Литература

[1] *Shannon C.* Communication Theory of Secrecy Systems // Bell System Techn. J. 1949. Vol. 28, № 4. P. 656—715. [Имеется перевод: *Шеннон К.* Теория связи в секретных системах // К. Шеннон. Работы по теории информации и кибернетики. М., 1963. С. 333—369.].

[2] *Dénes J., Keedwell A.* Latin Squares and their Applications. Budapest, 1974.

[3] *Носов В. А.* О построении классов латинских квадратов в булевой базе данных // Интеллектуальные системы. 1999. Т. 4, вып. 3—4. С. 307—320.

[4] *Носов В. А.* Построение параметрического семейства латинских квадратов в векторной базе данных // Интеллектуальные системы. 2004. Т. 8, вып. 1—4. С. 517—528.

[5] *Носов В. А., Панкратьев А. Е.* Латинские квадраты над абелевыми группами // Фундаментальная и прикладная математика. 2006. Т. 12, вып. 3. С. 65—71.

S-Box Design Using Random Walk Based Algorithm

S. Kazmi, N. Ikram

Annotation

Substitution boxes (S-Boxes) are important in the design of algorithms. Design of efficient and cryptographically strong S-boxes have always been an area of active research. In this paper we introduce a new cryptographic method for generating substitution boxes based on Graph Theory, which is efficient and has been analyzed to possess good cryptographic properties such as Differential Probability, Linear Probability, Algebraic Degree, Balance and particularly higher „Best Linear Approximation". The algorithm is based on rapidly mixing random walks. We show that an S-Box that meets the criterion of random walk is invulnerable to the cryptanalysis because of satisfying cryptographic properties alongwith randomness.

1. Introduction

S-h Boxes are important in the design of secure symmetric-key algorithms. These are designed prudently with high resistance against many statistical and cryptographic attacks as well as with low implementation cost on several platforms. In this paper, we present a new method on the design of S-Box using the basic concepts of graph theory. The study of random graphs started with the influential work of Erdős and Renyi in the 1950s and 1960s [1]. Random graph theory has turned into a prop of modern Discrete Mathematics. With particular focus on cryptographic and statistical properties, we present a design criterion for cryptanalysis-resistant S-Box using scaled up Random Walk based Algorithm (RWA). The design analysis characteristically involves analysis of simple statistical parameters such as path length, mixing time, degrees distribution and graph distribution. The random walk over its finite state space includes different steps iterated in the main set of commands of the RWA. This can be modeled by a graph G with N $(=64)$ nodes, and edges connecting nodes that differ by a transposition.

2. Random Walk based Algorithm (RWA)

In this section we describe the RWA and its basic constituent components. The prescribed method uses a small-sized (4×4) S-Box possessing balance, Minimal Differential Probability (MDP) and Minimal Linear Probability (MLP) to generate a large-sized (8×8) S-Box which is generated efficiently, utilizes less memory and has improved „Best Linear Approximation (BLA)" with acceptable „Differential Probability (DP)" and „Linear Probability (LP)". Design of S-box with good BLAs has gained importance as S-Box of Advanced Encryption Standard (AES) does not possess good BLAs for two Boolean functions i.e. $f_5 = 1 + X_2$ and $f_6 = 1 + X_1$. In our RWA based S-Box design, it is well improved for each Boolean function f_i $(0 \leqslant i \leqslant 7)$. It also satisfies balance and possesses reasonably good DP and LP.

RWA is presented as follows: $\ggg a$ denotes the right cyclic shift by a bits, addition is modulo 2^4, S is a randomly chosen 4×4 S-Box with $\mathrm{MDP} = 2^{-2}$, $\mathrm{MLP} = 2^{-2}$ and Balance containing values such as $\{S\} = \{D, 0, 9, 5, 3, 6, 1, B, 2, 4, A, 7, F, 8, E, C\}$. The structure has been designed to generate good and efficient S-Box which is later analyzed to possess good cryptographic properties. This design is memory efficient, making it suitable for implementation on smart cards and similar tokens.

```
Input: 8-bit input state X
Output: 8-bit output state Y
for i = 0 to 255
  X = i
  X[0] ← (X ≫ 4) & 0xf
  X[1] ← X & 0xf
  for j = 0 to 1
    Z[j] ← X[j] ⋙ 3
    O[j] ← S(Z[j])
  D ← (Z[0] + Z[1]) % 2^4
  O(2) ← S(D)
  for k = 2 to 3
    Z[k] ← O[k − 2] ⋙ 1
  for m = 0 to 1
    D[m] ← (Z[m + 2] + O[2]) % 2^4
  Y[0] ← S(D[0])
  Y[1] ← S(D[1])
  Y ← Y[0] ‖ Y[1]
```

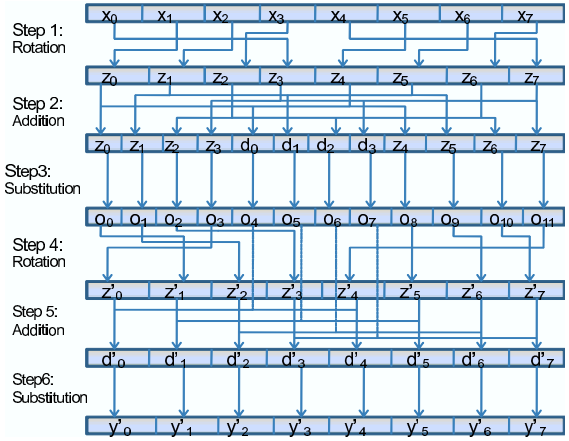


Рис. 1. Path from initial state to the final state

The use of random walks or, more precisely, pseudo-random walks is presented in Figure 1. This effectively comprises of two layers each with identical steps of Rotation, Addition and substitutions.

3. Design Rationale

It is important to indicate that the simple operations are extremely desirable for fast implementation. The updates of the states are based on several simultaneously applied random walks which are very simple and efficiently implementable.

3.1. Operations used in RWA

Note that the random walks are interleaved, and the randomness of each one of them relies on the randomness of the others. Also note that the updates use modular addition and not a bitwise XOR operation. This partially resolves the problem of high-probability short correlations in random walks. In an undirected random walk, there is a high probability that after a short number of steps, the state returns to a previous state, while in a directed random walk this phenomenon does not exist. The usage of addition, which unlike XOR is not an involution, prevents this property [2]. Another operation used in the algorithm is bit wise rotation. We know that it is sufficient to know the k LSBs of the input to retrieve the k LSBs of the output. An attacker can use this property to mount an attack based on analyzing only the k LSBs of the output, and disregard all the other bits. This makes the guess-and-determine attack possible with very low time complexity. For example, if no rotations were used in the algorithm, then a variant of the standard guess-and-determine attack would apply by examining only the LSBs of every output word, and reducing the time complexity of the attack to the fourth root of the original time complexity [2]. The third operation, substitution, provides confusion in the resultant output

3.2. Rapidly Mixing Random Walks

The good long term randomness properties of the internal state of algorithm are achieved by updates using rapidly mixing random walks. Since the algorithm is completely deterministic, the walks are only pseudo-random, so we try to make the update principle like a random walk. A random walk on a graph starts at a node z_0 (see Figure 2), and at each step moves to a node connected by one of its adjacent edges at random. Figure 2 shows the path from a single bit of input state to the output state bits. *A random walk is called „rapidly mixing“ if, after a relatively short time, the distribution of the state of the walk is close to the uniform distribution, regardless of the initial distribution of the walk* [2]. One of the most important parameters of RWA is its mixing time. This includes the number of steps required for a sequence of independent random moves from an initial state to an ending state achieving uniform distribution over the state space. The parameter „mixing time“ is typically not easy to determine but it can be shown that the random moves achieve uniform distribution over the state space. Lets assume that our null hypothesis is: H_0: *The process has a specified distribution i.e. uniform distribution*. We applied Pearson's Chi-Square test for goodness of fit with 7 classes (steps) and known probabilities p_i for each class that are 1/8, 1/8, 1/6, 1/4, 1/4, 1/4 and 1/4. The calculated value of test-statistic (χ^2) is 13.17 with degree of freedom equals 6 (d.f $= 7 - 1 - m$ where m is the number of parameters estimated from the sample). In our case $m = 0$, as we have not estimated the parameters of the specified distribution. A small computed value of χ^2 indicates a good fit and it leads to the acceptance of the null hypothesis. As our calculated value is smaller than the critical value (15.09) at 1 % level of significance, so we can conclude that the distribution of the state of the walk is uniform.

3.3. Degree Distribution

It is assumed that the presence or absence of an edge between two vertices is independent of the presence or absence of any other edge (see

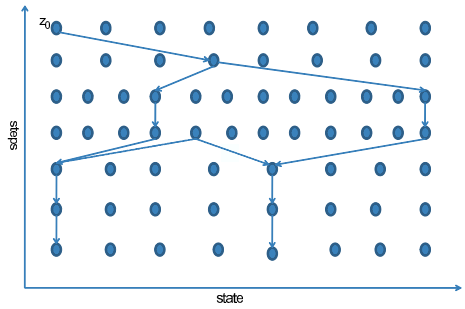


Рис. 2. Subgraph showing path of a single input bit

Figure 2), so that each edge may be considered to be present with independent probability p. If there are n $(=13)$ vertices in a sub graph, and each is connected to an average of l edges, then it is trivial to show that $p = l/(n-1)$, which for large n is usually approximated by l/n (As $n-1 \approx n$ for $n \to \infty$) [3].

The degree k for any particular vertex has a probability distribution p_k given by $p_k = \binom{n}{k} p^k (1-p)^{n-k}$.These probabilities are 0.381, 0.069, 0.207, 0.207, 0.207, 0.207, 0.069, 0.069, 0.207, 0.207, 0.381, and 0.381. For large n, the probabilities are calculated using the density function of Poisson distribution taking k as a random variable with mean l $(p_k = l^k e^{-l}/k!$ if $n \to \infty)$.

The degrees k_j of all j (for $j = 1, \ldots, n$) vertices are independently identically distributed (i.i.d) random integers drawn from a specified distribution with $\Pr(k_j \leqslant x) = F(x)$, as the graph is assumed to be entirely random. For a given choice of these degrees, also known as „degree sequence", a graph is chosen uniformly at random from the set of all graphs with that degree sequence (see Sec. 3.2). The probability mass function and the distribution function of the vertex degree k are denoted by $\Pr(k = j) = f_j$ for $j = 0, 1, 2, \ldots, n-1$ and $F(x) = \Sigma_{j=0}^{\lfloor x \rfloor} f_j$ where $\lfloor x \rfloor$ is the largest integer smaller than or equal to x. Note that $f_j = (1/jc_p)p(1-p)^{j-2}$ for all $j \geqslant 1$ where c_p is the normalizing constant [4]. For some $t > 3$ and some positive constant c, if $1 - F(x) \leqslant cx^{-t+1}$ for $x > 0$ then it concludes that the second moment of k is finite. We denote $\mu = \mathsf{E}[k_j]$, $v = \mathsf{E}[k_j(k_j-1)]/\mathsf{E}[k_j]$ and the distance or hopcount H_n between the starting and ending vertices as the minimum number of edges, is minimum. In some cases, the random graphs with appropriate distributions of vertex degree show a measurable discrepancy between theory and reality, perhaps due to the existence of additional structure in the network that is not captured by the random graph.

3.4. Thresholds: Concentration

There are a number of methods of showing concentration of a random variable that are now commonly used in random graph theory, such as Chernoff's bound, Azuma—Hoeffding inequalities, Martingale-based inequalities and Talagrand's inequalities [5]. But it is trivial to use the simplest one that is given as follows:

Chebyshev's inequality: Let X be a random variable with variance σ^2, and let $\epsilon \geqslant 1$. Then

$$\Pr(|X - \mathsf{E}[X]| > \epsilon\sigma) < \frac{1}{\epsilon^2}.$$

Using the measures of central tendency and dispersion mentioned above, we can analyze this inequality for showing concentration of the random variable k_j. For simplicity, lets assume $\epsilon = 1$, if $\Pr(|kj - \mathsf{E}[kj]| > \sqrt{v}) < 1$, then it can be shown that the particular vertex degree is concentrated close to its expected value. The probability that the random walk returns to a previously visited vertex is very important for cryptographic purposes, since short cycles lead to mathematical or statistical relations which an attacker can exploit.

4. Results and Summary

This paper proposes a new fast and secure algorithm for generating S-Box. The main ascribed features of the algorithm are simplicity, efficiency and less memory usage in software and low implementation cost. The algorithm is based upon trivially analyzable and simple components. The algorithm possesses reasonable security in terms of its operations used. In addition, the generated S-Box possesses cryptographic properties such as MDP, MLP, Balance, and higher BLA. The algorithm involves rapidly mixing random walks, to ensure the random walks in the long run. We also analyzed the algorithm with the help of statistical tools such as parametric distributions which can be used to find the concentration and randomness of the degrees and paths evolved through the main loop of algorithm. We have analyzed both theoretically and empirically, that the S-Box generated by the given design method has better cryptographic and statistical properties. The results are summarized in the Table 1.

Here, f_i $(0 \leqslant i \leqslant 7)$ are Boolean functions contained in the designed S-Box. Some statistical tests are applied to check the randomness of the output generated by AES algorithm by replacing its original S-box with our designed S-Box. The results show better randomness and uniformity.

Таблица 1. Results for the designed 8×8 S-Box

Best Linear Approximation	BLAP	Balance	AD
$f_0 = X_2 + X_6 + X_7$	0.5938	0.5	7
$f_1 = 1 + X_3 + X_5$	0.6172	0.5	7
$f_2 = 1 + X_3 + X_4 + X_6$	0.5859	0.5	7
$f_3 = 1 + X_0 + X_1 + X_2 + X_5$	0.5859	0.5	7
$f_4 = X_2 + X_3 + X_6$	0.5938	0.5	7
$f_5 = 1 + X_1 + X_7$	0.6172	0.5	7
$f_6 = 1 + X_0 + X_2 + X_7$	0.5859	0.5	7
$f_7 = 1 + X_0 + X_1 + X_5$	0.5859	0.5	7
Values of Cryptographic Properties			
MDP	2^{-4}	MLP	$2^{-4.15}$

Литература

[1] *Bollobas B.* Random graphs. London: Academic Press, 1985.

[2] *Keller N., Miller S.D., Mironov I., Venkatesan R.* MV3: A new stream cipher based on random walks and revolving buffers. Topics in Cryptology—Proceedings of CT-RSA 2007. LNCS. Vol. 4377. Springer-Verlag, 2007.

[3] *Newman M.E.J., Strogatz S.H., Watts D.J.* Random graphs with arbitrary degree distributions and their applications. July 24. 2001.

[4] *van der. Hofstad R.* Distances in random graphs with finite variance degrees // Gerard Hooghiemstra and Piet Van Mieghemy. October 13, 2004.

[5] *Hoeffding W.* Probability inequalities for sums of bounded random variables // Journal of the American Statistical Association. 1963. Vol. 58.

New Methods of Generating MDS Matrices

G. Murtaza, N. Ikram

Annotation

After the success of Rijndael as AES, MDS matrices have become necessary and important part in many block ciphers. In this paper we purpose two methods of generating MDS matrices. In first method we generate dynamically an MDS Matrix from an existing MDS matrix. This method can be used to generate random and non linear MDS matrices. In second method we use biregular array to construct an MDS matrix.This method has the advantage of generating MDS matrix with more number of 1s thereby improving the lower bound compared with earlier implementation.

1. Introduction

Security and efficiency are two main concerns in cryptographic applications. In block cipher, an invertible mapping on m variables is called MDS_{m+1} or simply MDS (Maximum Distance Separable) if any change in k inputs propagates to a change of at least $(m+1)-k$ outputs. This mapping is represented by a matrix called MDS matrix. MDS matrix has been used as a perfect diffusion primitive in block ciphers like AES [7], Twofish [8], Khazad [9] and Fox [10]. One can construct methods/algorithms to generate an MDS matrix for cryptographic purpose using coding theory and matrix theory; these methods include GRS Codes that are MDS codes, Cauchy and Vandermonde matrices [1]. The matrices constructed by these methods are linear and inefficient. Another approach to construct efficient MDS matrices is discussed in [2] by using biregular arrays. We present a method to generate a random MDS matrix. This method can also be used to generate non linear MDS matrix. We also improve the result about efficient MDS matrices discussed in [2].

2. Dynamic Generation of Non Linear MDS Matrices

In this section, we develop a method to dynamically generate an MDS Matrix. This method can be used to obtain random MDS matrices as well as nonlinear (inefficient) MDS Matrices. The following is the main result of this section.

Theorem 1. *Let $A = [a_{i,j}]_{m,m}$, $a_{i,j} \in \mathbb{F}_q$ be an MDS matrix. For an element $e \in \mathbb{F}_q \setminus \{0\}$, eA is an MDS matrix.*

Доказательство. Let A be an MDS Matrix. Then for any square submatrix S of A, $|S| \neq 0$, and let $A' = eA$, $e \in \mathbb{F}_q \setminus \{0\}$ be a new matrix which implies that $S' = eS$ for any square submatrix S' of A'. We suppose that $|S'| = 0$. Then

$$|eS| = 0 \;\Rightarrow\; e|S| = 0 \;\Rightarrow\; |S| = 0$$

since $e \neq 0$. A contradiction to that A is an MDS matrix. Hence A' is an MDS matrix. □

We can generate a random/dynamic MDS matrix using above result by taking a random value e. The inverse of each computed random MDS matrix can be obtain by using the following fact.

Theorem 2. *If $B = eA$, $e \in \mathbb{F}_q \setminus \{0\}$, then*

$$B^{-1} = e^{-1}A^{-1}.$$

We can also introduce nonlinearity in MDS matrix as follows.

$$(x_1, x_2, x_3, \ldots, x_i)x_k \begin{pmatrix} a_{1,1} & \ldots & a_{1,j} \\ \ldots & \ldots & \ldots \\ a_{i,1} & \ldots & a_{i,j} \end{pmatrix}, \quad 1 \leqslant k \leqslant i.$$

This is one of the methods to introduce non linearity in MDS which is however, expensive (e.g., for GF(2^8), 256 lookup tables or a modular multiplication at each step are required). Similarly, other field operation can also be employed to introduce non linearity in MDSs.

3. Efficient MDS Matrices

In this section, we present an improvement in the result of [2] for matrices of order greater than 7×7 and necessary condition for such matrix to be an MDS matrix.

Theorem 3. *For any $m \geqslant 8$, $n \geqslant m$, we have*

$$v_1^{m,n} \geqslant n + 2m - 1.$$

Доказательство. Consider the construction below:

a_1	a_2	a_3	a_4	$\ldots$	a_{m-2}	1	1	1	$\ldots$
a_2	1	1	a_3	$\ldots$		a_{m-2}	a_{m-1}	a_{m+1}	$\ldots$
1	a_2	1	1	a_3			a_{m-2}	a_{m+2}	$\ldots$
a_4	1	a_2	1	1	a_3		a_{m-3}	a_{m+3}	$\ldots$
a_5	a_4	1	a_2	1	1	a_3		a_{m+4}	$\ldots$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
1	a_{m-2}	$\ldots$	$\ldots$	1	a_2	1	a_2	a_{2m-1}	$\ldots$
1	1	a_{m-2}	$\ldots$	$\ldots$	1	a_2	1	a_{2m}	$\ldots$

The construction is clearly a biregular. First occurrence of 1 is at 3rd row of 1st column and it goes parallel to diagonal until last row, so we have $m-2$ 1s. Second diagonal array of 1s comprises of $m-1$ 1s, and third diagonal array of 1s contains $m-3$ elements. There are two 1's lying at 1st and 2nd columns of last row. There are a total of $n-m+2$ 1s in the first row. Therefore, we have a total of $m-3+m-2+m-1+3+n-m+2$ numbers of 1s. □

Hence we have the result in accordance with Theorem 3. However, the following result will ascertain the conditions for the generated matrix to be an MDS.

Lemma. *A necessary condition for the construction of a matrix given in Theorem 3 to be an MDS is $a_i \neq a_j^2$, $a_i \neq a_j + 1$, $a_i \neq a_j^{-1}$, $a_i a_j \neq a_k$ for any a_i, a_j, a_k.*

Доказательство. Without loss of generality, we have any submatrix after reduction by Gaussian elimination method

1	a_i	a_i	a_i	a_i	$\ldots$	a_i	a_i
0	1	a_i	a_i	a_i	$\ldots$	a_i	a_i
0	0	1	a_i	a_i	$\ldots$	a_i	a_i
0	0	0	1	a_i	$\ldots$	a_i	a_i
0	0	0	0	1	$\ldots$	a_i	a_i
0	0	0	0	0	1	a_i	a_i
0	0	0	0	0	0	a_1	a_2
0	0	0	0	0	$\ldots$	a_3	a_4

The determinant of this matrix become 0 in the following cases:

Case 1: $a_2a_3 = a_4$ and $a_1 = 1$.
Case 2: $a_1 = 1$, $a_4 = 1$ and $a_2 = a_3^{-1}$.
Case 3: $a_1 = 1$, $a_3 = a_2$ and $a_2^2 = a_4$.
Case 4: $a_1 = a_2$ and $a_3 = a_4 = a_1 + 1$. □

Using above lemma we have the following algorithm to construct efficient MDS matrix.

Algorithm

Input: q = field value, m = number of rows = number of columns.
Output: an $m \times m$ MDS Matrix over the field GF(2^n).
Process:
Step 1. Take any $m-1$ elements $a \in \mathrm{GF}(q)$, $q = 2^n$ that satisfy the following conditions: $a_i \neq a_j^2$, $a_i \neq a_j + 1$, $a_i \neq a_j^{-1}$, $a_i a_j \neq a_k$. For it do the following:

1. Select randomly a_1 and reject elements a_1^2, a_1^{-1}, $a_1 + 1$.
2. Select a_2 such that a_2 not in rejected elements. Add elements a_2^2, a_2^{-1}, $a_2 + 1$, $a_1 a_2$ in rejected elements.
3. Continue the above process until get $m-1$ elements.

Step 2. Construct matrix by placing elements in positions as given in construction of previous lemma.

4. Conclusion

We have presented new methods of generating MDS; first one to generate dynamic MDS matrices which is used to construct random and non linear MDS matrices while the second method generates efficient linear MDS matrices. MDS matrices generated by employing the former method are no more efficient. Our future work is aimed at the construction of efficient non linear MDS matrices which happens to be the current research pursuit at [4], [5] and [6] using T-functions.

Литература

[1] *J. Lacan and J. Fimes*. Systematic MDS Erasure Codes Based on Vandermonde Matrices // IEEE Transactions on Information Theory. Vol. 8. № 9. September 2004.

[2] *Junod P.*, *Vaudenay S.* Perfect Diffusion Primitives for Block Ciphers Building Efficient MDS Matrices. Ecole Polytechnique Federale de Lausanne (Switzerland), 1999.
[3] *Klimov A.*, *Shamir A.* A New Class of Invertible Mappings. Workshop on Cryptographic Hardware and Embedded Systems (CHES). 2002.
[4] *Klimov A.*, *Shamir A.* Cryptographic Applications of T-functions. Selected Areas in Cryptography (SAC). 2003.
[5] *Klimov A.*, *Shamir A.* New Cryptographic Primitives Based on Multiword T-functions. FSE 2004. 2004.
[6] *Klimov A.* Applications of T-functions in Cryptography. PhD Thesis, Weizmann Institute of Science, submitted, 2004.
[7] *Daemen J.*, *Rijmen V.* The Design of Rijndael: AES—The Advanced Encryption Standard. Springer-Verlag, 2002.
[8] *Schneier B.*, *Kelsey J.*, *Whiting D.*, *Wagner D.*, *Hall C.*, *Ferguson N.* Twofish: A 128" Bit Block Cipher. `http://www.counterpane.com/twofish.html`.
[9] *Barreto P.*, *Rijmen V.* The Khazad legacy-level block cipher. First open NESSIE Workshop, Leuven, November 13–14, 2000.
[10] *Junod P.*, *Vaudenay S.* FOX: a new family of block ciphers. To appear in Selected Areas in Cryptography 2004, Waterloo, Canada, August 9–10, 2004. Revised papers. Lecture Notes in Computer Science. Springer-Verlag.

Об обнаружении квазипериодов в бинарных последовательностях

А. Н. Ярмола

1. Введение

Генераторы псевдослучайных последовательностей(ПСП) используются во многих системах криптографической защиты информации [1]. Одной из важнейший характеристик ПСП является период выходной последовательности. Однако большая величина периода не гарантирует хороших криптографически свойств генератора, важную роль играет и структура периода (см., например, [2]).

Пусть $x_t \in \mathcal{A} = \{0, 1\}$ — бинарная периодическая последовательность, период которой равен $T^0 = m^* T^*$, и $X^* = (x_1, \ldots, x_{T^0})$ можно представить в виде:

$$X^* = (X^{(1)}, \ldots, X^{(m^*)}), \tag{1}$$

причем вектора $X^{(i)}$ мало отличаются между собой. Такая структура периода является слабостью генератора ПСП. Поэтому актуальной является задача распознавания последовательностей с такой структурой и оценивания величины «квазипериода» T^*.

Для обнаружения последовательностей вида (1) будем использовать следующие две модели дискретных временных рядов (ДВР). Модель векторной бинарной авторегрессии (VBAR):

$$X^{(i)} = X^{(i-1)} \oplus \Gamma^{(i)}, \quad i = 2, \ldots, m^*, \tag{2}$$

$X^{(1)}$ — случайный вектор с равномерным на $\mathcal{A}$ распределением вероятностей, $\Gamma^{(i)}$, $i = 2, \ldots, m^*$ — независимые одинаково распределенные случайные вектора. Модель векторной бинарной регрессии (VBR):

$$X^{(i)} = X^{(0)} \oplus \Gamma^{(i)}, \quad i = 2, \ldots, m^*, \tag{3}$$

$X(0)$ — случайный вектор с равномерным на распределением вероятностей, $\Gamma^{(i)}$, $i = 2, \ldots, m^*$ — независимые одинаково распределенные случайные вектора, вектор $X^{(0)}$ неизвестен.

Работа частично поддержана ГПФИ «Математические модели» (проект ММ-24).

Везде далее будем предполагать, что $\Gamma^{(i)} = (\gamma_1^{(i)}, \ldots, \gamma_{T^*}^{(i)})$, $i = 2, \ldots, m^*$, $\{\gamma_j^{(i)}, i = 2, \ldots, m^*, j = 1, \ldots, T^*\}$ — н. о. р. с. в. Бернулли, $\Pr\{\gamma_j^{(i)} = 1\} = \epsilon$.

В [2] предложен метод восстановления начального состояния генератора ПСП в случае, когда имеет место модель VBR, и X^0 — выходная последовательность LFSR с известным полином обратной связи. В данной работе мы не накладываем ограничений на структуру векторов $X^{(0)}$ (для модели VBR), $X^{(1)}$ (для модели VBAR), и основной нашей задачей является задача обнаружения квазипериода в наблюдаемой последовательности.

2. Постановка задачи

Более строго поставленная в предыдущем пункте задача формулируется так, по наблюдаемому участку последовательности $X = (x_1, \ldots, x_n)$ длительности $n < T^0$ необходимо проверить гипотезу H_0: x_t является равномерно распределенной последовательностью (РРСП), против гипотезы H_1: имеет место (1). Заметим, что гипотезу H_1 можно представить в виде $H_1 = \bigcup_{T^*=2}^{\infty} H_{1,T^*}$, где гипотеза H_{1,T^*}: имеет место (1) с «квазипериодом» T^*.

Пусть $2 \leqslant T \leqslant \lfloor n/2 \rfloor$, тогда наблюдения X можно представить в виде:

$$X^* = (X^{(1)}, \ldots, X^{(m)}, X^{(m+1)}), \quad m = \lfloor n/T \rfloor, \tag{4}$$

где $X^{(i)} = (x_{(i-1)T+1}, \ldots, x_{iT})$, $i = 1, \ldots, m$, $X_{(m+1)} = (x_{mT+1}, \ldots, x_n)$. Для решения задачи статистической проверки гипотезы H_0 против H_1, будем использовать следующие статистики ($m = \lfloor n/T \rfloor$, $1 \leqslant T_- \leqslant T \leqslant T_+ \leqslant \lfloor n/2 \rfloor$):

$$Z_1(T) = \frac{1}{m-1} \sum_{i=2}^{m} \mathrm{wt}(X^{(i)} \oplus X^{(i-1)}), \tag{5}$$

$$Z_2(T) = \arg \min_{X^{(0)} \in \mathcal{A}_2^T} \frac{1}{m} \sum_{i=1}^{m} \mathrm{wt}(X^{(i)} \oplus X^{(0)}), \tag{6}$$

где $\mathrm{wt}(a)$ — вес Хэмминга бинарного вектора a, T_-, T_+ — некоторые априорно заданные границы для возможной величины «квазипериода». Заметим, что в случае модели VBAR не целесообразно использовать статистику Z_2.

Лемма 1. *Статистика $Z_2(T)$ допускает эквивалентное представление $Z_2(T) = \sum_{j=1}^{T} Z_{2,j}/m$, где*

$$Z_{2,j} = \min\left\{\sum_{i=1}^{m} x_{(i-1)T+j},\ m - \sum_{i=1}^{m} x_{(i-1)T+j}\right\}.$$

3. Распределение статистик Z_1, Z_2 в случае гипотезы H_0

Лемма 2. *Если справедлива гипотеза H_0, то для любого T случайные величины $Z_{2,j}$ — независимы и их распределение имеет вид*

$$\Pr\{Z_{2,j} = r \mid H_0\} = \begin{cases} 2^{-m+1}\binom{r}{m}, & 0 \leqslant r < m/2; \\ 2^{-m}\binom{r}{m}, & r = m; \\ 0, \quad r > m/2. \end{cases}$$

Теорема 1. *Если справедлива гипотеза H_0, то для любого T*

$$\mathcal{L}\{(m-1)Z_1(T) \mid H_0\} = Bi(T,\, 1/2), \tag{7}$$

$$T^{-1}Z_2(T) \to \frac{1}{2}\left(1 - 2^{-m+1}\binom{\lfloor m/2 \rfloor}{m}\right) \ (\textit{п. н.}), \tag{8}$$

где $\mathcal{L}\{\eta\}$ — распределение вероятностей случайной величины η, Bi — биномиальное распределение.

Теорема 2. *Если имеет место гипотеза H_0, то для любых $T_1 < T_2$, $T_2 \neq kT_1$, статистики $Z_j(T_1)$, $Z_j(T_2)$ $(j = 1, 2)$ независимы.*

4. Распределение статистик Z_1, Z_2 в случае гипотезы H_1

Теорема 3. *Если имеет место одна из моделей VBAR, VBR и справедлива гипотеза H_{1,T^*}, то при $T \neq kT*$:*

$$\mathbf{E}\{Z_1(T) \mid H_{1,T^*}\} = T/2,$$

однако, $\mathcal{L}\{(m-1)Z_1(T)|H_{1,T^*}\} \neq Bi((m-1)T,\, 1/2)$.

Теорема 4. *Если имеет место модель VBAR и справедлива гипотеза H_{1,T^*}, то при $T = kT^*$:*

$$\mathcal{L}\{(m-1)Z_1(T) \mid H_{1,T^*}\} = Bi((m-1)T,\, \epsilon).$$

Теорема 5. *Если имеет место модель VBR и справедлива гипотеза H_{1,T^*}, то при $T = kT^*$*

$$\mathbf{E}\{Z_1(T) \mid H_{1,T^*}\} = 2T\epsilon(1-\epsilon),$$
$$\mathbf{E}\{Z_2(T) \mid H_{1,T^*}\} = T\mu/m,$$

где μ — математическое ожидание случайной величины с распределением вероятностей, определенным в лемме 2. Более того, если $T^* \to \infty$, то

$$(T^*)^{-1}Z_1(T^*) \to \mu/m \ (\textit{п. н.}).$$

5. Статистические оценки величины квазипериода

Теорема 6. *Если имеет место одна из моделей VBR, VBAR, и существует единственное $k \in \mathbf{N}$ такое, что $T_- \leqslant kT^* \leqslant T_+$, то*

$$\widehat{T}_{Z_1} = \arg \max_{T_+ \leqslant T \leqslant T_+} |Z_1^0(T)| \to kT^* \ (\textit{п. н.}),$$

где

$$Z_1^0(T) = \sqrt{\frac{m-1}{T}}(2Z_1(T) - T).$$

Теорема 7. *Если имеет место модель VBR, и существует единственное $k \in \mathbf{N}$ такое, что $T_- \leqslant kT^* \leqslant T_+$, то*

$$\widehat{T}_{Z_2} = \arg \max_{T_+ \leqslant T \leqslant T_+} |Z_2^0(T)| \to kT^* \ (\textit{п. н.}),$$

где

$$Z_1^0(T) = \frac{mZ_2(T) - \mu_{Z_2}T}{\sqrt{\sigma_{Z_2}T}},$$

μ_{Z_2}, σ_{Z_2} — математическое ожидание и дисперсия случайной величины $Z_2(T)$ в случае гипотезы H_0.

6. Статистические тесты на основе статистик Z_1, Z_2

Построим статистические тесты для проверки гипотезы $H_0 = \{x_t$ — РРСП$\}$ по реализации X длительности n следующего вида:

$$d(X) = \begin{cases} H_0, & d_T(X) = H_0 \text{ для всех } T_\leqslant T \leqslant T_+, \\ H_{1,\widehat{T}} & \text{иначе,} \end{cases}$$

где $d_T(X)$ — некоторый тест использующий статистику $Z_S(T)$, $S = 1, 2$ для проверки гипотеза H_0 против $H_{1,T}$, $\widehat{T} = \widehat{T}(Z_S(T_-, \ldots, T_+))$ — некоторая оценка «квазипериода».

На основе статистики $Z_1(T)$ можно построить статистический тест проверки гипотезы H_0 против $\overline{H}_0$ по реализации X длительности n имеющий размер α, положив:

$$d_T(X) = \begin{cases} H_0, & \Delta_{1-\alpha/2}((m-1)T) \leqslant (m-1)Z_1(T) \leqslant \Delta_{\alpha/2}((m-1)T), \\ \overline{H}_0 & \text{иначе,} \end{cases}$$

где $\Delta_\delta((m-1)T$ — квантиль уровня δ биномиального распределения с параметрами $(m-1)T$, $1/2$.

В предложенном тесте можно вычислить точные значения Δ_δ, однако эта задача является весьма трудоемкой, поскольку границы необходимо пересчитывать для каждого T, поэтому можно воспользовавшись теоремой Муавра — Лапласа [3], заметить что при $mT \to \infty$

$$\mathcal{L}\left\{\frac{2(T-1)Z_1(T)-(m-1)T}{\sqrt{((m-1)T)}}\right\} \to N(0,\,1),$$

и заменить предложенные выше тесты на более простые с вычислительной точки зрения

$$d_T(X) = \begin{cases} H_0, & \sqrt{m-1}|2Z_1(T)-T|/\sqrt{T} \leqslant \Phi^{-1}(1-\alpha/2), \\ \overline{H}_0 & \text{иначе,} \end{cases}$$

где Φ — функция распределения стандартного нормального распределения вероятностей.

Аналогично можно построить статистический тест на основе статистики Z_2.

Литература

[1] *Харин Ю. С.*, *Берник В. И.*, *Матвеев Г. В.*, *Агиевич С. В.* Математические и компьютерные основы криптологии. Минск: Новое знание, 2003.

[2] *Zeng K.*, *Huang M.* On the Linear Syndrome Method in Cryptoanalysis // Proc. of the Int. Cryptology Conf. on Advances in Cryptology. P. 469—478, 1988.

[3] *Боровков А. А.* Теория вероятностей. М.: Наука, 1986.

Идентификация двоичных последовательностей на основе искаженных цепей Маркова с частичными связями

Ю. С. Харин, А. И. Петлицкий

1. Введение

Цепи Маркова высокого порядка имеют широкое применение в криптологии [1, 2, 3]. Однако число параметров (вероятностей переходов) цепи Маркова s-го порядка растет экспоненциально при увеличении s, что ограничивает идентификацию этой модели на практике. Для разрешения этой проблемы разрабатываются «малопараметрические» модели цепей Маркова высокого порядка: модель Джекобса — Льюиса, MTD-модель Рафтери, цепь Маркова s-го порядка с r частичными связями [4], для которой принято использовать краткое обозначение ЦМ(s, r). Конструктивным примером цепи Маркова ЦМ(s, r) является линейный регистр сдвига с динамическим изменением закона рекурсии [1, 3]. Однако на практике используют еще более «хитроумные» усложнения линейных регистров [1, 2], адекватной математической моделью которых является цепь Маркова с частичными связями при наличии искажений. Статья посвящена решению актуальной задачи идентификации двоичной цепи Маркова ЦМ(s, r) при наличии аддитивных искажений.

2. Двоичная цепь Маркова ЦМ(s, r)

Пусть $A=\{0,\,1\}$ — пространство состояний; $J_i^l=(j_i,\,\ldots,\,j_l)\in A^{l-i+1}$ — мультииндекс $(l-i+1)$-го порядка, $l \geqslant i$; $x_t \in A$ — однородная стационарная цепь Маркова s-го порядка с вероятностями одношаговых пере-

Результаты работы получены при финансовой поддержке в рамках Государственной программы фундаментальных исследований Республики Беларусь «Математические модели» (проект № 24).

ходов

$$p_{J_1^{s+1}} = \mathsf{P}\{x_{t+s} = j_{s+1} \mid x_{t+s-1} = j_s, \ldots, x_t = j_1\}, \quad J_1^{s+1} \in A^{s+1}, \quad t \in \mathbb{N};$$

$r \in \{1, \ldots, s\}$ — параметр, называемый числом связей; $M_r^0 = (m_1^0, \ldots, m_r^0) \in \mathrm{M}$ — целочисленный r-вектор с упорядоченными компонентами, называемый шаблоном, M — множество всевозможных таких векторов; $Q = (q_{J_1^{r+1}})$, $J_1^{r+1} \in A^{r+1}$, — некоторая $(r+1)$-мерная стохастическая матрица.

Цепь Маркова x_t называется [4] цепью Маркова s-го порядка с r частичными связями, если ее вероятности одношаговых переходов имеют вид:

$$p_{j_1,\ldots,j_s,j_{s+1}} = q_{j_{m_1^0},\ldots,j_{m_r^0},j_{s+1}}, \quad J_1^{s+1} \in A^{s+1}. \tag{1}$$

Соотношение (1) означает, что вероятность перехода в состояние j_{s+1} зависит не от всех s предыдущих состояний, а лишь от r избранных.

Примем еще несколько обозначений:

$$X_1^n = (x_1, x_2, \ldots, x_n)$$

— реализация двоичной цепи Маркова ЦМ(s, r) длительности n;

$$F(K_t^{t+s}; M_r) = (k_{t+m_1-1}, \ldots, k_{t+m_r-1}, k_{t+s})$$

— функция, называемая селектором $(r+1)$-го порядка, $K_t^{t+s} \in A^{s+1}$; $\delta_{J_1^s,K_1^s} = \prod_{i=1}^s \delta_{j_i,k_i}$ — символ Кронекера для мультииндексов J_1^s, K_1^s;

$$\nu_{J_1^{r+1}}(X_1^n; M_r) = \sum_{t=1}^{n-s} \delta_{F(X_t^{t+s};M_r),J_1^{r+1}}, \quad J_1^{r+1} \in A^{r+1},$$

— частотные статистики; $\Pi^*_{K_1^s}$, $K_1^s \in A^s$, — стационарное распределение вероятностей эргодической ЦМ(s, r) [4];

$$\mu_{J_1^{r+1}}(M_r) = \mathsf{P}\{F(X_t^{t+s}; M_r) = J_1^{r+1}\} = \sum_{K_1^{s+1} \in A^{s+1}} \delta_{F(K_1^{s+1};M_r),J_1^{r+1}} \Pi^*_{K_1^s} p_{K_1^{s+1}}, \quad J_1^{r+1} \in A^{r+1},$$

— распределение вероятностей $(r+1)$-грамм;

$$\widehat{\mu}_{J_1^{r+1}}(M_r) = \frac{1}{n-s} \nu_{J_1^{r+1}}(X_1^n; M_r)$$

— частотная оценка вероятности $\mu_{J_1^{r+1}}(M_r)$, которая является несмещенной и состоятельной оценкой при $n \to \infty$. Условимся, что если вместо какого-то индекса стоит точка, то это означает суммирование по всем возможным значениям этого индекса: $\mu_{J_1^r.}(M_r) = \sum_{j_{r+1} \in A} \mu_{J_1^{r+1}}(M_r)$.

Состоятельные оценки для шаблона M_r^0 и матрицы Q имеют вид [4]:

$$\widehat{M}_r = \arg\max_{M_r \in \mathrm{M}} \widehat{I}(M_r), \qquad \widehat{q}_{J_1^{r+1}}(\widehat{M}_r) = \widehat{\mu}_{J_1^{r+1}}(\widehat{M}_r) / \widehat{\mu}_{J_1^r.}(\widehat{M}_r), \tag{2}$$

где $\widehat{I}(M_r) = \sum_{J_1^{r+1} \in A^{r+1}} \widehat{\mu}_{J_1^{r+1}}(M_r) \ln \dfrac{\widehat{\mu}_{J_1^{r+1}}(M_r)}{\widehat{\mu}_{J_1^r.}(M_r)\mu_{\cdot j_{r+1}}(M_r)}$ — «подстановочная» оценка количества информации.

Для оценивания параметров s и r использовался байесовский информационный критерий [4]:

$$h(\widehat{s}, \widehat{r}) = \min_{s_- \leqslant \overline{s} \leqslant s_+,\ r_- \leqslant \overline{r} \leqslant r_+} h(\overline{s}, \overline{r}), \tag{3}$$

где $h(s, r) = (s-n) \sum_{J_1^{r+1} \in A^{r+1}} \widehat{\mu}_{J_1^{r+1}}(\widehat{M}_r) \ln \widehat{q}_{J_1^{r+1}}(\widehat{M}_r) + 0.5 N^r (N-1) \ln n$.

3. Оценивание параметров двоичной ЦМ (s, r) при наличии аддитивных искажений

Пусть наблюдается двоичная цепь Маркова с частичными связями при наличии аддитивных искажений:

$$y_t = x_t \oplus \xi_t, \quad t \in \mathbb{N}, \tag{4}$$

где $x_t \in A$ — ненаблюдаемая двоичная ЦМ(s, r), $\xi_t \in A$ — ненаблюдаемая последовательность независимых случайных величин Бернулли с $\mathsf{P}\{\xi_t = i\} = p_i$, $i \in A$; $\{x_t\}$, $\{\xi_t\}$ — независимы. Идентификация заключается в оценивании параметров модели (4) по наблюдаемой реализации $Y_1^n = (y_1, \ldots, y_n)$ длительности n.

3.1. Метод частотных статистик

В этом методе будем предполагать, что p_0 известно. Обозначим: $b_{K_1^{r+1}}(M_r) = \mathsf{P}\{F(Y_t^{t+s}; M_r) = K_1^{r+1}\}$, $K_1^{r+1} \in A^{r+1}$. Заметим, что если $p_0 = 1$, т. е. искажения отсутствуют, то $b_{K_1^{r+1}}(M_r) = \mu_{K_1^{r+1}}(M_r)$.

Лемма 1. *Если x_t — стационарная цепь Маркова ЦМ(s, r), то*

$$b_{K_1^{r+1}}(M_r) = \sum_{J_1^{r+1} \in A^{r+1}} \mu_{J_1^{r+1}}(M_r) \prod_{i=1}^{r+1} p_{j_i \oplus k_i}, \quad K_1^{r+1} \in A^{r+1}.$$

Частотная оценка вероятности $b_{K_1^{r+1}}(M_r)$, $K_1^{r+1} \in A^{r+1}$, имеет вид:

$$\widetilde{b}_{K_1^{r+1}}(M_r) = \nu_{K_1^{r+1}}(Y_1^n; M_r)/(n-s).$$

Лемма 2. *Если x_t — стационарная цепь Маркова ЦМ(s, r), то оценка $\big(\widetilde{b}_{K_1^{r+1}}(M_r)\big)$, $K_1^{r+1} \in A^{r+1}$, является несмещенной и состоятельной в среднеквадратическом.*

Согласно леммам 1, 2, оценки параметров $\mu_{J_1^{r+1}}(M_r)$, $J_1^{r+1} \in A^{r+1}$, по наблюдаемой реализации Y_1^n предлагается находить как решение следующей системы линейных уравнений:

$$\begin{cases} \sum\limits_{J_1^{r+1} \in A^{r+1}} \widetilde{\mu}_{J_1^{r+1}}(M_r) = 1, \\ \sum\limits_{J_1^{r+1} \in A^{r+1}} \widetilde{\mu}_{J_1^{r+1}}(M_r) \prod\limits_{i=1}^{r+1} p_{j_i \oplus k_i} = \widetilde{b}_{K_1^{r+1}}(M_r), \end{cases} \tag{5}$$

где $K_1^{r+1} \in A^{r+1}$, $w(K_1^{r+1}) \neq 0$, $w(\cdot)$ — вес Хэмминга.

Теорема 1. *Если x_t — стационарная цепь Маркова ЦМ(s, r), то оценка $\big(\widetilde{\mu}_{J_1^{r+1}}(M_r)\big)$, $J_1^{r+1} \in A^{r+1}$, найденная из* (5)*, является несмещенной и состоятельной в среднеквадратическом.*

Используя «подстановочный» принцип, оценки $\widetilde{Q}$, $\widetilde{M}_r$, $\widetilde{r}$, $\widetilde{s}$ для матрицы Q, шаблона M_r^0, числа связей r и порядка s соответственно могут быть получены с помощью формул (2), (3), в которые подставлены оценки $\widetilde{\mu}_{J_1^{r+1}}(M_r)$, $J_1^{r+1} \in A^{r+1}$, найденные из системы (5).

Теорема 2. *Если x_t — стационарная цепь Маркова ЦМ(s, r), то оценка $\widetilde{M}_r$ является состоятельной, а оценка $\widetilde{Q}$ является несмещенной и состоятельной в среднеквадратическом.*

3.2. Метод на основе EM-алгоритма

Обозначим:

$$\alpha_1(J_1^s) = \Pi_{J_1^s} \prod_{l=1}^{s} p_{k_l \oplus j_l},$$

$$\alpha_{t+1}(J_1^s) = \mathsf{P}\big\{y_1 = k_1, \ldots, y_{t+s} = k_{t+s}, x_{t+1} = j_1, \ldots, x_{t+s} = j_s\big\} = \\ = p_{k_{t+s} \oplus j_s} \sum_{j_0 \in A} q_{F(J_0^s; M_r^0)} \alpha_t(J_0^{s-1}), \quad t = 1, \ldots, n-s;$$

$$\beta_{n-s+1}(J_1^s) = 1,$$

$$\beta_t(J_1^s) = \mathsf{P}\big\{y_{t+s} = k_{t+s}, \ldots, y_n = k_n \,|\, x_t = j_1, \ldots, x_{t+s-1} = j_s\big\} = \\ = \sum_{j_{s+1} \in A} q_{F(J_1^{s+1}; M_r^0)} p_{k_{t+s} \oplus j_{s+1}} \beta_{t+1}(J_2^{s+1}), \quad t = 1, \ldots, n-s.$$

Таким образом, функция правдоподобия для модели (4) имеет вид:

$$L(Q,\, p_0) = \mathsf{P}\big\{y_1 = k_1, \ldots, y_n = k_n\big\} = \sum_{J_1^s \in A^s} \alpha_{n-s+1}(J_1^s). \tag{6}$$

Аналогичный подход для вычисления функции правдоподобия использовался в [5].

Алгоритм оценивания параметров модели (4) имеет следующий вид:

1. Вычисляем $L^{(0)} = L\big(\widetilde{Q}^{(0)},\, \widetilde{p}_0^{(0)}\big)$, где $\widetilde{p}_0^{(0)}$ и $\widetilde{Q}^{(0)} ::= \widetilde{B} = \big(\widetilde{b}_{J_1^{r+1}}(M_r^0) / \widetilde{b}_{J_1^r \cdot}(M_r^0)\big)$, $J_1^{r+1} \in A^{r+1}$, — начальные значения.
2. Для $i > 0$ вычисляем
$$\widetilde{p}_0^{(i)} = \gamma_{k_t \cdot}^{(i-1)} / (n-s), \quad \widetilde{Q}^{(i)} = \big(\gamma_{J_1^{r+1}}^{(i-1)} / \gamma_{J_1^r \cdot}^{(i-1)}\big), \quad J_1^{r+1} \in A^{r+1},$$
где
$$\gamma_{J_1^{r+1}}^{(i-1)} = \sum_{t=1}^{n-s} \sum_{I_1^{s+1} \in A^{s+1}} \frac{\delta_{F(I_1^{s+1}; M_r^0), J_1^{r+1}}}{L^{(i-1)}} \alpha_t^{(i-1)}(I_1^s) \beta_{t+1}^{(i-1)}(I_2^{s+1}) \times \\ \times \widetilde{p}_{k_{t+s} \oplus i_{s+1}}^{(i-1)} \widetilde{q}_{F(I_1^{s+1}; M_r^0)}^{(i-1)}(M_r^0).$$
Вычисляем $L^{(i)}$ согласно (6).
3. Если $L^{(i)} - L^{(i-1)} < \varepsilon$, то $\widetilde{Q} = \widetilde{Q}^{(i)}$, $\widetilde{p}_0 = \widetilde{p}_0^{(i)}$, иначе возвращаемся к шагу 2 при $i ::= i + 1$; $\varepsilon > 0$ — «параметр останова» итерационного процесса.

4. Численные результаты

Для метода частотных статистик при известных $s = 32$, $r = 3$, $p_0 = 0.75$ в таблице 1 представлена зависимость экспериментальных значений среднеквадратической ошибки оценивания $\Delta^2(\widetilde{Q},\, Q) = \mathsf{E}\|\widetilde{Q} - Q\|$, полученных по методу Монте-Карло при числе прогонов $T = 190$, от n для двух случаев: 1) оценка матрицы Q вычисляется при известном шаблоне $M_r^0 = (1,\, 13,\, 31)$; 2) шаблон неизвестен. В последней строке таблицы 1 представлена зависимость частоты ошибки шаблона от длительности наблюдения n.

Для метода на основе EM-алгоритма в таблице 2 представлена зависимость экспериментальных значений $\Delta^2(\widetilde{Q},\, Q)$, $\Delta^2(\widetilde{p}_0,\, p_0)$, полученных по методу Монте-Карло при числе прогонов $T = 25$, от n при $p_0 = 0.9$, $s = 6$, $r = 3$, $M_r^0 = (1,\, 3,\, 5)$, $\widetilde{p}_0^{(0)} = 0.85$ и $\varepsilon = 0.1$.

Полученные численные результаты согласуются с теорией и иллюстрируют достаточно хорошие свойства полученных оценок.

Таблица 1. Точность метода частотных статистик

n		20000	25000	30000	35000	40000	45000
1	$\widehat{\Delta}^2(\widetilde{Q},\, Q)$	0.0321	0.0264	0.0210	0.0184	0.0158	0.0144
	$\widehat{\Delta}^2(\widetilde{B},\, Q)$	0.2136	0.2134	0.2133	0.2128	0.2127	0.2128
2	$\widehat{\Delta}^2(\widetilde{Q},\, Q)$	0.0459	0.0344	0.0244	0.0194	0.0165	0.0144
	$\widehat{\mathsf{P}}\{\widehat{M}_r \neq M_r^0\}$	0.1474	0.0895	0.0474	0.0158	0.0105	0

Таблица 2. Точность метода на основе EM-алгоритма

n	5000	7500	10000	12500	15000
$\widehat{\Delta}^2(\widetilde{p}_0,\, p_0)$	0.000072	0.000039	0.000032	0.000029	0.000024
$\widehat{\Delta}^2(\widetilde{Q},\, Q)$	0.009022	0.005630	0.004573	0.003672	0.003095
$\widehat{\Delta}^2(\widetilde{B},\, Q)$	0.661562	0.654260	0.649082	0.653161	0.656517

5. Заключение

В работе предложено два метода для оценивания параметров двоичной цепи Маркова ЦМ(s, r) при наличии аддитивных искажений. Метод частотных статистик при известном p_0 позволяет находить состоятельные оценки параметров исследуемой модели для достаточно больших значений порядка s. Метод на основе EM-алгоритма может работать и в случае, когда p_0 неизвестно, но при увеличении порядка s работает намного медленнее.

Литература

[1] *Алферов А. П. и др.* Основы криптографии. М.: Гелиос АРВ, 2001.

[2] *Харин Ю. С. и др.* Математические и компьютерные основы криптологии. Минск.: Новое знание, 2003.

[3] *Максимов Ю. И.* О цепях Маркова, связанных с двоичными регистрами сдвига со случайными элементами // Труды по дискретной математике. 1997. Т. 1. С. 203—220.

[4] *Харин Ю. С., Петлицкий А. И.* Цепь Маркова s-го порядка с r частичными связями и статистические выводы о ее параметрах // Дискретная математика. 2007. Т. 19. № 2. С. 109—130.

[5] *Rabiner L. R.* A tutorial on hidden Markov models and selected applications in speech recognition // IEEE. 1989. Vol. 77. № 2. P. 257—286.

Построение $O(L)$- и $U(L)$-стойких шифров в конечных плоскостях

С. С. Коновалова, С. С. Титов

Введение

В данной работе проводится исследование эндоморфных $O(L)$- и $U(L)$-стойких шифров, являющихся совершенными шифрами, стойкими к активным атакам.

Напомним, что совершенный шифр — это теоретически (абсолютно) стойкий шифр [1]. В криптографических приложениях представляет интерес построение эндоморфных совершенных шифров, стойких к активным атакам, для $L > 2$, и изучение конструкций, порождающих семейства таких шифров, так как с ростом L шифр становится более стойким. В [2] построены некоторые примеры $U(2)$-, $U(3)$-, $O(2)$- и $O(3)$-стойких шифров.

В работе использована методика исследования конструкций совершенных шифров, которая была разработана в [2, 3]) при решении трех задач теории линейных совершенных шифров. Задачи были поставлены западными криптографами в 1986 году, а их формулировка приведена в книге [1]. Методика опирается на следующее

Наблюдение 1 (см. наблюдение 2 из [2]). Построение эндоморфного $O(2)$-стойкого шифра сводится к построению конечной (аффинной) плоскости: любым двум x будут однозначно соответствовать пара y, что определяет на плоскости две точки, через которые можно провести единственную прямую, и наоборот — любые две непараллельные прямые пересекаются в единственной точке.

Она состоит в том, что для построения линейных совершенных шифров можно использовать не алгебраические, а геометрические конструкции; например, полуполя, не сводящиеся к полям. Применение этой методики позволяет конкретизировать проблему построения таких шифров, расширять их класс и изучать свойства конечных плоскостей.

В работе также будет усилена следующая

Теорема 1 (см. теорему 5 из [2]). *Эндоморфный $U(2)$-стойкий шифр с уравнением зашифрования $\vec{y} = \vec{x}M_{\vec{k}} + \vec{\ell}$, где $M_{\vec{k}}$ — набор матриц, может быть дополнен до линейного $O(2)$-стойкого шифра; обратно, если с каждой матрицей M_k в $O(2)$-стойком шифре содержится и матрица $-M_k$, то одну матрицу из любой такой пары (любую!) можно убрать и получить линейный $U(2)$-стойкий шифр.*

1. Использование групп Матьё для построения $O(L)$-стойких шифров

Известно, что построение $O(L)$-стойкого шифра эквивалентно построению точно L-транзитивной группы. Классической конструкцией $O(3)$-стойкого шифра является шифр, построенный при помощи точно 3-транзитивной группы $\mathrm{PGL}(2, q)$ на основе дробно-линейных подстановок в поле [4]. Для $L \geqslant 4$ единственными нетривиальными примеры точно L-транзитивных групп являются группы Матьё M_i [1].

Группа Матьё — конечная группа, изоморфная одной из пяти групп, открытых Эмилем Матьё. Так как для построения $O(L)$-стойких шифров мы исследуем массивы с $\omega = 1$ (то есть эндоморфные $O(L)$-стойкие шифры с минимальным количеством ключей), то для нас представляют интерес только точно L-транзитивные группы, то есть M_{11} и M_{12}, которые определяют $O(4)$- и $O(5)$-стойкие шифры соответственно.

Группы Матьё задаются как подгруппы симметрических групп соответствующих степеней. Группа M_{12} порождена шестью подстановками множества из 12 элементов:

$$\begin{aligned} a_1 &= (\mathbf{1}, \mathbf{2}, \mathbf{3})(\mathbf{4}, \mathbf{5}, \mathbf{6})(\mathbf{7}, \mathbf{8}, \mathbf{9}),\\ a_2 &= (\mathbf{2}, \mathbf{4}, \mathbf{3}, \mathbf{7})(\mathbf{5}, \mathbf{6}, \mathbf{9}, \mathbf{8}),\\ a_3 &= (\mathbf{2}, \mathbf{5}, \mathbf{3}, \mathbf{9})(\mathbf{4}, \mathbf{8}, \mathbf{7}, \mathbf{6}),\\ a_4 &= (\mathbf{1}, \mathbf{10})(\mathbf{4}, \mathbf{5})(\mathbf{6}, \mathbf{8})(\mathbf{7}, \mathbf{9}),\\ a_5 &= (\mathbf{1}, \mathbf{11})(\mathbf{4}, \mathbf{6})(\mathbf{5}, \mathbf{9})(\mathbf{7}, \mathbf{8}),\\ a_6 &= (\mathbf{1}, \mathbf{12})(\mathbf{4}, \mathbf{7})(\mathbf{5}, \mathbf{6})(\mathbf{8}, \mathbf{9}). \end{aligned} \tag{1}$$

Элементы a_i, $i \in \{1, 2, 3, 4, 5, 6\}$, представлены перестановками множества $\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots, \mathbf{12}\}$ (здесь и далее элементы этого множества будем обозначать жирным, а элементы поля $\mathrm{GF}(q)$ — обычным шрифтом).

Увеличение параметра стойкости L происходит путем добавления следующей подстановки в порождающее множество группы. Порождающие подстановки a_1, a_2, a_3 образуют $O(2)$-стойкий шифр. При добавлении a_4 в порождающее множество образуется $O(3)$-стойкий шифр; при добавлении к последнему подстановки a_5 — $O(4)$-стойкий шифр, соответствующий M_{11}. Таким образом, группы Матьё предоставляют возможность построения из $O(L)$-стойких шифров более имитостойких $O(L+1)$-шифров. Для получения других примеров $(L, 1)$-транзитивных множеств подстановок можно отказаться от групповой структуры множества [1]. Это возможно, так как класс подстановок, образующих интересующие нас шифры, шире класса групп, которые можно применить для этой цели. Таким образом, стоит вопрос о возможности построения $O(L)$-стойких шифров при $L > 6$ не на основе групп. Чтобы лучше понять, как это сделать, нужно подробнее рассмотреть группы Матьё, точнее, связи между ними.

Вернемся к рассмотрению $O(2)$-стойкого шифра на основе группы Матьё. По наблюдению 1 это должна быть конечная плоскость, а перестановки a_1, a_2, a_3 — это некоторые аффинные операции в аффинной группе конечной плоскости, то есть $a_i(x) = xk_i + \ell_i$, $i \in \{1, 2, 3\}$.

Пусть даны две перестановки $a'(x) = xk' + \ell'$ и $a''(x) = xk'' + \ell''$. В группе Матьё определена операция суперпозиции перестановок:

$$\begin{aligned} a'' \circ a' = a''(a'(x)) = (xk' + \ell')k'' + \ell'' = \\ = (xk')k'' + (\ell'k'' + \ell'') = (xk')k'' + L. \end{aligned}$$

Произведение подстановок является прямой на плоскости при условии ассоциативности умножения, то есть если существует такое k, что $(xk')k'' = x(k'k'') = xk$. Ключом в этом случае будет $K = (k'k'', \ell'k'' + \ell'')$.

Примером системы, задаваемой конечной плоскостью с ассоциативным умножением, является система Веблена—Веддербёрна (VW-система), которая является почти-полем (и, в частности, полем). VW-системы с неассоциативным умножением использовались для решения задач в [2].

Перемножим две перестановки из (1):

$$\begin{aligned} a_2 \circ a_3 = (\mathbf{2}, \mathbf{4}, \mathbf{3}, \mathbf{7})(\mathbf{5}, \mathbf{6}, \mathbf{9}, \mathbf{8}) \circ (\mathbf{2}, \mathbf{5}, \mathbf{3}, \mathbf{9})(\mathbf{4}, \mathbf{8}, \mathbf{7}, \mathbf{6}) = \\ = (\mathbf{2}, \mathbf{8}, \mathbf{3}, \mathbf{6})(\mathbf{4}, \mathbf{9}, \mathbf{7}, \mathbf{5}), \\ a_3 \circ a_2 = (\mathbf{2}, \mathbf{5}, \mathbf{3}, \mathbf{9})(\mathbf{4}, \mathbf{8}, \mathbf{7}, \mathbf{6}) \circ (\mathbf{2}, \mathbf{4}, \mathbf{3}, \mathbf{7})(\mathbf{5}, \mathbf{6}, \mathbf{9}, \mathbf{8}) = \\ = (\mathbf{2}, \mathbf{6}, \mathbf{3}, \mathbf{8})(\mathbf{4}, \mathbf{5}, \mathbf{7}, \mathbf{9}). \end{aligned}$$

Видно, что $a_2 \circ a_3 \neq a_3 \circ a_2$. Это означает, что операция суперпозиции некоммутативна в группе, поэтому эта группа не может быть группой с операцией умножения в конечном поле $\mathrm{GF}(3^2)$. В VW-системе только почти-поля, не сводящиеся к полям, обладают свойством некоммутативности (но ассоциативности) умножения. Отсюда следует

Теорема 2. *Группа* $M_9=\langle a_1, a_2, a_3\rangle$, *являющаяся подгруппой группы Матьё* M_{11}, *задает почти-поле* $K(9)$, *приводящее к эндоморфному* $O(2)$*-стойкому шифру.*

Другие группы Матьё задаются расширениями почти-полей некоторыми элементами θ_1, θ_2, θ_3:

M_{10} задается $K(9)\cup\{\theta_1\}$,

M_{11} — $K(9)\cup\{\theta_1, \theta_2\}$,

M_{12} — $K(9)\cup\{\theta_1, \theta_2, \theta_3\}$.

2. Почти-поля, не сводящиеся к полям

Почти-поля, не сводящиеся к полям, помимо семи особых случаев, были определены Цассенхаузом [5, 6].

Пусть $q=p^h$ — степень простого числа p, а $v>1$ — натуральное число, все простые делители которого делят $(q-1)$, причем $v\not\equiv 0 \pmod 4$ при $q\equiv 3 \pmod 4$. Положим $r=hv$ и построим почти-поле $K(p^r)$ с p^r элементами из конечного поля $\mathrm{GF}(p^r)$ следующим образом:

элементы и операция сложения — те же, что и в $\mathrm{GF}(p^r)$;

произведение $w\circ u$ в $K(p^r)$ выражается через произведение $x\cdot y$ в $\mathrm{GF}(p^r)$ так:

$$w\circ u = w^{q^i}\cdot u \quad \text{при } u=z^{gv+j},\ q^i\equiv 1+j(q-1) \pmod{v(q-1)}, \qquad (2)$$

где z — некоторый фиксированный первообразный элемент поля $\mathrm{GF}(p^r)$, $g=\{1, 2, 3, \ldots\}$, а целое число i по модулю v однозначно определяется ввиду биективности автоморфизма Фробениуса. Сравнение можно записать как $q^{i-1}+q^{i-2}+\ldots+q+1\equiv j \pmod v$.

Пусть $w=z^s$, $u=z^t \ \Rightarrow\ t=gv+j$, или $t\equiv j \pmod v$. Тогда и t однозначно определяется.

Рассмотрим частный случай: почти-поле вида $K(p^2)$. Тогда $r=2=hv$; так как $v>1$, то находим единственные значения $v=2$, $h=1$.

$u=z^{gv+j}=z^{2g+j}$, $q=p^h=p$,

$w\circ u=w^{p^i s}\cdot z^{2+j}$,

$p^i\equiv 1+j(p-1) \pmod{2(p-1)}$.

При четных j (тогда $t=gj+2$ тоже будет четным) получаем

$$j(p-1)\equiv 0 \bmod 2(p-1), \quad \text{поэтому} \quad p^i=1 \ \Rightarrow\ i=0.$$

При нечетных j (тогда $t=gj+2$ тоже будет нечетным) получаем

$$j(p-1)\equiv p-1 \pmod{2(p-1)} \ \Rightarrow\ p^i=1+(p-1)=p \ \Rightarrow\ i=1.$$

Произведение в почти-поле $K(p^2)$ определяется следующим образом:

$$w\circ u=\begin{cases} z^{p^0 s}\cdot z^t = z^{(s+t) \bmod (p^2-1)}, & t \text{ четно;}\\ z^{p^1 s}\cdot z^t = z^{(ps+t) \bmod (p^2-1)}, & t \text{ нечетно.}\end{cases} \qquad (3)$$

В целях уменьшения громоздкости формул далее будем опускать $\bmod (p^2-1)$, учитывая его наличие.

Почти-поля обладают свойством правой дистрибутивности, которое вытекает из того, что возведение в степень q есть автоморфизм Фробениуса:

$$(w+u)\circ v=(w+u)^{q^i}\cdot v=(w^{q^i}+u^{q^i})\cdot v=w^{q^i}\cdot v+u^{q^i}\cdot v=w\circ u+u\circ v.$$

Проверим ассоциативность умножения в почти-поле: если элементы почти-поля представить как степени z, то необходимо доказать, что $z^a\circ z^b\circ z^c=z^a\circ(z^b\circ z^c)=(z^a\circ z^b)\circ z^c$.

$$z^a\circ(z^b\circ z^c)=\begin{cases} z^a\circ z^{b+c}, & c \text{ четно;}\\ z^a\circ z^{pb+c}, & c \text{ нечетно}\end{cases}$$

$$\Rightarrow\ z^a\circ(z^b\circ z^c)=\begin{cases} z^{a+b+c}, & (b+c) \text{ четно, } c \text{ четно;}\\ z^{pa+b+c}, & (b+c) \text{ нечетно, } c \text{ четно;}\\ z^{a+pb+c}, & (pb+c) \text{ четно, } c \text{ нечетно;}\\ z^{p(a+b)+c}, & (pb+c) \text{ нечетно, } c \text{ нечетно.}\end{cases}$$

Если c четно, $b+c$ четно, то b четно;

если c четно, $b+c$ нечетно, то b нечетно;

если c нечетно, $pb+c$ четно:

$p=2$, то решения нет;

$p\neq 2$, то b нечетно;

если c нечетно, $pb+c$ нечетно:

$p=2$, то b любое;

$p\neq 2$, то b четно.

Тогда

$$z^a\circ(z^b\circ z^c)=\begin{cases} z^{a+b+c}, & b \text{ четно, } c \text{ четно;}\\ z^{pa+b+c}, & b \text{ нечетно, } c \text{ четно;}\\ z^{a+pb+c}, & b \text{ нечетно, } c \text{ нечетно, } p\neq 2;\\ z^{p(a+b)+c}, & b \text{ четно, } c \text{ нечетно;}\\ z^{p(a+b)+c}, & c \text{ нечетно, } p=2;\end{cases} \qquad (4)$$

$$(z^a \circ z^b) \circ z^c = \begin{cases} z^{a+b} \circ z^c, & b \text{ четно;} \\ z^{pa+b} \circ z^c, & b \text{ нечетно;} \end{cases}$$

$$\Rightarrow\ (z^a \circ z^b) \circ z^c = \begin{cases} z^{a+b+c}, & c \text{ четно, } b \text{ четно;} \\ z^{p(a+b)+c}, & c \text{ нечетно, } b \text{ четно;} \\ z^{pa+b+c}, & c \text{ четно, } b \text{ нечетно;} \\ z^{p(pa+b)+c} = z^{a+pb+c}, & c \text{ нечетно, } b \text{ нечетно.} \end{cases} \tag{5}$$

При сравнении (4) и (5) убеждаемся, что $z^a \circ (z^b \circ z^c) = (z^a \circ z^b) \circ z^c$ при условии, что $p \neq 2$.

Можно построить почти-поле $K(9)$, приводящее к $O(2)$-стойкому шифру. Формула зашифрования: $y = xk + \ell$, где $x,\ \ell \in \mathrm{GF}(3^2)$, $k \in \mathrm{GF}^*(3^2)$, $\mathrm{GF}(3^2) = \{0, z^0, z^1, \ldots, z^7\}$. Умножение элементов в почти-поле $K(9)$ определяется из (3) при $p = 3$ как

$$w \circ u = z^s \circ z^t = \begin{cases} z^{(s+t) \bmod 8}, & \text{если } t \text{ четно;} \\ z^{(3s+t) \bmod 8}, & \text{если } t \text{ нечетно.} \end{cases}$$

Сложение происходит по таблице степеней неприводимого многочлена $x^2 + 2x + 2$ над полем $\mathrm{GF}(3)$, для которого первообразным элементом является z.

Взаимосвязь эндоморфных $U(2)$- и $O(2)$-стойких шифров, задаваемых линейными функциями зашифрования, показана в теореме 1. Можно ли выделить $U(2)$-стойкие шифры из $O(2)$-стойких, задаваемых в почти-полях? Для ответа на этот вопрос сначала получим результат для шифров, задаваемых циклическими массивами.

3. Взаимосвязь между циклическими $U(2)$- и $O(2)$-стойкими шифрами

Пусть $y = E(x)$ — уравнение зашифрования. Тогда $U(2)$-стойкий шифр должен удовлетворять следующему условию:

$$\forall x_1 \neq x_2\ \forall y_1 \neq y_2\ \exists! E : \left[\begin{array}{l} \text{либо } E(x_1) = y_1 \text{ и } E(x_2) = y_2, \\ \text{либо } E(x_1) = y_2 \text{ и } E(x_2) = y_1. \end{array} \right. \tag{6}$$

Условие $O(2)$-стойкости:

$$\forall x_1 \neq x_2\ \forall y_1 \neq y_2\ \exists! E : E(x_1) = y_1 \text{ и } E(x_2) = y_2. \tag{7}$$

Перепишем условия (6) и (7) через обратную функцию $x = E^{-1}(y)$:

$$E^{-1} : \left[\begin{array}{l} \text{либо } E^{-1}(y_1) = x_1 \text{ и } E^{-1}(y_2) = x_2, \\ \text{либо } E^{-1}(y_1) = x_2 \text{ и } E^{-1}(y_2) = x_1. \end{array} \right.$$

Как видим, они аналогичны условиям $U(2)$-стойкости шифра. Итак, доказано

Утверждение 1. *Если набор перестановок E образует $U(2)$- или $O(2)$-стойкий шифр, то и набор обратных перестановок E^{-1} образует $U(2)$- или $O(2)$-стойкий шифр соответственно.*

Далее рассмотрим циклические перпендикулярные массивы вида $CPA_1(2, \lambda, \lambda)$, соответствующие эндоморфному $U(2)$-стойкому шифру. Для их построения необходимо $\pi = \binom{\lambda}{2} = \lambda(\lambda - 1)/2$ ключей [1].

Пусть $\alpha(x)$ и $\beta(x)$ — произвольные функции зашифрования, соответствующие различным значениям ключа и образующие массив $CPA_1(2, \lambda, \lambda)$. Это означает, что:

1. Вместе с $\alpha(x)$ массив содержит и все ее циклические сдвиги $\alpha(x - \ell)$, где $\ell \in \mathbb{Z}_\lambda$ произвольно.
2. $\alpha(x) \pm x$ являются перестановками. Таким образом, любые две функции зашифрования $\alpha(x)$ и $\beta(x)$ из $CPA_1(2, \lambda, \lambda)$ удовлетворяют условию:

$$(\alpha(x) \pm \beta(x)) \bmod \lambda = \gamma(x) \in S_\lambda, \tag{8}$$

т. е. являются перестановками.

Пусть $K' = \{\alpha : \alpha(0) = 0,\ \alpha(1) = k\}$. Рассмотрим ситуации, при которых условие (8) $U(2)$-стойкости не выполняется:

1. $\alpha(1) = \beta(1) = k$. Тогда $\alpha(0) - \beta(0) = \alpha(1) - \beta(1) = 0$ и разность функций не является перестановкой. Поэтому существует единственная функция $\alpha(1) = k$. Параметр k является частью ключа, на котором зашифровывается открытое сообщение, и геометрически является наклоном прямой, уравнение которой является уравнением зашифрования.
2. $\alpha(1) = k,\ \beta(1) = -k$. Тогда $\alpha(1) + \beta(1) = \alpha(0) + \beta(0) = 0$ и сумма функций не является перестановкой.

Обозначим через $K'' \subset \mathbb{Z}_\lambda^*$ множество таких значений k некоторого циклического $U(2)$-стойкого шифра. Тогда из второго случая следует, что $(-k) \notin K''$ при $k \in K''$.

Определим новые операции зашифрования $\alpha_{-k}(x)$ для $k \in K''$ равенством $\alpha_{-k}(x) = -\alpha_k(x)$ (это тождество выполняется для линейных функций в поле) и сформулируем

Утверждение 2. *Подстановки вида $\alpha_{-k}(x)$ для $k \in K''$ вместе с массивом $CPA_1(2, \lambda, \lambda)$ образуют циклический массив $CA_1(2, \lambda, \lambda)$, являющийся $O(2)$-стойким шифром.*

Доказательство. Количество ключей, необходимых [1] для построения эндоморфного $O(2)$-стойкого шифра, равно

$$\pi = \frac{\lambda!}{(\lambda - L)!} = \frac{\lambda!}{(\lambda - 2)!} = \lambda(\lambda - 1).$$

Множество K'' состоит из $\lambda(\lambda-1)/2$ элементов, так как оно образует $U(2)$-стойкий шифр. Такое же количество элементов и во множестве функций $\alpha_{-k}(x)$. В сумме получается необходимое число π для $O(2)$-стойкого шифра.

Условие $O(2)$-стойкости циклического шифра:

$$(\alpha_k(x) - \alpha_m(x)) \bmod \lambda = \gamma(x) \in S_\lambda. \tag{9}$$

Заметим, что условие (9) включено в условие (8). Проверим это условие для различных k и m.

$$\begin{aligned}
&k \in K'',\ m \in K'' : \alpha_k(x) - \alpha_m(x) = \gamma(x) \in S_\lambda;\\
&k \notin K'',\ m \notin K'' \ \Rightarrow\ -k \in K'',\ -m \in K'' : \alpha_k(x) - \alpha_m(x)\\
&\qquad = -\alpha_{-k}(x) + \alpha_{-m}(x) = -(\alpha_{-k}(x) - \alpha_{-m}(x)) = -\gamma(x) \in S_\lambda;\\
&k \in K'',\ m \notin K'' \ \Rightarrow\ -m \in K'' : \alpha_k(x) - \alpha_m(x)\\
&\qquad = \alpha_k(x) + \alpha_{-m}(x) = \gamma(x) \in S_\lambda;\\
&k \notin K'',\ m \in K'' \ \Rightarrow\ -k \in K'' : \alpha_k(x) - \alpha_m(x)\\
&\qquad = -\alpha_{-k}(x) - \alpha_m(x) = -(\alpha_k(x) + \alpha_{-m}(x)) = -\gamma(x) \in S_\lambda.
\end{aligned}$$

Функция $(-\gamma(x))$, противоположная перестановке, также является перестановкой. Для каждого из четырех сочетаний k и m разность функций — это перестановка, значит, утверждение доказано. □

Замечание. Обратные подстановки (подстановки расшифрования) образуют массив $D_1(2, \lambda, \lambda)$, тоже являющийся $O(2)$-стойким шифром. Он будет циклическим только в случае ассоциативности умножения, т. е. в поле.

Действительно, если уравнением зашифрования является $y = xk + \ell$, то обратное ему $x = (y - \ell)/k = y/k - \ell/k$. Вместо x подставим y, а вместо y подставим x: $y = x/k - \ell/k$. Это уравнение задает прямую, если существуют такие m и L, что $y = xm + L$:

$L = -\ell/k$; $x/k = xm \ \Rightarrow\ \forall x : x/k = x(1/k) \ \Rightarrow\ \forall x : x = [x(1/k)]k$, так как надо $m = 1/k$, чтобы равенство выполнялось при $x = 1$.

В поле в силу ассоциативности тождество выполняется:

$$[x(1/k)]k = x[(1/k)k] = x \cdot 1 = x.$$

В полуполе, не сводящемся к полю, умножение неассоциативно, поэтому обратный циклический массив $D_1(2, \lambda, \lambda)$ в полуполе не будет являться набором прямых, а значит, по наблюдению 1 не будет образовывать $O(2)$-стойкий шифр.

Вернемся к массиву $CA_1(2, \lambda, \lambda)$.

$d_k(x) = \alpha_k^{-1}(x)$ — функция расшифрования, обратная к $\alpha_k(x)$, причем $d_k(0) = 0$, $k \in \mathbb{Z}_\lambda^*$. Если $y = \alpha_k(x - \ell)$, то $\alpha_k^{-1}(y) = x - \ell$, т. е. $d_k(y) + \ell = x$. Переобозначая $x \leftrightarrow y$, получаем $y = d_k(x) + \ell$. Согласно наблюдению 1 и утверждению 1 семейство функций, обратных к $\alpha_k(x - \ell)$, образуют эндоморфный $O(2)$-стойкий шифр и их можно представить в виде прямых вида $y = d_k(x) + \ell = x \bullet s + \ell$, $s \in \mathbb{Z}_\lambda^*$, $d_k(x) = x \bullet s$.

При $x = 1$ получаем $y = 1 \bullet s + \ell = s + \ell \pmod{\lambda}$. Поэтому $d_k(1) = s$ — наклон прямой. Также $s = d_{-k}(-1)$. Обозначим через $\overline{s}$ наклон прямой $d_{-k}(x)$, т. е. $\overline{s} = d_k(-1) = d_{-k}(1)$.

Пусть $z = \alpha_k(x)$. Функцией, обратной к $\alpha_{-k}(x) = -\alpha_k(x) = -z$, является $d_{-k}(z) = d_k(-z)$. Применяя замену $m = -k$, приходим к уравнению $y = d_m(x) + \ell = (-x) \bullet s + \ell = x \bullet \overline{s} + \ell$. При $x = 1$ получим тождество $(-1) \bullet s = 1 \bullet \overline{s} \ \Rightarrow\ \overline{s} = -s \ \Rightarrow\ (-x) \bullet m = x \bullet (-m)$ для всех x.

Итак, доказана следующая

Теорема 3. *Циклический перпендикулярный массив $CPA_1(2, \lambda, \lambda)$ и соответствующий ему эндоморфный $U(2)$-стойкий шифр существуют тогда и только тогда, когда существует конечная аффинная плоскость порядка λ, наклонные прямые в которой задаются уравнениями зашифрования $y = x \bullet s + \ell$, где $+$ — это сложение по модулю λ, $\bullet$ — умножение в такой квазигруппе на множестве ненулевых вычетов по модулю λ, которая допускает инволюцию $\mathbb{Z}_\lambda^* \to \mathbb{Z}_\lambda^*$ такую, что $m \mapsto (-m)$, $(-x) \bullet m = x \bullet (-m)$ для любого $x \in \mathbb{Z}_\lambda^*$.*

Теорема 3 развивает теорему 1, в которой также есть инволюция, только другого вида. Умножение $x \bullet s$ является частным случаем теоремы 1: соотношения $(-x)m = -(xM_k) = x(-M_k)$ переносятся на циклический массив.

Обобщим обе теоремы и выдвинем предположение о взаимосвязи $U(2)$- и $O(2)$-стойких шифров произвольного вида, используя понятие системы Веблена—Веддербёрна. Система Веблена—Веддербёрна (или VW-система) [5] является одним из типов тернара, определяющего конечную плоскость, с операциями сложения и умножения, содержащий в том числе элементы 0 и 1.

Гипотеза. Если имеется эндоморфный $U(2)$-стойкий шифр, то существует VW-система с такой квазигруппой по умножению, которая допускает инволюцию $(-x)m = x(-m)$. Обратно: если имеется $O(2)$-стойкий эндоморфный шифр, представляющий собой набор прямых в VW-системе, то в нем можно выделить $U(2)$-стойкий подшифр только тогда, когда квазигруппа по умножению допускает такую инволюцию.

По полученной теореме 3 проверим, выделяются ли $U(2)$-стойкие шифры из $O(2)$-стойкого шифра, задающегося почти-полем. То есть необходимо проверить тождественность выражения $(-w)\circ u = w\circ(-u)$.

Зная, что $1 = z^0$, $-1 = z^{(q-1)/2} = z^\alpha$, где α — четное число, получаем:

$$\textbf{1.}\ (-w)\circ u = (z^\alpha \circ z^s)\circ z^t = \begin{cases} z^{\alpha+s}\circ z^t, & s \text{ четно;} \\ z^{p\alpha+s}\circ z^t, & s \text{ нечетно.} \end{cases}$$

При нечетном p, имеющем вид $p = 2\beta+1$ (а в силу его простоты — это все простые числа, за исключением числа 2), получаем:

$$p\alpha = \left((2\beta+1)\frac{q-1}{2}\right) \bmod (q-1) = \\ = \left(\beta(q-1) + \frac{q-1}{2}\right) \bmod (q-1) = 0 + \frac{q-1}{2} = \alpha.$$

Если же $p = 2$, то $p\alpha = 2(q-1/2) \bmod (q-1) = 0$. Поэтому

$$(-w)\circ u = \begin{cases} z^{\alpha+s}\circ z^t, & p \neq 2; \\ z^{\alpha+s}\circ z^t, & p = 2,\ s \text{ четно;} \\ z^{p\alpha+s}\circ z^t = z^s \circ z^t, & p = 2,\ s \text{ нечетно.} \end{cases}$$

При $p \neq 2$:

$$(-w)\circ u = \begin{cases} z^{\alpha+s+t}, & t \text{ четно;} \\ z^{p(\alpha+s)+t}\circ z^t = z^{\alpha+ps+t}, & t \text{ нечетно.} \end{cases} \qquad (10)$$

При $p = 2$:

$$(-w)\circ u = \begin{cases} z^{\alpha+s+t}, & s \text{ четно},\ t \text{ четно;} \\ z^{p(\alpha+s)+t} = z^{ps+t}, & s \text{ четно},\ t \text{ нечетно;} \\ z^{s+t}, & s \text{ нечетно},\ t \text{ четно;} \\ z^{ps+t}, & s \text{ нечетно},\ t \text{ нечетно.} \end{cases} \qquad (11)$$

$$\textbf{2.}\ w\circ(-u) = (z^\alpha \circ z^s)\circ z^t = \begin{cases} z^s \circ z^{\alpha+t}, & t \text{ четно;} \\ z^s \circ z^{p\alpha+t}, & t \text{ нечетно.} \end{cases}$$

Так как α четно, то $(\alpha+t)$ четно при четном t и нечетно при нечетном t. Учитывая это, получаем:

$$w\circ(-u) = \begin{cases} z^{s+\alpha+t}, & t \text{ четно;} \\ z^s\circ z^{p\alpha+t} = z^s\circ z^t = z^{ps+t}, & t \text{ нечетно},\ p = 2; \\ z^s\circ z^{p\alpha+t} = z^s\circ z^{\alpha+t} = z^{ps+\alpha+t}, & t \text{ нечетно},\ p \neq 2. \end{cases} \qquad (12)$$

Сравнивая (10) и (11) с (12), приходим к выводу, что они тождественны друг другу при $p \neq 2$. Так как умножение в почти-поле ассоциативно, то $(-w)\circ u = (z^\alpha \circ z^s)\circ z^t = z^\alpha \circ (z^s \circ z^t) = -(w\circ u) = w\circ(-u)$, а значит, справедлива следующая

Теорема 4. *В почти-поле $K(p^2)$, приводящем к эндоморфному $O(2)$-стойкому шифру, при $p \neq 2$ выделяется эндоморфный $U(2)$-стойкий шифр.*

Таким образом, построен новый класс $O(2)$- и $U(2)$-стойких шифров, полученных из недезарговых конечных плоскостей, то есть не сводящихся к полю.

4. Выражение элементов группы Матьё через операции в почти-поле

Вернемся к группам Матьё. С учетом теоремы 2 перестановки определяются формулой $a_i = x\circ k_i + \ell_i$. Теперь представим элементы множества $\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots, \mathbf{12}\}$ степенями первообразного элемента $z \in K(9)$, то есть найдем такие изоморфизмы $\phi(x)\colon M_9 \to K(9)$, и определим функции $a_i(x)$ через операции в почти-поле. Для этого выполним следующие действия, используя (1).

1. Возьмем $\mathbf{1} = 0$. В перестановках a_2 и a_3 элемент $\mathbf{1}$ переходит сам в себя:

$$a_2(0) = 0 \ \Rightarrow\ 0 = 0\circ k_2 + \ell_2 \ \Rightarrow\ \ell_2 = 0,$$
$$a_3(0) = 0 \ \Rightarrow\ 0 = 0\circ k_3 + \ell_3 \ \Rightarrow\ \ell_3 = 0.$$

2. Из первого цикла перестановки a_1 следует:

$$\begin{cases} \mathbf{1}\circ k_1 + \ell_1 = \mathbf{2}, \\ \mathbf{2}\circ k_1 + \ell_1 = \mathbf{3}, \\ \mathbf{3}\circ k_1 + \ell_1 = \mathbf{1} \end{cases} \Rightarrow \begin{cases} 0\circ k_1 + \ell_1 = \mathbf{2}, \\ \mathbf{2}\circ k_1 + \ell_1 = \mathbf{3}, \\ \mathbf{3}\circ k_1 + \ell_1 = 0 \end{cases} \Rightarrow \begin{cases} \mathbf{2} = \ell_1, \\ \mathbf{2}\circ k_1 + \mathbf{2} = \mathbf{3}, \\ \mathbf{3}\circ k_1 + \mathbf{2} = 0 \end{cases}$$
$$\Rightarrow\ (\mathbf{2}\circ k_1 + \mathbf{2})\circ k_1 + \mathbf{2} = 0 \ \Rightarrow\ \mathbf{2}\circ k_1\circ k_1 + \mathbf{2}\circ k_1 + \mathbf{2} = 0.$$

Пусть $\mathbf{2} = z^\delta$, $k_1 = z^\epsilon$. Тогда $z^\delta \circ z^\epsilon \circ z^\epsilon + z^\delta \circ z^\epsilon + z^\delta = 0$.

Если ϵ нечетно ($4\epsilon \equiv 4 \pmod 8$ при нечетном ϵ):

$$z^\delta \circ z^\epsilon \circ z^\epsilon + z^\delta \circ z^\epsilon + z^\delta = z^\delta \circ z^{3\epsilon+\epsilon} + z^{3\delta+\epsilon} + z^\delta$$
$$= z^\delta \circ z^{4\epsilon} + z^{3\delta+\epsilon} + z^\delta = z^{\delta+4} + z^{3\delta+\epsilon} + z^0 \circ z^\delta$$
$$= z^{3\delta+\epsilon} + (z^4 + z^0) \circ z^\delta = z^{3\delta+\epsilon} + 0 = z^{3\delta+\epsilon}$$
$$\Rightarrow\ z^{3\delta+\epsilon} = 0 \text{ не имеет решения.}$$

Если ϵ четно (2ϵ тоже четно):

$$z^\delta \circ z^\epsilon \circ z^\epsilon + z^\delta \circ z^\epsilon + z^\delta$$
$$= z^\delta \circ z^{\epsilon+\epsilon} + z^{\delta+\epsilon} + z^\delta = z^\delta \circ z^{2\epsilon} + z^{\delta+\epsilon} + z^\delta$$
$$= z^{\delta+2\epsilon} + z^{\delta+\epsilon} + z^\delta = \begin{cases} z^\delta + z^\delta + z^{\delta+\epsilon} = 2z^\delta + z^{\delta+\epsilon}, \\ z^{\delta+4} + z^\delta + z^{\delta+\epsilon} = z^{\delta+\epsilon} \end{cases}$$
$$\Rightarrow \begin{cases} 2z^\delta + z^{\delta+\epsilon} = 0\ \Rightarrow\ z^{\delta+\epsilon} = z^\delta\ \Rightarrow\ \epsilon = 0, \\ z^{\delta+\epsilon} = 0 \text{ не имеет решения.} \end{cases}$$

Отсюда следует, что есть только единственное значение $k_1 = z^0$.

3. $\mathbf{2} \circ k_1 + \mathbf{2} = \mathbf{3}\ \Rightarrow\ \mathbf{2} \circ z^0 + \mathbf{2} = \mathbf{3}$. Пусть $\mathbf{3} = z^\sigma$:

$$z^\delta \circ z^0 + z^\delta = z^\sigma\ \Rightarrow\ z^\delta + z^\delta = z^\sigma\ \Rightarrow\ z^\sigma = 2z^\delta.$$

Поэтому возможны следующие пары значений $(\mathbf{2}, \mathbf{3})$ в одном изоморфизме:

(0, 4); (1, 5); (2, 6); (3, 7); (4, 0); (5, 1); (6, 2); (7, 3).

4. Для каждой такой пары выписываем все возможные значения k_2, за исключением

- $k_2 = z^0$, так как тогда $\mathbf{2} \circ k_2 = \mathbf{4}\ \Rightarrow\ \mathbf{2} \circ z^0 = \mathbf{4}\ \Rightarrow\ \mathbf{2} = \mathbf{4}$, чего не может быть;
- $k_2 = z^4$, так как тогда $(\mathbf{2} \circ k_2) \circ k_2 = \mathbf{3}\ \Rightarrow\ \mathbf{2} \circ (z^4 \circ z^4) = \mathbf{3}\ \Rightarrow\ \mathbf{2} \circ z^0 = \mathbf{3}\ \Rightarrow$ $\Rightarrow\ \mathbf{2} = \mathbf{4}$, чего не может быть,

и выражаем остальные элементы множества через найденные.

5. $\mathbf{4} = \mathbf{2} \circ k_2$.

6. $\mathbf{5} = \mathbf{4} \circ k_1 + \ell_1$.

7. $\mathbf{6} = \mathbf{5} \circ k_1 + \ell_1$.

8. $\mathbf{7} = \mathbf{3} \circ k_2$.

9. $\mathbf{8} = \mathbf{7} \circ k_1 + \ell_1$.

10. $\mathbf{9} = \mathbf{8} \circ k_1 + \ell_1$.

11. $k_3 = \mathbf{2}^{-1} \circ \mathbf{5}$.

12. Составим таблицу изоморфизмов (см. таблицу 1). Например, для подчеркнутого изоморфизма перестановки задаются следующими функциями: $a_1 = x \circ z^0 + z^0$, $a_2 = x \circ z^7$, $a_1 = x \circ z^1$.

Таблица 1. Изоморфизмы $\phi(x)\colon M_9 \to K(9)$

k_2	k_3	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	2	$*$	0	4	1	2	7	5	3	6
2	7	$*$	0	4	2	7	1	6	5	3
3	6	$*$	0	4	3	6	5	7	1	2
5	3	$*$	0	4	5	3	6	1	2	7
6	5	$*$	0	4	6	5	3	2	7	1
7	1	$\underline{*}$	$\underline{0}$	$\underline{4}$	$\underline{7}$	$\underline{1}$	$\underline{2}$	$\underline{3}$	$\underline{6}$	$\underline{5}$
1	6	$*$	1	5	4	7	6	0	2	3
2	5	$*$	1	5	3	0	2	7	6	4
3	1	$*$	1	5	6	4	7	2	3	0
5	7	$*$	1	5	0	2	3	4	7	6
6	3	$*$	1	5	7	6	4	3	0	2
7	2	$*$	1	5	2	3	0	6	4	7
1	4	$*$	2	6	7	5	0	3	4	1
2	0	$*$	2	6	4	1	3	0	7	5
3	2	$*$	2	6	1	3	4	5	0	7
5	2	$*$	2	6	3	4	1	7	5	0
6	1	$*$	2	6	0	7	5	4	1	3
7	6	$*$	2	6	5	0	7	1	3	4
1	3	$*$	3	7	2	4	5	6	1	0
2	1	$*$	3	7	5	2	4	1	0	6
3	2	$*$	3	7	4	5	2	0	6	1
5	6	$*$	3	7	6	1	0	2	4	5
6	7	$*$	3	7	1	0	6	5	2	4
7	5	$*$	3	7	0	6	1	4	5	2

k_2	k_3	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	2	$*$	4	0	5	6	3	1	7	2
2	7	$*$	4	0	6	3	5	2	1	7
3	6	$*$	4	0	7	2	1	3	5	6
5	3	$*$	4	0	1	7	2	5	6	3
6	5	$*$	4	0	2	1	7	6	3	5
7	1	$*$	4	0	3	5	6	7	2	1
1	6	$*$	5	1	0	3	2	4	6	7
2	5	$*$	5	1	7	4	6	3	2	0
3	1	$*$	5	1	2	0	3	6	7	4
5	4	$*$	5	1	4	6	7	0	3	2
6	3	$*$	5	1	3	2	0	7	4	6
7	6	$*$	5	1	6	7	4	2	0	3
1	7	$*$	6	2	3	1	4	7	0	5
2	3	$*$	6	2	0	5	7	4	3	1
3	5	$*$	6	2	5	7	0	1	4	3
5	2	$*$	6	2	7	0	5	3	1	4
6	1	$*$	6	2	4	3	1	0	5	7
7	6	$*$	6	2	1	4	3	5	7	0
1	3	$*$	7	3	6	0	1	2	5	4
2	1	$*$	7	3	1	6	0	5	4	2
3	2	$*$	7	3	0	1	6	4	2	5
5	6	$*$	7	3	2	5	4	6	0	1
6	7	$*$	7	3	5	4	2	1	6	0
7	5	$*$	7	3	4	2	5	0	1	6

5. $O(3)$-стойкие шифры на основе почти-полей, не сводящихся к полям

В предыдущем разделе были выписаны изоморфизмы (см. таблицу 1) для построения 48-ми различных массивов, соответствующих $O(2)$-стойким шифрам. Поставим задачу расширения эндоморфного $O(2)$-стойкого до эндоморфного $O(3)$-стойкого шифра.

Обобщая конструкцию включения почти-поля $K(9)$ в группы Матьё, предложим следующую формулу.

Будем уравнение зашифрования записывать в виде либо $y = h(x+d) \circ$ $\circ\, k + \ell$, либо $y = x \circ k + \ell$, где $+$ и $\circ$ — сложение и умножение, d, k и ℓ — элементы почти-поля $K(p^r)$, соответствующего полю $\mathrm{GF}(p^r)$, $k \neq 0$, а функция $h(x)$ задается равенством $h(x) = 1/x$, где деление осуществляется в поле $\mathrm{GF}(p^r)$. При этом считаем, что $h(0) = \infty$, $h(\infty) = 0$.

Если $d = \infty$, то для любого x получаем $h(x+d) = 0$, то есть функция $y = h(x+d) \circ k + \ell$ не будет являться перестановкой множества $K(p^r) \cup \{\infty\}$. Поэтому при $d = \infty$ уравнением зашифрования будет $y = x \circ k + \ell$.

Лемма. *Функции зашифрования $f_{d,k,\ell} = h(x+d) \circ k + \ell$, где $h(x) =$ $= 1/x$ с делением в поле $\mathrm{GF}(p^r)$, $\circ$ — умножение в почти-поле $K(p^r)$, являются перестановками множества $K(p^r) \cup \{\infty\}$ мощности $\lambda = p^r + 1$.*

Доказательство. Рассмотрим систему

$$\begin{cases} y_1 = h(x_1 + d) \circ k + \ell, \\ y_2 = h(x_2 + d) \circ k + \ell. \end{cases}$$

Если функции не будут являться перестановками, то $\exists\, d,\ k,\ \ell : y_1 = y_2$. Поэтому

$$h(x_1 + d) \circ k + \ell = h(x_2 + d) \circ k + \ell \Leftrightarrow h(x_1 + d) \circ k = h(x_2 + d) \circ k.$$

Так как в обеих частях тождества правые множители одинаковые, из (2) следует, что левые множители тоже одинаковые:

$$h(x_1 + d) = h(x_2 + d) \;\Rightarrow\; \frac{1}{x_1 + d} = \frac{1}{x_2 + d} \Leftrightarrow x_1 + d = x_2 + d \Leftrightarrow x_1 = x_2,$$

чего не может быть. Лемма доказана. □

Проверим наличие $O(3)$-стойкости для предложенных формул зашифрования. Пусть требуется найти ключ функции зашифрования, переводящей три различные шифрвеличины x_1, x_2, x_3 в соответственно три шифрвеличины y_1, y_2, y_3. Составляем для трех неизвестных d, k и ℓ систему трех уравнений:

$$\begin{cases} y_1 = h(x_1 + d) \circ k + \ell; \\ y_2 = h(x_2 + d) \circ k + \ell; \\ y_3 = h(x_3 + d) \circ k + \ell. \end{cases} \tag{13}$$

Вычитанием с использованием правой дистрибутивности получим в качестве следствия два уравнения с исключенным ℓ:

$$\begin{cases} y_1 - y_3 = [h(x_1 + d) - h(x_3 + d)] \circ k; \\ y_2 - y_3 = [h(x_2 + d) - h(x_3 + d)] \circ k. \end{cases} \tag{14}$$

Исходя из (2) элемент k представляется как неизвестный правый множитель u в почти-поле, что позволяет записать (14) как уравнения в поле $\mathrm{GF}(p^r)$:

$$\begin{cases} y_1 - y_3 = [h(x_1 + d) - h(x_3 + d)]^{q^i} \cdot k; \\ y_2 - y_3 = [h(x_2 + d) - h(x_3 + d)]^{q^i} \cdot k. \end{cases}$$

Разделив одно уравнение на другое, исключаем k, получая в поле $\mathrm{GF}(p^r)$ одно уравнение для d:

$$\frac{y_1 - y_3}{y_2 - y_3} = \left[\frac{h(x_1 + d) - h(x_3 + d)}{h(x_2 + d) - h(x_3 + d)}\right]^{q^i}.$$

Так как $h(x) = 1/x$, вычисляем

$$h(x_i + d) - h(x_3 + d) = \frac{1}{x_i + d} - \frac{1}{x_3 + d} = \frac{x_3 + d - (x_i + d)}{(x_i + d)(x_3 + d)} = \frac{x_3 - x_i}{(x_i + d)(x_3 + d)}$$

и приводим это уравнение к виду

$$\frac{y_1 - y_3}{y_2 - y_3} = \left[\frac{\dfrac{x_3 - x_1}{(x_1 + d)(x_3 + d)}}{\dfrac{x_3 - x_2}{(x_2 + d)(x_3 + d)}}\right]^{q^i} = \left[\frac{(x_3 - x_1)(x_2 + d)(x_3 + d)}{(x_1 + d)(x_3 + d)(x_3 - x_2)}\right]^{q^i}.$$

Множители $x_3 + d$ сокращаются, а так как автоморфизм Фробениуса — линейное преобразование, это уравнение можно рассматривать как линейное:

$$\frac{y_1 - y_3}{y_2 - y_3} = \left[\frac{x_3 - x_1}{x_3 - x_2}\right]^{q^i} \frac{x_2^{q^i} + d^{q^i}}{x_1^{q^i} + d^{q^i}}.$$

Домножим правую и левую части на $x_1^{q^i} + d^{q^i}$:

$$\frac{y_1 - y_3}{y_2 - y_3}(x_1^{q^i} + d^{q^i}) = \left[\frac{x_3 - x_1}{x_3 - x_2}\right]^{q^i} (x_2^{q^i} + d^{q^i})$$

$$\Rightarrow \left[\frac{y_1 - y_3}{y_2 - y_3} - \left(\frac{x_3 - x_1}{x_3 - x_2}\right)^{q^i}\right] d^{q^i} = \left[\left(\frac{x_3 - x_1}{x_3 - x_2}\right)^{q^i} x_2^{q^i} - \frac{y_1 - y_3}{y_2 - y_3} x_1^{q^i}\right].$$

Если

$$\left[\frac{y_1-y_3}{y_2-y_3}-\left(\frac{x_3-x_1}{x_3-x_2}\right)^{q^i}\right]\neq 0,$$

то

$$d^{q^i}=\left[\frac{\left(\frac{x_3-x_1}{x_3-x_2}\right)^{q^i}x_2^{q^i}-\left(\frac{y_1-y_3}{y_2-y_3}\right)x_1^{q^i}}{\frac{y_1-y_3}{y_2-y_3}-\left(\frac{x_3-x_1}{x_3-x_2}\right)^{q^i}}\right].$$

Возведем обе части в степень q^{v-i}:

$$(d^{q^i})^{q^{v-i}}=\left[\frac{\left(\frac{x_3-x_1}{x_3-x_2}\right)^{q^i}\cdot x_2^{q^i}-\left(\frac{y_1-y_3}{y_2-y_3}\right)\cdot x_1^{q^i}}{\frac{y_1-y_3}{y_2-y_3}-\left(\frac{x_3-x_1}{x_3-x_2}\right)^{q^i}}\right]^{q^{v-i}},$$

$$(d^{q^i})^{q^{v-i}}=d^{q^iq^{v-i}}=d^{q^{i+v-i}}=d^{q^v}.$$

В силу того, что $q=p^h$, $r=hv$, то рассматриваемое нами поле $\mathrm{GF}(p^r)=\mathrm{GF}(q^v)$, а значит, $d^{q^v}=d$. Тогда d однозначно определяется (а вслед за ним k и ℓ) из равенства

$$d=\left[\frac{\left(\frac{x_3-x_1}{x_3-x_2}\right)^{q^i}x_2^{q^i}-\left(\frac{y_1-y_3}{y_2-y_3}\right)x_1^{q^i}}{\frac{y_1-y_3}{y_2-y_3}-\left(\frac{x_3-x_1}{x_3-x_2}\right)^{q^i}}\right]^{q^{v-i}},$$

а искомое уравнение зашифрования будет нелинейным и записываться с использованием функции h.

Если же

$$\left[\frac{y_1-y_3}{y_2-y_3}-\left(\frac{x_3-x_1}{x_3-x_2}\right)^{q^i}\right]=0,$$

то $d=\infty$ и уравнение зашифрования будем считать линейным.

Действительно, запишем систему (13) для двух неизвестных k, ℓ без использования функции h в виде $y_m=x_m\circ k+\ell$, $m=\{1,\,2,\,3\}$. Вычитанием исключая ℓ, получим, ввиду правой дистрибутивности, два уравнения для одной неизвестной k:

$$\begin{cases}y_1-y_3=(x_1-x_3)\circ k;\\ y_2-y_3=(x_2-x_3)\circ k.\end{cases}\tag{15}$$

Отсюда получается равенство $(x_1-x_3)\setminus(y_1-y_3)=(x_2-x_3)\setminus(y_2-y_3)$, означающее, что данные точки $(x_m,\,y_m)$ $(m=1,\,2,\,3)$ лежат на одной прямой в плоскости, определяемой данным почти-полем, а искомые k и ℓ существуют и единственным образом определены (здесь знак $\setminus$ означает левое деление в квазигруппе ненулевых элементов почти-поля).

По формуле (2) система (15) в терминах поля выглядит как

$$\begin{aligned}\frac{y_1-y_3}{y_2-y_3}&=\frac{(x_1-x_3)\circ k}{(x_2-x_3)\circ k}=\frac{(x_1-x_3)^{q^i}\cdot k}{(x_2-x_3)^{q^i}\cdot k}\\ &=\frac{(x_1-x_3)^{q^i}}{(x_2-x_3)^{q^i}}\cdot\frac{k}{k}=\left[\frac{x_1-x_3}{x_2-x_3}\right]^{q^i}.\end{aligned}\tag{16}$$

Целые числа i и j из уравнения (16) определяются однозначно (в случае существования k), см. (2). Для определения g из (2) запишем (16) в виде

$$\frac{y_1-y_3}{(x_1-x_3)^{q^i}}=\frac{y_2-y_3}{(x_2-x_3)^{q^i}},$$

а затем подставим в уравнения (15), записанные через умножение в поле:

$$\begin{cases}\frac{y_1-y_3}{(x_1-x_3)^{q^i}}=z^{gv+j};\\ \frac{y_2-y_3}{(x_2-x_3)^{q^i}}=z^{gv+j}.\end{cases}$$

Ясно, что это одно уравнение:

$$z^{gv+j}=z^t=\frac{y_1-y_3}{(x_1-x_3)^{q^i}}=\frac{y_2-y_3}{(x_2-x_3)^{q^i}}.$$

Из свойств числа v, выбранного при построении почти-поля так, чтобы получалась конечная плоскость, вытекает, что g определяется однозначно. Таким образом, доказана

Теорема 5. *Уравнение зашифрования*

$$\begin{cases}y=h(x+d)\circ k+\ell, & d\neq\infty;\\ y=x\circ k+\ell, & d=\infty,\end{cases}$$

где $h(x)=1/x$ (*деление осуществляется в поле* $\mathrm{GF}(p^r)$), $x,\,d\in K(p^r)\cup\{\infty\}$, $k\in K(p^r)\setminus\{0\}$, $\ell\in K(p^r)$, *дает* $O(3)$-*стойкий шифр*.

Из таблицы 1 найдем изоморфизмы, для которых $a_i(x)=\frac{1}{x}$, $i\in\{4,\,5,\,6\}$, где деление происходит в поле $\mathrm{GF}(9)$ и, значит, перестановка распадается на циклы

$$a_i=(0,\,\infty)(z^0)(z^1,\,z^7)(z^2,\,z^6)(z^3,\,z^5)(z^4),\quad i\in\{4,\,5,\,6\}.$$

Для выполнения этого условия необходимо, чтобы для a_4, a_5, a_6 соответственно было $\theta_1=\infty$, $\theta_2=\infty$, $\theta_3=\infty$.

Таблица 2. Изоморфизмы $\phi(x)$ при $a_i(x) = 1/x$

$a_i(x)$	k_2	k_3	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
$a_4(x) = 1/x$	5	3	$*$	0	4	5	3	6	1	2	7	∞	θ_2	θ_3
	7	1	$*$	0	4	7	1	2	3	6	5	∞	θ_2	θ_3
	5	3	$*$	4	0	1	7	2	5	6	3	∞	θ_2	θ_3
	7	1	$*$	4	0	3	5	6	7	2	1	∞	θ_2	θ_3
$a_5(x) = 1/x$	1	2	$*$	0	4	1	2	7	5	3	6	θ_1	∞	θ_3
	3	6	$*$	0	4	3	6	5	7	1	2	θ_1	∞	θ_3
	1	2	$*$	4	0	5	6	3	1	7	2	θ_1	∞	θ_3
	3	6	$*$	4	0	7	2	1	3	5	6	θ_1	∞	θ_3
$a_6(x) = 1/x$	2	7	$*$	0	4	2	7	1	6	5	3	θ_1	θ_2	∞
	6	5	$*$	0	4	6	5	3	2	7	1	θ_1	θ_2	∞
	2	7	$*$	4	0	6	3	5	2	1	7	θ_1	θ_2	∞
	6	5	$*$	4	0	2	1	7	6	3	5	θ_1	θ_2	∞

Исходя из таблицы 2 можно сделать вывод, что $O(3)$-стойкий шифр строится не только на основе группы $\langle a_1, a_2, a_3, a_4\rangle$, но и $\langle a_1, a_2, a_3, a_5\rangle$, и $\langle a_1, a_2, a_3, a_6\rangle$, где $a_4(x) = 1/x$, $a_5(x) = 1/x$, $a_6(x) = 1/x$.

Таким образом, на основе анализа групп Матьё построен эндоморфный $O(3)$-стойкий шифр на основе аналога дробно-линейных преобразований в произвольных почти-полях. Применяя аналогичные рассуждения, возможно, удастся построить новые классы $O(L)$-стойких шифров для $L > 3$.

Заключение

Полученные результаты показали важность и полезность развитой геометрической методики, основанной на наблюдения 1, для исследования современных аналогов совершенных шифров. Построен новый класс $O(2)$- и $U(2)$-стойких шифров, полученных из недезарговых конечных плоскостей.

Исследована взаимосвязь между циклическими $U(2)$- и $O(2)$-стойкими шифрами.

Найдена связь между группами Матьё и почти-полями, на основе их анализа построена бесконечная серия эндоморфных $O(3)$-стойких шифров на основе аналога дробно-линейных преобразований в произвольных

почти-полях, не сводящихся к полям, возможность чего для некоторых конечных плоскостей была анонсирована в [3].

Привлечение более тонких алгебраических, в том числе групповых свойств, может привести к новым критериям существования и эффективным комбинаторным конструкциям.

Авторы благодарят М. М. Глухова и В. В. Ященко за внимание к работе, Н. П. Варновского за направляющие дискуссии, а также В. В. Кабанова и А. А. Махнёва за полезные обсуждения.

Литература

[1] *Зубов А. Ю.* Криптографические методы защиты информации. Совершенные шифры: Учебное пособие. М.: Гелиос АРВ, 2005. 192 с.

[2] *Коновалова С. С.*, *Титов С. С.* О конструкциях эндоморфных совершенных шифров // Материалы межд. науч. конф. по проблемам безопасности и противодействия терроризму. Интеллектуальный Центр МГУ, 2—3 ноября 2005 г. М.: МЦНМО, 2006. С. 168—180.

[3] *Коновалова С. С.*, *Титов С. С.* О конструкциях эндоморфных совершенных шифров // В сб. Проблемы прикладной математики. Екатеринбург: УрГУПС, 2006. Т. 2. № 41(124). С. 70—106.

[4] *Глухов М. М.*, *Елизаров В. П.*, *Нечаев А. А.* Алгебра: Учебник в 2 т. М.: Гелиос АРВ., 2003. Т. 2. 416 с.

[5] *Холл М.* Комбинаторика. М.: Мир, 1970. 424 с.

[6] *Zassenhaus H.* Über endliche Fastkorper. Abh. Math. Sem. Hamburg, 1936. 11. P. 187—220.

Использование стохастических зависимостей в видеоконтейнере формата MPEG для оценки его емкости

А. В. Зырянов

Цифровые водяные знаки (далее ЦВЗ) получили широкое распространение в области защиты авторских прав, контроля целостности и подлинности различной мультимедиа-информации [3, 4]. В докладе рассматриваются видеоконтейнеры формата MPEG и вопросы защиты авторских прав на видео с использованием цифровых водяных знаков. В частности, исследуется оценка максимального размера ЦВЗ, которого можно поместить в видеоконтейнер алгоритмом, использующим для вставки информации спектр ДКП кадров видео.

Под *емкостью C* контейнера будем понимать отношение максимального объема данных, которые можно вставить в этот контейнер алгоритмом вставки ЦВЗ к размеру самого контейнера:

$$C(B, F) = \frac{V_{\text{emb}}(B, F)}{V_B}, \qquad (1)$$

где B — контейнер, F — конкретный алгоритм вставки ЦВЗ, V_B — размер контейнера (в байтах), $V_{\text{emb}}(B, F)$ — максимальный размер ЦВЗ (в байтах). Максимальный размер ЦВЗ обычно зависит от количества описывающих контейнер коэффициентов, которые возможно изменить с целью вставки ЦВЗ. Таким образом, емкость контейнера зависит как от контейнера, так и от метода вставки данных. Обозначим

$$C_{\max}(B, I) = \max_{F \in I} C(B, F)$$

— максимальная емкость контейнера для алгоритмов из некоторого класса I алгоритмов вставки ЦВЗ.

При разработке алгоритма ЦВЗ необходимо учитывать максимальную емкость, которую имеет контейнер, и, отталкиваясь от неё, искать компромисс между объемом передаваемого водяного знака, устойчивостью и незаметностью. Можно предположить, что с увеличением размера ЦВЗ, есть возможность улучшить устойчивость ЦВЗ к атакам. Примерами такого усиления могут служить методы сокрытия с расширением спектра (spread-spectrum) [2].

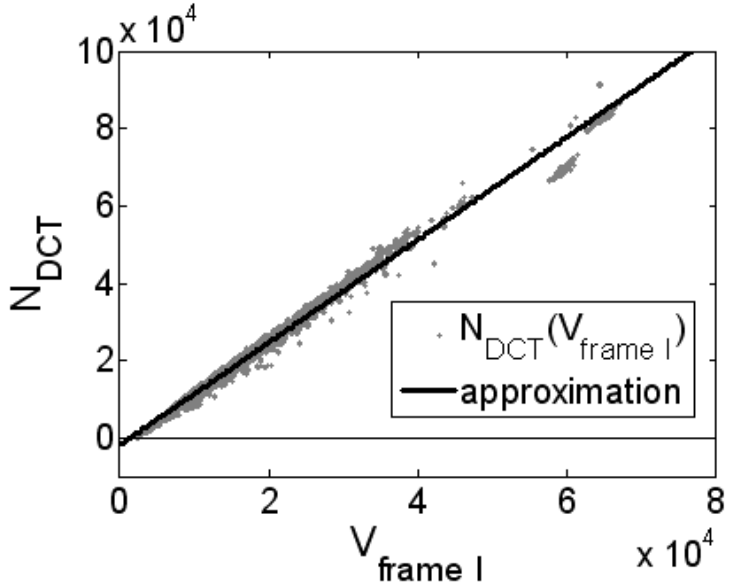


Рис. 1. Зависимость числа ненулевых коэффициентов ДКП от размера кадра (на примере опорных кадров видеопотока MPEG-2)

В работе рассматривается класс I_{DCT} алгоритмов, использующих для вставки ЦВЗ спектр ДКП кадров видео. Сегодня многие методы используют именно этот подход к сокрытию, что связано с легкой интеграцией модуля вставки ЦВЗ в кодер видеопотока и низкой вычислительной сложностью. Примерами таких алгоритмов могут служить работы [1, 2]. При этом, во избежание увеличения размера и ухудшения визуальных качеств контейнера, модификации подвергаются только ненулевые коэффициенты ДКП. Таким образом, для вычисления максимальной емкости $C_{\max}(B, I_{\text{DCT}})$ фактически требуется оценить количество ненулевых коэффициентов ДКП кадров видео.

Пусть $\xi(\omega)$ — случайная величина, которая задает размер битового потока (в байтах), представляющего собой сжатый кадр видео, а $\eta(\omega)$ — задает количество ненулевых коэффициентов ДКП, описывающих данный кадр. В докладе показана и продемонстрирована на практике линейная регрессия числа ненулевых коэффициентов ДКП на размер кадра (см. рис. 1). Исходя из этого, можно предложить статистическую оценку ем-

кости $\widehat{C}_{\max}(B,\, I_{\mathrm{DCT}})$, минимизирующую ошибку

$$D = \mathsf{M}\left[\left(C_{\max}(B,\, I_{\mathrm{DCT}}) - \widehat{C}_{\max}(B,\, I_{\mathrm{DCT}})\right)^2\right],$$

где $\mathsf{M}[\ldots]$ — математическое ожидание.

Утверждение. *Оценка $C_{\max}(B,\, I_{DCT})$ в указанных выше обозначениях может быть вычислена по следующей формуле*:

$$\widehat{C}_{\max}(B,\, I_{DCT}) = \rho_{\xi\eta}\frac{\sigma_\eta}{\sigma_\xi}\left(1 - \frac{\mu_\xi}{L_m}\right) + \frac{\mu_\eta}{L_m}, \tag{2}$$

где L_m — средняя длина кадра в видеопотоке. При этом достигается минимум ошибки, равный $D_{\min} = \sigma_\eta^2\left(1 - \rho_{\xi\eta}^2\right)$.

Учитывая тот факт, что в реальном видеопотоке (см. рис. 1) $\rho_{\xi\eta} \approx 1$, получаем $D_{\min} \approx 0$ и $C_{\max}(B,\, I_{\mathrm{DCT}}) \approx \mu_\eta/\mu_\xi$.

Сравнение экспериментальных данных и результатов моделирования отражено в таблице 1.

Таблица 1. Расчет емкости различных контейнеров формата MPEG

Тип контейнера	Результат эксперимента	Оценка $\widehat{C}_{\max}(B,\, I_{\mathrm{DCT}})$
«Интервью»	0.9426	0.9055
«Динамика»	0.9757	0.9764

Таким образом, показано, что задача оценки емкости видеоконтейнера может быть сведена к определению зависимости моментов статистических величин $\xi(\omega)$ и $\eta(\omega)$ от типа видеоконтейнера. Однако, как показали эксперименты, характер регрессионной зависимости, в частности, параметры b_0 и b_1 линейной регрессии, существенно зависят от вида видеопоследовательности (динамичное видео, интервью и т. д.), а также от типа исследуемых кадров (интра-кадры, интер-кадры). Эти зависимости отражаются на качестве приведенной выше оценки и являются предметом дальнейшего исследования.

Литература

[1] *C. Busch*, *W. Funk*, *S. Wolthusen*. Digital watermarking: from concepts to real-time video applications. IEEE Computer Graphics and Applications, v. 19, p. 25—35.

[2] *F. Hartung*, *B. Girod*. Digital watermarking of MPEG-2 coded video in the bitstream domain. Proceeding of International Conference on Acoustics, Speech and Signal Processing, v. 4. P. 2621—2624.

[3] *А. В. Аграновский*, *П. Н. Девянин*, *Р. А. Хади*, *А. В. Черемушкин*. Основы компьютерной стеганографии. М.: Радио и связь, 2003.

[4] *В. Г. Грибунин*, *И. Н. Оков*, *И. В. Туринцев*. Цифровая стеганография. М.: СОЛОН-Пресс, 2002.

[5] *Е. И. Куликов*. Прикладной статистический анализ. М.: Радио и связь, 2003, 376 с.

Построение адаптивных методов внедрения ЦВЗ в изображения с использованием контрастности

Б. Б. Борисенко

Адаптивные методы внедрения цифровых водяных знаков (ЦВЗ) в файлы графических форматов основаны в том числе и на использовании характеристик качества изображения. Применение характеристик позволяет успешнее противостоять методам визуального анализа изображений на предмет наличия ЦВЗ. Кроме того, статистические тесты также дают худшие результаты при внесении ЦВЗ адаптивными методами.

В исследовании автором был использован ряд характеристик качества изображения. Это объясняется тем, что различные характеристики обладают различной чувствительностью по отношению к используемому методу встраивания ЦВЗ. Например, такие характеристики, как среднеквадратичная ошибка, более чувствительны к аддитивному шуму, в то время как другие — к плавности переходов в изображении и т. д.

Установление характеристик изображений, пригодных для построения систем ЦВЗ, основывалось на дисперсионном анализе. Статистические тесты применялись для того, чтобы определить, является ли неустойчивость тех или иных характеристик изображений следствием встраивания ЦВЗ либо следствием всего многообразия изображений. Дисперсионный анализ проводился с целью выяснения, можно ли по предполагаемому изменению некоторого фактора, например, устойчивости ЦВЗ, вычислить различие между данными.

К основным характеристикам качества изображения можно отнести следующие: средняя абсолютная ошибка, среднеквадратическая ошибка, пиковое отношение сигнал/шум, мера качества изображения, взаимная корреляция и пр. [1, 2]. Кроме вышеперечисленных характеристик также рассматривалась функция чувствительности к контрасту (ФЧК), подробно описанная в [3] с точки зрения анализа изменений изображения при сжатии с потерями. В ходе исследования автором вычислялись значения ФЧК исходного изображения и изображения с ЦВЗ. После этого составлялась совместная карта порогов, и по данным карты находилось среднее

значение карты видимых ошибок

$$D = \frac{1}{H \cdot W} \sum_{1 \leqslant i \leqslant W} \sum_{1 \leqslant j \leqslant H} \Delta E_{Luv\ i,j} \cdot I_{i,j},$$

где H и W — высота и ширина изображения соответственно,

$$\Delta E_{Luv\ i,j} = \sqrt{(\Delta L)^2 + (\Delta u)^2 + (\Delta v)^2}$$

есть разность между значениями цвета в пикселе $(i,\ j)$, $i \in [1,\ W]$, $j \in\in [1,\ H]$, ΔL, Δu, Δv — разность цветовых компонент пикселя $(i,\ j)$ в пространстве LUV; $I_{i,j}$ вычисляется по формуле

$$I_{i,j} = \begin{cases} 1, & \text{если } \Delta E_{Luv\ i,j} > T_{i,j}, \\ 0, & \text{если } \Delta E_{Luv\ i,j} \leqslant T_{i,j}, \end{cases}$$

где $T_{i,j}$ — значение порога в пикселе $(i,\ j)$.

Если значение характеристики D превышает допустимый порог, определенный при предварительных тестированиях, необходимо уменьшить емкость системы ЦВЗ. Поскольку для вычисления ФЧК изображения предварительно следует разбить на квадратные блоки размера $l \times l$, емкость можно будет уменьшить за счет пропуска при внедрении ЦВЗ тех блоков, в которых пространственная частота двумерного ДПФ является максимальной.

Кроме того, для увеличения стойкости системы ЦВЗ (в случае пассивного противника) можно также вычислять среднее значение карты видимых ошибок на основе ФЧК изображения с ЦВЗ и его же, пропущенного через некоторый фильтр. В качестве примера можно предложить гауссовский сглаживающий фильтр $H(m,\ n) = Kg(m,\ n)$, где

$$g(m,\ n) = \frac{1}{2\pi\sigma^2} \cdot e^{-(m^2+n^2)/2\sigma^2}$$

— двумерное гауссовское ядро и

$$K = \left(\sum_m \sum_n |g(m,\ n)|^2 \right)^{0.5}$$

— нормализованная константа. В зависимости от того, превосходит значение характеристики D пороговое значение или нет, вносить ЦВЗ в данные блоки или пропускать их.

Литература

[1] *Грибунин В. Г.*, *Оков И. Н.*, *Туринцев И. В.* Цифровая стеганография. М.: СОЛОН-Пресс, 2002.

[2] *Avcibas I., Sankur B., Sayood K.* Statistical analysis of image quality measures // J. Electron. Imag. Vol. 11. Apr. 2002. P. 206—223.
[3] *Titov S.* Perceptually based image comparison method. 2000.

Об одной теореме из работы Импальяццо и Луби

А. А. Татузов

1. Введение

Понятие односторонней функции — одно из фундаментальных в математической криптографии. Для многих криптографических задач доказано, что их решение существует только в случае существования односторонней функции. Доказательства стойкости криптографических протоколов, реализующих эти задачи, также опираются на существование односторонней функции. Этим единообразием достигается возможность свести решения многих криптографических задач к одной — вопросу о существовании односторонней функции.

Односторонняя функция — многозначное понятие. Существуют разные определения разных типов односторонних функций. Наиболее распространенными являются сильные и слабые односторонние функции. Известно, что из существования слабой односторонней функции следует существование сильной. Поэтому часто при сведении криптографической задачи к вопросу существования односторонней функции в прямой части доказательства строится слабая односторонняя функция, а в обратной части построение криптографического протокола опирается на сильную одностороннюю функцию.

Кроме этих двух типов односторонних функций есть еще один, менее распространенный — односторонняя по распределению функция. Эта функция слабее, чем предыдущие две. То есть и сильная и слабая односторонняя функции являются односторонними по распределению функциями, но односторонняя по распределению функция не обязательно является хотя бы слабой односторонней функцией.

Это свойство односторонней по распределению функции позволяет строить ее на основе схем протоколов с существенно более слабой стойкостью, либо решающих задачи другого класса, чем те, исходя из которых удается построить слабую одностороннюю функцию. Примеры таких протоколов можно найти в статье Импальяццо и Луби [1]. Там же и было введено понятие односторонней по распределению функции.

Еще одним примером является работа [2], в которой доказано, что из существования доказательства со статистически нулевым разглашением для хотя бы одного трудного в среднем языка следует существование односторонней по распределению функции.

В статье [1] было анонсировано доказательство того, что из существования односторонней по распределению функции следует существование слабой односторонней функции.

Следует заметить, что если конструкции сильной и слабой односторонних функций отличаются, в некотором смысле, только количественно, то конструкция односторонней по распределению функции основана на принципиально других механизмах. Кратко разницу можно описать так. Для слабой односторонней функции сложно найти хотя бы один элемент из прообраза некоторого элемента ее образа, а у односторонней по распределению функции сложно задать на прообразе элемента ее образа равномерное распределение, то есть в некотором смысле описать этот прообраз.

Поэтому анонсированное в статье [1] доказательство представляется очень интересным. К сожалению, оно приводится не полностью и не демонстрирует взаимосвязь между двумя этими типами конструкций.

В этой статье предлагается полное доказательство частного случая рассматриваемой теоремы.

2. Обозначения и определения

2.1. Статистические понятия

Определение 10. Пусть $\mathcal{A}$ и $\mathcal{B}$ — две случайные величины в Σ^n. Статистическим расстоянием между ними называется следующая величина:

$$\operatorname{sdist}(\mathcal{A}, \mathcal{B}) = \frac{1}{2} \sum_{c \in \Sigma^n} |\Pr(\mathcal{A} = c) - \Pr(\mathcal{B} = c)|$$

Для удобства будем пользоваться удвоенным статистическим расстоянием:

$$\operatorname{dist}(\mathcal{A}, \mathcal{B}) = 2 \operatorname{sdist}(\mathcal{A}, \mathcal{B})$$

Обозначение 1. Пусть $\mathcal{A}$ и $\mathcal{B}$ — две случайные величины в Σ^n. Пусть Ω — вероятностное пространство, над которым задана случайная величина $\mathcal{A}$ и $C \subseteq \Omega$. Тогда положим

$$\operatorname{dist}(\mathcal{A} \mid C, \mathcal{B}) = \sum_{c \in \Sigma^n} |\Pr(\mathcal{A} = c \mid C) - \Pr(\mathcal{B} = c)|$$

2.2. Односторонние функции

Определение 11. $f\colon \Sigma^* \to \Sigma^*$ — слабая односторонняя функция, если

1) существует полиномиальная машина Тьюринга T такая, что $T(x) = f(x)$ для всех $x \in \Sigma^*$;

2) существует полином p такой, что для любой полиномиальной вероятностной машины Тьюринга M неравенство

$$\Pr_{x \in_R \Sigma^{s(n)}}(f(M(f(x))) \neq f(x)) > \frac{1}{p(n)}$$

верно для всех достаточно больших n (здесь $s(n)$ — некоторый полином).

Определение 12. $f\colon \Sigma^* \to \Sigma^*$ — односторонняя по распределению функция, если:

1) существует полиномиальная машина Тьюринга T такая, что $T(x) = f(x)$ для всех $x \in \Sigma^*$;

2) существует полином p такой, что для любой полиномиальной вероятностной машины Тьюринга M неравенство

$$\operatorname{dist}\left((x,\ f(x))_{x \in_R \Sigma^n},\ (M(f(x)),\ f(x))_{x \in_R \Sigma^n}\right) \geqslant \frac{1}{p(n)}$$

верно для всех достаточно больших n.

При этом предполагается существование полиномиальной машины Тьюринга K такой, что $K(f(x)) = n$ для всех $x \in \Sigma^n$.

Определение 13. $f\colon \Sigma^* \to \Sigma^*$ — регулярная функция, если

$$\forall\, x \in \Sigma^n\ \#\{x' \in \Sigma^n \mid f(x') = f(x)\} = 2^{k(n)},$$

где $k(n)$ вычисляется за полиномиальное время.

2.3. Технические определения

Обозначение 2. Пусть $A \in \Sigma^{n \times m}$, $b \in \Sigma^m$. Тогда примем

$$\mathcal{L}^{A,b} = \{x \in \Sigma^n \mid Ax = b\}.$$

Обозначение 3. Введем следующее обозначение для множества всех пар (A, b):

$$\mathcal{H}^{n,m}_{\mathcal{L}} = \Sigma^{n \times m} \times \Sigma^m.$$

Обозначение 4. Пусть $\mathbb{X} \subseteq \Sigma^n$, $0_n \in \Sigma^n$ — элемент с нулевыми координатами пространства Σ^n. Введем следующее обозначение

$$\lfloor \mathbb{X} \rceil_{M \pm \Delta} = \begin{cases} \mathbb{X}, & |\#\mathbb{X} - M| < \Delta; \\ \{0_n\}, & |\#\mathbb{X} - M| \geqslant \Delta. \end{cases}$$

3. Основные результаты

Теорема 1 (о случайном выборе). *Пусть* $\mathbb{X} \subseteq \Sigma^n$ *и* $\#\mathbb{X} = 2^k$. *Тогда*

$$\operatorname{dist}\left((x)_{x\in_R\mathbb{X}},\ (x)_{\substack{(A,b)\in_R\mathcal{H}^{n,m}_{\mathcal{L}},\\ x\in_R\left\lfloor \mathbb{X}\cap\mathcal{L}^{(A,b)}\right\rceil_{2^\nu\pm 2^{2\nu/3}}}}\right) < \frac{6}{2^{\nu/3}},$$

где $m = k - \nu$.

Теорема 2 (о функциях). *Если существует регулярная односторонняя по распределению функция, то существует и слабая односторонняя функция.*

4. Доказательства

4.1. Технические утверждения

Обозначение 5. Введем следующее обозначение.

$$\chi(Ax = b) = \begin{cases} 1, & Ax = b; \\ 0, & Ax \neq b. \end{cases}$$

В построении используется идея универсального семейства хэш-функций. Используется конкретный ее представитель, семейство линейных функций $Ax + b$.

Утверждение 1 (см. [3]). *Для любых различных* $x,\ y \in \Sigma^n$

$$\Pr_{(A,b)\in_R\mathcal{H}^{n,m}_{\mathcal{L}}}(Ax = b \ \ \&\ \ Ay = b) = 2^{-2m}.$$

Для всех универсальных семейств хэш-функций верно следующее утверждение.

Утверждение 2. *Пусть* $\mathbb{X} \subseteq \Sigma^n$ *и* $\#\mathbb{X} = 2^k$. *Тогда*

$$\forall\,\epsilon \leqslant \frac{k}{2} \in \mathbb{N}\ \forall\,\delta \leqslant \epsilon \ \Pr_{(A,b)\in_R\mathcal{H}^{n,s}_{\mathcal{L}}}\left(\left|\#\left(\mathcal{L}^{A,b}\cap\mathbb{X}\right) - 2^{2\epsilon}\right| \geqslant 2^{\epsilon+\delta}\right) \leqslant 2^{-2\delta},$$

где $s = k - 2\epsilon$.

Доказательство. По утверждению 1 случайные величины $\chi(Ax = b)$ для $x \in \mathbb{X}$ одинаково распределены и попарно независимы. При этом $p = \mathsf{E}_{(A,b)\in_R\mathcal{H}^{n,s}_{\mathcal{L}}}\chi(Ax = b) = \Pr(\chi(Ax = b) = 1) = 2^{-s}$.

Применим неравенство Чебышева:

$$\Pr_{(A,b)\in_R\mathcal{H}^{n,s}_{\mathcal{L}}}\left(\left|\frac{\sum_{x\in\mathbb{X}}\chi(Ax = b)}{\#\mathbb{X}} - p\right| \geqslant 2^{\epsilon+\delta-k}\right) \leqslant \frac{\mathsf{D}\chi(Ax = b)}{\#\mathbb{X}2^{2(\epsilon+\delta-k)}}$$

$$\Rightarrow\ \Pr\left(\left|\sum_{x\in\mathbb{X}}\chi(Ax = b) - 2^{2\epsilon}\right| \geqslant 2^{\epsilon+\delta}\right) < 2^{-k+2\epsilon}2^{-k}2^{-2(\epsilon+\delta-k)}$$

$$\Rightarrow\ \Pr\left(\left|\#(\mathcal{L}^{A,b}\cap\mathbb{X}) - 2^{2\epsilon}\right| \geqslant 2^{\epsilon+\delta}\right) < 2^{-2\delta},$$

так как

$$\mathsf{D}\chi(Ax = b) = 2^{-s}(1 - 2^{-s}) < 2^{-s}, \quad \#\mathbb{X} = 2^k,$$
$$p = 2^{-s} \quad \text{и} \quad s = k - 2\epsilon. \qquad \square$$

В ходе доказательства потребуется инструмент для удаление из подсчета статистического расстояния маловероятных событий.

Утверждение 3. *Пусть* $\mathcal{A}$ *и* $\mathcal{B}$ *— две случайные величины в* Σ^n. *Пусть* Ω *— вероятностное пространство, над которым задана случайная величина* $\mathcal{A}$ *и* C *— событие в этом вероятностном пространстве. Тогда*

$$\operatorname{dist}(\mathcal{A},\mathcal{B}) \leqslant 2\Pr\left(\overline{C}\right) + \operatorname{dist}(\mathcal{A} \mid C, \mathcal{B}).$$

Доказательство.

$$\begin{aligned}
\operatorname{dist}(\mathcal{A},\mathcal{B}) &= \sum_{c\in\Sigma^n}|\Pr(\mathcal{A} = c) - \Pr(\mathcal{B} = c)| \leqslant \\
&\leqslant \sum_{c\in\Sigma^n}\left|\Pr\left(\mathcal{A} = c \mid \overline{C}\right)\Pr\left(\overline{C}\right) - \Pr(\mathcal{B} = c)\Pr\left(\overline{C}\right)\right| + \\
&\quad + \sum_{c\in\Sigma^n}|\Pr(\mathcal{A} = c \mid C)P(C) - \Pr(\mathcal{B} = c)\Pr(C)| = \\
&= \Pr\left(\overline{C}\right)\sum_{c\in\Sigma^n}\left|\Pr\left(\mathcal{A} = c \mid \overline{C}\right) - \Pr(\mathcal{B} = c)\right| + \\
&\quad + \Pr(C)\sum_{c\in\Sigma^n}|\Pr(\mathcal{A} = c \mid C) - \Pr(\mathcal{B} = c)| \leqslant \\
&\leqslant 2\Pr\left(\overline{C}\right) + \sum_{c\in\Sigma^n}|\Pr(\mathcal{A} = c \mid C) - \Pr(\mathcal{B} = c)| = \\
&= 2\Pr\left(\overline{C}\right) + \operatorname{dist}(\mathcal{A} \mid C, \mathcal{B}). \qquad \square
\end{aligned}$$

4.2. Доказательства теорем

Теорема о случайном выборе

Из утверждения 2 имеем

$$\Pr_{(A,b)\in_R\mathcal{H}^{n,s}_{\mathcal{L}}}\left(\left|\#(\mathcal{L}^{A,b}\cap\mathbb{X})-2^{2\epsilon}\right|\geqslant 2^{\epsilon+\delta}\right)\leqslant 2^{-2\delta}. \tag{1}$$

Пусть $C=\left\{(A,\,b)\in\mathcal{H}^{n,s}_{\mathcal{L}}\;\middle|\;\left\lfloor\mathcal{L}^{A,b}\cap\mathbb{X}\right\rceil_{2^{2\epsilon}\pm 2^{(\epsilon+\delta)}}=\mathcal{L}^{A,b}\cap\mathbb{X}\right\}\subseteq\mathcal{H}^{n,s}_{\mathcal{L}}$.

Преобразуем левую часть доказываемого неравенства — статистическое расстояние — с использованием определения 10:

$$\begin{aligned}
&\operatorname{dist}\left((x)_{x\in_R\mathbb{X}},\,(x)_{\substack{(A,b)\in_R\mathcal{H}^{n,s}_{\mathcal{L}},\\ x\in_R\left\lfloor\mathbb{X}\cap\mathcal{L}^{(A,b)}\right\rceil_{2^{2\epsilon}\pm 2^{(\epsilon+\delta)}}}}\right)\\
&\quad=\sum_{x\in\mathbb{X}}\left|\Pr_{\substack{(A,b)\in_R\mathcal{H}^{n,s}_{\mathcal{L}},\\ \widehat{x}\in_R\left\lfloor\mathbb{X}\cap\mathcal{L}^{(A,b)}\right\rceil_{2^{2\epsilon}\pm 2^{(\epsilon+\delta)}}}}(\widehat{x}=x)-\Pr_{\widehat{x}\in_R\mathbb{X}}(\widehat{x}=x)\right|=\\
&\quad=\sum_{x\in\mathbb{X}\setminus\{0_n\}}\left|\sum_{(A,b)\in C}\frac{\Pr_{(\widehat{A},\widehat{b})\in_R\mathcal{H}^{n,s}_{\mathcal{L}}}\left((A,\,b)=\left(\widehat{A},\,\widehat{b}\right)\right)\chi(Ax=b)}{\#\left(\mathbb{X}\cap\mathcal{L}^{A,b}\right)}-2^{-k}\right|+\\
&\qquad+\left|\sum_{(A,b)\in C}\frac{\Pr_{(\widehat{A},\widehat{b})\in_R\mathcal{H}^{n,s}_{\mathcal{L}}}\left((A,\,b)=\left(\widehat{A},\,\widehat{b}\right)\right)\chi(A0_n=b)}{\#\left(\mathbb{X}\cap\mathcal{L}^{A,b}\right)}+\right.\\
&\qquad\qquad\left.+\Pr_{(A,b)\in_R\mathcal{H}^{n,m}_{\mathcal{L}}}\left((A,\,b)\in\overline{C}\right)-2^{-k}\right|\\
&\quad\leqslant\sum_{x\in\mathbb{X}}\left|\sum_{(A,b)\in C}\frac{\Pr_{(\widehat{A},\widehat{b})\in_R\mathcal{H}^{n,s}_{\mathcal{L}}}\left((A,\,b)=\left(\widehat{A},\,\widehat{b}\right)\right)\chi(Ax=b)}{\#\left(\mathbb{X}\cap\mathcal{L}^{A,b}\right)}-2^{-k}\right|+2^{-2\delta}.
\end{aligned}\tag{2}$$

Здесь использовано то, что по определению C из неравенства (1) следует неравенство $\Pr_{(A,b)\in_R\mathcal{H}^{n,m}_{\mathcal{L}}}\left((A,\,b)\in\overline{C}\right)\leqslant 2^{-2\delta}$.

Мы можем вынести знаменатель из-под внутренней суммы, используя утверждение 2.

$$\begin{cases}
\dfrac{\Pr_{(A,b)}(Ax=b\;\;\&\;\;(A,\,b)\in C)}{2^{2\epsilon}+2^{\epsilon+\delta}}\leqslant\displaystyle\sum_{(A,b)\in C}\frac{\Pr(A,\,b)\chi(Ax=b)}{\#\left(\mathbb{X}\cap\mathcal{L}^{A,b}\right)},\\
\displaystyle\sum_{(A,b)\in C}\frac{\Pr(A,\,b)\chi(Ax=b)}{\#\left(\mathbb{X}\cap\mathcal{L}^{A,b}\right)}\leqslant\frac{\Pr_{(A,b)}(Ax=b\;\;\&\;\;(A,\,b)\in C)}{2^{2\epsilon}-2^{\epsilon+\delta}}.
\end{cases}\tag{3}$$

Заметим, что если бы $C=\mathcal{H}^{n,s}_{\mathcal{L}}$, то $\Pr_{(A,b)}(Ax=b\;\&\;(A,\,b)\in C)=2^{2\epsilon-k}$ и ввиду близости знаменателя к $2^{2\epsilon}$ сумма должна была бы оказаться близкой к нулю. К сожалению, это не так.

Однако, пользуясь оценками снизу на размер пересечения $\mathcal{L}^{A,b}\cap\mathbb{X}$ и утверждением 2, можно произвести следующую оценку:

$$\begin{aligned}
\sum_{x\in\mathbb{X}}\Pr_{(A,b)}\left(Ax=b\;\;\&\;\;(A,\,b)\in\overline{C}\right)&=\sum_{x\in\mathbb{X}}\Pr(Ax=b)-\frac{\sum_{(A,b)\in C}\#\left(\mathcal{L}^{A,b}\cap\mathbb{X}\right)}{\#\mathcal{H}^{n,s}_{\mathcal{L}}}\\
&\leqslant\sum_{x\in\mathbb{X}}\Pr(Ax=b)-\frac{\#C}{\#\mathcal{H}^{n,s}_{\mathcal{L}}}\left(2^{2\epsilon}-2^{\epsilon+\delta}\right)\quad\text{(из определения }C)\\
&\leqslant 2^{2\epsilon}-\left(1-2^{-2\delta}\right)\left(2^{2\epsilon}-2^{\epsilon+\delta}\right)\quad\text{(из (1) и утверждения 2)}\\
&\leqslant 2^{\epsilon+\delta}+\frac{2^{2\epsilon}-2^{\epsilon+\delta}}{2^{2\delta}}.
\end{aligned}\tag{4}$$

Теперь у нас есть все необходимое, чтобы завершить доказательство. Воспользуемся неравенствами (3), (4) и преобразуем сумму из (2):

$$\begin{aligned}
&\sum_{x\in\mathbb{X}}\left|\sum_{(A,b)\in C}\frac{\Pr(A,\,b)\chi(Ax=b)}{\#\left(\mathbb{X}\cap\mathcal{L}^{A,b}\right)}-2^{-k}\right|\\
&\quad\leqslant\sum_{x\in\mathbb{X}}\frac{\left|\Pr_{(A,b)}(Ax=b\;\;\&\;\;(A,\,b)\in C)-2^{-k+2\epsilon}\right|+2^{-k+\epsilon+\delta}}{2^{2\epsilon}-2^{\epsilon+\delta}}\\
&\quad\leqslant\frac{\sum_{x\in\mathbb{X}}\left|\Pr_{(A,b)}(Ax=b\;\;\&\;\;(A,\,b)\in C)-2^{-k+2\epsilon}\right|+2^{\epsilon+\delta}}{2^{2\epsilon}-2^{\epsilon+\delta}}\\
&\quad\leqslant\frac{\sum_{x\in\mathbb{X}}\left|\Pr_{(A,b)}(Ax=b)-2^{-k+2\epsilon}\right|+2^{\epsilon+\delta}}{2^{2\epsilon}-2^{\epsilon+\delta}}\\
&\qquad+\frac{\sum_{x\in\mathbb{X}}\Pr_{(A,b)}\left(Ax=b\;\;\&\;\;(A,\,b)\in\overline{C}\right)}{2^{2\epsilon}-2^{\epsilon+\delta}}\\
&\quad\leqslant\frac{2^{\epsilon+\delta}+2^{\epsilon+\delta}+\frac{2^{2\epsilon}-2^{\epsilon+\delta}}{2^{2\delta}}}{2^{2\epsilon}-2^{\epsilon+\delta}}\quad\left(\text{так как }\Pr_{(A,b)}(Ax=b)=2^{-s}=2^{-k+2\epsilon}\right)\\
&\quad<\frac{2}{2^{\epsilon-\delta}-1}+2^{-2\delta}<2^{-(\epsilon-\delta)+2}+2^{-2\delta}.
\end{aligned}\tag{5}$$

Подставим результат в неравенство (2) и получим, что

$$\operatorname{dist}\left((x)_{x\in_R\mathbb{X}},\,(x)_{\substack{(A,b)\in_R\mathcal{H}^{n,m}_{\mathcal{L}},\\ x\in_R\left\lfloor\mathbb{X}\cap\mathcal{L}^{(A,b)}\right\rceil_{2^{2\epsilon}\pm 2^{(\epsilon+\delta)}}}}\right)<2^{-(\epsilon-\delta)+2}+2^{-2\delta+1}. \tag{6}$$

Требуемое неравенство получается из (6) при $\epsilon=\nu/2$ и $\delta=\nu/6$.

Теорема о функциях

Пусть f — регулярная (с параметром $k(n)$) односторонняя по распределению (с полиномом $q(n)$) функция. Построим функцию g (с использованием f) и докажем от противного то, что эта новая функция является слабой односторонней функцией. А именно,

$$g(j,\, A,\, i,\, x) = (j,\, A,\, Ax \uparrow j,\, i,\, x \uparrow i,\, f(x)),$$

где $x \in \Sigma^n$, $(A,\, b) \in \mathcal{H}_{\mathcal{L}}^{n,n}$, $i,\, j \in \overline{0,\, n}$, а $x \uparrow i$ — первые i битов строки x (здесь мы полагаем $x \uparrow 0 = 0$).

Легко видеть, что функция g может быть вычислена полиномиальной машиной Тьюринга. В таком случае из предположения о том, что g не является слабой односторонней функцией, следует, что для любого полинома p существуют полиномиальная вероятностная машина Тьюринга M и возрастающая последовательность $\{n_t\}_{t \in \mathbb{N}}$ натуральных чисел такие, что

$$\Pr_{\substack{x \in_R \Sigma^{n_t},\\ A \in_R \Sigma^{n_t \times n_t},\\ i \in_R \overline{1,n_t}}} (g(M(g(j,\, A,\, i,\, x))) \neq g(j,\, A,\, i,\, x)) \leqslant \frac{1}{p(n_t)} \tag{7}$$

для всех $j \in \overline{1,\, n_t}$ и $t \in \mathbb{N}$. Выберем некоторый полином $p(n)$, явное выражение которого через $q(n)$ будет приведено в конце доказательства, и соответствующую машину M. Построим полиномиальную вероятностную машину M' на основе машины M, для которой

$$\operatorname{dist}\left((x,\, f(x))_{x \in_R \Sigma^{n_t}},\, (M'(f(x)),\, f(x))_{x \in_R \Sigma^{n_t}}\right) < \frac{1}{q(n_t)}. \tag{8}$$

Неравенство (8) противоречит второму условию определения односторонней по распределению функции, из чего следует утверждение теоремы.

Обозначим через $M_{\mathfrak{r}}(n,\, j,\, A,\, b,\, i,\, r,\, y)$, где $j = \overline{0,\, n}$, $A,\, b \in \mathcal{H}_{\mathcal{L}}^{n,j}$ (при $j = 0$ эти два параметра опускаются, b присваиваем значение 0), следующий алгоритм. Выбираем $A' \in_R \Sigma^{n \times (n-j)}$, строим $\widehat{A} = \left[\begin{smallmatrix} A \\ A' \end{smallmatrix}\right]$, на входе $(j,\, \widehat{A},\, b,\, i,\, r,\, y)$ запускаем алгоритм M, чей выход считаем выходом алгоритма. Будем говорить, что алгоритм $M_{\mathfrak{r}}$ правильно инвертировал функцию g в том случае, если для x из выхода алгоритма выполняются условия $x \uparrow i = r$, $f(x) = y$ и $Ax = b$ при $j > 0$.

Заметим, что для любого $j \in \overline{0,\, n}$ и всех r, i, y вероятность того, что алгоритм $M_{\mathfrak{r}}$ правильно инвертирует функцию g, равна

$$\Pr_{(A,b) \in_R \mathcal{H}_{\mathcal{L}}^{n,n}} (g(M(g(j,\, A,\, i,\, x))) = g(j,\, A,\, i,\, x).)$$

Теперь приведем конструкцию машины M'.

В квадратных скобках будут записаны модификации алгоритма для случая $\nu(n) \geqslant k(n)$.

Вход. На вход машина M' получает $y \in \operatorname{Im}_f(\Sigma^n)$.

Шаг 1. Выбираем $(A,\, b) \in_R \mathcal{H}_{\mathcal{L}}^{n,k(n)-\nu(n)}$. Конструкция множества $\mathcal{H}_{\mathcal{L}}^{n,k(n)-\nu(n)}$ позволяет произвести эту операцию. [Этот шаг не производится.]

Шаг 2. Находим все элементы множества $\mathcal{L}^{A,b} \cap f^{-1}(y)$ $[f^{-1}(y)]$ в случае, если $\#\left(\mathcal{L}^{A,b} \cap f^{-1}(y)\right) \leqslant 2^{\nu(n)} + 2^{2\nu(n)/3}$ [этого ограничения нет]. Операцию производим согласно следующему алгоритму.

Последовательно подаем на вход машине $M_{\mathfrak{r}}$ для i от 1 до n наборы

$$(n,\, k(n) - \nu(n),\, A,\, b,\, i,\, r,\, f(x)) \quad (n,\, 0,\, i,\, r,\, f(x))]$$

для всех p со следующими свойствами:

1) старшие $n - i$ координат заполнены нулями;
2) при $i > 1$ младшие $i - 1$ координат берутся равными соответствующим координатам тех значений r, которые подавались на вход машине $M_{\mathfrak{r}}$ при выборе $i - 1$, и на которых машина смогла правильно инвертировать функцию g;
3) i-я координата берется равной и нулю и единице.

Как только количество наборов r, для которых функцию удалось инвертировать, превысит $n(2^{\nu(n)} + 2^{2\nu(n)/3})$, алгоритм останавливается. При этом запоминаем, что перебор элементов закончился неудачно. [Эта проверка не производится.]

Алгоритм также останавливается в случае, когда были перечислены все значения r для $i = n$. Обозначим через $L(A,\, b,\, y)$ $[L(y)]$ множество найденных при $i = n$ наборов r, для которых машина M смогла инвертировать функцию g. Заметим, что

$$L(A,\, b,\, y) \subseteq \mathcal{L}^{A,b} \cap f^{-1}(y) \quad [L(y) \subseteq f^{-1}(y)].$$

Шаг 3. В случае, если перебор элементов закончился неудачно, либо количество найденных элементов оказалось меньше $2^{\nu(n)} - 2^{2\nu(n)/3}$, возвращаем 0_n [эта проверка не производится]. В противном случае возвращаем случайный элемент из уже известного нам множества $L(A,\, b,\, y)$ $[L(y)]$.

Замечание 1. В тех случаях, когда $2^{\nu(n)}$ — полином, машина Тьюринга, определяемая приведенным алгоритмом, является полиномиальной.

Докажем, что машина M' удовлетворяет требуемым свойствам.

Заметим, что если бы машина M безошибочно инвертировала функцию g, то приведенный выше алгоритм в случае $k(n) \leqslant \nu(n)$ работал бы точно так же, как случайный выбор из прообраза y, а при $k(n) > \nu(n)$ полностью соответствовал бы схеме перебора множества $f^{-1}(y)$ из теоремы 1. Однако машина M может допускать ошибки. Эту проблему можно обойти с помощью утверждения 3. Теперь о каждом шаге подробнее.

Лемма 1. *Пусть $\mathcal{A}(x)$ и $\mathcal{B}(x)$ — две случайные величины в Σ^n, а x берется из конечного множества $\mathbb{X} \subseteq \Sigma^*$. Пусть также задана некоторая функция $f\colon \mathbb{X} \to \Sigma^*$. Тогда*

$$\operatorname{dist}\left(\mathcal{A}(x)_{x\in_R\mathbb{X}},\, \mathcal{B}(x)_{x\in_R\mathbb{X}}\right) \leqslant \mathsf{E}_{\substack{t\in_R\mathbb{X},\\ y=f(t)}} \operatorname{dist}\left(\mathcal{A}(x)_{x\in_R f^{-1}(y)},\, \mathcal{B}(x)_{x\in_R f^{-1}(y)}\right). \quad (9)$$

Доказательство. Распишем левую часть доказываемого равенства:

$$\begin{aligned}
\operatorname{dist}\left(\mathcal{A}(x)_{x\in_R\mathbb{X}},\, \mathcal{B}(x)_{x\in_R\mathbb{X}}\right) &\leqslant \sum_{c\in\Sigma^n}\left|\sum_{y\in f(\mathbb{X})}\left[\Pr_{x\in_R\mathbb{X}}(\mathcal{A}(x)=c \;\;\&\;\; f(x)=y)\right.\right. \\
&\qquad \left.\left. -\Pr_{x\in_R\mathbb{X}}(\mathcal{B}(x)=c \;\;\&\;\; f(x)=y)\right]\right| = \\
&= \sum_{y\in f(\mathbb{X})}\Pr_{x\in_R\mathbb{X}}(f(x)=y)\sum_{c\in\Sigma^n}\left|\Pr(\mathcal{A}(x)=c \mid f(x)=y) - \right. \\
&\qquad \left. -\Pr(\mathcal{B}(x)=c \mid f(x)=y)\right| \\
&= \mathsf{E}_{\substack{t\in_R\mathbb{X},\\ y=f(t)}}\sum_{c\in\Sigma^n}\left|\Pr_{x\in_R f^{-1}(y)}(\mathcal{A}(x)=c) - \Pr_{x\in_R f^{-1}(y)}(\mathcal{B}(x)=c)\right|. \qquad \square
\end{aligned}$$

Рассмотрим теперь случай $k(n) > \nu(n)$.

Из леммы 1, а также из теоремы 1 и свойства регулярности функции f следует, что

$$\begin{aligned}
&\operatorname{dist}\left((x,\, f(x))_{x\in_R\Sigma^n},\, (\widehat{x},\, f(x))_{\substack{x\in_R\Sigma^n,\\ (A,b)\in_R\mathcal{H}_{\mathcal{L}}^{n,k(n)-\nu(n)},\\ \widehat{x}\in_R\left\lfloor f^{-1}(f(x))\cap\mathcal{L}^{(A,b)}\right\rceil_{2^{\nu(n)}\pm 2^{2\nu(n)/3}}}}\right) \leqslant \mathsf{E}_{\substack{t\in_R\Sigma^n,\\ y=f(t)}}, \\
&\operatorname{dist}\left((x,\, f(x))_{x\in_R f^{-1}(y)},\, (\widehat{x},\, f(x))_{\substack{(A,b)\in_R\mathcal{H}_{\mathcal{L}}^{n,k(n)-\nu(n)},\\ \widehat{x}\in_R\left\lfloor f^{-1}(y)\cap\mathcal{L}^{(A,b)}\right\rceil_{2^{\nu(n)}\pm 2^{2\nu(n)/3}}}}\right) \leqslant \frac{6}{2^{\nu(n)/3}}.
\end{aligned} \quad (10)$$

Фиксируем $y \in f(\Sigma^n)$. Обозначим алгоритм работы машины M' начиная с шага 2 через $M'_{(A,b)}$, где $(A,\, b)$ характеризует результат шага 1. Тогда из построения шага 1 получим $M'(y) = M'_{(A,b)\in_R\mathcal{H}_{\mathcal{L}}^{n,k(n)-\nu(n)}(y)}$. Два раза используя лемму 1, заметим, что

$$\begin{aligned}
&\operatorname{dist}\left((M'(x),\, f(x)),\, (\widehat{x},\, f(x))_{\substack{x\in_R\Sigma^n,\\ (A,b)\in_R\mathcal{H}_{\mathcal{L}}^{n,k(n)-\nu(n)},\\ \widehat{x}\in_R\left\lfloor f^{-1}(f(x))\cap\mathcal{L}^{(A,b)}\right\rceil_{2^{\nu(n)}\pm 2^{2\nu(n)/3}}}}\right) \\
&\leqslant \mathsf{E}_{\substack{t\in_R\Sigma^n,\\ y=f(t)}}\operatorname{dist}\left(M'(y),\, (\widehat{x},\, f(x))_{\substack{(A,b)\in_R\mathcal{H}_{\mathcal{L}}^{n,k(n)-\nu(n)},\\ \widehat{x}\in_R\left\lfloor f^{-1}(y)\cap\mathcal{L}^{(A,b)}\right\rceil_{2^{\nu(n)}\pm 2^{2\nu(n)/3}}}}\right) \\
&\leqslant \mathsf{E}_y\mathsf{E}_{(A,b)\in_R\mathcal{H}_{\mathcal{L}}^{n,k(n)-\nu(n)}} \\
&\qquad \operatorname{dist}\left(M'_{(A,b)}(y),\, (\widehat{x},\, f(x))_{\widehat{x}\in_R\left\lfloor f^{-1}(y)\cap\mathcal{L}^{(A,b)}\right\rceil_{2^{\nu(n)}\pm 2^{2\nu(n)/3}}}\right). \qquad (11)
\end{aligned}$$

Пусть $G_{A,b,y}$ — событие, состоящее в том, что алгоритм M на протяжении шага 2 алгоритма M' ни разу не ошибется. Тогда

$$\operatorname{dist}\left(M'_{(A,b)}(y)\,\middle|\, G_{A,b,y},\, (\widehat{x},\, f(x))_{\widehat{x}\in_R\left\lfloor f^{-1}(y)\cap\mathcal{L}^{(A,b)}\right\rceil_{2^{\nu(n)}\pm 2^{2\nu(n)/3}}}\right) = 0.$$

Обозначим через $N_{j,A,i,x}$ утверждение

$$g\left(M\left(g\left(j,\, \begin{bmatrix}A\\ A'\end{bmatrix},\, i,\, x\right)\right)\right) \neg \left(j,\, \begin{bmatrix}A\\ A'\end{bmatrix},\, i,\, x\right).$$

Заметим, что

$$\Pr\left(\overline{G_{A,b,y}}\right) \leqslant \sum_{\substack{x\in\mathcal{L}^{A,b}\cap f^{-1}(y),\\ i=\overline{1,n}}} \Pr_{A'}(N_{k(n)-\nu(n),A,i,x}).$$

Используя это неравенство и утверждение 3 продолжим цепочку равенств (11). Дополнительно введем обозначение $N_{A,i,x} = N_{k(n)-\nu(n),A,i,x}$.

$$\begin{aligned}
&\mathsf{E}_{\substack{t\in_R\Sigma^n,\\ y=f(t)}}\mathsf{E}_{(A,b)}\operatorname{dist}\left(M'_{(A,b)}(y),\, (\widehat{x},\, f(x))_{\substack{(A,b)\in_R\mathcal{H}_{\mathcal{L}}^{n,k(n)-\nu(n)},\\ \widehat{x}\in_R\left\lfloor f^{-1}(y)\cap\mathcal{L}^{(A,b)}\right\rceil_{2^{\nu(n)}\pm 2^{2\nu(n)/3}}}}\right) \\
&\leqslant \leqslant 2\mathsf{E}_{\substack{t\in_R\Sigma^n,\\ y=f(t)}}\mathsf{E}_{(A,b)}\sum_{\substack{x\in\mathcal{L}^{A,b}\cap f^{-1}(y),\\ i=\overline{1,n}}}\Pr(N_{A,i,x}) \\
&\leqslant 2n\sum_{y\in f(\Sigma^n)}\Pr_{x\in_R\Sigma^n}(f(x)=y)\mathsf{E}_A 2^{-(k(n)+\nu(n))}\sum_{x\in f^{-1}(y)}\Pr_i(N_{A,i,x}) \\
&\leqslant 2n\cdot\frac{2^n}{2^{n-k(n)}\cdot 2^{k(n)-\nu(n)}}\Pr_{A,i,x}(N_{A,i,x}) \leqslant 2n\cdot 2^{\nu(n)}\Pr_{A,i,x}(N_{A,i,x}). \qquad (12)
\end{aligned}$$

Здесь использовано то, что

$$\sum_{\substack{x\in\mathcal{L}^{A,b}\cap f^{-1}(y),\\ b\in\Sigma^{k(n)-\nu(n)}}} \Pr(N_{A,i,x}) = \sum_{x\in f^{-1}(y)} \Pr(N_{A,i,x})$$

для всех $A\in\Sigma^{n\times k(n)-\nu(n)}$.

Покажем справедливость неравенства (8). Используя неравенство треугольника для статистических расстояний (оно следует из линейности сумм и верности неравенства треугольника для модулей) и вспоминая результаты (10), (11) и (12) можем записать

$$\operatorname{dist}\left((x,\ f(x))_{x\in_R\Sigma^n},\ (M'(f(x)),\ f(x))_{x\in_R\Sigma^n}\right) \leqslant 2n\cdot 2^{\nu(n)} \Pr_{A,i,x}(N_{A,i,x}) + \frac{6}{2^{\nu(n)/3}}.$$

Рассмотрим теперь случай $k(n)\leqslant\nu(n)$. При тех же обозначениях аналогично получим, что

$$\begin{aligned}\operatorname{dist}\left((x,\ f(x))_{x\in_R\Sigma^n},\ (M'(f(x)),\ f(x))_{x\in_R\Sigma^n}\right) &\leqslant\\ &\leqslant \mathsf{E}_{\substack{t\in_R\Sigma^n,\\ y=f(t)}} \operatorname{dist}\left((x)_{x\in_R f^{-1}(y)},\ M'(y)\right) \leqslant\\ \leqslant 2n\sum_{y\in f(\Sigma^n)} \Pr_{x\in_R\Sigma^n}(f(x)=y) &\sum_{x\in f^{-1}(y)} \Pr_{A,i}(N_{0,A,i,x}) \leqslant 2n\cdot 2^{\nu(n)} \Pr_{A,i,x}(N_{0,A,i,x}).\end{aligned}$$

Выберем $\nu(n)/3=\log(6q(n))+1$, а $p(n)=4\cdot 2n\cdot 2^{\nu(n)}q(n)$. Заметим, что так как $2^{\nu(n)}$ — полином, $p(n)$ также является полиномом. Алгоритм M' согласно замечанию 1 работает за полиномиальное время.

Применение неравенства (7) при заданных константах завершает доказательство.

Литература

[1] *Impagliazzo R., Luby M.* One-way Functions are Essential for Complexity-Based Cryptography, Proc. FOCS'89 (1989).

[2] *Ostrovsky R.* One-way Functions, Hard on Average Problems, and Statistical Zero-Knowledge Proofs. Proc. STRUCTURE'91.

[3] *Luby M.* Pseudorandomness and Cryptographic Applications. Princeton University Press, 1996.

Аффинная классификация смежных классов кода Рида—Маллера RM(2, 6)

С. Н. Калиниченко, А. Я. Гаранджук, А. В. Черемушкин

Пусть $n\geqslant 1$, $\mathcal{F}_n$ — множество двоичных функций от n переменных, $\mathrm{AGL}(n,\,2)$ — полная аффинная группа преобразований пространства $V_n(2)=\mathrm{GF}(2)^n$. При $s\geqslant 0$ полагаем

$$\mathcal{U}_s = \mathrm{RM}(s,\,n) = \{f : \deg f\leqslant s\}\leqslant\mathcal{F}_n,$$

где $\deg f$ — степень нелинейности функции f.

Известны следующие аффинные классификации функций от шести переменных. В [1] построена аффинная классификация смежных классов кода Рида—Маллера $\mathrm{RM}(1,\,6)$, или во введенных обозначениях — аффинная классификация факторпространства $\mathcal{F}_6/\mathcal{U}_1$. Таблицы представителей этой классификации можно найти на сайте [2]. В [3] найдена аффинная и линейная классификация факторпространств $\mathcal{F}_6/\mathcal{U}_3$ и $\mathcal{U}_4/\mathcal{U}_2$. В работе [4] предложен общий способ вычисления числа классов эквивалентности для действия группы $\mathrm{AGL}(n,\,2)$ на факторпространствах $\mathcal{U}_k/\mathcal{U}_s$, $-1\leqslant s\leqslant n-1$. В частности, показано, что число классов аффинной эквивалентности факторпространства $\mathcal{F}_6/\mathcal{U}_2$ равно 205.

В данной работе получена аффинная классификация смежных классов пространства $\mathcal{F}_6/\mathcal{U}_2$. Для ее получения был использован следующий подход: для всех 150357 представителей аффинной классификации $\mathcal{F}_6/\mathcal{U}_1$ вычислялись различные инварианты действия аффинной группы на множестве $\mathcal{F}_6/\mathcal{U}_2$ до тех пор, пока число классов с различными значениями инвариантов не совпадет с 205.

Определим рассматриваемые инварианты.

Напомним, что производной по направлению $a\in V_n(2)$ функции f называется функция $\Delta_a f(x)=f(x\oplus a)\oplus f(x)$, $x\in V_n(2)$. Единичная окрестность функции $f\in\mathcal{F}_n$ — это множество из 2^n функций, отличающихся от f значением на одном из векторов $x\in V_n(2)$.

Воспользуемся следующими известными свойствами:

Работа выполнена при поддержке гранта Президента РФ НШ № 8564.2006.10.

- если I — инвариант аффинной классификации $\mathcal{F}_n/\mathcal{U}_s$, то набор частот встречаемости значений инварианта I для всех 2^n ее производных будет инвариантом аффинной классификации $\mathcal{F}_n/\mathcal{U}_{s+1}$, $-1 \leqslant s < n$;
- если I — инвариант аффинной классификации $\mathcal{F}_n/\mathcal{U}_s$, то набор частот встречаемости значений инварианта I для всех 2^n функций из единичной окрестности исходной функции также будет инвариантом аффинной классификации $\mathcal{F}_n/\mathcal{U}_s$, $-1 \leqslant s < n-1$.

Для построения инвариантов действия аффинной группы на пространстве $\mathcal{F}_6/\mathcal{U}_2$ в качестве исходных использовались следующие инварианты действия аффинной группы на пространстве $\mathcal{F}_6/\mathcal{U}_1$:

- $s(f)$ — набор частот встречаемости модулей коэффициентов преобразования Уолша функции f:

$$W_f(a) = \sum_x (-1)^{f(x)\oplus(x,a)}, \quad a \in V_n(2).$$

- $\sigma(f)$ — набор частот встречаемости модулей значений функции автокорреляции функции f.

$$r_f(a) = \sum_x (-1)^{f(x)\oplus f(x\oplus a)}, \quad a \in V_n(2).$$

Проверялись следующие инварианты действия аффинной группы на факторпространстве $\mathcal{F}_6/\mathcal{U}_2$:

1) I_1 — набор частот встречаемости значений инварианта s для всех 64 производных по направлению;

2) I_2 — набор частот встречаемости значений инварианта σ для всех 64 производных по направлению;

3) I_3 — набор частот встречаемости значений инварианта I_2 для всех функций из единичной окрестности исходной функции.

4) их комбинации.

В результате вычислений получено, что:

- I_1 различает 202 класса;
- I_2 различает 200 классов;
- I_3 различает 84 класса;
- совместное использование I_1 и I_2 привело к получению 204 классов;
- совместное использование I_1 и I_3 привело к получению 203 классов;
- совместное использование I_2 и I_3 привело к получению 201 класса;
- совместное использование I_1, I_2 и I_3 позволяет различить все 205 классов аффинной эквивалентности $\mathcal{F}_6/\mathcal{U}_2$.

Таким образом, полным инвариантом аффинной классификации факторпространства $\mathcal{F}_6/\mathcal{U}_2$ является инвариант (I_1, I_2, I_3). В табл. 1 для всех

классов аффинной эквивалентности факторпространства $\mathcal{F}_6/\mathcal{U}_2$ приведены табличные задания функций-представителей в шестнадцатиричной записи, а также указано число содержащихся в них классов аффинной эквивалентности факторпространства $\mathcal{F}_6/\mathcal{U}_1$.

Литература

[1] *Maiorana J. A.* A Classification of the Cosets of the Reed–Muller code $R(1, 6)$ // Mathematics of Computation, July 1991, vol. 57, № 195. P. 403—414.

[2] *Fuller J.* Affine equivallence classes. `http://www.isrc.qut.edu.au/people/fuller/`.

[3] *Черемушкин А. В.* Классификация двоичных функций от шести переменных // 4 межгосуд. семинар по дискретной математике и ее приложениям, 2—4 февраля 1993 г.: Сб. трудов / Под ред. О. Б. Лупанова. М.: Изд-во механико-матем.ф-та МГУ, 1998, с. 143—144.

[4] *Hou X.-D.* AGL$(m, 2)$ acting on $R(r, m)/R(s, m)$ // J. of Algebra, 1995, vol. 171, № 3. P. 921—938.

Таблица 1:

№	function	class	№	function	class
1	0000000000000000	4	2	0000000100000000	4
3	0000000300000000	6	4	0000000700000000	10
5	0000000F00000000	10	6	0000001700000000	17
7	0000011700000000	27	8	0000001F00000000	17
9	0000811700000000	19	10	0001011700000000	43
11	0000011F00000000	48	12	0000003F00000000	17
13	0001811700000000	43	14	0001011700000001	54
15	0000111F00000000	34	16	0001011F00000000	109
17	0000007F00000000	10	18	0000013F00000000	48
19	000000FF00000000	6	20	0001011780000001	26
21	1001011F00000000	46	22	0000033F00000000	25
23	0001811700000001	116	24	0001111F00000000	127
25	2001011F00000000	100	26	0001011F00000001	214
27	0000017F00000000	20	28	0000053F00000000	41
29	0001013F00000000	161	30	0001811700080001	110
31	0021111F00000000	159	32	0001111F00000001	476
33	1001011F00000001	132	34	2001011F00000001	444
35	0001011F10000001	170	36	0001017F00000000	43
37	0001053F00000000	165	38	0101013F00000000	201
39	4001013F00000000	109	40	0001013F00000001	372
41	0001033F00000000	62	42	0001111F00010001	110

Таблица 1 (продолжение)

№	function	class	№	function	class
43	8001017F00000000	28	44	0009053F00000000	46
45	0001013F02000001	170	46	0421111F00000000	75
47	0021111F00000001	996	48	0001111F00020001	476
49	0001111F00200001	1106	50	1001011F00002001	394
51	2001011F00004001	388	52	0101017F00000000	63
53	0001017F00000001	54	54	0011053F00000000	159
55	1001053F00000000	259	56	0001053F00000001	560
57	0101013F00000001	1210	58	4001013F00000001	530
59	0001013F01000001	182	60	0001013F04000001	492
61	0005033F00000000	116	62	4001033F00000000	72
63	0001033F00000001	148	64	0003033F00000000	22
65	0421111F00000001	396	66	0021111F00000041	996
67	0021111F00000401	2600	68	0021111F04000001	1756
69	1001011F00402001	358	70	0101017F00000001	214
71	8001017F00000001	72	72	1009053F00000000	75
73	0009053F00000001	151	74	0111053F00000000	108
75	0011053F00000001	996	76	1001053F00000001	1600
77	0001053F00010001	1106	78	0001053F00100001	1284
79	0101013F00000101	574	80	0101013F00000201	982
81	0101013F00000401	2696	82	0101013F00004001	3008
83	4001013F00004001	476	84	4001013F00008001	448
85	1005033F00000000	94	86	0005033F00000001	442
87	4001033F00000001	242	88	0001033F00010001	372
89	4003033F00000000	22	90	0003033F00000001	43
91	C003033F00000000	10	92	0421111F80000001	268
93	1001011F08402001	44	94	8111053F00000000	25
95	0011053F00000081	200	96	1001053F00008001	562
97	5005033F00000000	29	98	0005033F00000005	89
99	4001033F00004001	76	100	0003033F00000003	10
101	0421111F00000041	2504	102	0021111F01000041	3036
103	0021111F00080401	900	104	0101017F00000101	306
105	0101017F00000201	352	106	8001017F00008001	45
107	1009053F00000001	330	108	0009053F00000011	628
109	0009053F00001001	556	110	0111053F00000001	688
111	0011053F00000101	2536	112	0011053F00001001	4928
113	1001053F00001001	602	114	1001053F00002001	952
115	1001053F00010001	4608	116	1001053F00100001	2800
117	1001053F00200001	2728	118	0101013F00400101	884
119	0101013F00040201	2504	120	0101013F00400201	1396
121	0101013F00100401	5728	122	4001013F00404001	79
123	4001013F00804001	247	124	9005033F00000000	39
125	1005033F00000001	412	126	0005033F00000009	125

Таблица 1 (продолжение)

№	function	class	№	function	class
127	0005033F00000011	950	128	0005033F00001001	496
129	0005033F00100001	948	130	4001033F00008001	69
131	4001033F00010001	352	132	4003033F00000001	29
133	0003033F00000005	120	134	0421111F00000841	3036
135	0021111F81000041	144	136	0101017F00010101	132
137	0101017F00020101	612	138	0101017F00040201	280
139	8001017F00808001	20	140	1009053F00000011	1756
141	1009053F00001001	1600	142	0009053F00000111	4736
143	0009053F00101001	552	144	0009053F00201001	552
145	8111053F00000001	63	146	0111053F00000081	3168
147	0111053F80000001	2000	148	0011053F00010101	3036
149	0011053F00020101	5728	150	0011053F00041001	5728
151	1001053F00011001	2704	152	1001053F00201001	358
153	1001053F00012001	4424	154	1001053F00018001	2408
155	0101013F10040201	1576	156	5005033F00000001	64
157	9005033F00000001	109	158	1005033F00000005	414
159	1005033F00000009	414	160	1005033F00000011	2912
161	0005033F00100009	327	162	0003033F00001005	108
163	8001017F01808001	4	164	0101017F80010101	14
165	0101017F40020101	56	166	0101017F10040201	58
167	0009053F02201001	61	168	0011053F80010101	252
169	0011053F40020101	148	170	0003033F00009005	40
171	0421111F00200841	304	172	0101017F04020101	528
173	1009053F00000111	2880	174	1009053F00000211	4416
175	1009053F00201001	488	176	0009053F00008111	269
177	0009053F00020111	1504	178	0009053F00100111	860
179	0009053F00200111	4352	180	0009053F10000111	2908
181	0009053F02101001	264	182	8111053F00002001	268
183	1001053F40012001	836	184	5005033F00000009	53
185	5005033F00000011	232	186	5005033F00008001	57
187	9005033F00000005	193	188	9005033F00000011	512
189	1005033F00100005	294	190	1005033F00002009	96
191	1005033F00100009	816	192	0421111F08200841	38
193	1009053F00008111	175	194	1009053F00200111	880
195	0009053F00028111	302	196	5005033F00002009	19
197	5005033F00100009	105	198	9005033F00100005	196
199	5005033F00006009	7	200	0421111F18200841	9
201	5005033F00900009	14	202	9005033F00900005	30
203	0009053F00828111	43	204	0009053F01828111	10
205	0009053F21828111	3			

Об одном варианте метода Ленстры факторизации целых чисел

А. Ю. Нестеренко

В 1985 году [4] Х. Ленстра предложил алгоритм поиска делителей целого числа, использующий вычисления с эллиптическими кривыми. Данный алгоритм не является самым эффективным алгоритмом разложения целых чисел на множители и используется в качестве составной части в других алгоритмах, например, в алгоритмах квадратичного решета и решета числового поля.

В настоящем докладе мы приводим описание модификации алгоритма Ленстры, доказательство асимптотической оценки сложности предложенной нами модификации и результаты практических экспериментов.

1. Группа решений системы уравнений второй степени

В первоначальном варианте алгоритма Ленстры предлагалось использовать для факторизации эллиптические кривые, заданные в аффинной форме записи. Позднее, П. Монтгомери [5] предложил использовать проективные координаты эллиптической кривой, а Р. Брент [2] — дополнить алгоритм вторым этапом, увеличивающем вероятность успешного завершения алгоритма. В работе братьев Чудновских [3] было замечено, что для реализации алгоритма можно использовать проективные абелевы многообразия, однако до последнего времени не было известно многообразий, допускающих эффективную реализацию группового закона.

В работе [1] автором была рассмотрена система уравнений, множество решений которой образует абелеву группу. Позднее автор показал, что множество решений рассмотренной системы уравнений может быть сведено к множеству решений хорошо известной системы уравнений

$$\begin{cases} u_1^2 + u_2^2 = u_4^2, \\ \lambda u_1^2 + u_3^2 = u_4^2, \quad \lambda \neq 0,\ 1. \end{cases} \tag{1}$$

Если решения системы принадлежат некоторому полю, характеристики отличной от двух, то множество решений образует абелеву группу относительно операции сложения.

Пусть (u_1, u_2, u_3, u_4) и (v_1, v_2, v_3, v_4) — два различных решения системы (1), тогда их сумма (w_1, w_2, w_3, w_4) определяется равенствами

$$\begin{cases} w_1 = \xi_3(\xi_1 - \xi_2), \quad \text{где } \xi_1 = u_1 v_3,\ \xi_2 = u_3 v_1,\ \xi_3 = \xi_1 + \xi_2, \\ w_2 = \xi_1\xi_4 - \xi_2\xi_5, \quad \text{где } \xi_4 = u_2 v_4,\ \xi_5 = u_4 v_2, \\ w_4 = w_2 + \xi_3(\xi_5 - \xi_4), \\ w_3 = w_4 - (u_1 v_2 + u_2 v_1)(u_4 v_3 - u_3 v_4). \end{cases} \tag{2}$$

Для сложения решения (u_1, u_2, u_3, u_4) с самим собой можно использовать соотношения

$$\begin{cases} w_2 = \xi_3 - \xi_4, \\ w_4 = \xi_3 + \xi_4, \quad \text{где } \xi_1 = u_2 u_4,\ \xi_2 = u_1 u_3,\ \xi_3 = \xi_1^2,\ \xi_4 = \xi_2^2, \\ w_1 = (\xi_1 + \xi_2)^2 - w_4, \\ w_3 = 2(u_2 u_3)^2 - w_2. \end{cases} \tag{3}$$

Единичным элементом данной группы является решение (0, 1, 1, 1), обратным к элементу (u_1, u_2, u_3, u_4) является элемент $(-u_1, u_2, u_3, u_4)$.

В нашем варианте алгоритма факторизации, мы используем множество решений системы (1) в $\mathbb{Z}_N$ — кольце вычетов по модулю целого числа N, которое мы пытаемся разложить на множители.

При фиксированном значении параметра λ задача нахождения хотя бы одного решения системы (1) в $\mathbb{Z}_N$ является достаточно трудоемкой. В случае, когда нам надо выбрать произвольное решение произвольной системы уравнений, можно воспользоваться следующим замечанием.

Выберем произвольные целые числа n, t, удовлетворяющие неравенствам $0 < n < N$, $0 < t < N$, и определим

$$\begin{cases} u_1 \equiv 2nt \pmod N, \\ u_2 \equiv n^2 - t^2 \pmod N, \\ u_4 \equiv n^2 + t^2 \pmod N. \end{cases}$$

Тогда выполнено $u_1^2 + u_2^2 \equiv u_4^2 \pmod N$ и мы получаем параметризацию первого уравнения системы (1). Подставляя полученные соотношения во второе уравнение системы и выбирая значение u_3 случайным образом, мы получим решение

$$(2nt,\ n^2 - t^2,\ u_3,\ n^2 + t^2),$$

а также параметр λ, удовлетворяющий сравнению

$$\lambda \equiv \frac{(n^2 + t^2)^2 - u_3^2}{4n^2t^2} \pmod N, \tag{4}$$

если $nt \in \mathbb{Z}_N^*$. В противном случае $(nt, N) > 1$ и мы находим нетривиальный делитель числа N.

2. Алгоритм факторизации

Пусть задано нечетное составное число N, для которого надо найти нетривиальный делитель. Алгоритм поиска этого делителя может быть схематично описан следующим образом.

1. Выбрать параметры алгоритма — целые неотрицательные числа b_1, b_2, b_3, b_4, а также целое число m, определяемое равенством
$$m = \prod_i p_i^{\alpha_i},$$
где p_i — все маленькие простые числа, не превосходящие границы b_1, а степени α_i имеют небольшие значения. Определить значение счетчика $j = 0$.
2. Выбрать произвольное ненулевое решение (u_1, u_2, u_3, u_4) системы (1).
3. Используя равенства (2), (3), возвести решение (u_1, u_2, u_3, u_4) в степень m, то есть вычислить равенство
$$(w_1, w_2, w_3, w_4) = [m](u_1, u_2, u_3, u_4).$$
Если $(w_1, N) > 1$, то завершить работу алгоритма.
4. Для всех k от 1 до b_4 вычислить
   (a) Случайным образом выбрать простое число p_k, $b_1 < p_k \leqslant b_2$, и вычислить точку
   $$(z_1, z_2, z_3, z_4) = [p_k](w_1, w_2, w_3, w_4).$$
   (b) Если $(z_1, N) > 1$, то завершить работу алгоритма, в противном случае выбрать новое значение p_k.
5. Вычислить $j = j + 1$. Если $j < b_3$, то вернуться на шаг 2. В противном случае, завершить работу с уведомлением о неудаче.

Представим m в виде $m = c_0 m_0$, $m_0 = \prod_i p_i$, для некоторого постоянного значения c_0 и воспользуемся неравенством $\log m_0 = \sum \log p_i < b_1$. Тогда оценка сверху сложности приведенного алгоритма составит

$$T = 2Mb_3(\log c_0 + b_1 + b_4 \log b_2), \tag{5}$$

где M это максимум из числа операций, необходимых для вычисления соотношений (2) или (3).

Мы будем использовать данную оценку дважды. Сначала мы получим асимптотическую оценку, а после, подбирая значения параметров b_1, b_2, b_3, b_4, минимизируем сложность алгоритма.

Начнем с выбора параметра b_4 и определим его таким образом, что

$$b_1 > b_4 \log b_2, \tag{6}$$

тогда неравенство (5) принимает вид $T < 6Mb_3b_1$, из которого легко получить асимптотическую оценку сложности алгоритма.

Обозначим символом p наименьший простой делитель числа N. Значение p нам неизвестно, его отыскание и является нашей задачей.

Если мы приведем любое решение системы (1) по модулю p, то оно будет принадлежать абелевой группе решений системы, рассматриваемой над конечным полем, и иметь конечный порядок, который мы обозначим символом N_p. Для данного значения выполнено неравенство

$$p - 2\sqrt{p} - 1 \leqslant N_p \leqslant p + 2\sqrt{p} + 1,$$

аналогичное неравенству Хассе для эллиптических кривых. Предположим, что в данном интервале находится s чисел таких, что $N_p \mid m$. Тогда для этих чисел описанный нами алгоритм найдет нетривиальный делитель числа N и нам потребуется $4\sqrt{p}/s$ попыток случайного выбора системы уравнений. Естественно выбрать эту величину в качестве значения параметра b_3.

Обозначим символом $\psi(x, y)$ функцию, обозначающую количество натуральных чисел, не превосходящих x таких, что их наибольший простой делитель не превосходит y. Для данной функции выполнена асимптотическая оценка

$$\psi(x, y) = xe^{-u \log u + o(u \log u)}, \quad \text{где } u = \frac{\log x}{\log y}.$$

Воспользовавшись этим утверждением мы получим, что параметр s может быть оценен величиной

$$s = \psi(p + 2\sqrt{p}, b_1) - \psi(p - 2\sqrt{p}, b_1).$$

Введем в рассмотрение действительный параметр $\alpha > 0$ и определим

$$b_1 = \sqrt[\alpha]{p},$$

тогда, преобразуя выражение для s, получим

$$s = 4\sqrt{p}e^{-\alpha \log \alpha} \quad \text{и} \quad b_3 = e^{\alpha \log \alpha}.$$

Последнее равенство позволяет нам записать асимптотическую оценку сложности рассматриваемого алгоритма в виде

$$O\left(e^{\alpha \log \alpha + (\log p)/\alpha}\right). \tag{7}$$

Нам осталось минимизировать значение функции $t(\alpha) = \alpha \log \alpha + (\log p)/\alpha$. Известно аналитическое представление для α, а именно

$$\alpha = \sqrt{\frac{2\log p}{\log\log p}}, \tag{8}$$

позволяющее получить асимптотическую оценку алгоритма в окончательном виде. Подставляя значение для α в (7) получим оценку

$$O\left(e^{\sqrt{2\log p \log\log p}}\right).$$

Данная оценка зависит от размера наименьшего делителя числа N, что ограничивает область применения данного алгоритма лишь числами с маленькими простыми делителями.

На практике нам интересна не асимптотическая оценка, а реальная. Поскольку нам неизвестно значение простого делителя, мы можем сделать предположение о его величине и точно рассчитать значение функции $t(\alpha)$ и параметров b_1, b_3.

Приведем таблицу значений параметра α рассчитанного с использованием равенства (8) и рассчитанного на ЭВМ значения параметра $\widetilde{\alpha}$, минимизирующего значение $t(\alpha)$. Для чисел вида $p = 10^k$ при $k = 10, 15, 20, \ldots$ мы получили следующие значения:

k	α	$t(\alpha)$	$\widetilde{\alpha}$	$t(\widetilde{\alpha})$
10	3.831705	11.156463	3.250793	10.915505
15	4.416102	14.380149	3.837866	14.161084
20	4.904015	17.188262	4.323180	16.981373
25	5.329782	19.718939	4.744712	19.520038
30	5.711432	22.046609	5.121589	21.853459

Из этой таблицы видно, что формула (8) дает достаточно точное приближение к минимуму функции $t(\alpha)$. Вместе с тем, избавление от возникшей погрешности позволило нам получить следующие значения параметров $b_1 = \lfloor \sqrt[\widetilde{\alpha}]{p} \rfloor$, $b_3 = \lfloor e^{\widetilde{\alpha}\ln\widetilde{\alpha}} \rfloor$:

k	b_1	b_3
10	1 192	47
15	8 099	175
20	42 289	561
25	185 791	1 616
30	720 373	4 299

Нам осталось рассчитать значения параметров b_2, b_4. Введем в рассмотрение параметр β, удовлетворяющие неравенству $\alpha > \beta > 0$, и определим

$$b_2 = \sqrt[\beta]{p}.$$

Параметр b_4 задает максимально возможное количество простых чисел в интервале от b_1 до b_2, удовлетворяющее неравенству (6). Таким образом выполнено неравенство

$$b_4 = \pi(b_2) - \pi(b_1) \leqslant \frac{b_1}{\log b_2}.$$

Воспользовавшись приближенной оценкой $\pi(x) \sim x/\log x$, получим условие на параметр b_2 или, что аналогично, на параметр β:

$$\beta \sqrt[\beta]{p} - \alpha \sqrt[\alpha]{p} \leqslant \beta \sqrt[\alpha]{p}.$$

Упрощая, получаем неравенство $b_1^{\gamma-1} \leqslant \gamma$, где $\gamma = \alpha/\beta$. Выбирая наибольшее значение γ, удовлетворяющее данному неравенству, получаем точное значение параметра b_2.

В заключение доклада приведем результаты практической реализации изложенного алгоритма. Основной задачей при проведении экспериментов была оценка вероятности успешного завершения алгоритма при рассчитанных значениях параметров. Одно и тоже число подвергалось многократному разложению и проводился сравнительный анализ полученных значений с рассчитанными заранее значениями.

Приведем полученные экспериментально значения. Как и ранее, символом p мы обозначаем наименьший делитель числа N, символом S количество попыток факторизации. Столбцы «Шаг 3» и «Шаг 4» показывают процент успешного разложения на третьем и, соответственно, четвертом шагах алгоритма. Параметр min определяет минимальное число попыток выбора случайного решения на втором шаге алгоритма, потребовавшихся для успешной факторизации, cnt — количество успешных разложений с минимальным числом попыток, max — максимальное число попыток, в случае успешного разложения. Параметр avg определяет среднее число попыток, необходимых для успешного разложения на множители (в процентах от значения b_3).

$N = 10723261738237112839, \quad \log_2(N) = 64$:

$\log_2(p)$	S	Шаг 3	Шаг 4	b_3	min	cnt	max	avg
32	100	79 (79 %)	21 (21 %)	42	1	10	23	6.68 (16 %)

$N = 458125662174126526570165492 99$, $\log_2(N) = 96$:

$\log_2(p)$	S	Шаг 3	Шаг 4	b_3	min	cnt	max	avg
48	72	53 (74 %)	19 (26 %)	153	1	1 (1 %)	134	28.54 (19 %)

$N = 142657541002063195275367942016858713253$, $\log_2(N) = 127$:

$\log_2(p)$	S	Шаг 3	Шаг 4	b_3	min	cnt	max	avg
64	100	67 (67 %)	33 (33 %)	476	1	2 (2 %)	429	82.24 (18 %)

Как следует из приведенных значений, среднее число успешных попыток существенно меньше, чем значение параметра b_3, определяющего максимальное число попыток. С увеличением размерности раскладываемых чисел это значение растет, но не слишком сильно: отношение числа успешных попыток к теоретически рассчитанному не превышает 25 %. К сожалению, точное математическое обоснование данного результата автору не известно.

После проведения большого числа экспериментов, необходимость второго этапа алгоритма (шаг 4) является обоснованной. Даже не смотря на то, что процент успешных разложений на четвертом шаге не превышает одной трети.

Проведенные эксперименты показывают, что способ расчета параметров, предложенный автором доклада, позволяет получать значения, которые приводят к разложению числа N на множители, без уведомления о неудаче. Получаемые значения верны и позволяют получить точную оценку сверху для сложности алгоритма при сделанном предположении о размере наименьшего делителя числа N.

Литература

[1] *Нестеренко А. Ю.* О групповых свойствах одной системы уравнений // Математика и безопасность информационных технологий. Материалы конференции в МГУ 23—24 октября 2003 г., М.: МЦНМО, 2004, с. 221—222.

[2] *Brent R. P.* Some integer factorization algorithms using elliptic curves // Australian Computer Science Communacations. 1986. № 8. P. 149—163.

[3] *Chudnovsky D., Chudnovsky G.* Sequences Of numbers generated by addition in formal groups and new primality and factorization tests // Advances in Applied Mathematics. 1987. № 7. P. 385—434.

[4] *Lenstra H. W.* Factoring integers with elliptic curves // Ann. Math. 1987. № 126. P. 649—673.

[5] *Montgomery P. L.* Speeding the Pollard and elliptic curve methods of factorization // Math. of Comp. 1987. Vol. 48. № 177. P. 243—267.

Весовой спектр одного кода

А. В. Покровский

Аннотация

В данной работе описан весовой спектр одного подкода кода Рида—Маллера t-го порядка. А так же описано, как устроен полином Жегалкина функций из этого кода, имеющих данный вес. По своей сути данная работа является обобщением работы [1].

1. Основные определения и весовой спектр одного подкода

Пусть t, $n \in \mathbb{N}$, $t \leqslant n$ и $\mathcal{F}_n$ — множество булевых функций от n переменных. Обозначим $\widetilde{\mathcal{F}}_t$ — множество булевых функций от t переменных, номера которых начинаются с $n-t+1$ и $\mathrm{wt}(f)$ — вес функции f, $\deg f$ — степень нелинейности. Определим $\mathcal{K}_t \subset \mathcal{F}_n$ как множество всех функций вида $g \oplus h \in \mathcal{F}_n$, где $g \in \widetilde{\mathcal{F}}_t$ и

$$h = \bigoplus_{1 \leqslant i < j \leqslant n-t} a_{ij} x_i x_j \oplus \bigoplus_{i=n-t+1}^{n} x_i l_i(x_1, \ldots, x_{n-t}) \oplus l(x_1, \ldots, x_{n-t}) \oplus \epsilon,$$

$l(x_1, \ldots, x_{n-t})$, $l_i(x_1, \ldots, x_{n-t})$, $i = \overline{n-t+1, n}$ — линейные функции.

Определение 14. Линейным блочным кодом $\mathcal{C}$ длины n называется подпространство векторного пространства V_n.

В дальнейшем под V_n будем понимать множество двоичных векторов длины n.

Через Ω_f будем обозначать вектор-столбец функции f, т. е.

$$\Omega_f = (f(u_0), f(u_1), \ldots, f(u_{2^n-1})), \quad u_i \in V_n,\ i = 0, 1, \ldots, 2^n - 1.$$

Определение 15. Для произвольных n, $r \in \mathbb{N}$, $0 \leqslant r \leqslant n$, кодом Рида—Маллера $\mathrm{RM}(r, n)$ порядка r и длины 2^n называется множество всех строк Ω_f тех булевых функций $f \in \mathcal{F}_n$, степень нелинейности которых не превосходит r, т. е.

$$\mathrm{RM}(r, n) = \{\Omega_f \mid f \in \mathcal{F}_n,\ \deg f \leqslant r\}.$$

Определение 16. Весовым спектром кода $\mathcal{C}$ называется совокупность чисел $A_0, A_1, \ldots, A_n$, где

$$A_i = |\{c \in \mathcal{C} \mid \mathrm{wt}(c) = i\}|, \quad i \in \overline{0, n}.$$

Несложно видеть, что $\mathcal{K}_t$ — подкод кода $\mathrm{RM}(t, n)$.

Обозначим через AGL группу аффинных преобразований на V_n.

Определение 17. Функции $f_1, f_2 \in \mathcal{F}_n$ называются аффинно эквивалентными, если существует пара $(A, \vec{\gamma}) \in \mathrm{AGL}$ такая, что

$$f_1(\vec{x}A \oplus \vec{\gamma}) = f_2(\vec{x})$$

для любого $\vec{x} \in V_n$.

Справедлива следующая теорема (см., например, [3] или [4]).

Теорема 1. *Пусть f — квадратичная булева функция из $\mathcal{F}_{n-t}$, тогда аффинной заменой переменных она может быть приведена лишь к одному из следующих видов*:

1) $q_1^k(x_1, \ldots, x_{n-t}) = x_1x_2 \oplus \ldots \oplus x_{2k-1}x_{2k}$;
2) $q_2^k(x_1, \ldots, x_{n-t}) = x_1x_2 \oplus \ldots \oplus x_{2k-1}x_{2k} \oplus 1$;
3) $q_3^k(x_1, \ldots, x_{n-t}) = x_1x_2 \oplus \ldots \oplus x_{2k-1}x_{2k} \oplus x_{2k+1}$.

Число k называется рангом квадратичной формы и может изменяться в интервале $k \in \overline{1, [(n-t)/2]}$. Каждая из канонических форм q_1^k, q_2^k, q_3^k имеет вес

$$2^{n-t-1} - 2^{n-t-k-1}, \quad 2^{n-t-1} + 2^{n-t-k-1}, \quad 2^{n-t-1}$$

соответственно и лежат на разных орбитах (см., например, [3, 2]). Обозначим $O_{q_i}(k)$, $i = \overline{1, 3}$, мощность орбиты, на которой лежит i-я каноническая форма ранга k. Эти величины приведены в работе [2]. Обобщим понятие ранга квадратичной формы на случай $k = 0$. Тогда все множество аффинных функций, от $n-t$ переменных, разбивается на три орбиты:

$$O_{q_1}(0) = |\{0\}| = 1,$$
$$O_{q_2}(0) = |\{1\}| = 1,$$
$$O_{q_3}(0) = \Big|\big\{a_1x_1 \oplus \ldots \oplus a_{n-t}x_{n-t}, \oplus\epsilon\big| a_i, \epsilon \in V_1,\ i = \overline{1, n-t},\ (a_1, \ldots, a_{n-t}) \neq \vec{0}\big\}\Big| = 2^{n-t+1} - 2.$$

В случае орбиты $O_{q_3}(0)$ канонической формой будем считать функцию x_1.

При введенных обозначениях справедлива теорема:

Теорема 2. *Весовой спектр кода $\mathcal{K}_t$ имеет вид*:

1) *в случае, когда $n-t$ нечетно*:

Количество функций	*Вес*
$O_{q_3}(k)\left(2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t, n-t-2k\}} M(t, n-t-2k, r)\right) 2^{2^t+2kt}$	2^{n-1}
$\binom{2^{t-r}}{i} O_{q_3}(k) + M(t, n-t-2k, r) \times 2^{2^t-2^{t-r}+2kt}$	$i\,\mathrm{wt}(q_1^k) + (2^{t-r} - i)\,\mathrm{wt}(q_2^k) + (2^t - 2^{t-r})\,\mathrm{wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_1}(k) N(t, n-t-2k, r) \times 2^{2^t-2^{t-r}+2kt}$	$i\,\mathrm{wt}(q_1^k) + (2^{t-r} - i)\,\mathrm{wt}(q_2^k) + (2^t - 2^{t-r})\,\mathrm{wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_2}(k) N(t, n-t-2k, r) \times 2^{2^t-2^{t-r}+2kt}$	$i\,\mathrm{wt}(q_2^k) + (2^{t-r} - i)\,\mathrm{wt}(q_1^k) + (2^t - 2^{t-r})\,\mathrm{wt}(q_3^k)$

$$i = \overline{0, 2^{t-r}},\ r = \overline{0, \min\{t, n-t-2k\}},\ k = \overline{0, [(n-t)/2]};$$

2) *в случае, когда $n-t$ четно*:

Количество функций	*Вес*
$O_{q_3}(k)\left(2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t, n-t-2k\}} M(t, n-t-2k, r)\right) 2^{2^t+2kt}$	2^{n-1}
$\binom{2^{t-r}}{i} O_{q_3}(k) M(t, n-t-2k, r) \times 2^{2^t-2^{t-r}+2kt}$	$i\,\mathrm{wt}(q_1^k) + (2^{t-r} - i)\,\mathrm{wt}(q_2^k) + (2^t - 2^{t-r})\,\mathrm{wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_1}(k) N(t, n-t-2k, r) \times 2^{2^t-2^{t-r}+2kt}$	$i\,\mathrm{wt}(q_1^k) + (2^{t-r} - i)\,\mathrm{wt}(q_2^k) + (2^t - 2^{t-r})\,\mathrm{wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_2}(k) N(t, n-t-2k, r) \times 2^{2^t-2^{t-r}+2kt}$	$i\,\mathrm{wt}(q_2^k) + (2^{t-r} - i)\,\mathrm{wt}(q_1^k) + (2^t - 2^{t-r})\,\mathrm{wt}(q_3^k)$
$O_{q_1}((n-t)/2)\binom{2^t}{j} 2^{t(n-t)}$	$j\,\mathrm{wt}\big(q_1^{(n-t)/2}\big) + (2^t - j)\big(q_2^{(n-t)/2}\big)$
$O_{q_2}((n-t)/2)\binom{2^t}{j} 2^{t(n-t)}$	$j\,\mathrm{wt}\big(q_2^{(n-t)/2}\big) + (2^t - j)\,\mathrm{wt}\big(q_1^{(n-t)/2}\big)$

$$i = \overline{0, 2^{t-r}}, \quad j = \overline{0, 2^t}, \quad r = \overline{0, \min\{t, n-t-2k\}}, \quad k = \overline{0, (n-t)/2-1}.$$

Здесь

$$N(t, n-t-2k, r) = \begin{cases} 0, & \text{если } r > \min\{t, n-t-2k\}; \\ 1, & \text{если } r = 0; \\ N(t-1, n-t-2k, r-1) \times & \\ \quad (2^{n-t-2k} - 2^{r-1}) + & \\ \quad N(t-1, n-t-2k, r)2^r, & \text{если } 0 < r \leqslant \min\{t, n-t-2k\} \end{cases}$$

и

$$M(t,\, n-t-2k,\, r) = \begin{cases} 0, & \text{если } r > \min\{t,\, n-t-2k\} \\ & \text{или } r = 0; \\ 2^t - 1, & \text{если } r = 1; \\ N(t,\, n-t-2k,\, r) - & \\ \quad N(t,\, n-t-2k-1,\, r)2^r, & \text{если } 0 < r \leqslant \min\{t,\, n-t-2k\}. \end{cases}$$

Доказательство. Для фиксированной функции из $\mathcal{K}_t$ возможен лишь один из трех случаев:

1) $\bigoplus_{1\leqslant i<j\leqslant n-t} a_{ij}x_ix_j \oplus l(x_1,\, \ldots,\, x_{n-t}) \underset{\mathrm{AGL}}{\sim} q_1^k(x_1,\, \ldots,\, x_{n-t})$;
2) $\bigoplus_{1\leqslant i<j\leqslant n-t} a_{ij}x_ix_j \oplus l(x_1,\, \ldots,\, x_{n-t}) \underset{\mathrm{AGL}}{\sim} q_2^k(x_1,\, \ldots,\, x_{n-t})$;
3) $\bigoplus_{1\leqslant i<j\leqslant n-t} a_{ij}x_ix_j \oplus l(x_1,\, \ldots,\, x_{n-t}) \underset{\mathrm{AGL}}{\sim} q_3^k(x_1,\, \ldots,\, x_{n-t})$.

Пусть $(A,\, \vec{\gamma}) \in \mathrm{AGL}$ — преобразование, приводящее

$$\bigoplus_{1\leqslant i<j\leqslant n-t} a_{ij}x_ix_j \oplus l(x_1,\, \ldots,\, x_{n-t})$$

к одному из канонических видов. Применим это преобразование к функции $f \in \mathcal{K}_t$ и будем рассматривать вес функции $f(\vec{x}A \oplus \vec{\gamma}) = \widehat{f}(\vec{x})$, равный $\mathrm{wt}(f)$. Она может иметь один из трех видов:

1) $g(x_{n-t+1},\, \ldots,\, x_n) \oplus q_1^k(x_1,\, \ldots,\, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^{n} x_i l^{(i)}(x_1,\, \ldots,\, x_{n-t}) \oplus \epsilon'$;
2) $g(x_{n-t+1},\, \ldots,\, x_n) \oplus q_2^k(x_1,\, \ldots,\, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^{n} x_i l^{(i)}(x_1,\, \ldots,\, x_{n-t}) \oplus \epsilon'$;
3) $g(x_{n-t+1},\, \ldots,\, x_n) \oplus q_3^k(x_1,\, \ldots,\, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^{n} x_i l^{(i)}(x_1,\, \ldots,\, x_{n-t}) \oplus \epsilon'$.

Вес функции $\widehat{f}$ равен

$$\mathrm{wt}\left(\widehat{f}\right) = \sum_{(i_{n-t+1},\ldots,i_n)\in V_t} \mathrm{wt}\left(\widehat{f}^{\,i_{n-t+1},\ldots,i_n}_{n-t+1,\ldots,n}\right),$$

где $\widehat{f}^{\,i_{n-t+1},\ldots,i_n}_{n-t+1,\ldots,n}$ — подфункция функции $\widehat{f}$, полученная фиксацией переменных с номерами $n-t+1,\, \ldots,\, n$ константами $i_{n-t+1},\, \ldots,\, i_n$ соответственно.

Рассмотрим $t \times (n-t)$-матрицу $\mathcal{L}$, состоящую из коэффициентов линейных функций $l^{(i)}(x_1,\, \ldots,\, x_{n-t})$, $i = \overline{1,\, t}$:

$$\mathcal{L} = \begin{pmatrix} l_1^{(1)} & \ldots & l_{n-t}^{(1)} \\ l_1^{(2)} & \ldots & l_{n-t}^{(2)} \\ & \ddots & \\ l_1^{(t)} & \ldots & l_{n-t}^{(t)}. \end{pmatrix}$$

Разобьем матрицу $\mathcal{L}$ на две подматрицы:

$$\mathcal{L} = (\mathcal{L}'_{t\times 2k} \mid \mathcal{L}''_{t\times n-t-2k})$$

и пусть $\mathrm{rang}\,\mathcal{L}'' = r$, $r = \overline{0,\, \min\{t,\, n-t-2k\}}$. Для сокращения записи обозначим число $t \times n-t-2k$ матриц ранга r через $N(t,\, n-t-2k,\, r)$:

$$N(t,\, n-t-2k,\, r) = \begin{cases} 0, & \text{если } r > \min\{t,\, n-t-2k\}; \\ 1, & \text{если } r = 0; \\ N(t-1,\, n-t-2k,\, r-1) \times & \\ \quad (2^{n-t-2k} - 2^{r-1}) + & \\ \quad N(t-1,\, n-t-2k,\, r)2^r, & \text{если } 0 < r \leqslant \min\{t,\, n-t-2k\}. \end{cases}$$

Пусть

$$\widehat{f} = g(x_{n-t+1},\, \ldots,\, x_n) \oplus q_1^k(x_1,\, \ldots,\, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^{n} x_i l^{(i)}(x_1,\, \ldots,\, x_{n-t}) \oplus \epsilon'$$

и $\mathrm{rang}\,\mathcal{L}'' = r$. Тогда система

$$\vec{x}\mathcal{L}'' = \vec{0} \tag{1}$$

имеет 2^{t-r} решений. Если $\vec{x} \in V_t$ является решением системы, то

$$\mathrm{wt}\left(q_1^k(x_1,\, \ldots,\, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^{n} x_i l^{(i)}(x_{n-t+1},\, \ldots,\, x_n) \oplus \epsilon'\right) = \begin{cases} \mathrm{wt}(q_1^k), & \text{если } \epsilon' = 0; \\ \mathrm{wt}(q_2^k), & \text{если } \epsilon' = 1. \end{cases}$$

В противном случае этот вес равен $\mathrm{wt}(q_3^k)$.

При этом значение константы ϵ' определяется суммой значений константы ϵ и значением функции $g(x_{n-t+1}, \ldots, x_n)$. Поскольку g пробегает все $\widetilde{\mathcal{F}}_t$, то для всех фиксаций переменных $x_{n-t+1}, \ldots, x_n$ набор констант ϵ' пробегает все возможные 2^t значений.

Далее рассмотрим два случая:

1) $n-t$ нечетно и $0 \leqslant k \leqslant \left[\frac{n-t}{2}\right]$ или $n-t$ четно и $0 \leqslant k \leqslant \frac{n-t}{2} - 1$;

2) $n-t$ четно и $k = \frac{n-t}{2}$.

Из сказанного выше следует, что в случае, когда $n-t$ нечетно и $0 \leqslant k \leqslant [(n-t)/2]$ или $n-t$ четно и $0 \leqslant k \leqslant (n-t)/2 - 1$, ровно

$$\binom{2^{t-r}}{i} N(t, n-t-2k, r) O_{q_1}(k) 2^{2^t - 2^{t-r} + 2kt}$$

функций имеют вес

$$i \operatorname{wt}(q_1^k) + (2^{t-r} - i) \operatorname{wt}(q_2^k) + (2^t - 2^{t-r}) \operatorname{wt}(q_3^k),$$

где $r = \overline{0, \min\{n-t-2k, t\}}$, $i = \overline{0, 2^{t-r}}$.

В случае, когда $\bigoplus_{1 \leqslant i < j \leqslant n-t} a_{ij} x_i x_j \oplus l(x_1, \ldots, x_{n-t}) \underset{\text{AGL}}{\sim} q_2^k$, рассуждения переносятся аналогичным образом, заменяя q_1^k на q_2^k и наоборот. Получим, что

$$\binom{2^{t-r}}{i} N(t, n-t-2k, r) O_{q_2}(k) 2^{2^t - 2^{t-r} + 2kt}$$

функций имеют вес

$$i \operatorname{wt}(q_2^k) + (2^{t-r} - i) \operatorname{wt}(q_1^k) + 2^t - 2^{t-r} \operatorname{wt}(q_3^k),$$

где $r = \overline{0, \min\{n-t-2k, t\}}$, $i = \overline{0, 2^{t-r}}$

Теперь рассмотрим случай, когда $n-t$ четно, $k = (n-t)/2$ и

$$\bigoplus_{1 \leqslant i < j \leqslant n-t} a_{ij} x_i x_j \oplus l(x_1, \ldots, x_{n-t}) \underset{\text{AGL}}{\sim} q_1^k(x_1, \ldots, x_{n-t}).$$

В этом случае матрица $\mathcal{L} = \mathcal{L}'$ и при любой фиксации $x_{n-t+1}, \ldots, x_n$ прибавление к q_1^k линейной комбинации $\bigoplus_{i=n-t+1}^{n} x_i l^{(i)}(x_1, \ldots, x_t)$ будет либо оставлять ее на орбите содержащей q_1^k, либо переводить ее на орбиту содержащую q_2^k. Таким образом, вес подфункции будет определяться лишь значением соответствующей константы ϵ', которая в свою очередь определяется значением функции g.

Случай, когда $n-t$ четно и

$$\bigoplus_{1 \leqslant i < j \leqslant n-t} a_{ij} x_i x_j \oplus l(x_1, \ldots, x_{n-t}) \underset{\text{AGL}}{\sim} q_2^k(x_1, \ldots, x_{n-t}),$$

рассматривается аналогично предыдущему случаю.

Остается рассмотреть случай, когда

$$\bigoplus_{1 \leqslant i < j \leqslant n-t} a_{ij} x_i x_j \oplus l(x_1, \ldots, x_{n-t}) \underset{\text{AGL}}{\sim} q_3^k.$$

В этом случае рассмотрим систему:

$$(\vec{x}\mathcal{L}'')^T = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{2}$$

Если вектор $\vec{x}$ является ее решением, то $q_3^k \oplus \bigoplus_{i=1}^{n-t} x_i l^{(i)}(x_1, \ldots, x_{n-t})$ будет иметь вес $\operatorname{wt}(q_1^k)$ или $\operatorname{wt}(q_2^k)$, в зависимости от константы, определяемой как и для случая $\bigoplus_{1 \leqslant i < j \leqslant n-t} a_{ij} x_i x_j \oplus l(x_1, \ldots, x_{n-t}) \underset{\text{AGL}}{\sim} q_1^k$. Для всех остальных векторов $\vec{\alpha}$, для которых система $\vec{x}\mathcal{L}'' = \vec{\alpha}$ совместна, функция $q_3^k \oplus \bigoplus_{i=1}^{n-t} x_i l^{(i)}(x_1, \ldots, x_{n-t})$ имеет вес 2^{n-t-1}. Число $t \times (n-t-2k)$-матриц ранга r, для которых система (2) совместна, обозначим через $M(t, n-t-2k, r)$. Поскольку система совместна тогда и только тогда, когда $\operatorname{rang}(\mathcal{L}'')^T = \operatorname{rang}((\mathcal{L}'')^T | \beta^{\downarrow})$, где

$$\beta^{\downarrow} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

имеет место рекуррентная формула:

$$M(t, n-t-2k, r) =$$

$$= \begin{cases} 0, & \text{если } r > \min\{t, n-t-2k\} \\ & \quad \text{или } r = 0; \\ 2^t - 1, & \text{если } r = 1; \\ N(t, n-t-2k, r) - & \\ \quad N(t, n-t-2k-1, r) 2^r, & \text{если } 0 < r \leqslant \min\{t, n-t-2k\}. \end{cases}$$

Из этого следует, что $t \times (n-t-2k)$ матриц ранга r, для которых система (2) несовместна, ровно

$$2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t,n-t-2k\}} M(t,\, n-t-2k,\, r).$$

Поэтому в исследуемом коде содержится

$$O_{q_3}(k)(2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t,n-t-2k\}} M(t,\, n-t-2k,\, r))2^{2^t+2kt}$$

функций веса

$$\mathrm{wt}(q_3^k)2^t = 2^t 2^{n-t-1} = 2^{n-1}$$

и

$$\binom{2^{t-r}}{i} O_{q_3}(k) M(t,\, n-t-2k,\, r) 2^{2^t-2^{t-r}+2kt}$$

функций веса

$$i\,\mathrm{wt}(q_1^k) + (2^{t-r}-i)\,\mathrm{wt}(q_2^k) + 2^{2^t-2^{t-r}}\,\mathrm{wt}(q_3^k),$$

где $i = \overline{0,\, 2^{t-r}}$, $r = \overline{1,\, \min\{t,\, n-t-2k\}}$, $k = \overline{1,\, [(n-t)/2]}$. □

Литература

[1] *Никифоров М. С.*, *Покровский А. В.* Весовой спектр одного подкода кода RM(3, n) // XIV Международная конференция «Проблемы теоретической кибернетики». Пенза, 2005.

[2] *Черёмушкин А. В.* Методы аффинной и линейной классификации булевых функций // Труды по дискретной математике. Т. 4. Российская Академия наук, Академия криптографии Российской Федерации. М.: Физико-математическая литература, 2001.

[3] *Мак-Вильямс Ф. Дж.*, *Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.

[4] *Логачёв О. А.*, *Сальников А. А.*, *Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.

[5] *О'Мира О.* Лекции о симплектических группах. М.: Мир, 1979.

Часть III

СЕКЦИЯ «МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ»

Автоматическое обнаружение уязвимостей настроек безопасности в защищенных информационных системах с использованием логики предикатов

П. Д. Зегжда, Д. П. Зегжда, М. О. Калинин

Современные операционные системы предоставляют набор разнообразных механизмов защиты. Если программные ошибки, допущенные при проектировании и реализации средств защиты, можно исправить путем обновления ПО, то несоблюдение мер безопасности или некорректная реализация администраторами политик информационной безопасности при настройке системы вследствие чрезвычайной сложности и перегруженности управления системной безопасностью приводят к тому, что многокомпонентная защита может стать бесполезной. Просчеты администрирования приводят к возникновению так называемых уязвимостей настроек безопасности. Типичными примерами таких уязвимостей являются разрешение модификации системных каталогов и использование настроек, задаваемых по умолчанию. По этой причине безопасность систем обработки информации нуждается в регулярно проводимом доказательстве, что позволит гарантировать реализацию и выполнение необходимых ограничений на доступ к информации.

Авторами предложен подход автоматического доказательства безопасности, основанный на логическом описании состояния настроек безопасности анализируемой системы и использовании алгоритмической модели контроля и управления доступом с целью проверки состояния на соответствие критериям обнаружения уязвимостей. Логическое описание состояния настроек безопасности — это абстракция состояния системы в контексте реализованной модели контроля и управления доступом, представленная в форме предикатов. Правила алгоритмической модели определяют ограничения, накладываемые на поведение системы при принятии решения о доступе. Причины возникновения уязвимостей, переформулированные в виде логических условий — критериев обнаружения уязвимостей, — позволяют разделить множество состояний на безопасные и небезопасные.

Процесс оценки соответствия состояний ограничениям, накладываемым на них, называется разрешением проблемы безопасности. Представим проблему безопасности формально как $\Lambda = \{M, \Sigma, D\}$, где M — модель безопасности, $M = \{S, R, C\}$; Σ — система, $\Sigma = \left\{S^{\Sigma}, T, s^{\Sigma}_{\text{init}}, Q\right\}$; D — функция соответствия состояний, $D: S^{\Sigma} \to S$; S^{Σ} — множество состояний системы; Q — множество запросов, обрабатываемых системой; T — функция перехода из состояний в состояние, $T: Q \times S^{\Sigma} \to S^{\Sigma}$, $s^{\Sigma}_{i+1} = T\left(q, s^{\Sigma}\right)$; s^{Σ}_{init} — начальное состояние системы. Состояние s^{Σ} достижимо в системе $\Sigma = \left\{S^{\Sigma}, T, s^{\Sigma}_{\text{init}}, Q\right\}$ тогда и только тогда, когда существует последовательность $\left\langle \left(q_0, s^{\Sigma}_0\right), \ldots, \left(q_n, s^{\Sigma}_n\right)\right\rangle$, в которой $s^{\Sigma}_0 = s^{\Sigma}_{\text{init}}$, $s^{\Sigma}_n = s^{\Sigma}$, а $s^{\Sigma}_{i+1} = T\left(q_i, s^{\Sigma}_i\right)$, $0 \leqslant i < n$.

Доказательство проблемы безопасности для общего случая выполнено в теории мандатных моделей контроля и управления доступом. Для дискреционных моделей, которых реализовано абсолютное большинство, показано, что проблема в общем случае неразрешима. Однако проведение такого доказательства возможно в частном случае для конкретных систем для каждого состояния путем проверки текущих настроек безопасности системы на соответствие или не соответствие критериям. Таким образом, система Σ, реализующая модель безопасности M, является безопасной в соответствии с набором проверяемых критериев тогда и только тогда, когда выполняются условия:

1) $\forall s^{\Sigma}_i, s^{\Sigma}_{i+1} \in S^{\Sigma} : s^{\Sigma}_{i+1} = T(q, s^{\Sigma}_i)\ \exists s_i, s_{i+1} : s_i = D(s^{\Sigma}_i), s_{i+1} = D(s^{\Sigma}_{i+1}), \forall r \in R : r(s_i, s_{i+1}) =$ ИСТИНА;
2) $\forall c \in C : c\left(D\left(s^{\Sigma}_{\text{init}}\right)\right) =$ ИСТИНА;
3) $\forall s^{\Sigma}_i \in S^{\Sigma}, s^{\Sigma}_i = T\left(q_{i-1}, T\left(\ldots, T\left(q_0, s^{\Sigma}_{\text{init}}\right)\ldots\right)\right)$, $0 \leqslant i < n$: $\exists s_i, s_i = D\left(s^{\Sigma}_i\right), \forall c \in C\ c(s_i) =$ ИСТИНА.

Разрешение проблемы безопасности путем проверки станций в сети, а значит, и решение задачи обеспечения корректного администрирования, невыполнимо вручную, т. к., например, для Windows-сети число комбинаций настроек безопасности исчисляется миллионами. Поэтому авторами разработан автоматизированный инструментарий — система «Декарт», которая помогает справиться с объемом обрабатываемых параметров и множеством проверок для компьютеров под управлением ОС Windows 2000/XP/2003/Vista.

Метод логического моделирования, использованный в системе «Декарт», позволяет добиться простоты практической реализации и проведения автоматического обнаружения уязвимостей, поскольку процедура доказательства безопасности системы задана в терминах логики предикатов. Способ моделирования и анализа посредством логических методов

основан на описании системы и правил ее поведения в виде логических структур. Формальная база метода позволяет получать спецификацию системы и применять аппарат предикативного представления и резолюции для моделирования и анализа ОС.

Рассмотрим использование принципов логического программирования, реализованных в системе «Декарт», при проверке безопасности ОС Windows на примере вычисления реальных прав доступа пользователей к файлу-шаблону MS Word *normal.dot*. В системе «Декарт» состояние системы представляется как конфигурация настроек безопасности (субъектов, объектов и их атрибутов), зафиксированных в некоторый момент времени:

```
object('c:\documents and settings\admin\...\normal.dot',
[type(file),owner(['s-1-5-21-73586283-4847638-8545398-
500']),inheritance(yes)],
[['s-1-5-21-73586283-4847638-8545398-
500',[0,1,2,3,4,5,6,7,8,16,17,18,19,20]],
['s-1-5-18',[0,1,2,3,4,5,6,7,8,16,17,18,19,20]],
['s-1-5-32-544',[0,1,2,3,4,5,6,7,8,16,17,18,19,20]],
['s-1-5-32-545',[0,1]]]).
```

В примере задан предикат описания файла. Предикат инкапсулирует информацию о SID владельца, флаге наследования прав, и собственно о правах доступа, заданных в виде списка в формате «SID-права». Логическое представление используется на этапе проверки критериев обнаружения уязвимостей.

Описание функционирования системы контроля и управления доступом записывается в виде логической программы, в которой правила срабатывания предикатов заданы на множестве логических условий доступа, определяемых системой. Например, контроль чтения файлов выполняется согласно следующей логической функции, определенной на множестве атрибутов безопасности субъектов и объектов:

```
allow_file_read(U, F):-
% Security settings allow user U to traverse through dir of file F.
allow_traverse(U, F),
% EPL is effective permissions list for user U and file F.
effective_permissions(U, F, EPL),
% Get the list of user privileges.
privileges_list(U, PL),
% Privilege Backup is granted to user U.
(member(backup, PL), !;
```

```
% Read data is granted to user U.
member(0, EPL),
% Read attributes is granted to user U.
member(7, EPL); ...).
```

Доступ на чтение файла предоставляется, например, если для пользователя установлено разрешение на чтение или у ему предоставлена привилегия резервного копирования. Таким образом, выполняется замена атрибутов безопасности, определяющих возможность доступа, на множество эквивалентных им эффективных разрешений субъекта.

В общем случае для i-го уровня иерархии атрибутов безопасности множество эффективных разрешений $E_i = f(\text{subject}, E_{i-1}, A_i)$, где $2 \leqslant i \leqslant m$, m — количество уровней иерархии. Функция f вычисляет множество E_i, доступных пользователю или группе subject, на уровне i с учетом влияния атрибута безопасности A_i. Например, для уровня 5, на котором учитываются запреты, E_5 вычисляется следующим образом: $E_5(\text{subject}) = E_4^+(\text{subject})\ \text{XOR}\ E_4^-(\text{subject})$, где E_4^+ — E_4, вычисленный для разрешений, E_4^- — для запретов;

$$E_4(\text{subject}) =$$
$$= E_3(\text{subject})\text{AND}E_3(\{\text{groups}_j\} \mid \forall i\ \text{groups}_j \supset \text{subject}); \ldots; E_1(\text{subject}) =$$
$$= \{\text{bits}_k\},$$

где $\{\text{bits}_k\}$ — множество битов доступа в маске прав дискреционного списка прав доступа данного субъекта. Наличие процедуры вычисления эффективных разрешений позволяет свести задачу проверки критериев к сравнению множеств прав, заданных в системе и в критерии. Жесткость иерархии факторов и взаимооднозначность соответствия «фактор-разрешения» позволяют при несовпадении множеств определить причину нарушения.

Проверяемый критерий представляет собой логическую цель, которая должна быть согласована на множестве настроек безопасности, например:

```
criterion('Criterion #1: Users not allowed to edit Normal.dot', mask,
[object('c:\documents and settings\admin\... \normal.dot'),
check_zone('this_object'),
's-1-5-32-544'(0,1,2,3,4,5,7,8,6,16,17,18,19,20),
's-1-5-18'(0,1,2,3,4,5,7,8,6,16,17,18,19,20)]).
```

Данный предикат описывает критерий, заданный относительно файла *normal.dot*. Тип критерия '*mask*' указывает на то, что это критерий

проверки списка прав доступа. В критерии задано условие безопасности: только субъект *SYSTEM* (S-1-5-18) и группа *Administrators* (S-1-5-32-544) могут иметь полный доступ к файлу. Отклонение от заданного условия считается нарушением. Критерии в системе «Декарт» задаются графически путем заполнения формы критерия элементами состояния и задания параметров проверки. Перед проверкой критерии автоматически формализуются.

Система «Декарт» при проверке критерия вычисляет логическую функцию *Cr*. Ее входными параметрами являются вычисленное множество эффективных прав, имеющихся у субъекта, и множество прав, указанное в критерии. Правило вычисления функции *Cr*, а значит, правило выявления уязвимостей настроек безопасности, можно сформулировать следующим образом: функция *Cr* принимает значение ИСТИНА, если входные множества эквивалентны. В остальных случаях функция *Cr* принимает значение ЛОЖЬ.

Рассмотрим формальный механизм проверки критериев. Пусть R_{all} — множество всех прав доступа, которые может иметь пользователь для объекта некоторого типа. R_{PA} — «необходимые» права, т. е. множество прав доступа, которые должны быть предоставлены пользователю, чтобы система была безопасна. R_{S} — множество эффективных прав, которые системой разрешено иметь пользователю с учетом влияния иерархии атрибутов безопасности, $R_{\text{S}} \subseteq R_{\text{all}}$. R_{excess} — «лишние» права, т. е. множество прав, разрешенных настройками безопасности, но не являющихся «необходимыми» правами. R_{miss} — «недостающие» права, т. е. множество прав, которых недостает пользователю для получения множества прав, разрешенных настройками безопасности. Тогда для критериев можно сформулировать в терминах теории множеств следующее условие безопасности системы:

Условие П. Система безопасна (в соответствии с данным критерием), если множество прав доступа, разрешенных пользователю настройками безопасности R_{S} эквивалентно множеству «необходимых» прав R_{PA}, $R_{\text{S}} = R_{\text{PA}}$.

Для выявления уязвимости необходимо произвести проверки:

Тест П.1. $R_{\text{excess}} = R_{\text{S}} - R_{\text{PA}}$. Если $R_{\text{excess}} \neq \emptyset$, то система уязвима, т. к. текущие настройки разрешают пользователю права доступа, которые ему запрещены.

Тест П.2. $R_{\text{miss}} = R_{\text{PA}} - R_{\text{S}}$. Если $R_{\text{miss}} \neq \emptyset$, то система уязвима, т. к. текущими настройками пользователю запрещены права, которые ему необходимы.

Если при выполнении теста П.1 обнаружено, что множество R_{excess} не является пустым, то система уязвима, т. к. настройки безопасности разрешают пользователю права доступа R_{excess}. Если при выполнении теста П.2 обнаружено, что множество R_{miss} не является пустым, то система уязвима, т. к. настройки безопасности не разрешают пользователю права доступа R_{miss}.

Результатом проверки критерия в системе «Декарт» является отчет, содержащий сведения о выявленном несоответствии настроек, например, в текстовом виде:

SAFETY RESOLUTION CRITERION #1:
Users are not allowed to edit the file
'c:\documents and settings\admin\ . . . \normal.dot'
VIOLATION DETECTED:
Group <Users> has unauthorized rights [Read Data, Write Data]
. . .

Критерий не выполнился, что означает наличие уязвимости в настройках системы. Анализ причин уязвимости, выполняемый системой «Декарт», показывает, что члены группы *Users* могут выполнять чтение и запись.

Система «Декарт» позволяет проводить анализ состояний системы и выявление уязвимостей настроек безопасности с использованием логики предикатов. Множество поддерживаемых логических критериев содержит разнотипные проверки безопасности информационных систем.

Оценка эффективности работы системы обнаружения вторжений с учетом контекста

П. Д. Зегжда, С. С. Корт, А. А. Немчанинов

С ростом пропускной способности сетей, возрастает и трафик передаваемой информации по каналам связи, а значит, увеличивается и нагрузка на системы обнаружения вторжений (СОВ). Увеличение количества DoS-атак лишний раз указывает на данную проблему. В результате возникает необходимость в оптимизации СОВ для повышения эффективности анализа возросшего объема трафика. Одним из способов повышения эффективности работы СОВ, основанной на сигнатурном анализе, является уменьшение количества анализируемых правил без увеличения ошибок первого рода.

В рассматриваемом подходе защищаемый хост (станция) представлен операционной системой (ОС) и функционирующими сервисами. Назовем контекстом защищаемой станции информацию об объектах защищаемой станции. Контекстом будет являться элемент из следующего упорядоченного множества:

$$\left\{K^{\text{none}}, K^{\text{name}(1)}, \ldots, K^{\text{name}(T)}, K^{\text{ver}}\right\},$$

на котором определенно следующее отношение порядка:

$$K^{\text{none}} \subset K^{\text{name}(1)} \subset \ldots \subset K^{\text{name}(T)} \subset K^{\text{ver}},$$

где K^{none} — отсутствие информации о защищаемом объекте;

$\left.\begin{matrix} K^{\text{name}(1)} \\ \cdots \\ K^{\text{name}(T)} \end{matrix}\right\}$ — известно имя защищаемого объекта;

K^{ver} — известно имя и версия защищаемого объекта.

$K^{\text{name}(1)}, \ldots, K^{\text{name}(T)}$ — это так называемая *родовая цепочка*. То есть $K^{\text{name}(1)}$ является родительским для всех последующих элементов $K^{\text{name}(1)}$, $1 < t \leqslant T$.

Таким образом, получается два упорядоченных множества:

$\left\{K_{\text{OS}}^{\text{none}}, K_{\text{OS}}^{\text{name}(1)}, \ldots, K_{\text{OS}}^{\text{name}(W)}, K_{\text{OS}}^{\text{ver}}\right\} = A$ — упорядоченное множество контекста ОС;

$\left\{K_{\text{SRV}}^{\text{none}}, K_{\text{SRV}}^{\text{name(1)}}, \ldots, K_{\text{SRV}}^{\text{name}(V)}, K_{\text{SRV}}^{\text{ver}}\right\} = B$ — упорядоченное множество контекста сервисов.

Создадим на эти двух множествах A и B новое множество C по следующему правилу: $c = (a, b) \in C$, $\forall a \in A$, $\forall b \in B$. Полученное множество будет частично упорядоченно по следующему правилу:

$$\left.\begin{array}{l} c_1 = (a_1, b_1) \\ c_2 = (a_2, b_2) \\ c_1 \subset c_2 \end{array}\right\} \Leftrightarrow \left[\begin{array}{l} a_1 = a_2,\ b_1 \subset b_2 \\ b_1 = b_2,\ a_1 \subset a_2 \end{array}\right.$$

Причем в этом множестве у каждого элемента будет как точная верхняя грань ($K_{\text{OS}}^{\text{ver}}$, $K_{\text{SRV}}^{\text{ver}}$), так и точная нижняя грань ($K_{\text{OS}}^{\text{none}}$, $K_{\text{SRV}}^{\text{none}}$).

Таким образом, контекст описывается решеткой. Тогда можно определить контекст о защищаемой станции с одной службой как элемент математической решетки:

$$I = (K_{\text{OS}}, K_{\text{SRV}}). \tag{1}$$

Данная решетка имеет нижний элемент (точная нижнюю грань, $I_\perp$), который обозначает отсутствие информации о защищаемой станции. Верхний элемент (точная верхняя грань, $I_\perp$) означает наличие информации не только о названии ОС и службы, но и об их версиях.

Тогда, для защищаемой станции с несколькими службами контекст будет иметь вид:

$$\text{Comp} = \left(K_{\text{OS}}, \bigcup_{i=1}^{n} K_{\text{SRV}_i}\right), \tag{2}$$

где n — количество служб, функционирующих на защищаемой станции.

Информация о сегменте сети, защищаемом датчиком сигнатур, примет следующий вид:

$$\text{Net} = \bigcup_{j=1}^{m} \text{Comp}_j = \bigcup_{j=1}^{m} \left(K_{\text{OS}_j}, \bigcup_{i=1}^{n_j} K_{\text{SRV}_i}^{(j)}\right), \tag{3}$$

где m — количество защищаемых хостов в сегменте сети, n_j — количество сервисов на j-ом защищаемом хосте, а $K_{\text{SRV}_i}^{(j)}$ — контекст i-го сервиса на j-й защищаемой станции.

В современных СОА сигнатура атаки описывает признак атаки без учета контекста. Для оценки эффективности работы датчика сигнатур с учетом контекста введем функцию соответствия контекста защищаемой станции и необходимым множеством сигнатур, которая должна использовать СОА для нормального функционирования (без повышения количества ошибок первого рода):

$$f(K_{\text{OS}}, K_{\text{SRV}}) = \{\text{sig}\}_{k=1}^{L}, \tag{4}$$

где $\{\text{sig}\}_{k=1}^{L}$ — множество сигнатур, количество которых в этом множестве равно L.

Функция в зависимости от контекста об ОС и контекста о сервисах позволяет определить множество сигнатур СОА без повышения количества ошибки первого рода. В дальнейшем запись количества сигнатур может иметь следующий вид:

- $L(i)$ — количество сигнатур для i-й службы одного защищаемого хоста, $1 \leqslant i \leqslant n$;
- $L(N)$ — количество всех сигнатур для защищаемого хоста, $L(N) = \sum_{i=1}^{n} L(i)$;
- $L(j, i)$ — количество сигнатур для i-й службы на j-ом защищаемом хосте, $1 \leqslant i \leqslant n_j$, $1 \leqslant j \leqslant m$;
- $L(j, N_j)$ — количество всех сигнатур для j-ого защищаемого хоста, $L(j, N_j) = \sum_{i=1}^{n_j} L(i)$, $1 \leqslant j \leqslant m$;
- $L(M, N_M)$ — количество всех сигнатур для всех защищаемых хостов.

Обозначим через $\{\text{sig}\}_{k=1}^{\text{ALL}}$ множество всевозможных сигнатур СОА.

За количественную оценку работы датчика сигнатуры можно принять мощность этого множества:

$$\left|\{\text{sig}\}_{k=1}^{L}\right| = L, \tag{5}$$

$$\left|\{\text{sig}\}_{k=1}^{\text{ALL}}\right| = \text{ALL}. \tag{6}$$

Таким образом, контекст об ОС и контекст о сервисах определяют мощность используемого множества сигнатур, а значит, и позволяют оценить эффективность работы СОА.

Спроецируем данные вычисления на защищаемую станцию с несколькими сервисами:

$$f(\text{Comp}) = \{\text{sig}\}_{k=1}^{L(N)}. \tag{7}$$

Мощность этого множества равна:

$$\left|\{\text{sig}\}_{k=1}^{L(N)}\right| = L(N), \tag{8}$$

т. е. сумме мощностей множеств сигнатур для каждой службы.

Так как возможно наличие одинаковых сигнатур в $\{\text{sig}\}_{k=1}^{L(1)}$, $\{\text{sig}\}_{k=1}^{L(2)}$, … … …, $\{\text{sig}\}_{k=1}^{L(n)}$, то

$$L(N) < L_1 + L_2 + \ldots + L_n. \tag{9}$$

Для сегмента сети получаем: $f(\mathrm{Net}) = \{\mathrm{sig}\}_{k=1}^{L(M,N_M)}$, мощность которого равна:

$$\left|\{\mathrm{sig}\}_{k=1}^{L(M,N_M)}\right| = L(M,\, N_M) < \left|\{\mathrm{sig}\}_{k=1}^{L(1,N_1)}\right| + \left|\{\mathrm{sig}\}_{k=1}^{L(2,N_2)}\right| + \ldots + \left|\{\mathrm{sig}\}_{k=1}^{L(m,N_m)}\right|. \quad (10)$$

Обозначим через $\{\mathrm{sig}\}_{k=1}^{\mathrm{cur}}$ множество сигнатур СОА, необходимых для работы без повышения количества ошибок первого рода.

В результате эффективность работы датчика сигнатур по количеству правил можно определить как:

$$\frac{\left|\{\mathrm{sig}\}_{k=1}^{\mathrm{ALL}}\right| - \left|\{\mathrm{sig}\}_{k=1}^{\mathrm{cur}}\right|}{\left|\{\mathrm{sig}\}_{k=1}^{\mathrm{ALL}}\right|}. \quad (11)$$

А эффективность работы датчика сигнатур по времени определяется следующей формулой:

$$\frac{\left|T^{\mathrm{ALL}}\right| - \left|T^{\mathrm{cur}}\right|}{\left|T^{\mathrm{ALL}}\right|}, \quad (12)$$

где T^{ALL} — время работы со всеми правилами СОА, а T^{cur} — время работы с необходимыми правилами в зависимости от контекста.

Таким образом, чем меньше мощность множества сигнатур необходимых для датчика сигнатур, тем эффективнее работа СОА без повышения количества ошибок первого рода.

В заключении следует отметить, что подход, предложенный в данной работе, может быть применен для любой системы, основанной на сигнатурном анализе.

О разработке моделей безопасности информационных потоков в компьютерных системах с ролевым управлением доступом

П. Н. Девянин

Ролевое управление доступом (РУД) [8, 5, 2] является современным, эффективным механизмом защиты компьютерных систем (КС), особенно систем управления базами данных (СУБД). С использованием иерархии ролей возможно обеспечение управления доступом, точно соответствующего должностным обязанностям пользователей КС. При этом используемые в РУД механизмы статических и динамических ограничений позволяют реализовать на основе РУД дискреционное или мандатное управление доступом.

В известной автору литературе основное внимание при исследовании РУД, как правило, уделяется вопросам администрирования РУД или разработке моделей РУД, адаптированных к условиям функционирования конкретных существующих КС. Анализу безопасности информационных потоков, возникающих в результате реализации субъектами (субъектами-сессиями) доступов к сущностям, уделяется недостаточно внимания. Кроме того, основные модели РУД не содержат описания правил перехода КС из состояния в состояние. В то же время результаты проведенных на практике экспериментов показали, что нарушитель, используя часто разрешенные политикой безопасности КС доступы к сущностям, может эффективно реализовать запрещенные информационные потоки по памяти или по времени. При этом отсутствие четких правил перехода КС из состояния в состояние может привести к разработке и использованию для анализа безопасности КС неадекватных ей формальных моделей.

Следовательно, целесообразно создание семейства новых моделей РУД, соответствующих условиям функционирования современных КС и обеспечивающих возможность эффективного анализа безопасности информационных потоков. Так как модели семейства ориентированы на анализ КС с РУД, то в них следует использовать элементы основных моделей РУД, в том числе базовой ролевой модели, модели ролевого администрирования, модели мандатного ролевого управления доступом.

Кроме того, целесообразно при разработке моделей РУД взять за основу апробированное на практике семейство моделей управления доступом и информационными потоками (сокращенно, ДП-моделей) [1] КС с дискреционным или мандатным управлением доступом, которое было создано с применением положений классической модели *Take-Grant* и ее основных расширений [5], модели Белла—ЛаПадулы [4] и ее интерпретаций [7], субъектно-ориентированной модели изолированной программной среды [3] и модели систем военных сообщений [6].

В семейство моделей КС с РУД (или, сокращенно, ролевых ДП-моделей) следует включить следующие основные элементы: множество сущностей (E), множество пользователей (U), множество субъектов-сессий пользователей (S), множество доверенных (L_S) и недоверенных (N_S) субъектов-сессий, множество ролей (R).

Для анализа условий передачи прав доступа и реализации информационных потоков предполагается использовать:

$$R_r = \{\text{read}_r, \text{write}_r, \text{append}_r, \text{execute}_r, \text{own}_r\}$$

— множество видов прав доступа, при этом право доступа own_r к сущности позволяет включать во множество прав доступа любой роли любые права доступа к данной сущности, $R_a = \{\text{read}_a, \text{write}_a, \text{append}_a, \text{own}_a\}$ — множество видов доступа, при этом own_a — доступ владения к субъекту-сессии, $R_f = \{\text{write}_m, \text{write}_t\}$ — множество видов информационных потоков.

В отличие от дискреционных ДП-моделей, в рамках ролевой ДП-модели наличие у субъекта-сессии роли, обладающей правом доступа own_r к сущности, позволяет субъекту-сессии передавать другим ролям любые права доступа к данной сущности.

Доступом own_a может обладать только субъект-сессия к другому субъекту-сессии. Наличие доступа own_a у первого субъекта-сессии означает, что он владеет вторым субъектом-сессией (например, в случае, когда первый субъект-сессия получил контроль над вторым субъектом-сессией).

По аналогии с моделями РУД [8] предлагается использовать обозначения и определения для следующих элементов ролевых ДП-моделей: $P \subset E \times R_r$ — множества прав доступа к сущностям, $\text{UA}: U \to 2^R$ — функции авторизованных ролей пользователей, задающей для каждого пользователя множество ролей, на которые он может быть авторизован, $\text{PA}: R \to 2^P$ — функции прав доступа ролей, $\text{user}: S \to U$ — функции принадлежности субъекта-сессии пользователю, $\text{roles}: S \to 2^R$ — функции текущих ролей субъектов-сессий, $H_E: E \to 2^E$ — функции иерархии сущностей, $H_R: R \to 2^R$ — функции иерархии ролей.

Для задания используемых в КС с РУД статических и динамических ограничений в ролевых ДП-моделях используем следующие элементы: множество всех функций авторизованных ролей пользователей (UA^*), множество всех функций прав доступа ролей (PA^*), множество всех функций текущих ролей субъектов-сессий roles^*, $C^U: \text{UA}^* \to \{\text{true, false}\}$ функцию, задающую статическое ограничение на значения множеств авторизованных ролей пользователей, $C^P: \text{PA}^* \to \{\text{true, false}\}$ — функцию, задающую статическое ограничение на значения множеств прав доступа ролей, $C^S: \text{roles}^* \to \{\text{true, false}\}$ — функцию, задающую динамическое ограничение на значения множеств текущих ролей субъектов-сессий.

Таким образом, можно задать элементы аналогичные описанным в рамках моделей РУД и семейства ДП-моделей КС с дискреционным или мандатным управлением доступом, которые целесообразно использовать в семействе новых ролевых ДП-моделей, и с применением которых можно дать определения состояния системы и системы в целом.

Определение 18. Пусть определены: множества U, E, S, P, L_S, множества доступов субъектов-сессий к сущностям $A \subseteq S \times E \times R_a$ и информационных потоков $F \subseteq E \times E \times R_f$, функции UA, PA, user, roles, H_R, H_E, множества функций, задающих статические ограничения на значения множеств авторизованных ролей пользователей, $\text{Constraint}_U = \{C_1^U, \ldots, C_{nU}^U\}$, где $n_U \geqslant 0$, функций, задающих статические ограничения на значения множеств прав доступа ролей,

$$\text{Constraint}_P = \{C_1^P, \ldots, C_{nP}^P\},$$

где $n_P \geqslant 0$, функций, задающих динамические ограничения на значения множеств текущих ролей субъектов-сессий, $\text{Constraint}_S = \{C_1^S, \ldots, C_{nS}^S\}$, где $n_S \geqslant 0$. Определим

$$G = (\text{UA, PA, user, roles, } A, F, H_R, H_E = \text{Constraint}_U, \text{Constraint}_P, \text{Constraint}_S, L_S)$$

— состояние системы.

Определение 19. Пусть $\Sigma(G^*, \text{OP})$ — система, при этом G^* — множество всех возможных состояний системы, OP — множество правил преобразования состояний системы.

Рассмотрим предположения, которые целесообразно сделать при описании множества правил, задающих порядок перехода системы из состояния в состояние на траекториях ее функционирования.

Ролевые ДП-модели предназначены для анализа условий реализации в КС с РУД информационных потоков и в их рамках не предполагается исследовать вопросы администрирования множества ролей, иерархии

ролей, множеств авторизованных ролей пользователей, параметров ограничений. При этом создание (удаление) сущности требует реализации в правилах преобразования состояний механизма каскадного добавления (удаления) прав доступа к сущностям во множества прав доступа ролей с учетом их иерархии.

В ДП-моделях КС с дискреционным или мандатным управлением доступом предполагалось, что все субъекты сессии могут быть либо доверенными, либо недоверенными, причем доверенные субъекты не могли участвовать в реализации информационных потоков по времени. В современных СУБД, в которых, как правило, реализуется РУД, недоверенные субъекты-сессии при доступе к записям баз данных могут инициировать выполнение доверенных субъектов-триггеров, которые потенциально могут реализовывать информационные потоки по времени. Следовательно, вопрос о невозможности участия доверенных субъектов при реализации информационных потоков по времени требует дополнительного исследования.

В ролевых ДП-моделях функционально ассоциированными с субъектом-сессией являются сущности, от которых зависит вид преобразования данных, реализуемого субъектом-сессией. При этом только информационный поток по памяти к сущности, функционально ассоциированной с субъектом-сессией, приводит к изменению вида преобразования данных, реализуемого этим субъектом-сессией.

В КС с РУД право доступа к сущности может быть получено субъектом-сессией только через обладание ролью, содержащей данное право. Реализация субъектом-сессией s_1 информационного потока по памяти на сущность, функционально ассоциированную с субъектом-сессией s_2, позволит s_1 получить контроль над s_2, включая возможность использовать права доступа ролей, которыми обладает s_2. При этом множество текущих ролей s_1, как правило, останется неизменным. Кроме того, в современных КС часто для изменения субъектом-сессией множества своих текущих ролей требуется ввод аутентификационных данных пользователем, от имени которого функционирует субъект-сессия. Таким образом, если субъект-сессия s_1 реализовал информационный поток по памяти от себя к сущности, функционально ассоциированной с другим субъектом-сессией s_2, то s_1 получает доступ владения к s_2 и возможность использовать роли из его множества текущих ролей.

Существенную трудность при описании правил преобразования состояний может составить решение задачи корректного использования статических и, особенно, динамических ограничений. Например, в ДП-моделях КС с дискреционным управлением доступом наличие у субъекта права доступа к сущности всегда позволяло получить к ней доступ, вне

зависимости от уже имеющих у этого или других субъектов доступов. В КС с РУД динамические ограничения взаимного исключения ролей могут препятствовать пользователю в рамках одной сессии реализовать информационный поток между двумя сущностями путем получения к ним доступа, так как может оказаться, что правами доступа к этим сущностям обладают две взаимоисключающие друг друга роли. При этом остается открытым вопрос о возможности алгоритмической проверки безопасности системы путем сведения ее к монотонной системе, по аналогии с тем как данная задача решается в большинстве известных формальных моделях (например, в модели *Take-Grant* или ДП-моделях).

Таким образом, при описании правил преобразования состояний в ролевых ДП-моделях целесообразно использовать правила ДП-моделей КС с дискреционным и мандатным управлением доступом, модифицировав и пополнив их правилами, в которых реализуются механизмы статических и динамических ограничений, каскадного добавления (удаления) прав доступа и учитываются особенности реализации доверенных и недоверенных субъектов-сессий в КС с РУД.

Формальные ролевые ДП-модели могут быть использованы для анализа безопасности управления доступом и информационными потоками в современных и перспективных КС с РУД, а также КС с дискреционным или мандатным 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, № 3. P. 198—222.

[7] *McLean J.* The Specification and Modeling of Computer Security // Computer. 1990. Vol. 23, № 1.

[8] *Sandhu R.* Role-Based Access Control // Advanced in Computers. Academic Press. 1998. Vol. 46.

Моделирование кооперативных механизмов защиты компьютерных сетей

А. В. Уланов, И. В. Котенко

1. Введение

Одна из наиболее критичных компьютерных атак — атака «распределенный отказ в обслуживании» (Distributed Denial of Service — DDoS) [1, 2]. Перспективная система защиты от атак, и, в том числе DDoS, должна функционировать за счет кооперации разнообразных системных, сетевых и глобальных механизмов защиты, осуществляемых как в рамках конкретной корпоративной сети, так и в масштабах всей сети Интернет [1].

К распределенным кооперативным механизмам защиты от атак DDoS можно отнести [1], например, механизмы, реализующие защиту с помощью переноса ресурсов (Server Roaming), изменения количества ресурсов, разграничения ресурсов (Market-based Service Quality Differentiation (MbSQD), Transport-aware IP router architecture (tIP)), аутентификации (tIP, Secure Overlay Services (SOS)), а также механизмы, выполняющие отслеживание с разметкой пакетов и хранением их сигнатур, в том числе осуществляющие «отталкивание», генерацию служебных пакетов и др (ACC pushback, COSSACK, Perimeter-based DDoS defense, DefCOM, Gateway-based).

В отличие от предыдущих работ авторов, например [2], в которых был представлен общий подход к многоагентному моделированию, разрабатываемая среда моделирования и некоторые примеры экспериментов, в данной работе рассматриваются особенности моделирования распределенных кооперативных механизмов защиты и представляются различные эксперименты по исследованию кооперативных механизмов защиты.

Работа выполнена при финансовой поддержке РФФИ (проект № 07-01-00547), программы фундаментальных исследований ОИТВС РАН (контракт № 3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза POSITIF (контракт IST-2002-002314) и RE-TRUST (контракт № 021186-2).

2. Особенности моделирования

Предлагаемый подход к моделированию предполагает, что кибернетическое противоборство представляется в виде взаимодействия как минимум двух команд программных агентов [2]: команды агентов-злоумышленников по реализации атак DDoS и команды агентов защиты. Они воздействуют друг на друга и на среду, являющейся моделью Интернета. Структуризация знаний агентов представлена в виде частных онтологий предметной области. Их поведения описывается сценариями, а взаимодействие происходит по протоколам.

Модель команды атаки включает два класса агентов [2]: «демоны», непосредственно реализующие атаку, и «мастер», выполняющий действия по координации остальных компонентов системы. Команда атаки использует следующие протоколы: протокол составления команды; протокол проверки работоспособности; протокол рассылки параметров атаки; протокол атаки. Используются следующие классы агентов защиты [2]: первичной обработки информации («сэмплеры»), обнаружения атаки («детекторы»); фильтрации («фильтры»); ограничения трафика («ограничители»); агенты расследования. Команда защиты использует следующие протоколы: протокол составления команды; протокол сбора информации у сэмплеров; протокол рассылки адресов возможных источников атаки; протокол обезвреживания агентов атаки.

Кооперативное взаимодействие происходит между командами, преследующими общую цель по защите сети: команды защиты обмениваются информацией для повышения эффективности противодействия атаке. В данной работе исследуются модели кооперативных механизмов защиты DefCOM, COSSACK и предлагается ряд новых. В соответствии с архитектурой системы DefCOM вводятся следующие классы агентов: «Alert generator» — обнаруживает атаку и сообщает о ней остальным узлам сети; атака регистрируется, если трафик превышает допустимый предел; «Rate limiter» — ограничивает объем трафика, направляемого на цель атаки; «Classifier» — обеспечивает выборочное ограничение объема трафика, пытается определить и отбросить пакеты атаки. «Alert generator» строится на базе детектора и сэмплера, «Rate limiter» задается агентом «ограничитель», «Classifier» представляет собой агента «фильтр», получающего данные по фильтрации от детектора.

Система COSSACK состоит из следующих классов агентов: «snort» — составляет статистику по количеству переданных пакетов для различных потоков трафика; потоки группируются по префиксам адреса. Если для какого-то потока происходит превышение заданного порога, то его сигнатура передается к агенту «watchdog». Последний получает

данные по трафику от агента «snort» и применяет правила фильтрации на маршрутизаторах. Агент «snort» строится на базе агента «сэмплер», а агент «watchdog» агента «детектор». На основе данных от «snort» агент «watchdog» принимает решение о наступлении атаки. Для имитации фильтра на маршрутизаторе используется агент «фильтр». Для моделирования кооперации агентов «watchdog» применяется кооперация «детекторов», которые могут передавать правила фильтрации друг другу, используя для этого агентов «фильтр», установленных на маршрутизаторы.

В предлагаемом подходе к кооперации используются следующие четыре класса агентов команд защиты: обработки информации («сэмплеры»), обнаружения атаки («детекторы»), фильтрации («фильтры») и «агенты расследования». Команды агентов защиты могут взаимодействовать по различным схемам кооперации: (1) без кооперации: все команды агентов работают сами по себе; (2) кооперация на уровне фильтров: команда, на сеть которой направлена атака, может применять правила фильтрации на фильтрах других команд; (3) кооперация на уровне сэмплеров: команда, на сеть которой направлена атака, может получать информацию о трафике от сэмплеров других команд; (4) слабая кооперация: команды могут получать информацию о трафике от сэмплеров некоторых других команд и применять правила фильтрации на фильтрах также некоторых других команд. В зависимости от степени кооперации каждой команде задается то или иное количество «известных» ей команд; (5) полная кооперация: команда, на сеть которой направлена атака, может получать информацию о трафике от всех сэмплеров других команд и применять правила фильтрации на всех фильтрах других команд.

3. Среда моделирования и эксперименты

Для проведения моделирования кооперативных механизмов защиты используется разработанная на основе представленного подхода четырехуровневая среда моделирования [2]. Она состоит из следующих компонентов: базовая система имитационного моделирования; модуль моделирования сети Интернет; подсистема многоагентного моделирования и библиотека имитации процессов предметной области. Среда разработана на основе OMNeT++ INET Framework и предназначена для многоагентного моделирования распределенных атак и механизмов защиты от них. Для проведения эксперимента необходимо специфицировать следующие компоненты: топология сети, параметры клиентов, команда атаки, параметры атаки, команда защиты, параметры защиты, параметры кооперации, схема адаптации.

Эксперименты по исследованию кооперативных моделей включают схемы DefCOM, COSSACK, «без кооперации», «на уровне фильтров», «на уровне сэмплеров» и «полная кооперация».

Кооперативные методы COSSACK или DefCOM применяют собственные методы обнаружения атак. В работе для исследования различных кооперативных методов защиты предлагается использовать одинаковые методы обнаружения атаки, например, Hop counts Filtering (HCF), Source IP address monitoring (SIPM), Bit Per Second (BPS) [1, 2] 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. Использование одних и тех же методов обнаружения позволяет исследовать различные кооперативные механизмы в одинаковых условиях. Сравниваемые методы реализуются на одинаковых сетях с учетом требований к расположению их компонентов.

Задаются следующие входные параметры. Топология опорной сети: минимальное количество связей у каждого узла — 2, количество узлов — 10, параметр вероятностного распределения $z = 2.25$, 10 клиентов подключены случайным образом к маршрутизаторам опорной сети, задан защищаемый сервер и параметры осуществления запросов к нему клиентов. Маршрутизаторы опорной сети соединены между собой волоконно-оптическими каналами связи (OC-48) со следующими параметрами: задержка распространения сигнала — 1 мс; скорость передачи данных — 2488 Мбит. Остальные узлы соединены каналами связи Ethernet (задержка распространения сигнала — 0.1 мс; скорость передачи данных — 100 Мбит).

В команду атаки входят 10 демонов, реализующих атаку UDP flood на сервер. Команды защиты сконфигурированы в соответствии с указанными кооперативными схемами. Исследуемыми выходными параметрами являются: величина входного трафика до и после фильтра команды, чья сеть под атакой; процент ложных срабатываний и пропусков атак команды, чья сеть под атакой.

На рис. 1 изображены графики объема трафика внутри (вторая линия сверху) и на входе (остальные линии) в атакуемую подсеть для схем кооперации DefCOM, COSSACK и «полная кооперация». Атака начинается на отметке 300 секунд. Применяется подмена адреса на случайный из той же подсети (как наиболее сложная для определения атакующих). Для защиты используется метод SIPM. Рисунок для DefCOM содержит четыре графика трафика, так как трафик измерялся на входе в подсеть. Там расположен маршрутизатор, имеющий 4 интерфейса.

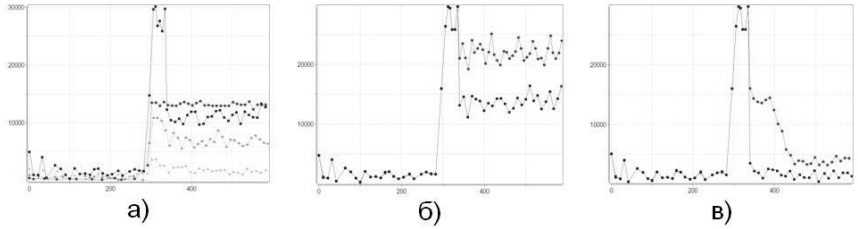


Рис. 1. Объем трафика для DefCOM (а), COSSACK (б) и полной схемы кооперации (в)

Проведенные эксперименты показали, что лучшая кооперативная схема — с полной кооперацией. Решающую роль в защите от атаки сыграла кооперация сэмплеров, благодаря чему осуществлялся постоянный обмен данными по трафику в различных командах защиты. Схема DefCOM показывает стабильное сдерживание трафика атаки за счет ограничителя на входе в защищаемую подсеть и классификаторов в исходной подсети. Схема COSSACK характеризуется схожим уровнем трафика в защищаемой подсети, однако во внешней ее части трафик атаки остается достаточно высок.

4. Заключение

В работе предложен подход к моделированию распределенных кооперативных механизмов защиты от компьютерных атак. Подход заключается в представлении стороны защиты в виде кооперирующихся команд агентов защиты, которые противостоят команде реализации атаки. Подход был применен для моделирования нескольких кооперативных механизмов защиты от DDoS атак. Были разработаны модели механизмов DefCOM, COSSACK и предложены новые модели кооперации команд защиты.

В разработанной на основе предложенного подхода среде многоагентного моделирования распределенных атак и механизмов защиты от них были проведены эксперименты по сравнению их эффективности. На основе величины трафика в защищаемой подсети наиболее эффективной признана схема с полной кооперацией.

В дальнейшем планируется более расширение моделей кооперативных механизмов защиты, совершенствование среды моделирования и проведения экспериментов по исследованию адаптивных кооперативных схем защиты.

Литература

[1] *Уланов А. В.*, *Котенко И. В.* Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. Инсайд, № 1—3, 2007.

[2] *Котенко И. В.*, *Уланов А. В.* Противостояние в Интернет: моделирование противодействия распределенным кибератакам // Пятая Общероссийская конференция «Математика и безопасность информационных технологий» (МаБИТ-06). М.: МГУ, 2006.

Логико-динамические аспекты моделирования процессов контентной фильтрации прикладных протоколов

В. С. Заборовский, А. В. Силиненко

1. Введение

При решении многих задач защиты информации компьютерную сеть можно рассматривать как сложную логико-динамическую систему, для характеризации свойств которой используются различные средства моделирования. Так, совокупность виртуальных соединений может рассматриваться как система массового обслуживания пакетов, управляемых протоколом IP. С другой стороны, описание трафика на уровне транспортных соединений опирается на модели, характеризующие динамические свойства протокола TCP, функционирующего в среде с ярко выраженными стохастическими или даже хаотическими свойствами. Широкий класс задач защиты информации может моделироваться с использованием методов предикатного или сигнатурного задания правил фильтрации на допустимых множествах сетевых индикаторов и/или латентов. Уточним, что в этих задачах индикаторами являются параметры трафика, непосредственно доступные для прямых измерений, например заголовки пакетов, а латентами — скрытные переменные или их совокупности, для определения числовых характеристик которых используются различные алгоритмы и/или характеристические функции. Целью работы является исследование логико-динамических аспектов моделирования процессов контентной фильтрацией трафика, порождаемого различными прикладными протоколами. Исследование основывается на модели TCP соединения, используемого для организации виртуальных соединений. При этом фильтрация рассматривается как двухэтапный процесс идентификации контентных признаков, в котором на первом этапе выделяются последовательности пакетов, принадлежащие отдельным TCP сессиям, а на втором определяется набор данных, подлежащих контролю, для чего используется механизм сигнатурного анализа в области данных, ограниченных рамками выделенной TCP сессии. Работа состоит из трех разделов.

В первом разделе рассматриваются особенности моделирования сетевых процессов, связанные с динамическими свойствами TCP протокола и вероятностным характером среды передачи пакетов. Во втором разделе анализируются возможности реализации процессов контентной фильтрации при решении задачи информационной безопасности. В третьем разделе проводится формализация задачи контентной фильтрации сетевых приложений, в рамках введенной алгебры правил фильтрации.

2. Модель TCP сессии

TCP соединение как объект моделирования характеризуется параметрами и индикаторами — пропускная способность, размер входного и выходного буфера, окно перегрузки, окно приемника, размер порога медленного старта, RTT, номера последовательности и подтверждения, номера портов, размеры сегментов и др. В качестве латентных признаков или латентов рассматривается дисперсия пропускной способности, корреляционные и спектральные характеристики трафика, свойства персистентности (параметр Херста) и др.

TCP обеспечивает гарантированную доставку данных за счет механизма повторной передачи потерянных пакетов и устранения дублирования пакетов при получении нескольких копий. В каждый дискретный момент времени поток TCP сегментов, которые обозначим переменной y_k, изменяется согласно принятым спецификациям (1) протокола и значению индикаторной функции $\psi(\xi)$. Значение этой функции выбирается из множества $\{0, 1\}$ в зависимости от того, произошло ли событие, связанное с потерей или повторной передачей пакета.

$$y_{k+1} = \begin{cases} y_k + 1, & \text{если } \psi(\xi) = 0; \\ y_k/2, & \text{если } \psi(\xi) = 1. \end{cases} \tag{1}$$

В (1) $\psi(\xi)$ — индикаторная функция, ξ — стохастическая переменная момента перегрузки, имеющая равномерное распределение на интервале текущего динамического диапазона изменения окна перегрузки.

Модель (1) позволяет определить статистики, характеризующие свойства TCP сессии на различных интервалах наблюдения, например:

$$\begin{aligned} M_1(\tau_{10}) &= \int_0^T \frac{\partial\tau_1}{T} \int_{-\infty}^{\infty} \tau\delta(\tau - \tau_{10})\,\partial\tau; \\ D(\tau_{10}) &= M_2(\tau_{10}) - M_1^2(\tau_{10}); \\ M_1(\tau_{20}) &= \int_0^T \frac{\partial\tau_1}{T} \int_{\tau_1}^{\tau_{10}} \frac{\partial\tau_2}{\tau_{10} - \tau_1} \int_{-\infty}^{\infty} \tau\delta(\tau - \tau_{20})\,\partial\tau; \end{aligned} \tag{2}$$

$$D(\tau_{20}) = M_2(\tau_{20}) - M_1^2(\tau_{20});$$
$$M_1(\tau_{30}) = \int_0^T \frac{\partial\tau_1}{T} \int_{\tau_1}^{\tau_{10}} \frac{\partial\tau_2}{\tau_{10}-\tau_1} \int_{\tau_2}^{\tau_{20}} \frac{\partial\tau_3}{\tau_{20}-\tau_2} \int_{-\infty}^{\infty} \tau\delta(\tau-\tau_{30})\,\partial\tau;$$
$$D(\tau_{30}) = M_2(\tau_{30}) - M_1^2(\tau_{30}).$$

Эти статистики позволяют получить выражение для дисперсии потока пакетов, что важно для решения задачи прогнозирования пропускной способности:

$$D(t) = K(t-64)^{1+\alpha}, \quad \text{где } K = 1{,}17,\ \alpha = 0{,}82.$$

Характер этой зависимости говорит о положительной персистентности или фрактальности процессов, что подтверждается данными реальных измерений трафика для различных приложений и режимов работы сети.

3. Анализ возможности реализации контентной фильтрации

Рассматривая персистентность как характеристику устойчивости состояния TCP соединения, сформулируем задачу контентной фильтрацией пакетов, порождаемых различными прикладными протоколами как задачу определения множества латентов, к которым относятся различные параметры TCP сессии, среди которых имеется и такие параметры, точная структура которых неизвестна. Для моделировании процесса контентной фильтрации с использованием межсетевого экрана (МЭ) будем учитывать контекст TCP-соединения, отражающий состояния, в котором находится конкретное виртуальное соединение. При этом будем опираться на автоматную модель TCP-соединения, позволяющую описать последовательности смены состояний TCP-соединения в результате прохождения пакетов через МЭ. В данной модели предлагается расширенное описание состояния ESTABLISHED (соединение установлено), что позволяет учесть особенности функционирования прикладных протоколов, использующих TCP как протокол транспортного уровня (рис. 1).

Для формирования алгоритмов контентной фильтрации на базе автоматной модели TCP соединения требуется согласованное решение следующих задач:

- формализация алгоритмов контентной фильтрации;
- параметризация требований политики безопасности;
- синтез модели безопасности и требований к МЭ с использованием средств описания правил фильтрации прикладных протоколов.

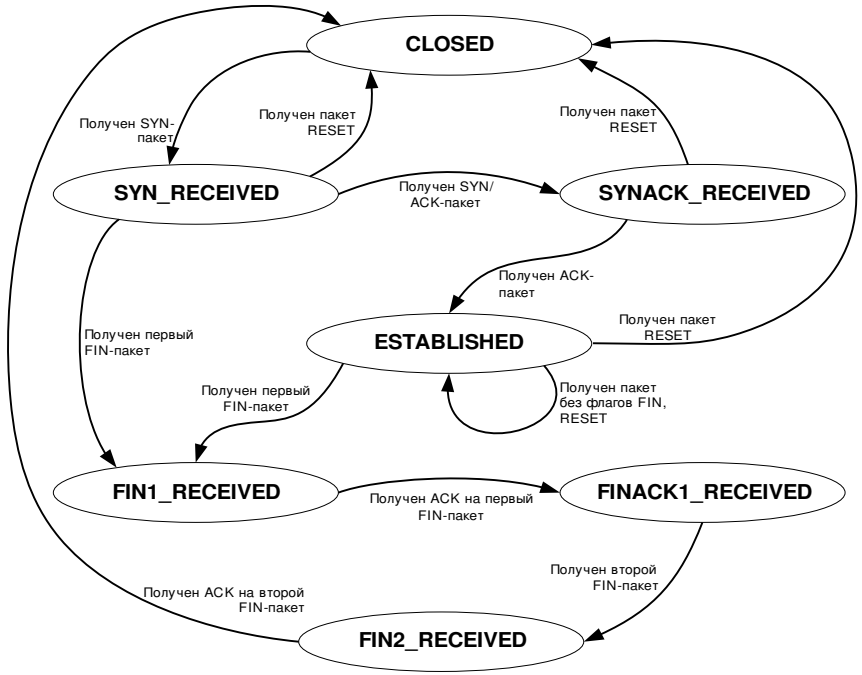


Рис. 1. Модель соединений TCP соединения

4. Формализация методов описания правил фильтрации

Повысить эффективность синтеза средств защиты информации на базе МЭ предлагается на основе формализации используемых понятий, введения новых абстракций и формирования алгебры правил фильтрации. Для этого введем следующее описание: $\mathbf{R} = \langle R, \Sigma\rangle$, где $R = \{R_1, R_2, \ldots R_n\}$ — множество правил фильтрации, несущее множеств алгебры $\mathbf{R}$, $R_i = \{x_{i1}, x_{i2}, \ldots, x_{ik}, a_{i1}, a_{i2}, \ldots, a_{im}\}$ — правило фильтрации, состоящее из параметров $\{x_i\}$ и атрибутов $\{a_i\}$ $(i = 1, \ldots, n)$, $\Sigma = \phi_1, \phi_2\}$ — сигнатура алгебры $\mathbf{R}$, ϕ_1 — символ операции сложения, ϕ_2 — символ операции умножения.

Для задач фильтрации функция сложения определяется следующим образом:

$$R_3 = R_1 + R_2 = \{x_{11}, x_{12}, \ldots, x_{1k}, a_{11}, a_{12}, \ldots, a_{1m}\} +$$
$$+ \{x_{21}, x_{22}, \ldots, x_{2k}, a_{21}, a_{22}, \ldots, a_{2m}\} =$$

$$= \begin{cases} \{x_{11} \vee x_{21},\ x_{12} \vee x_{22},\ \ldots,\ x_{1k} \vee x_{2k}, \\ \qquad a_{11},\ a_{21} \vee a_{22},\ \ldots,\ a_{1m} \vee a_{2m}\}, & \text{если } a_{11} = a_{21}; \\ \{x_{11} \setminus x_{21},\ x_{12} \setminus x_{22},\ \ldots,\ x_{1k} \setminus x_{2k}, \\ \qquad a_{11},\ a_{21} \vee a_{22},\ \ldots,\ a_{1m} \vee a_{2m}\}, & \text{если } a_{11} \neq a_{21}. \end{cases} \tag{3}$$

Здесь $a_{i1} \in \{0,\ 1\}$ — атрибут действия правила фильтрации; при $a_{i1} = 0$ правило производит удаление пакета, а при $a_{i1} = 1$ правило разрешает пропуск пакета. Другими словами, сумма правил R_1 и R_2 есть объединение их одноименных параметров при одинаковом действии правил R_1 и R_2 (например, пропуск) и разность их одноименных параметров при различных действиях правила R_1 и R_2 (например, правило R_1 на пропуск, правило R_2 на удаление).

Функция умножения для правил фильтрации задается следующим образом:

$$\begin{aligned} R_3 = R_1 * R_2 &= \{x_{11},\ x_{12},\ \ldots,\ x_{1k},\ a_{11},\ a_{12},\ \ldots,\ a_{1m}\} * \\ &\quad * \{x_{21},\ x_{22},\ \ldots,\ x_{2k},\ a_{21},\ a_{22},\ \ldots,\ a_{2m}\} = \\ &= \{x_{11} \wedge x_{21},\ x_{12} \wedge x_{22},\ \ldots,\ x_{1k} \wedge x_{2k}, \\ &\quad a_{11} \wedge a_{21},\ a_{21} \vee a_{22},\ \ldots,\ a_{1m} \vee a_{2m}\}. \end{aligned} \tag{4}$$

Другими словами, произведение правил R_1 и R_2 есть пересечение их одноименных параметров, при этом действие правила представляет собой результат конъюнкции значений атрибутов a_{i1} правил R_1 и R_2.

В результате процесс обработки пакетов в МЭ представляется функций $\psi(\phi,\ R)$, которая определяется следующим образом:

$$\psi(\phi,\ R) = \begin{cases} \{a_1,\ a_2,\ \ldots,\ a_m\}_d, & \text{если } \phi(R,\ p) = 0, \\ \{a_1,\ a_2,\ \ldots,\ a_m\}_i, & \text{если } \phi(R,\ p) = i > 0, \end{cases} \tag{5}$$

где R — множество правил фильтрации, $\{a_1,\ a_2,\ \ldots,\ a_m\}_d$ — вектор атрибутов по умолчанию для обработки сетевых пакетов, $\{a_1,\ a_2,\ \ldots,\ a_m\}_i$ — вектор атрибутов правила фильтрации, p — обрабатываемый пакет, $p = \{y_1,\ y_2,\ \ldots,\ y_k\}$, y_i — параметры принятого пакета, $i = 1,\ \ldots,\ k$, $\phi(R,\ p)$ — характеристическая функция правила фильтрации, которая вычисляется следующим образом:

$$\phi(R,\ p) = \begin{cases} i, & \text{если } \bigwedge_{j=1}^{k} x_{ij} \wedge y_j = 1,\ \ i = \{1,\ \ldots,\ n\}; \\ 0, & \text{если } \bigvee_{i=1}^{n} \bigwedge_{j=1}^{k} x_{ij} \wedge y_j = 0. \end{cases}$$

В последней формуле в качестве параметров $\{x_j\}$, $j = 1,\ \ldots,\ k$, могут выступать как индикаторные параметры пакета (такие, как IP-адреса и порты), так и латентные параметры, задаваемые регулярными выражениями и позволяющими производить контентную фильтрацию прикладных протоколов.

5. Заключение

В работе рассматривались актуальные вопросы построения моделей сетевых процессов, учитывающие логико-динамические аспекты, связанные с реализацией методов контентной фильтрации трафика. Представленные модели позволяют получить верифицируемые характеристики, определяемые динамическими свойствами TCP протокола и особенностями его использования для контроля состояний виртуальных транспортных соединений. Проведенный анализ созданных моделей показывает возможность реализации двухуровневой системы контентной фильтрации, в которой разделение трафика осуществляется с использованием средств контроля состояний TCP сессий и сигнатурного анализа выделенных последовательностей пакетов. Для формализации процесса синтеза правил фильтрации предлагается использовать элементы новой алгебры, в которой операции могут интерпретироваться в контексте теоретико-множественного описания индикаторных и латентных переменных.

Исследование проактивных механизмов защиты от сетевых червей

И. В. Котенко, В. В. Воронцов, А. В. Тишков,
А. А. Чечулин, А. В. Уланов

1. Введение

В соответствии с имеющимися статистическими данными [1] рост числа компьютерных инцидентов за прошедший период 2007 года не уменьшился. Большая часть (52 %) зарегистрированных происшествий была связана с вирусной активностью. Урон, нанесенный сетевыми эпидемиями, составил более чем $8.300.000.

Учитывая динамику современных сетевых эпидемий, большую роль при ограничении размеров эпидемии играют механизмы обнаружения подозрительной активности и сдерживания распространения сетевых червей. Посредством сокращения скорости инфицирования конечных сетевых узлов (хостов), эти механизмы позволяют уменьшить скорость распространения эпидемии, тем самым, предоставляя время для ответных мер, включающих реконфигурацию сети или использование «заплат» («патчей»), устраняющих уязвимости.

В работе предлагается *проактивный подход к защите от сетевых червей*, *базирующийся на использовании механизмов обнаружения и ограничения интенсивности соединений сетевых червей*, *а также рассматриваются модели и разрабатываемое программное средство для исследования механизмов защиты от сетевых червей на основе моделирования различных типов и экземпляров сетевых червей и механизмов защиты от них*.

Работа выполнена при финансовой поддержке РФФИ (проект № 07-01-00547), программы фундаментальных исследований ОИТВС РАН (контракт № 3.2/03), Фонда содействия отечественной науке и при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза POSITIF (контракт IST-2002-002314) и RE-TRUST (контракт № 021186-2).

2. Сущность проактивного подхода

Предлагаемый подход предназначен для обнаружения сетевых червей (посредством выявления их действий по сканированию уязвимых хостов) и сдерживания их дальнейшего распространения (за счет ограничения и блокирования посылаемых инфицированными узлами сетевых пакетов).

Основными требованиями к разрабатываемым механизмам обнаружения и сдерживания сетевых червей являются следующие:

- адекватность обнаружения: должны обеспечиваться низкие показатели пропуска атаки и ложного срабатывания;
- оперативность обнаружения: вредоносная сетевая активность должна обнаруживаться как можно раньше, данное требование напрямую влияет на величину ущерба, приносимого в результате эпидемии сетевых червей;
- эффективность использования системных ресурсов и возможность реализации на сетевом оборудовании;
- автоматическое выполнение: разрабатываемые механизмы должны выполняться без вмешательства (или при минимальном вмешательстве) администратора;
- возможность обнаружения (кроме быстро сканирующих сетевых червей) также червей, использующих скрытные алгоритмы сканирования.

Предлагаемые проактивные механизмы обнаружения и сдерживания характеризуются следующими особенностями:

1) «многорезолюционный» подход к обнаружению, сочетающий использование нескольких интервалов времени («окон») наблюдения сетевого трафика и применение различных порогов для отслеживаемых параметров;

2) гибридный подход к обнаружению, базирующийся на использовании отличающихся механизмов обнаружения, основанных на реализации различных алгоритмов и математических методов, и их многоуровневом комбинировании (как системы базовых классификаторов и мета-классификатора);

3) адаптивные механизмы обнаружения.

3. «Многорезолюционный» подход

Для увеличения эффективности обнаружения сетевых червей на основе пороговых методов и алгоритмов ограничения частоты соединений предлагается использовать так называемый «многорезолюционный» подход к обнаружению.

При использовании данного подхода возможно обнаружение с низкой частотой ложных срабатываний не только агрессивных червей (червей, использующих для своего распространения сканирование с небольшой временной задержкой между посылкой сетевых пакетов), но и менее агрессивных червей.

В основе данного метода лежит следующее наблюдение [2]: во время функционирования хоста возможно изменение его сетевой активности, а именно чередование периодов, когда хост передает большие объемы данных (или демонстрирует быстрый рост числа соединений с другими хостами), с периодами относительного бездействия.

Таким образом, с одной стороны, использование большого порогового значения для отслеживаемых параметров (например, количества соединений с новыми хостами за заданный временной интервал) не позволяет обнаруживать распространение червей, использующих для распространения маленькую скорость сканирования, а, с другой стороны, низкое пороговое значение приводит к увеличению частоты ложных срабатываний при повышении сетевой активности неинфицированного узла.

«Многорезолюционный» подход — это подход к обнаружению распространения сетевых червей на основе использования множества механизмов обнаружения, применяемых для разных периодов отслеживания параметров, характеризующих инфицированность хостов. Иными словами, данный подход заключается в применении семейства различных пороговых значений для разных интервалов времени (например, 1 сек, 5 сек, 1 мин и др.).

«Многорезолюционный» подход обеспечивает не только возможность обнаружения «быстрых» сетевых червей, но и позволяет выявлять некоторые методы скрытого сканирования. Таким образом, используя данный подход, становиться возможным обнаружение широкого спектра сетевых червей, независимо от используемых сигнатур и стратегий сканирования, при одновременном сохранении легкости использования, свойственной алгоритмам, базирующимся на пороговых значениях.

4. Гибридный подход

Предлагаемый подход основан на использовании комбинации различных методов обнаружения нелегитимной сетевой активности.

В частности, предлагается применение следующих механизмов и их модификаций: «дросселирование/регулирование вирусов» («virus throttling»); ограничение интенсивности на основе данных о неудачных соединениях («failed connection rate limiting»); ограничение интенсивности на основе DNS-статистики («DNS-based rate limiting»), базирующееся на использовании корреляции DNS-запросов с исходящими из сети соединениями; ограничение интенсивности соединений, основанное на кредитах доверия («credit-based rate limiting»); ограничение интенсивности на базе метода «порогового случайного прохождения» (Threshold RandomWalk), базирующееся на наблюдении за удачными/неудачными попытками соединения с новыми хостами и представлении соединений с новыми хостами как случайных блужданий с использованием двух стохастических процессов, и др.

В разрабатываемом программном обеспечении реализуется двухуровневая система обнаружения, состоящая из следующих уровней: *первый уровень* — основные классификаторы, которые реализуют отдельные методы (алгоритмы) обнаружения; *второй уровень* — мета-классификатор, осуществляющий комбинирование различных алгоритмов обнаружения и сдерживания, а также общие процедуры, необходимые для реализации при сетевой защите (например, поддержка списков контроля доступа для механизмов обнаружения и т. д.).

5. Адаптация механизмов обнаружения

В разрабатываемом программном обеспечении предлагается использовать адаптивную схему обнаружения, способную изменять критерии обнаружения на основе статистических параметров сетевого трафика. В качестве таких параметров используются следующие величины: частота соединений (учитываются попытки соединения с новыми узлами); частота и количество возникновения ошибочных соединений; частота и количество «первоначальных» соединений; частота и количество соединений с узлами, которые не содержатся в стеке (кэше) локального DNS-сервера и др. Кроме того, реализуются следующие дополнительные механизмы: отслеживание неиспользуемых адресов (dark addresses); использование списков контроля доступа (ACL-листов) для игнорирования соединений по определенным портам и протоколам; обработка сообщений от ложных (обманных) информационных систем (при наличии последних в защищаемой сети), например, коммутатор может блокировать адреса, обращающиеся к таким системам, и др.

6. Программный комплекс моделирования

Обобщенная архитектура разрабатываемого программного средства моделирования, реализующего предлагаемый подход к исследованию механизмов защиты от сетевых червей, включает три основных компонента:

- *Модели источников трафика*. Эти модели предназначены для предоставления сетевого трафика для механизмов обнаружения и сдерживания сетевых червей. Они включают как модели трафика атаки, так и модели обычного сетевого трафика. Возможно моделирование трафика как уже известных сетевых червей, так и будущих. Это достигается путем возможности генерировать трафик с определенными параметрами (частоты генерации пакетов, размера генерируемого пакета, вида сканирования и т. д.).
- *Модели предобработки и синхронизации источников трафика*. Они предназначены для приведения трафика из формата источников в формат, удобный для анализа механизмами защиты, синхронизации нескольких источников трафика и передачи трафика механизмам обнаружения и сдерживания в упорядоченном во времени виде.
- *Модели механизмов обнаружения и сдерживания трафика червя*. Дополнительными элементами являются таблица фильтрации метода и генератор отчетов. Входными параметрами метода являются те поля пакета, полученного от источника трафика, которые им обрабатываются. В качестве управляющих параметров вводятся различные внутренние параметры каждого метода, которые влияют на его эффективность.

Для проведения оценки механизмов обнаружения и сдерживания сетевых червей задаются различные сценарии моделирования. Сценарии включают набор экземпляров источников трафика и механизмов обнаружения и сдерживания. В результате моделирования определяются такие параметры работы механизмов защиты, как количество ложных срабатываний, количество сгенерированных червем пакетов, которые не были обнаружены защитой, время реакции, минимальное, среднее и максимальное время обработки пакета и др.

7. Заключение

В работе предложен проактивный подход к защите от сетевых червей, базирующийся на использовании механизмов обнаружения и сдерживания распространения сетевых червей.

Предложен подход и разработано средство для исследования механизмов защиты на основе моделирования. Проведен ряд экспериментов.

Планируется проведение большой серии исследований на основе моделирования различных сетевых червей и предлагаемых проактивных механизмов защиты от них.

Литература

[1] CSI/FBI 2006 Computer Crime and Security Survey, 2007.

[2] *Котенко И. В.*, *Воронцов В. В.* Проактивный подход к обнаружению и сдерживанию сетевых червей // Труды Международных научно-технических конференций «Интеллектуальные системы (AIS'07)» и «Интеллектуальные САПР (CAD-2007)». М.: Физматлит, 2007.

Информационные угрозы в контексте противодействия терроризму

В. Д. Недильниченко

1. Международная позиция

Участие в процессах борьбы с терроризмом и нераспространения, присоединение к программе Глобального партнерства и Глобальной инициативе борьбы с актами ядерного терроризма (ГИБЯТ) нуждается в усилении мероприятий по предупреждению терроризма или распространения средств массового поражения (СМП). В Плане действий G-8 (2006, Санкт-Петербург) отмечена важность прозрачности, стабильности, предсказуемости национальных систем регулирования по обеспечению стойкости систем нераспространения, ядерной и энергетической безопасности. В заявлении G-8 (2006) относительно ГИБЯТ сделано ударение на необходимости систематической борьбы с терроризмом путем усовершенствования возможностей участников. Декларация G-8 (2006) [1] одним из направлений деятельности провозглашает противодействие намерениям использования информационных технологий (ИТ) в террористических целях.

Опережающее развитие ИТ и их внедрение в процессы учета, защиты и управления технологическими процессами критической инфраструктуры нуждается в реализации адекватных мероприятий по обеспечению ИБ.

2. Национальная позиция Украины

Необходимость обеспечения ИБ отображена в «Стратегии национальной безопасности Украины» (2007). В частности, отражена необходимость разработки и внедрения национальных стандартов и технических регламентов в сфере ИТ, гармонизованных с соответствующими европейскими стандартами, в том числе согласно требованиям ратифицированной Украиной европейской Конвенции «О киберпреступности». В Законе Украины «О борьбе с терроризмом» отмечена необходимость

защиты информации, которая может быть использована для совершения актов технологического терроризма.

Государственная позиция Украины в части информационной защиты критической инфраструктуры совпадает с позицией международного сообщества.

3. Значимость информационных технологий

Безопасность критической инфраструктуры определяется взаимозависимостью двух контуров: технологического и информационно-управляющего. При этом технологический контур изменяется сравнительно медленно, в силу чего имеет наработанные механизмы технического регулирования и оценки безопасности.

Внедрение ИТ в системы управления осуществляется с целью получения экономических и технологических преимуществ. Оборотной стороной этого процесса являются увеличение уязвимостей. Уязвимости ИТ обусловлены наличием принципиальных недостатков и конкурентными условиями, которые приводят к ускоренному выпуску новых информационных продуктов без адекватного обеспечения ИБ. Для уменьшения затрат и сокращения срока разработки используются общедоступные средства COTS, привносящие присущие им уязвимости:

1. Содержащие принципиально неустранимые недостатки операционные системы.
2. Незащищенные системы SCADA, уязвимые серверы, например, OLE for Process Control (OPC).
3. Незащищенные сетевые протоколы, слабые системы идентификации и аутентификации.
4. Уязвимости электронных компонентов, например, интерфейс JTAG, и прочее.

В маркетинговых целях происходит освещение особенностей систем управления, в том числе и в отношении конкретных объектов . Имеет место интеграция систем управления технологическими процессами и производством с последующей организацией доступа в глобальные сети. Дополнительным фактором риска является отсутствие адекватного технического регулирования ИБ критической инфраструктуры.

Понимание значимости ИБ критической инфраструктуры все же обозначается. К примеру, государственная стратегия противодействия терроризму США официально признает зависимость инфраструктуры государства от ИТ [2], их уязвимость и нацеливает на создание Единой национальной системы реагирования [3] на информационные угрозы. Принятый

Сенатом США в средине марта 2007 «Акт об улучшении безопасности Америки» предписывает Департаменту внутренней безопасности разработать программы стандартизации и сертификации защиты информации и степени готовности к экстренным ситуациям для критических инфраструктур США. Действенной позиции в отношении защиты критической инфраструктуры придерживается Европейский Союз [4]. Однако ситуация требует вовлечения в противодействие информационным угрозам большего числа участников.

Отсутствие соответствующего технического регулирования в части ИБ обуславливает уязвимость информационно-управляющих систем (ИУС) критической инфраструктуры. В определенных условиях ИУС может стать средством деструктивного воздействия. Например, авария на заводе BP в марте 2005 обусловлена установкой всего одного клапана технологического контура в несоответствующее положение. Официальная версия — ошибка оператора! Достоверность информации с контролируемых пунктов и корректность управляющих воздействий на технологический контур предопределяют безопасность технологических процессов и стабильность управляемых систем: генерации, транспортировки и распределения энергии, добычи и транспортировки в нефтегазовом комплексе, транспортировки и переработки техногенно-опасных веществ.

Необходимость защиты критической инфраструктуры от информационных угроз становится ключевой для обеспечения энергетической и техногенной безопасности, противодействия терроризму.

4. Межнациональный характер безопасности критической инфраструктуры

Значимость ИБ наглядно обозначается на примере обеспечения энергоресурсами. Растущая потребность в энергоресурсах и транзитный характер транспортировки предопределяет международную заинтересованность в поддержании стабильности, которая определяется также и защищенностью ИУС. Прохождение энергетических маршрутов через страны с разной степенью готовности к противодействию угрозам ИУС предопределяет снижение общей безопасности и, естественно, энергетической стабильности.

ИБ также является важным фактором стойкости системы нераспространения. Как отмечено в Декларации G-8 (2006) «О борьбе с терроризмом», усилия международного сообщества должны быть также направлены на предотвращение намерений террористов получить доступ к СМП, и одним из направлений этих усилий должна стать защита ИТ

от использования в террористических целях. В совместном заявлении Президентов РФ и США, G-8 (2006) относительно ГИБЯТ отмечена необходимость усовершенствования процессов: учета, контроля, физической защиты ядерных и радиоактивных материалов, сотрудничества в разработке технических средств для борьбы с терроризмом. Сказанное, а также предотвращение попадания критических технологий и материалов к террористическим группировкам, которые ставят цель создания СМП, требует обеспечения защиты соответствующей информации и систем.

В Плане действий G-8 (2006) отмечена важность прозрачности, стабильности, предсказуемости национальных систем регулирования по обеспечению стойкости системы нераспространения и надежности систем обеспечения энергетической, ядерной, радиологической безопасности.

Неотъемлемой частью национальной системы технического регулирования должна быть система обеспечения ИБ в критической инфраструктуре.

5. Международная координация усилий по регулированию безопасности ИТ

Последствия реализации уязвимостей ИБ критической инфраструктуры выйдут за границы национальных масштабов: энергетическая стабильность, стойкость системы нераспространения, техногенная безопасность и противодействие терроризму. Опережающее развитие ИТ при сохранении ведомственных подходов и игнорирования уровня угроз требуют координации усилий по выработке адекватных подходов к техническому регулированию ИБ. Адекватная позиция отдельных компаний [5] не является всеобъемлющей, национальные рамки и ведомственные различия препятствуют созданию стабильного механизма противодействия информационным угрозам, к примеру, в сфере энергоснабжения. Техническое регулирование по защите от информационных угроз не отвечает уровню развития ИТ. Необходимость защиты ИУС не регулируется должным образом, отсутствуют механизмы аудита ИБ. Ведомственная политика в сфере защиты информации осуществляется формально. Смена собственников на объектах критической инфраструктуры, обновление систем управления технологическими процессами усугубляют ситуацию с ИБ.

Реализация террористами уязвимости ИУС может привести к потере управляемости и возникновению техногенных аварий критической инфраструктуры. Особенностями этих воздействий может быть:

1) скрытность подготовки и реализации — отсутствие проявлений и следов проникновения;

2) масштабность воздействия — нанесение удара по множеству объектов;

3) синхронность воздействия — вторжение может быть одновременным по многим объектам;

4) распределенность — источник нападения может находиться за пределами страны воздействия;

5) интернациональность — ущерб может распространяться на многие государства.

Что нужно для этого: относительно небольшие ресурсы и мотивация, причем второе есть ключевым! Есть ли данный фактор актуальным? Исходя из геополитической ситуации, обострения мировой ситуации с распределением энергоресурсов, роста террористических угроз и методов их реализации — однозначно ДА.

На данный момент энергетическая стабильность обеспечивается совместной деятельностью ряда государств: добыча или генерация, транспортировка, переработка или хранение. В то же время эти государства имеют различные системы технического регулирования ИБ. И если в части защиты закрытой информации в этих странах имеется понимание, то в части обеспечения ИБ критической инфраструктуры оно может отсутствовать.

С целью усиления влияния на защищенность критической инфраструктуры, исходя из взаимозависимости в обеспечении экономической и техногенной стабильности, в развитие имеющихся наработок [6], предлагается создать из уполномоченных представителей заинтересованных стран, к примеру по транспортировке энергоносителей, рабочие группы, которые бы выработали рекомендации по обеспечению ИБ, например, на основе наработок ISO/IEC JTC1:

1. Разработать модель информационных угроз в соответствующей критической инфраструктуре.
2. Усовершенствовать техническое регулирование информационных и управляющих систем критической инфраструктуры.
3. Усовершенствовать механизмы аккредитации и сертификации ИУС критической инфраструктуры.
4. Проанализовать мероприятия по обеспечению информационной безопасности ИУС критической инфраструктуры.
5. Разработать механизмы аудита и контроля по выполнению требований ИБ в критической инфраструктуре.
6. Разработать механизм обновления нормативной базы по обеспечению ИБ в соответствии с уровнем ИТ и характером угроз.

7. Разработать механизмы партнерских проверок по обеспечению ИБ критической инфраструктуры, имеющей межнациональную значимость.
8. Разработать механизмы координации и взаимодействия в части предупреждения, отражения, устранения последствий информационных атак на объекты критической инфраструктуры.

Учитывая мировой опыт и уровень развития ИТ, значимость критической инфраструктуры для международной стабильности, предлагается усиление ИБ критической инфраструктуры посредством международной координации технического регулирования.

Литература

[1] Декларация саммита Группы восьми — G8 «о борьбе с терроризмом» (Санкт-Петербург, 2006).

[2] The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets. February 2003. USA.

[3] The National Strategy to Secure Cyberspace. February 2003. USA.

[4] On a European Programme for Critical Infrastructure Protection. Brussels, 12.12.2006, COM(2006) 786 final.

[5] *Ефимов А. И.* Актуальные проблемы обеспечения информационной безопасности газовой сферы. Материалы международной научной конференции по проблемам безопасности и противодействия терроризму (Москва, МГУ, 2—3 ноября 2005 г.). М.: МЦНМО, 2006. С. 477—479.

[6] *Васенин В. А.* Научные проблемы противодействия кибертерроризму. Материалы международной научной конференции по проблемам безопасности и противодействия терроризму (Москва, МГУ, 2—3 ноября 2005 г.). М.: МЦНМО, 2006. С. 49—63.

Обзор и анализ актуальных в сети Интернет атак

Ю. Н. Гуркин

1. Статистика атак

Для детектирования атак была установлена Система Обнаружения Вторжений (СОВ) SNORT, с помощью которой регистрировались атаки в реальном сегменте сети. Весь трафик идущий внутрь и наружу защищаемого сегмента сети зеркалировался и направлялся на сенсор. Использовался рекомендованный разработчиками SNORT набор правил «VRT certified rules».

Сегмент сети (см. рис. 1) включал в себя

- более 1000 ip-адресов, из них в среднем около 200 активных;
- 3 http сервера;
- 2 сервера баз данных SQL;
- 1 ftp сервер;
- 1 mail сервер.

В СОВ SNORT атакам присваивается приоритет.

Атаки которым присвоен приоритет 1 — это реальные попытки атак;

Атаки с приоритетами 2, 3 — это аномальная активность, которая может свидетельствовать об атаке или разведке.

Статистика зарегистрированных атак:

- суммарная частота атак всех видов: 52000/час;
- высшего приоритета 1: 12/час;
- приоритета 2: 46000/час;
- приоритета 3: 6000/час.

Необходимо отметить, что часть регистрируемых атак — это атаки изнутри сети, с зараженных компьютеров пользователей (попытки распространения червей).

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант № 06-07-89127).

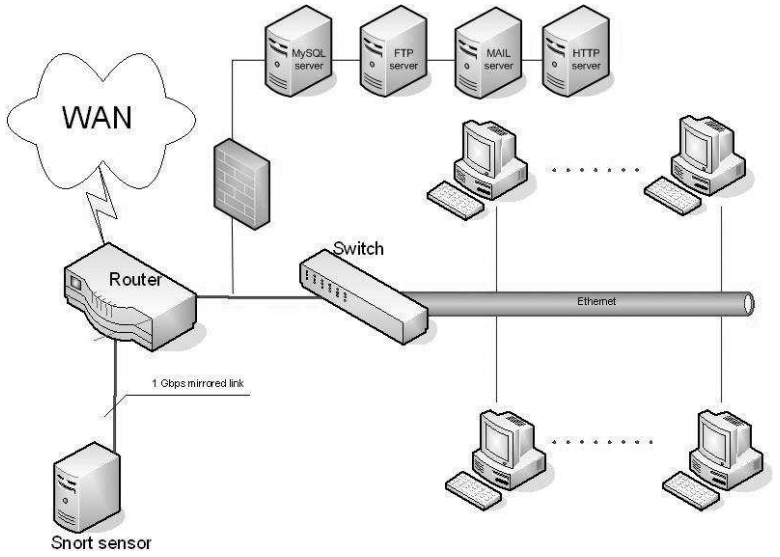


Рис. 1. Защищаемый с помощью Snort сегмент сети

Относительно стран происхождения внешних атак (чаще всего это атаки со взломанных компьютеров пользователей), было установлено, что атаки проводятся из разных стран, лидируют Россия, Китай, США. Часто домен атакующего не зарегистрирован.

Атакам подвергся широкий класс серверных приложений, в том числе:

- Попытки атак на HTTP сервер и установленные web-applications php, jsp, cgi, asp: 8/час;
- Попытки атак баз данных MS-SQL MySQL: 2/час;
- Попытки атак почтового сервера: 1/час;
- Попытки атак файлового сервера: 1/час;
- Сканирования ICMP, SNMP: 3/мин.

Таким образом, можно утверждать, что для большинства типов серверов

не менее 1 *раза в минуту идет сканирование*;

не менее 1 *раза в час сервер подвергается попытке атаки.*

Рабочие станции пользователей также подвергаются угрозам; так были выявлены попытки использования уязвимостей icq.

В целом использование СОВ SNORT как одного из поясов системы защиты эффективно, (см. [1]). Из достоинств и недостатков СОВ можно упомянуть следующие достоинства:

- возможность работы по широкому спектру протоколов;
- возможность редактирования сигнатур;
- большое количество предустановленных сигнатур

и недостатки:

- детектируются атаки лишь с известными сигнатурами;
- невозможность детекции атак с использованием шифрования;
- не детектируются атаки, использующие разрешенные возможности, например, атаки подбора пароля.

Немалая часть (более половины), зарегистрированных реальных попыток атак серверов, это атаки основанные на использовании уязвимостей типа «переполнение буфера», в частности стека. Это старый, но до сих пор очень актуальный тип атак.

2. Разбор механизма атаки переполнения стека (stack overflow)

Атаки переполнения буфера основываются на уязвимостях, связанных с отсутствием проверки передаваемых в программу или подпрограмму данных, поэтому может так получиться, что данные копируемые в буфер, превышают размер самого буфера (buffer overflow), такие данные запишутся не только на адреса памяти, выделенные для них, но и на соседние, при этом перезаписывая их содержимое. Такая перезапись может привести к перехвату управления и исполнению внедренного атакером shell-кода.

Разберем механизм переполнения подробнее на примере следующей простой программы, читающей в буфер данные введенные пользователем:

```
void fillarray (int a, int b) {
char array[4];
gets(array);
}

main () {
fillarray(1,2);
return 0;
}
```


В программе предполагается, что пользователь введет менее 4 символов. Допустим пользователь ввел символы `AAAA`. При выполнении функции `fillarray` стек будет заполнен следующим образом:

```
Адресация стека & Младшие адреса, основание стека
0xFFFFFFFCh     & 2
0xFFFFFFF8h     & 1
0xFFFFFFF4h     & RETURN ADDRESS
0xFFFFFFF0h     & EBP
0xFFFFFFECh     & AAAA
0xFFFFFFE8h     & Старшие адреса, вершина стека
```

(Реальные адреса в стеке будут другими. Приведенные адреса призваны показать, что стек распространяется вниз по адресному пространству и каждая адресуемая «ячейка» стека занимает 4 байта.)

В стеке сохраняются в обратном порядке передаваемые в функцию данные, затем адрес возврата из подпрограммы в основную программу, затем значение регистра `EBP`, затем заполняются пользовательскими данными `AAAA` выделенные для хранения массива `array` 4 байта.

Предположим теперь, что нерадивый пользователь ввел не 4 символа `A`, а 12 символов. Стек будет выглядеть следующим образом:

```
Адресация стека & Младшие адреса, основание стека
0xFFFFFFFCh     & 2
0xFFFFFFF8h     & 1
0xFFFFFFF4h     & AAAA
0xFFFFFFF0h     & AAAA
0xFFFFFFECh     & AAAA
0xFFFFFFE8h     & Старшие адреса, вершина стека
```

Будет заполнено место в памяти выделенное под массив, затем будет перезаписано сохраненное значение `EBP`, а затем адрес возврата (на его место будет записано двойное слово, соответствующее 16-ричному представлению символов `AAAA` — `0x41414141h`).

При исполнении программы в данном случае процессор попытается исполнить команду находящуюся по «новому» адресу `0x41414141h`.

Чаще всего попытка подобного перезаписывания вызывает хорошо знакомую C++ программистам ошибку — segmentation fault, и аварийное завершение программы. Однако «правильное» переполнение может привести к перезаписи адреса возврата таким образом, что он будет указывать на адрес памяти, в котором хранится внедренный атакером shell-код. (см. [2])

Литература

[1] Andrew Baker, Jay Beale, Brian Caswell, Mike Poore. Snort 2.1 Intrusion Detection. Syngress Publishing Inc., 2004.

[2] Jack Koziol, David Litchfield, Dave Aitel, Chris Anley, Sinan „noir“ Eren, Neel Mehta, Riley Hassell. The Shellcoder's Handbook: Discovering and Exploiting Security Holes. Willey Publishing Inc., 2004.

Безопасность клиентов в публичных беспроводных сетях

С. Л. Коваленко

Аннотация

Данная статья освещает проблемы безопасности клиента в публичной беспроводной сети. Предлагается модель инфраструктуры беспроводной сети, основанная на сервисах безопасности. Данная модель позволяет обеспечить соответствие функционирования сети требованиям политики безопасности клиента. Описывается возможный процесс выбора клиентом безопасной беспроводной сети.

1. Актуальность

В настоящее время происходит бурное развитие беспроводных телекоммуникационных технологий. Уже не редкость когда в одном месте параллельно существуют и работают несколько беспроводных сетей. Часто такая ситуация встречается в крупных транспортных узлах, таких как аэропорты и железнодорожные вокзалы, в бизнес и торговых центрах, гостиницах, и даже в центральных частях крупных мегаполисов таких как Москва, или Сан-Франциско в США. Постоянно увеличивается количество компьютеров и других устройств имеющих возможность работать в беспроводных сетях. Большое количество потенциальных пользователей беспроводных сетей подталкивает компании поставщиков услуг активно разворачивать беспроводные сети. Например, компания «Голден Телеком» вводит в эксплуатацию в Москве самую большую [9], на начало 2007 года, беспроводную сеть в мире, построенную на технологии WiFi. Компания планирует разместить примерно 6700 точек доступа и покрыть около 800 000 домохозяйств в Москве.

2. Публикации по теме статьи

Проблемы безопасности в беспроводных сетях освещаются большим количеством как отечественных, так и зарубежных публикаций. Примера-

ми могу быть [2, 7, 3]. Основная часть публикаций посвящена вопросам безопасного конфигурирования сетей на базе существующих технологий и вопросам криптографического закрытия данных. Также подробно освещены известные атаки на беспроводную сеть извне. Крупные компании производители и поставщики оборудования предлагают свои модели построения безопасных беспроводных сетей. Примерами являются Madge Networks [11] и Cisco Systems [12].

Однако в стороне оставлен вопрос о безопасности клиента в беспроводных публичных сетях. В работе [6] сформулирована адаптивная модель управления правами доступа в зависимости от внешних условий. С рядом поправок данная модель может быть применена для регулирования работы клиентских устройств в беспроводной сети. Однако для этого требуется всесторонняя поддержка со стороны инфраструктуры сети. В [8] описан возможный подход для построения инфраструктуры позволяющей осуществлять управление правами доступа внутри сети. Комбинация этих подходов выглядит перспективной и может быть применена для решения проблем безопасности в публичных беспроводных сетях.

3. Проблемы безопасности клиента в публичной беспроводной сети

3.1. Описание проблемы

Публичной беспроводной сетью будем называть сеть, доступ к которой может получить любой желающий, неважно на коммерческой ли безвозмездной основе. Количество публичных беспроводных сетей растет и будет увеличиваться и далее. Из общедоступности подключения к сети возникает возможность не просто атаки одного клиента сети на другого, а возникает возможность целенаправленной атаки злоумышленника на заранее выбранного клиента. При этом, если в проводных сетях злоумышленник в общем случае не мог рассчитывать на нахождение с атакуемым в одном сегменте, то в публичных беспроводных сетях это стало реальностью. Нахождение атакующего и атакуемого в одном сегменте сети значительно расширяет возможное множество атак, например появляется возможность использовать для атак протоколы не поддерживающие маршрутизацию. И если в корпоративной сети мобильное устройство сотрудника защищено инфраструктурой и средствами обеспечения безопасности сети, то при попадании в публичную беспроводную сеть мобильное устройство может оказаться совершенно не защищенным. Также необходимо учитывать значимое различие между публичными проводными и беспроводными сетями. В публичных проводных сетях

клиент обычно работает на постоянной основе, не является анонимным и может быть относительно легко отключен в случае необходимости. В публичной беспроводной сети, в большинстве случаев, клиенты анонимны. Это делает затруднительным или невозможным блокирование входа определенного человека в сеть, что еще больше усложняет обеспечение безопасности клиентов сети.

3.2. Существующие решения

Типовое решение приведенной выше проблемы незащищенности клиента в публичной беспроводной сети, предлагаемые ведущими компания, во многом сходны.

Например компания Microsoft приводит свое решение официальном сайте [10] которое сводится к перенастройке межсетевого экрана ОС Windows и отказу от передачи в публичных сетях конфиденциальной информации.

Однако рекомендации по отказу от передачи конфиденциальных данных с использование публичных сетей не решает задачу безопасности самого клиента в беспроводной сети. Более того зачастую подобные подходы не являются приемлемым и жизнеспособным решением как в силу производственной необходимости, так и в силу человеческого фактора. Необходим некоторый комплексный единый инфраструктурный механизм в публичных беспроводных сетях, позволяющий максимально автоматизировано обеспечивать необходимый уровень безопасности для клиентов сети.

3.3. Задача выбора безопасной публичной беспроводной сети

При наличии беспроводной сети к которой клиент может произвести подключение возникает задача определения соответствия сети с политикой безопасности клиента. На данный момент клиент имеет очень ограниченный перечень характеристик сети на основании которых затруднительно принимать решения о соответствии сети требованиям политики безопасности клиента. Обычно характеристики, известные клиенту при подключении к беспроводной сети семейства стандартов IEEE 802.11 [1], включают в себя:

- Идентификатор сети — ESSID.
- Тип шифрования, применяющегося в сети.
- Ключи для входа в сеть.

Подобных данных явно недостаточно для определения соответствие сети требованиям политики безопасности клиента. Несмотря на это, например, ОС Windows XP автоматически относит к безопасным беспровод-

ным сетям любую сеть в которой включено шифрование WEP/WPA [1, 4, 5], чем может вводить пользователя в заблуждение. Подобный критерий выбора безопасной сети и принятия решения о подключении к ней не допустим для публичных сетей. Одно лишь шифрование не способно защитить клиента от множества возможных атак в публичной сети.

На данный момент выбирая ту или иную сеть для подключения пользователь фактически полностью лишен какой-либо информации о соответствия сети требованиям его политики безопасности. Также не существует общего механизма позволяющего ответить на вопрос безопасности самой сети для клиента.

4. Модель организации беспроводной сети на основе сервисов безопасности

4.1. Сеть и сервисы безопасности

Для решения проблемы, приведенной в подразделе 3.1, предлагается организовать в сети сервисы безопасности. Сервисом безопасности будем считать программный или программно-аппаратный комплекс выполняющий четко формализованные функции безопасности. Примером сервиса безопасности могут быть:

- межсетевой экран, находящийся на стороне точки доступа с которой ассоциирован клиент;
- антивирусный сканер, с возможность удаленного использования.

Будем считать что сеть N содержит множество сервисов безопасности S. Каждый сервис безопасности $s_i \in S$ имеет множество функций безопасности F_{s_i}.

4.2. Политика безопасности клиентского устройства

Политика безопасности P клиентского устройства выражает множество формализованных требований $p_i \in P$ к беспроводной сети N, с которой возможно безопасное взаимодействие. Создавая политику безопасности пользователь, или администратор, должен явно указать какие сервисы безопасности s_i должны быть доступны в беспроводной сети N, и каким образом программное обеспечение клиента должно с ними взаимодействовать.

4.3. Принятие решения о безопасности подключения

Процесс подключения клиента к беспроводной сети представляет собой диалог, в процессе которого сеть сообщает клиенту о предоставляемом множестве сервисов безопасности S. Клиентское устройство использует функцию принятия решения о безопасности подключения $R(S, P)$ с помощью которой оценивает соответствие безопасности сети требованиям своей политики безопасности. В случае решения о возможности подключения клиента к сети производиться настройка программного обеспечения на использование сервисов безопасности. Подключение может быть произведено только в случае его разрешения функцией R.

4.4. Пример возможной реализации функции R

Ниже приведены примеры возможной реализации функции принятия решения о безопасности подключения. Функция $R(S, P)$ может проверять наличие всех необходимых сервисов безопасности s_i и всех необходимых функций f_{s_i} в них согласно множеству требований политики безопасности $p_j \in P$.

Возможно использовать подход, на основе весовых коэффициентов. Для этого требуется ввести множество M весовых коэффициентов для правил $p_j \in P$ политики безопасности. Тогда функция решения будет иметь вид:

$$R(S, P) = \sum_{j=1}^{n} m_j p_j.$$

5. Выводы

В настоящий момент не достаточно развиты средства обеспечения безопасности клиента в публичной беспроводной сети. Так сетевая инфраструктура семейства стандартов IEEE 801.11 не имеет механизмов защиты одного клиента от другого. В данной статье предложена модель построения инфраструктуры беспроводной сети обеспечивающая механизмы защиты клиента в публичной сети.

Литература

[1] ANSI/IEEE. ANSI/IEEE Std 802.11, 1999 Edition (R2003).

[2] *Владимиров А. А.* Wi-фу боевые приемы взлома и защиты беспроводных сетей.

[3] Wireless Network Security 802.11, Bluetooth and Handheld Devices. Tom Karygiannis Les Owens Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg.

[4] IEEE. IEEE Std 802.11b-1999. (Supplement to ANSI/IEEE Std 802.11, 1999 Edition)

[5] IEEE. IEEE Std 802.11g-2003. (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001)
[6] *Ferrante A.*, *Taddeo A.*, *Sami M.*, *Mantovani F.*, *Fridkins J.* Self-Adaptive Security at Application Level: a Proposal. ALaRI, Faculty of Informatics, University of Lugano, Lugano, Switzerland. Dipartimento di Elettronica e Informazione, Politecnico di Milano, Milano, Italy.
[7] *Максим М.*, *Поллино Д.* Безопасность беспроводных сетей.
[8] *Peter F. Linington*. A Policy-Based Model-Driven Security Framework. University of Kent, UK.
[9] Голден Телеком. «Голден Телеком» запускает в коммерческую эксплуатацию самую большую сеть WiFi в Европе. `http://www.goldentelecom.ru/presscenter/news/news.html?ID=8959`.
[10] Microsoft Corporation. Use public wireless networks more safely. `http://www.microsoft.com/protect/yourself/mobile/publicwireless.mspx`.
[11] Madge Networks. White Paper Wireless LAN Security. `http://www.madge.com/assets/documents/guides/wlansecurity.pdf`.
[12] Cisco Systems. Пять шагов, которые необходимо предпринять для обеспечения безопасности беспроводной сети. `http://www.cisco.com/web/RU/products/hw/wireless/pdf/stepstosecurity.pdf`.

Часть IV

СЕМИНАР-КРУГЛЫЙ СТОЛ «ПРОБЛЕМЫ РАЗВИТИЯ СИСТЕМЫ СТРАХОВАНИЯ РИСКА „ТЕРРОРИСТИЧЕСКИЙ АКТ“»

Проблемы развития системы страхования риска «террористический акт»

И. В. Ломакин-Румянцев

В настоящее время терроризм является одним из наиболее опасных деяний, дестабилизирующих общественную безопасность и угрожающих жизни, здоровью, достоинству личности.

Жертвам террористических актов гарантируется справедливая, соответствующая и своевременная компенсация за тот ущерб, который им был нанесен. Если компенсация не может быть получена из других источников, в частности, через конфискацию собственности инициаторов, организаторов и спонсоров террористических актов, то государство, на территории которого был совершен террористический акт, должно вносить свой вклад в компенсацию жертвам прямого физического или психологического ущерба, независимо от их гражданства (пункт 1 раздела VII. Компенсация. Руководящие принципы защиты жертв террористических актов, принятые Комитетом Министров Совета Европы 2 марта 2005 года).

В Российской Федерации порядок возмещения вреда регламентируется Федеральным законом «О борьбе с терроризмом», ст. 17 которого определяет порядок возмещения вреда, причиненного в результате террористической акции, оставляя при этом определенный вакуум, заключающийся в отсутствии каких-либо критериев определения размера компенсации, а также механизма возмещения вреда, причиненного террористической акцией, а также Федеральным законом «О противодействии терроризму», который однако не уточнил механизм возмещения вреда, причиненного террористическим актом, более того, он усугубил положение потерпевших, закрепив в ст. 18 положение о компенсации морального вреда, причиненного в результате террористического акта, за счет лиц, его совершивших.

Вместе с тем имущественные и человеческие потери, вызванные международными террористическими актами в действительности не сопоставимы к примеру с числом погибших вследствие ДТП. Данные, собранные за период с 1994 по 2003 г. в 29 странах-участницах Организации

экономического сотрудничества и развития показали, что среднегодовой показатель смертности на дорогах этих стран в 390 раз превышает число погибших от рук террористов.

Однако психологические последствия террористических актов более глубоки и масштабны, поскольку в силу мощного общественного резонанса им подвержены не только «прямые» жертвы террористических актов, но и прочие граждане. Пристальное внимание общества направлено, в том числе, и на незамедлительное по возможности возмещение ущерба, причиненного террористическим актом.

Страхование является финансовым инструментом, способным устранить лишь имущественные неблагоприятные последствия террористических актов, предполагающим точное документальное фиксирование события, соблюдение процедуры выплаты страхового возмещения, что очевидно не может быть осуществлено незамедлительно после совершения теракта.

Террористические акты являются, как правило, следствием социального внутреннего или внешнего события, что может привести к их серийности. Т. е. частотность и прогнозируемость террористических рисков в отличие от обычных рисков, предполагающих равномерное распределение их во времени, предполагает высокую кумуляцию во времени терактов, а это требует иной перестраховочной защиты и другого подхода к формированию страховых резервов.

Также следует учитывать, что потенциальный ущерб может и не находится в прямой причинно-следственной связи с терактом, а быть следствием аварий, вызванных им. В частности в результате взрыва 11 сентября 2001 года в США имели место косвенные убытки:

- перерыв хозяйственной деятельности — 11 млрд долл.;
- ответственность перед третьими лицами — 10 млрд долл.;
- имущество (без зданий ВТЦ) — 6 млрд долл.;
- имущество 2-х зданий ВТЦ — 3,5 млрд долл.;
- ответственность владельцев воздушного судна перед третьими лицами — 3,5 млрд долл.;
- страхование жизни — 2,7 млрд долл.;
- ответственность работодателя — 2 млрд долл.;
- риск отмены мероприятий — 1 млрд долл.;
- КАСКО 4-х воздушных судов — 0,5 млрд долл.

Еще одной проблемой осуществления страхования по рассматриваемому риску является скачкообразность востребованности данного страхования, которая резко возрастает непосредственно после терактов и снижается по прошествии времени.

По моему мнению, наиболее целесообразно предусмотреть для возмещения ущерба в результате терактов двухуровневую систему:

1. Государственные гарантии.
2. Страхование.

Примером может являться (TRIA) — система государственной (США) поддержки страховщиков, возмещающих ущерб, возникший в результате терроризма.

Общий лимит госгарантий по программе (TRIA) составляет 100 млрд долларов США. Ущерб, в случае его возникновения распределяется в пропорции 90 % к 10 %, где большую нагрузку несёт Правительство США. Механизм распределения убытков сверх установленного лимита, в случае его фактического превышения в 100 млрд долларов США устанавливается по решению Конгресса США.

Terrorism Insurance: What Is To Be Done?

T. Russell

Introduction

The simplest way an enterprise can reduce future losses from a terrorism attack is to purchase a contract of terrorism insurance from a commercial insurance company. Unfortunately, following a terrorism attack, private providers of terrorism insurance typically withdraw from the terrorism insurance market, leaving target industries totally exposed.

This pattern is now well established. Usually it is the re-insurers who first refuse to underwrite this type of risk. Primary insurers, unwilling to carry all of the risk themselves, then follow by excluding this risk from standard contracts. In the pre 9/11 world, the collapse of this market following an attack was observed in, for example, Spain, Northern Ireland, Israel, South Africa, and Great Britain, and following 9/11, the pattern was repeated in the United States, Germany, France, Australia, and other countries.

The failure of this market has consequences for the health of the macroeconomy. After a terrorist attack, lenders will not write mortgages on vulnerable property unless that property carries terrorism coverage. Since this coverage is not available, lending slows, and the reduction in the level of mortgage lending then flows through to a reduction in the level of property development and on to a reduction in employment in the construction and other industries (tourism, transportation, sports) facing lending restrictions.

Governments, charged with maintaining full employment, are now faced with the problem of how best to restore the risk transfer mechanism provided by private insurance markets. In this paper we examine some of the issues and options, particularly as they relate to the situation in the United States.

Why Does the Private Market Fail?

Before Governments can design a plan for intervening in this market, it is necessary to have an understanding of why the private market fails. Two reasons are usually given.

1. Terrorism losses are potentially so large, they exceed the total capacity of the industry.
2. The underlying probabilities of terrorism attack are too vague and ambiguous to allow private insurers to calculate an actuarially sound premium.

We examine each of these in turn.

The Size of the Loss

There is no doubt that scenarios can be developed in which terrorism losses exceed the total available capital of the private insurance and reinsurance industries. For example, Risk Management Solutions, a risk modeling company, estimates the expected loss from a 5 kiloton nuclear terrorism attack at $630b with an upper estimate of $1.9tr. The American Association of Actuaries has a mean estimate of $778b. Losses of this magnitude far exceed the losses from Hurricane Katrina, $66b, to date the world's largest insured loss.

Given such large potential losses, managers of insurance companies argue that it would be imprudent to risk the survival of the company by staying in this market. This argument, however, is economically suspect. For the individual insurance company aggregate losses are irrelevant. Underwriting, the most basic concept in insurance, assumes that an individual insurance company will take only part of a risk, not all of it, and this part can be as large or as small as the company wishes.

What we observe, however, is that rather than take a small part of this risk, insurers and re-insurers refuse to take any. This behavior is puzzling. Refusal to write any coverage suggests that the typical insurance company is being driven by considerations other than profit maximization. Excessive timidity on the part of insurance company managers is a fact with which government programs must contend.

Ambiguity of Probabilities

It is very difficult to make a scientific prediction of the likelihood of a terrorism attack. This allows commentators to make whatever statement suits their own agenda. For example, William Frist, the former United States Senate majority leader in 2005 stated. „The greatest existential threat we have in the world today is biological... An inevitable bio-terror attack will occur at some time in the next 10 years."[1]

[1] „US Senate Leader Urges 'Manhattan Project' Against Bio-Terror Threat," Agence France Presse, January 27, 2005.

On the other hand, if future probabilities are determined by past frequencies, the probability of a major loss would seem to be quite small. As Mueller (2007) has pointed out

> „Even with the September 11 attacks included in the count, however, the number of Americans killed by international terrorism over the period [1975–2003] is not a great deal more than the number killed by lightning—or by accident-causing deer or by severe allergic reactions to peanuts over the same period. In almost all years the total number of people worldwide who die at the hands of international terrorists is not much more than the number who drown in bathtubs in the United States—some 300–400."

It is clearly very difficult to attach a precise number to the probability of attack. Thus this risk becomes 'ambiguous' in the sense of Ellsberg (1961). It is well known that insurers are 'ambiguity averse' see Hogarth and Kunreuther (1989), Kunreuther et al (1995), preferring to insure risks with known probabilities which are subject to actuarial calculation, to risks where it is difficult to attach likelihoods. As Kunreuther et al (op.cit.) noted, managers of insurance companies which face ambiguous probabilities demand a large premium over expected loss to write these lines. But, in the absence of price regulation, there is no reason why such larger premiums cannot be set. So again it is puzzling that insurers refuse to write any terrorism coverage at all.

What Should Governments Do?

Governments around the world have solved the problem of supporting their terrorism insurance markets in many different ways. In this paper we will not review these programs, but instead refer to OECD (2004) or Guy Carpenter (2007) for summaries of the various country initiatives.

Many of these programs share a common feature. Borrowing from programs designed to remedy the failure of natural catastrophe insurance markets, the government itself takes on the risk of the upper tail of the loss distribution. This in effect provides managers and owners of publicly traded insurance companies with a double protection.

In the first place, limited liability, by shifting the upper tail of the loss distribution to the other stakeholders in the company, already guarantees that shareholders can never lose more than 100 % of their equity investment. This is a very valuable protection for shareholders, and was a crucial contributor to the success of capitalist systems, Moss (2002). What government terrorism insurance programs provide is a second limit of liability, this time at a level

far smaller than the bankruptcy level as measured by the reserves of the insurance providers.

Clearly managers have it in their power to achieve this outcome themselves. All they have to do is limit the size of the total contracts which they write. However, this is a solution which insurers seen very reluctant to undertake on their own. But if governments legislate that private insurers can never lose more than $\$X$, where $\$X$ is low enough to guarantee that the company will remain in business, insuring terrorism loss seems again to become a viable business. Although shareholders are presumably aware that they may lose 100 % of their investment, managers will not take that risk and will write policies only if the maximum loss is a significantly smaller fraction than that.

In the US, private insurance markets are currently regulated by the Terrorism Risk Insurance Extension Act (TRIEA) of 2005. This Act expires in December 2007, but is widely expected to be extended for a further 7 years. The most important features of this Act are

1. Insurance against conventional terrorism losses (but not Chemical, Nuclear, Biological, or Radiological [CNBR] attacks) must be offered to all buyers of commercial property/casualty insurance.
2. The industry must meet a loss deductible of 20 % of previous year's direct written premiums.
3. Above this deductible the US Treasury will meet 85 % of losses, the insurance co-pay being 15 %.
4. Treasury payments up to $27.5b will be recouped by a levy on all relevant insurance lines.
5. Above $27.5b, Treasury payments may or may not be recouped.
6. Total losses to the industry are capped at $100b.

These provisions have been generally credited with reinvigorating the private market for terrorism insurance. Insurance broker Marsh Inc. (2006) reports that take-up rates for terrorism coverage—the percentage of firms buying the insurance—have increased significantly since 2003, when Marsh began tracking purchases made by clients. In 2003, only 27 percent of survey participants bought terrorism insurance but, according to the latest Marsh study of trends, in 2006, 59 percent of the 1,437 clients participating in the survey purchased the coverage.

On the other hand, the provision of subsidized government re-insurance with no up-front cost has effectively killed the private market re-insurance market. In testimony before the United States House of Representatives, Jacque Dubois, President and CEO of Swiss Re stated (2006)

„If terrorism risk lessens in the world, the need for a public-private backstop should also ameliorate. But absent these world improvements, Swiss Re does not see a time in the foreseeable future when frequency or severity of terrorism risk can be successfully modeled and underwritten."

However, Swiss Re is more than willing to re-insure earthquake risk, although for this risk the difficulties in modeling frequency and severity are just as large. The only obvious difference between terrorism risk and earthquake risk is that in the case of earthquake risk Swiss Re is not competing with a large agency (the US Treasury) which has set the effective price of re-insurance at zero.

This is not the place to go over the pros and cons of state intervention, though it does seem paradoxical that a Republican administration, dedicated to opposing state intervention in everything from health care to pensions, so willingly embraces the socialization of terrorism re-insurance. What does need to be pointed out is that nationalization of this industry is quite unnecessary.

As has been demonstrated in other catastrophe lines (for example, the state scheme for earthquake insurance in California, the California Earthquake Authority) all that is required to overcome private insurer's reluctance to write any line of insurance is a manageable cap on their total liability. The current cap on terrorism loss, $100b ($65b after tax) seems more than reasonable as a limit on liability, given that primary property/casualty insurers in the US have reserves in excess of $600b.

A case can therefore be made for the following program. Scrap all provisions of the Terrorism Risk Insurance Extension Act with one exception. Keep the cap on total liability at some manageable level. This minimal intervention has several advantages.

1. If losses are capped at a reasonable level, there seems no reason why CNBR losses cannot be added to the coverage which insurers must offer. Adding this risk cannot increase maximum loss, and although it increases the probability of loss, insurers can price this risk as a separate add-on, leaving it to the buyer to decide if they wish to purchase it.
2. If all other government support is removed, private re-insurers have an incentive to re-enter his market. This has the advantage that the financial expertise of re-insurers, particularly in the area of catastrophe bonds and other sophisticated capital market instruments, can be brought to bear on the terrorism insurance market.

On the other hand it must be noted that unless current legislation is changed, and this now seems unlikely, we can expect government provision of re-insurance in the US into the foreseeable future.

Special Problems of Terrorism Insurance in the US 1: CNBR Insurance

As we noted earlier, in the US firms are required to offer conventional terrorism coverage but are not required to offer CNBR insurance. This special treatment of CNBR loss is made possible by a specific clause written into the way the original legislation was worded. It does not seem to have been the intent of the legislation to exclude CNBR events, because if an insurer were to offer CNBR coverage, it would be treated by the Treasury in exactly the same way as conventional losses. However, private insurers view this form of loss as so unmanageable that even with the Treasury backstop, they have taken the opportunity afforded by the wording of the legislation to exclude it.

At the time of writing, it appears that if TRIEA is renewed (it expires on December 31, 2007) it will continue to allow firms to exclude CNBR risk. (An earlier attempt by the House of Representatives to make the offer of CNBR insurance mandatory was threatened with a presidential veto and now appears unlikely to be enacted)

Yet as noted above, there is no obvious reason why CNBR coverage should not be mandated. In both the United Kingdom and France, CNBR risk was originally excluded from the government insurance scheme, but in both countries it is now included. Since the federal government in the US is providing unpriced re-insurance to all comers, it would seem a very reasonable quid pro quo to require mandatory coverage of CNBR risk.

Special Problems of Terrorism Insurance in the US 2: Workers Compensation

Workers compensation insurance (coverage for employment related injuries) also poses special problems for terrorism insurance in the US. In the early 20th century workers struck an agreement with employers in which they gave up the right to sue for on-the-job injuries, but were in turn guaranteed that all employers would provide their workers with insurance (worker's compensation) against such losses. As part of this agreement, workers compensation insurance cannot contain any exclusions. Thus insurers who offer this line of insurance are de facto offering terrorism coverage including coverage against CNBR attacks. In the 9/11 World Trade Center

attack, some 11 % of losses ($3b in 2001 dollars) were due to workers compensation.

The fact that insurers willingly provide even CNBR coverage to this line again raises interesting questions of insurability. Presumably, by diversifying their loss portfolio, workers compensation insurers are able to provide CNBR coverage with manageable consequences for firm survival, but if this can be done for this line, why not for other lines involving terrorism risk? This question is explored further in Jaffee and Russell (forthcoming).

Conclusion

This paper has presented an overview of some of the issues raised by the failure of terrorism insurance markets in the US. There, as has been the case in a number of other countries, terrorism losses caused private insurers to declare terrorism an „uninsurable risk“ and led to a collapse of the terrorism insurance market. In order to support this market, the US government „socialized“ the terrorism re-insurance market providing unpriced re-insurance and capping losses at $100b. Originally this was done on a temporary 3 year basis, then it was extended for a further 2 years, and now it is likely to be extended for a further 7 years. Indeed it is seems quite possible that unpriced government re-insurance will become a permanent feature of the terrorism insurance landscape in the US.

Although this destruction of the private re-insurance market has drawn little attention, it clearly has consequences for the operation of the primary markets. The lack of actuarial pricing of re-insurance causes primary insurers to lower prices and in this way weakens the incentive to mitigate loss. Moreover, private re-insurers, having left this market, have no reason to use their financial expertise to develop innovative financial instruments such as terrorism cat bonds or indeed to give any thought to how to transfer this large risk to general capital markets.

As we have suggested, this outcome is quite unnecessary. The evidence suggests that insurers will remain in a catastrophic risk market if they can be given a guarantee that they will not be required to make a payout that threatens their viability. A cap on total losses in the region of the current $100b limit achieves this purpose.

More generally, by far the simplest way for governments to support any catastrophe insurance market is to accept the upper tail of the loss distribution and leave all other aspects of the insurance to the private markets. This would permit all the usual efficiencies of market solutions, while at the same time recognizing that terrorists do have the ability to inflict losses large enough to significantly erode the capital of the global insurance market.

Литература

[1] D. Ellsberg (1961), ‘Risk, Ambiguity, and the Savage Axioms’, *Quarterly Journal of Economics* (75), 643–669.

[2] R. Hogarth and H. Kunreuther (1989), ‘Risk, Ambiguity and Insurance’, *Journal of Risk and Uncertainty* (2), 5–35.

[3] H. Kunreuther, J. Meszaros, R. Hogarth, and M. Spranca (1995), ‘Ambiguity and Underwriter Decision Processes’, *The Journal of Economic Behavior and Organization* (26), 337–352.

[4] G. Carpenter (2007), ‘Global Terror Insurance Market’, `http://gcportal.guycarp.com/portal/extranet/popup/pdf_2007/GCPub/Terror%20Report%202007.pdf`.

[5] D. M. Jaffee and T. Russell (Forthcoming), ‘NBCR Terrorism: Who Should Bear the Risk?’ In Global Business and Terrorism, Harry Richardson, ed. Elgar.

[6] Marsh (2006), ‘Market Watch: Terrorism Insurance’ `http://global.marsh.com/news/articles/terrorism/documents/MarketwatchTerrorism2006.pdf`.

[7] D. Moss (2002) *When All Else Fails*: *Government as the Ultimate Risk Manager*, Harvard University Press.

[8] J. Mueller (2007), ‘Reacting to Terrorism: Probabilities, Consequences, and the Persistence of Fear’, `http://psweb.sbs.ohio-state.edu/faculty/jmueller/ISA2007T.PDF`.

[9] OECD (2004) Conference on Catastrophic Risks and Insurance, `http://www.oecd.org/document/34/0,2340,en_2649_34851_33753570_1_1_1_1,00.html`.

[10] Testimony of Jacques Dubois (2006), `http://financialservices.house.gov/media/pdf/092706jed.pdf`.

Направления действий страхового сообщества по профилактике рисков терроризма

И. Е. Осокина

Прежде всего, уважаемые коллеги, дамы и господа, хочу дать краткую информацию об организации, которую я представляю.

Российский Союз Автостраховщиков (РСА) представляет собой общероссийское профессиональное объединение страховых компаний, осуществляющих обязательное страхование гражданской ответственности владельцев транспортных средств (ОСАГО), которое было создано в соответствии с требованием Федерального закона № 40-ФЗ от 25.04.2002 «Об обязательном страховании гражданской ответственности владельцев транспортных средств».

Основными функциями РСА является формирование информационных ресурсов по ОСАГО, противодействие страховому мошенничеству, осуществление функций в рамках международных систем ОСАГО, а также осуществление компенсационных выплат и подготовка обоснований по тарифам.

Проблемы профилактики и борьбы с терроризмом, которые рассматриваются на нашей конференции, также затрагивают интересы всего страхового сообщества, в том числе и членов РСА.

20 декабря 2001 года шестью крупнейшими российскими страховыми компаниями РОСНО, ВСК, Ингосстрах, Росгосстрах, РЕСО-Гарантия, Интеррос-Согласие (Согласие) было подписано соглашение о создании Российского Антитеррористического Страхового Пула (РАТСП).

Целью создания такого страхового пула является страхование юридических и физических лиц, находящихся на территории Российской Федерации от риска гибели и убытков вследствие террористических актов.

В настоящее время РАТСП насчитывает уже 38 участников. Для реализации целей пула создается специализированный страховой фонд.

Важным антитеррористическим направлением в настоящее время является проведение профилактических мероприятий, где большую роль играет создание многоуровневой системы слежения, *основанной на современных технологиях*, *позволяющих исключить влияние* человеческого фактора.

Так, информационная система ОСАГО, создаваемая в соответствии с Постановлениями Правительства РФ № 567 от 14.09.05 и № 391 от 21.06.07 предусматривающая сбор, обработку и обмен информацией между государственными органами и страховщиками при осуществлении страхования по ОСАГО, может быть использована и в антитеррористических целях.

Например, очень интересен зарубежный опыт по установке автоматизированных систем контроля за дорожной обстановкой.

Во Франции действует полностью автоматизированная система, которая предусматривает:

- подготовку цифровых фотографий со стационарных и мобильных камер;
- дистанционную передачу в Национальный центр обработки информации;
- автоматическое считывание регистрационного номера с помощью оптической системы распознавания.
- автоматический запрос в Национальную регистрационную базу данных, а также подготовку и почтовую отправку извещений о штрафе владельцам автотранспортных средств.

Основой такой системы во Франции является Национальный центр обработки информации.

Он введен в действие в мае 2005 года с целью предоставления национальным и региональным государственным органам статистической информации о зафиксированных нарушениях в каждом округе и в стране в целом. Статистические данные, выданные информационным центром, используются в целях управления и обмена информацией.

В соответствии с решением Рабочей группы «Транспорт и дорожное хозяйство» российско-французского Совета по экономическим, финансовым, промышленным и торговым вопросам (СЕФИК) (17—19 октября 2005 года), по реализации совместных российско-французских инициатив по созданию системы автоматизированного контроля за соблюдением водителями скоростного режима на территории Российской Федерации, Российский Союз Автостраховщиков был определен координатором действий Рабочей группы по созданию системы автоматизированного контроля скоростного режима на территории Российской Федерации.

Учитывая зарубежный опыт по использованию автоматизированных систем, Российским Союзом Автостраховщиков в 2006 году был реализован проект РСА совместно с Минтрансом России по внедрению автоматизированной системы контроля за дорожной обстановкой на опытном участке федеральной трассы «М1 Беларусь».

Учитывая сложившуюся ситуацию на дорогах, Российский Союз Автостраховщиков видит целесообразность в реализации таких проектов на уровне регионов по установке средств фото-видео фиксации, электронных маячков с целью контроля за дорожной обстановкой.

РСА готов принимать участие в такого рода проектах и видит необходимость в первую очередь осуществлять их в проблемных регионах, например, в Южном федеральном округе и Московской области.

Реализация пилотных проектов в регионах позволит обеспечить решение целого комплекса задач, связанных с

- повышением безопасности на дорогах, включая проведение антитеррористических мероприятий;
- обеспечением контроля за дорожным движением;
- снижением аварийности и тяжести последствий ДТП;
- повышением эффективности взаимодействия спасательных служб на месте ДТП.

The U.S. Model for Terrorism Insurance: Analysis of the U.S. Model

J. E. Thomas

Annotation

After the September 11th terrorist attacks, the United States adopted the Terrorism Risk Insurance Act to provide a federal backstop to support the market for terrorism insurance. This program helped to reduce the price for terrorism insurance and increase its availability while using market mechanisms. Congress is now considering renewal of the act beyond 2007. This paper summarizes TRIA and outlines its primary strengths and weaknesses. It suggests that the program should be expanded to cover domestic terrorism and nuclear, chemical, biological and radiological risk. Structural problems in the program also should be addressed by preempting state price regulation and mandatory ensuing fire coverage. In addition, the insurer deductibles should be designed to more closely track the insurer's ability to pay claims rather than be based on a percentage of direct earned premium and should be set at a lower level to reduce the amount of risk being borne by primary insurers.

1. Introduction

The insurance industry was permanently changed by the terrorist attack on the World Trade Center on September 11, 2001. It was „the largest single insured event in history."[1] Depending on which estimate is used, the insured losses from the September 11 attack were at least *double* the next largest

Work on this paper has been influenced by work done by the author as the Reporter to the Task Force on Federal Involvement in Insurance Regulation Modernization for the Tort Trial and Insurance Practice Section of the American Bar Association. The author acknowledges the input and participation of Task Force members, which has influenced this paper, but the views presented here are his alone and not those of the Task Force or any other member of the Task Force.

[1] Jeff Woodward, *The ISO Terrorism Exclusions*: *Background and Analysis*, IRMI INSIGHTS, Feb. 2002, `http://www.irmi.com/insights/articles/woodward006.asp`.

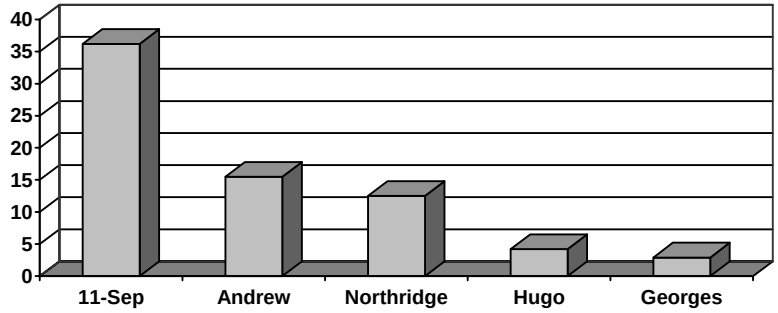


Рис. 1. Five Largest Single-Event Insurance Losses (in billions of dollars). Data for this chart comes from the Chief Economist of the Insurance Information Institute. *See* Hartwig, *supra* note 2

loss in history, and could be as much as *five times greater*[1]. The four next largest single-event losses were Hurricane Andrew (1992—$15.5 billion), the Northridge Earthquake (1994—$12.5 billion), Hurricane Hugo (1989—$4.2 billion) and Hurricane Georges (1998—$2.9 billion)[2]. The chart in Figure 1 shows the proportional differences between the five largest single-event losses in insurance history.

Significantly, the other large single-event losses were all natural disasters. Man-made disasters generally have not contributed to the industry's greatest losses. The two largest man-made disasters before September 11 caused damages of $3 billion (the 1988 explosion of the Piper Alpha drilling platform) and $2.9 billion (the 1989 explosion of a petrochemical factory in Texas)[3]. When comparing the size of losses from man-made disasters, the September 11th damages take on even greater significance. Damages from the attack were at least *ten times greater*, to as much as ***ten*** *times greater*, than the next largest man-made disaster[4]. The chart in Figure 2 illustrates the difference.

[1]Hurricane Andrew caused $15.5 billion in insured losses. *See* Robert P. Hartwig, *The Long Shadow of September* 11: *Terrorism & Its Impacts on Insurance and Reinsurance Markets*, Mar. 2002, `http://www.iii.org/media/hottopics/insurance/sept11/`. This is compared to $36 billion in insured losses for the September 11 attack. *See infra* note 6.

[2]This data comes from the Chief Economist of the Insurance Information Institute. *See* Hartwig, *supra* note 2.

[3]*See* Swiss Re, *Terrorist Attack in New York Causes Record Losses for Property Insurers in* 2001, Press Release, Dec. 20, 2001 (available at `www.swissre.com`).

[4]The damages of $3 billion, *see supra* note 3, were compared to between $36 billion in insured losses for the September 11 attack. Estimates of the insured losses from the Sept. 11th attack were from $30 million to as much as $90 billion, with consensus estimates in the range of $36–$54 billion. *See* Mark J. Warshawsky, Deputy Assistant Secretary for Economic Policy,

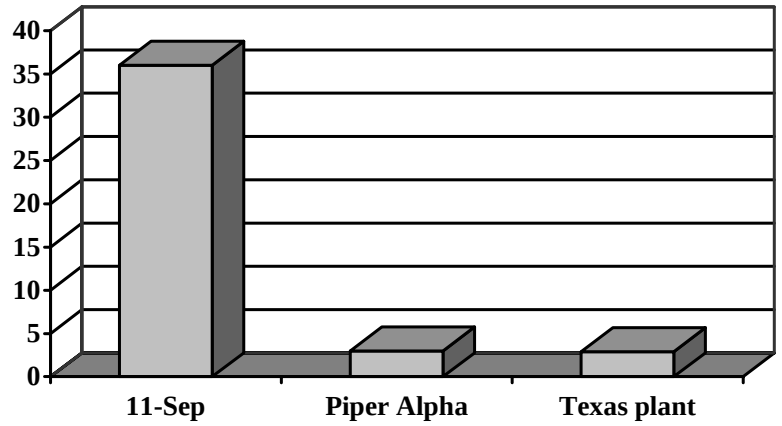


Рис. 2. Three Largest Man-Made Single-Event Insurance Losses (in billions of dollars)

Finally, not only were the losses extraordinary in their size, they were also widely distributed throughout the insurance industry. Although the property and casualty market bore a large proportion of the losses, substantial claims were paid for claims under workers compensation insurance, life insurance, and liability insurance. The Insurance Information Institute estimated the following distribution of losses: property insurance for the World Trade Center, 9 %; other property, 13 %; aviation hull, 1 %; business interruption, 26 %; event cancellation, 3 %; workers compensation, 10 %; life insurance, 16 %; aviation liability, 9 %; other liability, 13 %[1].

These figures begin to covey the significance of the insurance losses associated with the September 11 attack. Not only are these losses the largest in history for a single event, they are the largest by a factor of between three and five. In addition, they may be as much as thirty times greater than the next largest man-made loss in history. These enormous losses, while concentrated to some extent among property and casualty insurers, also affected other segments of the industry, notably providers of workers compensation and life insurance.

The attack radically altered the way the U.S. insurance industry perceives terrorist-related risks. Prior to the September 11th attack, terrorist-related losses were sufficiently small and infrequent that insurers did not take them

Testimony before the Financial Services Subcommittee on Oversight and Investigation, U.S. House of Representatives, February 27, 2002 (available online at 2002 WL 2011117).

[1]*See* Hartwig, *supra* note 2. It should be noted that these percentages are based on an estimate total loss of about $40 billion.

into account when underwriting risks[1]. The industry did not even conceive of an attack that could generate such astronomical losses[2]. Now insurers are keenly aware of real and potential losses and their inability to calculate the probable risk. As a result, most insurers consider terrorist risks „uninsurable" from an underwriting perspective[3]. They believe that uncertainty about the probability of a future attack and amount of damages that it could cause made it impossible to calculate an appropriate premium for such coverage[4].

Because insurers perceived terrorism risks as essentially uninsurable, the industry sought Federal legislative intervention. The industry wanted the Federal government to provide a „back-stop" to limit the potential impact of future catastrophic losses. Several different proposals were considered,[5] though only the House proposal made it to a vote in 2001[6].

When it became clear that Federal legislation assistance would not be adopted by the end of 2001, the industry began to exclude terrorism-related losses from coverage[7]. Reinsurers were the first to adopt such exclusions, in part because they bore about 2/3 of the losses from the September 11th attack[8]. Because reinsurers are international in character, conduct business world wide, and deal exclusively with sophisticated insurance companies rather than consumers, reinsurers are subject to more limited regulation and could adopt terrorism exclusions without governmental approval[9]. A majority of reinsurance contracts were renewed in January

[1] *See* MUNICH RE, 11TH SEPTEMBER 2001, §§ 3.3–3.4 (2001); Warshawsky, *supra* note 6.

[2] *See* MUNICH RE, *supra* note 8, § 3.4.

[3] *See* Warshawsky, *supra* note 6.

[4] *See* Richard J. Hillman, Terrorism Insurance: Rising Uninsured Exposure to Attacks Heightens Potential Economic Vulnerabilities, United States General Accounting Office Report, Testimony before the Subcommittee on Oversight and Investigations, Committee on Financial Services, House of Representatives, at 3, February 27, 2002 (available at `www.gao.gov`); *see also Terrorism Uninsurable*, INS. DAY, Feb. 21, 2002, at 1.

[5] *See*, *e.g.*, Stephen Labaton, *A Nation Challenged*: *The Legislation*; *House Committee Approves Measure to Aid Insurance Industry in Terrorist Attacks*, N.Y. TIMES, Nov. 1, 2001. P. B7; Stephen Labaton, *A Nation Challenged*: *The Aid Bill*; *White House and Key Senators Revise Proposal on Aid to Insurers*, N.Y. TIMES, Oct. 27, 2001. P. B1; Stephen Labaton with Jospeh B. Treaster, *Bush Details Plans to Help Insurers on Future Terror Claims*, N.Y. TIMES, Oct. 16, 2001. P. C1; Stephen Labaton with Jospeh B. Treaster, *A Nation Challenged*: *The Insurers*; *Government Role at Issue In Proposal to Help Industry*, N.Y. TIMES, Oct. 11, 2001. P. C4.

[6] *See Action on Legislation*, *Terrorism Insurance*, AMERICAN BANKER, Feb. 14, 2002 (available online at 2/14/02 Am. Banker 52002 WL 4100042).

[7] *See What Makes Terrorism Different*?, 23 VIEWPOINT № 3, Winter 2002 (available at `http://www.aais.org`).

[8] *See* Hillman, *supra* note 11, at 8.

[9] *See* Hillman, *supra* note 11, at 3-4.

2002,[1] and the great majority of them excluded coverage for terrorist-related losses[2].

The reinsurers' decision to exclude terrorism from coverage left the primary insurers bearing the risk of future terrorist attacks. Without reinsurance, a major loss from a terrorist attack could force many primary insurers into insolvency[3]. According to the National Association of Insurance Commissioners („NAIC"), a $25 million loss for a single primary property/casualty insurer in 2001 would have threatened the solvency of 886 companies, or 44 % of the companies writing commercial property/casualty insurance[4]. Consequently, the regulators endorsed a terrorism exclusion for commercial property/casualty insurers[5]. As of February, „45 states and the District of Columbia and Puerto Rico" had approved a standard terrorism exclusion drafted by the Insurance Services Organization,[6] which provides many standard form policies and endorsements used by the industry.

Because the reduced availability of terrorism insurance began to cause a „drag" on the U.S. economy,[7] Congress passed the Terrorism Risk Insurance Act („TRIA") of 2002. Although that Act was set to expire in 2005, Congress decided to extend it for two years. The extended act is now scheduled to expire in December 2007. Congress is starting to investigate long-term

[1] The majority of reinsurance policies expired in January, and by some reports could account for as much as 70 % of reinsurance. *See id.* at 4 n. 2.

[2] „Industry sources confirm that little reinsurance is being written today that includes coverage for terrorism." Hillman, *supra* note 11, at 4; *see also* Warshawsky, *supra* note 6 („the reinsurance industry has almost entirely stopped assuming terrorism risk"). This trend has been confirmed in surveys. The New York Insurance Department received responses from companies that represented 89 % of commercial insurance writings in NY state, and 83 % of those companies reported that their reinsurers were excluding or limiting coverage for terrorism. Gregory V. Serio, Testimony before the U.S. House of Representatives Committee on Financial Services Subcommittee on Oversight and Investigations, Feb. 27, 2002, at 20-1 (available at `www.ins.state.ny.us`). Similarly, the AAIS found that „[m]ore than 80 % of the 37 personal lines companies [surveyed] indicated that 'their current or upcoming reinsurance contracts exclude or in some way limit coverage for loss caused by terrorism."' American Association of Insurance Services, *AAIS Weighs Action In Wake Of NAIC Decision On Personal Lines Terrorism Exclusions* (available at `http://www.aais.org`).

[3] *See* Insurance Information Institute, Updates and Releases, *Terrorism Coverage is a Taxpayer—Not Insurance Company—Responsibility*, *Industry Forum Told*, Jan. 23, 2002 (available at `www.iii.org`); *California*, *New York take Big Risks on Terrorism Policies*, National Underwriter—Property Casualty, Jan. 24, 2002, at 24.

[4] *See* Hillman, *supra* note 11, at 17.

[5] *See* National Association of Insurance Commissioners, News Release, NAIC Members Come to Agreement Regarding Exclusions for Acts of Terrorism, Dec. 21, 2001 (available at `www.naic.org`, last visited 4-3-2002).

[6] *See* Hillman, *supra* note 11, at 5.

[7] *See* Joint Economic Committee of the U.S. Congress, *Economic Perspectives on Terrorism Insurance* (2002) (available from the Government Printing Office).

arrangements for terrorism insurance, which has generated considerable debate about the proper role of government in assisting the insurance market. The purpose of this paper is to describe and analyze the approach to terrorism insurance being taken in the U.S.

The paper will first summarize TRIA and the changes made when it was extended. It will then analyze the strengths of the approach, including some analysis of the effects that TRIA had on the insurance market. The next section will analyze several weaknesses of TRIA, including its limited scope and the structural features that interfere with its support for the market mechanism.

2. Summary of TRIA as Amended

The Terrorism Risk Insurance Act of 2002 created a Federal „backstop" for terrorism insurance. A „backstop" is a statutory mechanism to provide Federal financial support for payment of terrorism claims in the event of a fairly large terrorism incident. This financial support is similar to reinsurance in that it provides reimbursement to insurers[1] after they pay a certain amount of claims (a „deductable"). It is also similar to reinsurance in that insurers retain a proportion of the risk. But the „backstop" is different from reinsurance because insurers don't pay any premiums to be eligible and the government does not establish any reserves or „underwrite" particular risks or books of business. Instead, the costs of the program are borne by the government[2] with some or all of those costs subject to being recouped after the payments through a premium tax on property and casualty insurance.

The basic structure of the „backstop" is as follows. Insurers for those lines covered by the Act are required to „offer" coverage for terrorism on the same conditions as coverage under the policy. For those policies that policyholders choose to buy, the Act provides that the government will reimburse for terrorism losses once aggregate insured losses for a certified

[1] It should be noted that the Secretary of Treasury has authority to pay policyholders directly rather than reimbursing insurers, but that is likely to be an exceptional circumstance.

[2] TRIA covered commercial property and casualty insurance, including excess insurance, workers compensation insurance and surety insurance. It did not include Federal crop insurance, private mortgage insurance, financial guaranty insurance, insurance for medical malpractice, health or life insurance, flood insurance, or reinsurance. Terrorism Risk Insurance Act („TRIA") § 102(12). When TRIA was extended, the commercial automobile, burglary and theft insurance, surety insurance, professional liability insurance and farm owners multiple peril insurance were added to the excluded lines of commercial property and casualty insurance. (Terrorism Risk Insurance Extension Act („TRIEA") § 3).

event exceed $100,000,000[1]. After the triggering event, the government will pay 85 % of terrorism losses[2] for policies covered by the program in excess of 20 % of an insurer's direct earned premium for property and casualty insurance eligible for the program covering losses in the United States[3].

Payments by the Federal government are subject to being recouped from the industry by a premium tax on eligible property and casualty insurance. The Act requires a mandatory recoupment for amounts above the insurers' share and deductible up to a maximum of $27,500,000,000[4]. If aggregate insured losses exceed $27,500,000,000, while there is no mandatory recoupment, the Secretary of Treasury has discretion to recoup more than the mandatory amount, up to a maximum 3 % premium tax on property and casualty insurance[5]. While 3 % of premiums will not recoup a large loss in a single year, the duration of the tax is not specified in the Act, so the process of recoupment could continue for a number of years after the loss should the Secretary of Treasury require it. In exercising discretion for recoupment, the Secretary is to take various factors into account and may set different taxes for different lines of insurance or smaller policyholders[6]. The payments made by the Secretary of Treasury under the program are limited to no more than $100,000,000,000. If that amount is likely to be exceeded, the Secretary is to notify Congress, which is to determine the procedures for any sources of any additional payments beyond the $100,000,000,000[7].

3. Benefits of the TRIA Approach

The purpose of TRIA was to provide a backstop so that the insurance market would be better able to provide terrorism coverage. In general, TRIA has met its objective. This section will begin with a description of the increased availability of terrorism insurance after the adoption of TRIA, followed by an analysis of the justification for the government role in supplementing the usual market mechanisms. The next section will explain that TRIA, as amended, continues to support the operation of the insurance market for terrorism coverage. The final section will discuss the cost savings of the TRIA approach.

[1] TRIEA § 6.
[2] TRIEA § 4.
[3] TRIEA § 3; TRIA § 102(5)–(6).
[4] TRIEA § 5; TRIA § 103(e)(6)–(7).
[5] TRIA § 103(e)(7)–(8).
[6] TRIA § 103(e)(8)(D).
[7] TRIA § 103(e)(2).

3.1. TRIA increased availability of insurance

TRIA was adopted to provide a backstop so as to encourage insurers to participate in the market for terrorism insurance. After the adoption of TRIA, the price for terrorism insurance came down. In the first nine months after the adoption of TRIA, rates declined between 50 and 75 %, and they continued to fall in 2003. By the third quarter of 2004, the typical price for terrorism coverage was about 4 % of total premium for property coverage, compared to 10 % a year before[1]. As prices declined, more policyholders purchased terrorism coverage[2]. According to a study conducted by Wharton Risk Management and Decision Processes Center at the University of Pennsylvania, „about 50 % of commercial enterprises have purchased TRIA-line terrorism insurance."[3]

Under the present market circumstances the availability of terrorism insurance would have decreased if TRIA had been permitted to expire[4]. Although reinsurers have re-entered the market for terrorism risk, reinsurers have only indicated a willingness to provide up to approximately $5–6 billion in coverage[5]. This is only a fraction of the $27.5 billion industry aggregate in the current program year, and is less than one-fourth of the estimated $30 billion in individual insurer retentions. Survey data shows that reinsurers are not likely to significantly increase the coverage available for terrorism[6]. Without access to reinsurance or TRIA, if actions post-September 11 are any guide, many primary insurers would take actions to avoid underwriting terrorism risk. The Treasury Department study included a survey of insurers which found that nearly 50 % of insurers responding reported that they did not plan to write terrorism coverage if TRIA expired[7].

3.2. The Unique Nature of Terrorism Risk Justifies Governmental Involvement

Government involvement to make terrorism insurance more available is justified because of the unique nature of terrorism risk. Terrorism is more difficult to predict and model than other kinds of risks. Terrorism is perpetrated by human actors who have the intention of causing harm. In order to generate greater fear and alarm, terrorists may act in ways that are unexpected[1]. Although terrorists have sometimes attacked „hard" targets in the past because of their symbolic significance, terrorists are showing an increased willingness to attack „soft" targets with significant civilian exposures[2]. The religious or political fervor of some terrorists and their willingness to commit suicide is another consideration that makes it difficult to model or prevent terrorist behavior[3].

The challenge of modeling terrorist behavior is compounded by a lack of information. The historical data available on terrorism are limited because of a relatively few number of incidents, and the utility of the available data for those incidents is limited by the wide variety of cultural and operational contexts within which the events took place[4]. In addition, although much of the focus has been on al Qaeda after September 11, there are various terrorist organizations that have substantial differences in ideology, structure and methodology[5].

Moreover, much of the information about terrorism risk has been collected by governmental agencies, which are understandably unwilling to share that information because of national security and law enforcement concerns. The government also has a role in affecting the nature and scope of the risk through anti-terrorism and other policies. The government, the Federal government in particular, devotes substantial resources to combating terrorism, which may reduce or increase the risk of terrorism, or may have an impact on certain kinds of risks or risks in specific geographical areas. Because the risk of terrorism is a national security concern, a terrorist attack often can be interpreted as an attack on the country as a whole even though the attack may be harmful to many.

Another characteristic of terrorism risk is the variability of its impact. While much progress has been made in modeling the consequences of a terrorist attack, even with these models there are many different impact scenarios[6]. Although certain areas tend to present greater risk of terrorism, it is impossible to rule out any potential target. As some targets become more difficult to attack, it is possible that terrorists could switch to easier targets in less-protected locations. Nuclear, biological, chemical or radiological attacks could affect very large geographic areas and potentially millions of people,

[1] Chalk, Peter; Hoffman, Bruce; Reville, Robert; & Kasupski, Anna-Britt; *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act* (RAND Corp. 2005).

[2] Ibid.

[3] Wharton Risk Management and Decision Process Center, *TRIA and Beyond*, at 2 (Wharton School of Business 2005) [hereinafter Wharton].

[4] Chalk, et al., *supra* note 33, at 10; Wharton, *supra* note 35, at 168.

[5] Wharton, *supra* note 35, at 27.

[6] Ibid. at 27-28.

[7] U.S. Department of Treasury, *Assessment: the Terrorism Risk Insurance Act of* 2002, at 6 (2005).

[1] *See* Wharton, *supra* note 35, at 52-53.

[2] Chalk, et al., *supra* note 33, at 15-16.

[3] Ibid. at 26-29.

[4] *See* Wharton, *supra* note 35, at 58.

[5] Chalk, et al., *supra* note 33.

[6] *See* Wharton, *supra* note 35, at 56-59.

while attacks with conventional weapons could be limited to a single business or individual[1]. Some terrorist activity appears to be specifically aimed at the U.S. economy, which presents the possibility of attacks in more remote areas[2].

Taken together, these characteristics make terrorism very different from other kinds of risks and pose significant challenges for underwriting. The risk is so variable and difficult to predict that insurers and reinsurers are cautious about taking on that risk. In addition, because the size of the risk is so variable, it is hard to determine the amount of capital reserves that should be maintained for that risk[3]. Whatever those reserves, capital maintained for terrorism risk has an impact on other risks because that capital cannot be used to underwrite other, non-terrorism risks. By providing a source of capital for payment of claims in the case of a catastrophic terrorist attack, TRIA frees up some capital and reduces the exposure for insurers to a level that provides an opportunity for the market to function.

Because of the unpredictability of a terrorist attack and the amount of losses caused by such an attack, insurers who plan for the worst have an incentive to not insure terrorism events or to charge a high premium to reflect the unpredictability of a terrorism event. TRIA, by reducing the amount of risk to be borne by insurers, has helped stabilize the price for terrorism insurance. Without a federal backstop, it is expected that prices for terrorism insurance would increase[4]. From a theoretical standpoint, larger and more uncertain risks generally have higher prices reflecting the greater risk, so it is not surprising that terrorism insurance would be expensive. Competition provides an incentive to lower prices, but even competitive pricing for risks with high levels of unpredictability are likely to reflect a higher premium for the high risk.

3.3. TRIA Supports A Market Mechanism For Terrorism Insurance

Because insurers have substantial exposure even with the TRIA backstop, they still have market incentives. The insurer deductible is substantial, equal to 20 % of directed earned premiums, and insurers have a 15 % co-pay requirement after the deductible has been met. This encourages insurers to develop models that will help predict risks and potential losses from terrorism. In addition, TRIA does not regulate the price of terrorism coverage, so the Act does not interfere with the market mechanism for pricing

[1] *See* Chalk, et al., *supra* note 33, at 30-37; Wharton, *supra* note 35, at 50-51.
[2] *See* Chalk, et al., *supra* note 33, at 21-23.
[3] *See* Wharton, *supra* note 35, at 49-54.
[4] *See* Wharton, *supra* note 35, at 28.

insurance. (State regulators, however, retain some authority over pricing, which is a limitation of the Act discussed below.) Notwithstanding insurer contributions, the Federal government bears a significant portion of the loss if a major terrorist attack takes place. Depending on the size of the losses, some or perhaps all of the government payments made under TRIA would be recouped through post-event surcharges. But the availability of federal funds reduces the catastrophic front-end risk to insurers, which gives market forces greater capability to function for the remaining risk. Because the catastrophic risk is backstopped by the Federal government and would be spread to the industry through the post-event mechanism, insurers are more willing to put capital at risk while still retaining capital for other kinds of risks (such as natural disasters). As a result, TRIA makes more capital available in the insurance market for terrorism insurance.

TRIA also supports the affordability of terrorism insurance in the market. By reducing the amount of front-end capital at risk, insurers have greater capacity to offer terrorism insurance at lower prices. In addition, while TRIA does not mandate the price for terrorism coverage, it does require that participating insurers offer such coverage. The combination of a reduction in an insurer's capital at risk, the requirement of mandatory offering, and competition to satisfy policyholders who were purchasing property and other insurance products, encouraged lower prices for terrorism insurance. As explained above, prices for terrorism insurance decreased after the adoption of TRIA.

By improving availability of terrorism insurance, TRIA has encouraged pre-event planning rather than reliance on after-event ad hoc governmental assistance for victims. Insurance offered before an event creates an opportunity for risk assessment and management, and market forces create an incentive to take advantage of such opportunities. On the other hand, a mechanism that operates primarily after the event, such as government aid for victims of terrorism, may work against market incentives. If potential victims rely on the government to provide aid after the fact, they may not have incentives to assess and manage their risks. The government, as the provider of the assistance, has an incentive, of course, but this is not reliance on the market. By encouraging availability and use of terrorism insurance, TRIA provides opportunities to use market incentives for assessing and managing terrorism risk.

3.4. The Costs Associated with TRIA Have Been Low

The final benefit of the TRIA program is that it has provided backstop benefits at a minimal cost. This, of course, is because the United States

has not been subjected to another major terrorist attack within it borders. Nevertheless, the cost has been much lower than if the U.S. had created a true reinsurance mechanism similar to Pool Re.

If, or perhaps when, a terrorist attack takes place, the cost will be greater, but if the government pays no more than $27.5 billion, the costs will be recouped through post-event premium taxes. Even if the government bears a significant part of the losses, insurers are partners with the government and would bear a portion of the losses. Considering that the government is likely to step in with assistance after an attack, as it did with the 9/11 Victims Compensation Fund and as it has after natural disasters, society and the economy may as well have the benefit of that commitment prior to the event. Moreover, supporting terrorism insurance has the additional benefits of having insurers at least bear a portion of the losses and of using the insurance underwriting and clams-adjusting apparatus, rather than having to distribute assistance through a new or ad hoc government assistance mechanism.

An additional advantage of the TRIA mechanism is that recoupment is likely to result in more accurate pricing for insurance coverage. Because it is so difficult to predict the likelihood or the cost of a terrorist attack, it is very difficult to calculate an actuarially correct premium. The premium is likely to be either too high for the risk, or too low, but is not very likely to be just right. The TRIA mechanism, but providing the back-stop at the front end without any cost, and then recouping the costs after the fact will allow a more accurate calculation of costs because they will be based on what actually happened, not what was predicted. Whether the full cost will be recouped, of course, depends on the amount of the costs (whether it is $27.5 billion or less and subject to mandatory recoupment) and the decision of the Secretary of Treasury to recoup discretionary costs, but at least there is will be more accurate information after the event and, if the government finds that the economy can support it, the appropriate amount of money can be collected through the premium surcharge.

4. Problems with the TRIA approach

Although TRIA has been successful in reducing the price of terrorism insurance and in increasing its availability, the Act has several limitations. Those limitations have not caused any significant problems yet because there has not been a major terrorist attack in the United States. But certain kinds of attacks could demonstrate the limitations of the Act. The problems with TRIA can be grouped into two categories: 1) limitations on the scope of TRIA coverage, and 2) structural problems with TRIA. We will consider these below.

4.1. Scope problems

TRIA has three principle limitations in its scope of coverage. First, it is limited to international terrorism that causes injury within the United States. Second, TRIA is limited in the lines of insurance that it covers. Third, TRIA does not cover nuclear, biological, chemical or radiological losses.

Limitation on Domestic Terrorism

By the statutory definition of terrorism in TRIA, domestic terrorism is excluded from the scope of coverage. Terrorism is defined as a violent act or an act dangerous to life, property or infrastructure that resulted in damage in the U.S.[1] that was committed „by an individual or individuals acting on behalf of any foreign person or foreign interest, as part of an effort to coerce the civilian population of the U.S. or to influence the policy or affect the conduct of the U.S. Government by coercion."[2] It is up to the Secretary of Treasury to decide and certify whether a terrorist act has taken place. This decision is not subject to appeal[3].

The statutory definition of terrorism has created a sizable coverage gap for domestic terrorism and for international terrorism that causes damage overseas. Although some insurers are selling domestic coverage without TRIA support, about 25 % of those who buy TRIA-eligible terrorism insurance do not buy coverage for domestic terrorism[4]. The absence of the TRIA backstop for this coverage also creates an elevated risk of insolvency for insurers in the event of a major domestic terrorist attack[5].

Although limiting coverage reduces the program's financial exposure, distinguishing between domestic and international terrorism for purposes of a federal backstop for insurance is not justified and the boundaries of this distinction are elusive[6]. Domestic terrorism has many of the same characteristics as international terrorism and therefore presents similar challenges for insurers trying to underwrite it. Although September 11th was an incident of international terrorism, the Oklahoma bombing, a domestic incident, was

[1] Including an air carrier or vessel or a U.S. mission.
[2] TRIA § 102(1)(A)(iv).
[3] Ibid.
[4] Congressional Budget Office, *Federal Terrorism Reinsurance: An Update*, at 7 (GPO January 2005).
[5] Chalk, et al., *supra* note 33, at 53.
[6] Ibid. at 52-53.

the second or third most damaging terrorist incident in the United States[1]. Domestic terrorism continues to be a serious threat in the U.S.[2]

Moreover, determining whether an event meets the TRIA definition of terrorism may be difficult, as shown by both the anthrax incidents in 2001 and the London bombings in 2005. The culprits of the anthrax incidents have not been identified. As a result, we do not know whether the culprits had a sufficient relationship to an international terrorist organization to satisfy the TRIA definition. Similarly, although the culprits of the London bombings have been identified as British citizens apparently sympathetic to al Qaeda, it is unclear whether this connection is direct enough to satisfy the definition.

TRIA gives the Secretary of the Treasury the responsibility for determining whether an event falls within the TRIA definition of terrorism, which avoids some of the transaction costs associated with the determination. TRIA, however, does not impose a deadline or otherwise place parameters on the certification decision. Because of the significant risk of terrorism from within the United States and the difficulty of determining whether an event was by an international terrorist organization, there are good reasons to extend the scope of TRIA coverage to include domestic terrorism.

This distinction between domestic and international terrorism is very likely to be eliminated after 2007. Both the House and Senate bills that were recently passed eliminate the distinction, so it is likely that what ever legislation is ultimately adopted will address this limitation.

Limitations on Covered Lines of Insurance

Although differences in the lines of insurance and the way that terrorism impacts certain lines may warrant different treatment, one of the limitations of TRIA is that it does not cover all lines of insurance that are at risk of terrorism losses. TRIA initially covered commercial property & casualty insurance, including workers compensation and automobile coverage. Health and life insurance, including group life, were not covered. The extension of TRIA omitted commercial automobile, burglary and theft, surety coverage, professional liability, and farm owners multiple peril insurance, and specifically included directors and officers' liability. Health and life insurance, including group life, and personal automobile and homeowners coverage continue to be outside the scope of TRIA.

Heath and Life Insurance. The exclusion of health and life insurance creates a gap in the coverage provided by TRIA. Terrorism risk is significant for group life, disability, accident and health insurance. The September 11th attack generated $1 billion in losses for life insurers[1]. A nuclear, chemical, biological or radiological attack could substantially increase such losses. In addition, because group life insurance policies are sold to groups of employees, they present a concentrated risk that could magnify the impact of a terrorist attack for a single carrier. For example, a group life insurance policy may be sold to a company with the underwriting expectation that just a few people will die in any given year. A terrorist attack, however, could dramatically alter that risk so that hundreds or even thousands of people in the group would die at the same time. Because of the significant risk, the difficulty in predicting terrorism, and the concentration of that risk with large insurers, the exclusion of life insurance is a limitation of TRIA.

Group life, disability, accident and health insurance all service an important public interest of providing resources to sick and injured individuals, their families, and the survivors of those who die. Because such resources are provided through a private market mechanism, the availability of such insurance helps to reduce the demands on government programs, funded through taxes, which may otherwise be called upon to provide support.

While the level of risk is significant for these kinds of insurance, the Treasury Department chose not to include group life insurance in TRIA because it found that group life insurers continued to offer insurance after the September 11th attacks[2]. Thus, it may be that the risk to these lines of insurance is not so high as to create difficulty in providing sufficient capital to underwrite the risk.

Auto and Homeowners. Terrorism is a significant risk for auto and homeowners insurance as well. After September 11th, claim were paid on auto and homeowners insurance policies, but the total losses associated with those lines of insurance has not been calculated separately, and therefore may not be of a sufficient size to warrant including these lines of insurance in TRIA coverage. Like life insurance, auto and homeowners insurers have not sought to exclude terrorism from those lines. But unlike group life, auto and homeowners insurers tend to avoid the concentration of losses. Although a large number of cars or homes might be damaged by a terrorist attack,

[1] Whether it is second or third most damaging depends on what is considered. The World Trade Center garage bombing in 1993 caused more losses in terms of costs ($725 million compared to $145 million), but the Oklahoma City bombing killed many more people (166 compared to 6). Zanetti, Auriela, et al., *Natural Catastrophes and Man-Made Disasters in* 2001: *Man-Made Losses Take on a New Dimension*, sigma №1. P. 17 (Thomas Hess, ed., Swiss Re 2002).

Moreover, even when one considers terrorism events around the world, the Oklahoma bombing was the eighth most costly and the sixth most deadly in history. *Id.*

[2] Chalk, et al., *supra* note 33, at 39-52.

[1] Wharton, *supra* note 35, at 44.

[2] Wharton, *supra* note 35, at 17.

the distribution of the insurance losses from the damage to those properties is likely to be more random. While these policies face the risk of terrorism losses, the risk has been considered low enough that the market is still willing to underwrite such coverage in these lines of insurance. Because of the nature of terrorism, however, and the risk that an even larger loss might be caused by terrorism in the future, there may be benefits to including these lines in TRIA. If TRIA were expanded to cover nuclear, chemical, biological or radiological risks, losses could be so great and could affect such a large number of consumers that absence of a Federal backstop could be a significant limitation.

Limitation on Nuclear, Chemical, Biological and Radiological Coverage

A final significant limitation is the absence of applicability to nuclear, chemical, biological, and radiological (sometimes referred to as „NCBR“) attacks. At the present, there is little insurance coverage available for such attacks. Although TRIA requires that insurers offer terrorism insurance to their policyholders, they are only required to offer terrorism insurance on the same terms and conditions as property and casualty coverage for non-terrorism losses[1]. Because most property insurance policies have long specifically excluded losses from nuclear events and for release of contaminants, which would likely exclude coverage for chemical, biological and radiological materials, TRIA does not require terrorism insurance to cover such events[2].

The absence of coverage for NCBR attacks represents a significant gap in insurance coverage for terrorism. The use of NCBR materials for a terrorist attack is a serious risk. According to RAND, „al Qaeda has long expressed an interest in the offensive employment of NBCR materials.“[3] Although al Qaeda has yet to demonstrate any such capability in an actual attack, they have made efforts to develop it[4]. Models have shown that a large-scale biological attack, such as with anthrax, could generate as much as $90 billion in losses[5]. Nuclear or radiological attacks could have an even more severe impact. A „dirty bomb“ could contaminate an area

[1] TRIA § 103(C)(1).

[2] Chalk, et al., *supra* note 33, at 6-7; Wharton, *supra* note 35, at 81. It should be noted that workers compensation insurance is a notable exception to this because of the mandatory scope of coverage of workers compensation insurance. Wharton, *supra* note 35, at 81.

[3] The RAND study cites a news interview of bin Laden in which he „specifically asserted that acquiring weapons of mass destruction (WMD) was a religious duty for all Muslims.“ Chalk, et al., *supra* note 33, at 30.

[4] Ibid. at 31-32.

[5] Wharton, *supra* note 35, at 50.

as large as ten square miles requiring demolition on a massive scale and astronomical losses. The RAND study concluded that the „most profound risk“ of uninsured losses is in the area of a NCBR attack[1]. There failure to address NCBR risk in TRIA is therefore a significant limitation.

It is possible, though at this point unlikely, that legislation extending TRIA past 2007 will address this limitation. The House legislation proposes a mechanism to address NCBR risk on terms similar to conventional terrorism risk, but the Senate legislation does not include any similar provision. Moreover, the President has made clear his preference for the Senate version and the White House has threatened to veto legislation that expands TRIA beyond the Senate version.

4.2. Structural Problems

The second set of problems of TRIA arise from the way the program and the statute is structured. The first problem is that the statute did not do enough to pre-empt state insurance regulation, which undermines the ability of the program to support a market mechanism for terrorism risk. Secondly, the way insurer deductibles are set may prevent TRIA from meeting its objective of maintaining insurer solvency in the event of a major terrorism loss.

Failure to Pre-empt State Insurance Regulation

Insurance regulation is done primarily at the state level in the United States, resulting in 50 different regulatory systems applicable to insurance. Although the Federal government has the authority to regulate insurance if it chooses to, since the 1940's the Federal government has tended to stay out of insurance regulation. TRIA is a federal statute, and it pre-empts or overrides state regulations that are inconsistent, but the way it was structured allows some state regulation of terrorism insurance to continue in the areas of pricing and with regard to the required coverage for ensuing fires.

Price Regulation. TRIA is designed to provide support for the market mechanism, not to displace it. One of the primary characteristics of a market mechanism is the ability to change prices according to market circumstances. In recognition of this principle, TRIA did not set a price for terrorism insurance. At the same time, however, TRIA did not completely preempt the state regulation of insurance premium rates. Instead, for the first year TRIA preempted the states' prior approval of rates (and any applicable „waiting period“), but allowed states to invalidate rates as excessive, inadequate, or

[1] Chalk, et al., *supra* note 33, at xii.

unfairly discriminatory on subsequent review of the rate[1]. Thus, while federal law did not regulate pricing of terrorism insurance, state regulations continue to apply.

The Insurance Services Office developed a methodology to price terrorism risk, and suggested that a price of $0.10 per $100 of value for property coverage would be appropriate in high risk cities. Regulators in New York and District of Columbia, however, approved $0.03 and $0.018, depending on the property[2]. Other states have taken other approaches that have kept down the rates for terrorism insurance[3]. Regulators have taken a similar approach to the suggested pricing model developed for workers compensation coverage[4]. None of the states has adopted pricing at the level that was suggested by the Insurance Services Office. Some states used regulatory authority to lower the price requested by insurers, while others used their regulatory power to negotiate adjustments to the proposed pricing model[5].

Although lower rates in some states may improve access and the willingness of policyholders to buy terrorism coverage, they create inequity from state to state. For example, suppose that state *A* permits pricing at 30 % of an appropriate premium, while state *B* allows a premium at 100 %. This is inequitable because companies in state *A* would be forced to bear the same or even higher terrorism risk for premiums that are lower than what was approved in state *B*. In addition, if the same company does business in both states, it might seek approval for even higher premium in state *B* to make up for the artificially low premium in state *A*.

This inequality may be magnified after a terrorism event by the operation of the post-event recoupment surcharges. The surcharges apply to total premiums, which would include the portion for terrorism, so policyholders in state *A* in the example would pay a lower surcharge than that paid by policyholders in state *B*. The inequity of this distribution would be especially unfair if the terrorist event was only in state *A*, in which case the higher surcharges in state *B* would subsidize the payment of benefits to insurers in state *A*.

This state rating regulation also makes it more difficult for insurers to charge an appropriate premium. Theoretically, the premium charged for any particular risk should reflect the level of that risk. If approved premiums are artificially too low, then insurers are less able to develop the capital necessary to pay claims in the event of an insured loss.

[1] TRIA § 106(a)(2)(B).

[2] American Insurance Association, *How the Free Market Fails* (April 2005).

[3] Ibid.

[4] Ibid.

[5] Wharton, *supra* note 35, at 84-88.

Another consequence of state pricing regulation is that it interferes with the development of the reinsurance market. When state regulators require that premiums be less than the market price, insurers find it more difficult to purchase reinsurance, which is subject to no price regulation and therefore reflects the market price. Where the primary insurance is priced below market, insurers may not be able to afford reinsurance. In addition, some reinsurance is priced according to a percentage of the premium for the primary insurance, and reinsurers sometimes refuse to provide reinsurance unless the primary insurance is priced higher. There is some evidence that the pricing for primary terrorism coverage is interfering with development of the reinsurance market. The Wharton study found that „there is relatively little private insurance to cover portions of losses below the TRIA deductible in urban areas and/or the price of reinsurance is prohibitively high relative to the premium that insurers can charge for coverage to commercial firms."[1]

State price regulation also reduces the flexibility of terrorism insurance pricing, which reduces the ability to use market incentives for risk assessment and management. Market pricing allows differentials for efforts to mitigate or reduce various risks. Although regulated prices can also recognize such differentials, it is difficult to develop such differentials if regulation makes prices artificially low. In addition, it can be difficult and time consuming to get approval for price differentials, which makes them more cumbersome and less responsive to the market forces.

Mandatory Coverage for Ensuing Fires. Another form of state regulation that interferes with the ability of market forces to function for terrorism insurance is the requirement for ensuing fire coverage. At the time of the September 11th attacks, 29 states required commercial property insurance to conform to the coverage of the so-called „standard fire insurance policy."[2] This mandates that property insurance provide coverage for fires that ensue from a terrorist event even if other damages from the terrorist events are specifically excluded by the policy[3]. After TRIA was adopted, twelve states modified their statutes to exclude in various ways ensuing fire coverage caused by acts of terrorism[4]. This leaves ensuing fire coverage for terrorism events mandated in 17 states.

Such mandated coverage raises concerns similar to those of pricing regulation. Insurers in states with the mandate are forced to provide terrorism

[1] Wharton, *supra* note 35, at 19-20.

[2] Wharton, *supra* note 35, at 85.

[3] New York State Insurance Department, *General Counsel Opinion Regarding Commercial Property Insurance Terrorism Limitation for Fire Following*, June 26, 2003, available at `http://www.ins.state.ny.us/rg030627.htm` [last visited Nov. 4, 2005].

[4] Wharton, *supra* note 35, at 85. Amendments are under consideration in additional states.

coverage. This means that those carriers may be at a comparative disadvantage to those selling insurance in other states where terrorism coverage is more easily priced separately. This raises the same problems as explained above: it is inequitable to insurance carriers because some may be more able to collect a premium for terrorism coverage compared to others; it reduces the ability of insurers to buy reinsurance for the terrorism risk mandated by the ensuing fire provisions; and it limits the flexibility of insurance pricing which reduces the effectiveness of market incentives for risk management.

The Structure of Insurer Deductibles

Insurer deductibles in TRIA are set as a percentage of direct earned premium, which does not have very much relationship to the insurer's ability to pay. In addition, the levels of the retentions are so high that they create a risk of insurer insolvency. The deductibles represent that portion of terrorism risk borne directly by insurers. Ideally, the deductibles should be set high enough to create an incentive for insurers to take measures to reduce the risk of loss and to buy reinsurance, but low enough that there is not too great a risk of insurer insolvency in the event of a terrorist event. If insurer deductibles are set too high, they may create a significant risk of insurer insolvency in the event of another major terrorist attack. If retentions are set too low, the government bears more risk than is necessary and insurers may not have a sufficient incentive to develop the reinsurance market for terrorism insurance.

Although direct earned premium has some bearing on the ability of an insurer to bear a loss, it is only one part of the financial condition of an insurer. Factors that affect the financial condition of the insurers include: the price they can charge for terrorism and other insurance, the level of surplus capital, capital reserves required for other kinds of risks, and the returns on insurers' investments. The deductibles should also take market circumstances for terrorism reinsurance into account. Availability of reinsurance strengthens the ability of primary insurers to pay claims up to the retention levels. But if the retentions are too low, insurers will not have an incentive to buy reinsurance, which will inhibit the development of the reinsurance market. Thus, the correct level of retention requires a balance between reducing the retained risk to an acceptable financial level, on the one hand, while leaving enough risk to maintain an incentive to develop the reinsurance market on the other.

Present information suggests that approximately $5–6 billion of reinsurance capital is available for terrorism coverage at this time[1]. It is unclear how

[1] *See supra* note 37.

quickly that market will grow, but even it grows by 60 %, only about $10 billion in capital would be available at that time. This suggests total deductibles for insurers should come to a figure somewhat above $6 billion. Although total deductibles above the available reinsurance capital will help to promote market demand for reinsurance, at some level, depending on some of the other factors discussed above, they also a risk of insolvency for insurers.

The insurer deductibles should also take surplus capital into account. Surplus capital is a reflection of the ability of an insurer to pay claims without becoming insolvent. Certain lines of insurance and some companies may have more capital available than others, and surplus may be affected by the payment of, or reserves for, non-terrorist claims, such as those from hurricane losses.

To account for the multiplicity of possible risks, rating agencies generally require that no single risk account for more than 10 % of an insurer's surplus. Because TRIA uses direct earned premiums to calculate retentions and does not consider surplus, it may not sufficiently protect against insolvency. The Wharton study analyzed the impact of TRIA deductibles on company surplus and found that the 2005 deductibles (15 % of direct earned premiums), would amount to less than 10 % of surplus for only 139 (or about 30 %) of the top 451 insurers[1]. Deductibles represented 15 % or more of surplus for 172 of the 451 insurers (or about 38 %)[2]. The Wharton study also made projections of the impact of deductibles on surplus for 2006 and 2007 for the 30 largest insurers. It found that a 15 % deductible of direct earned premiums would likely exceed 10 % of surplus for 14 out of the largest 30 insurers, and when the deductibles are moved up to 17.5 % and 20 % of direct earned premium, 8 insurers out of the top 10 and 18 out of the top 30 would exceed 10 % of surplus[3]. These figures suggest that the deductibles are too high and that it might be more sensible to based them on surplus rather than direct earned premiums.

5. Conclusion

TRIA has been successful in reducing the price for terrorism insurance and increasing its availability through the backstop mechanism. The terrorism risk is so hard to predict and underwrite that government involvement in the market is justified. The combination of mandatory offering and providing a „backstop" to help finance the payment of major losses from a terrorism

[1] Wharton, *supra* note 35, at 96.
[2] Ibid. For 80 insurers the 2005 deductibles represent between 10–15 % of surplus. Ibid.
[3] Ibid. at 126-27.

attack supports market mechanisms. It also creates the benefits of insurance for terrorism at a relatively low cost.

Notwithstanding these benefits, TRIA has some weaknesses that should be addressed as an extension or a new measure is considered. The scope of TRIA should be extended to include domestic terrorism nuclear, chemical, biological, and radiological risks. The government should also consider whether to extend the TRIA program to other lines of insurance. TRIA also has several structural problems that should be addressed. Its effort to support a market-based structure is limited by the fact that states continue to regulate terrorism insurance, and, in particular, the price. A number of states also have mandatory ensuing-fire coverage for property insurance, which makes it difficult for insurers to separately underwrite terrorism risk. The most serious structural limitation is the use of the direct earned premium formula for the insurer deductible, which is not an accurate determinant of an insurer's ability to pay. The current insurer deductible of 20 % of direct earned premiums creates serious risk of insolvency for insurers. At this insurer deductible, 60 % of the top 30 insurers face exposure beyond the 10 % of surplus level recommended by rating agencies as permissible level of risk. Smaller insurers have considerably less surplus, and so face even greater risk. Although the reinsurance market can help to address some of that risk, current information suggests that available reinsurance will be far short of the risk being borne by insurers due to current deductibles.

Методические основы страхования риска террористического акта

И. Б. Котлобовский

Страхование как метод управления рисками способствует защите имущественных интересов предприятий и граждан, безопасности и стабильности предпринимательства. Исторически страхование развивалось, начиная с очень простых форм раскладки убытка между несколькими участниками рискованных предприятий, например: перевозки товара. Позднее стали возникать простейшие виды страхования — кредитное, морское, огневое и т. д.

Современная страховая индустрия насчитывает тысячи видов страхования и откликаясь на вызовы времени и запросы потребителей, создает все новые и новые страховые продукты. К таким относится и страхование риска террористического акта.

Террористические риски некоторые специалисты относят к числу «нестрахуемых», однако в силу того, что первоначально они не приводили к катастрофическому ущербу, страхование риска терроризма развивалось как нагрузка к имущественному страхованию.

Переосмысление роли страхования террористических рисков и необходимости взаимодействия государства и бизнеса по противодействию террористическим рискам и возмещению возможного ущерба произошло после событий 11 сентября 2001 года в Нью-Йорке и Вашингтоне.

О социальной значимости проблемы можно судить по данным института социологии РАН:

- 24 % граждан убеждены в том, что суть терроризма состоит в порождении страха у всего общества;
- 13 % граждан считают, что суть терроризма — в устранении политических, идеологических и религиозных противников.

Совершение теракта в том месте, где они живут, считают:

- возможным — 54 % опрошенных;
- маловероятным — 38 %;
- практически невозможным — 8 %;

- 15 % опрошенных считают, что они сами или члены их семей могут оказаться жертвами терактов;
- 74 % опрошенных ощущают свою беззащитность перед угрозой терроризма.

К настоящему времени накоплен значительный международный опыт страхования террористических рисков[1]. В РФ в декабре 2001 г. создан антитеррористический страховой пул (РАТСП), объединяющий около 30 страховых компаний и заключающий ежегодно около тысячи договоров на страхование риска терроризма.

Однако, до сих пор многие вопросы страхования риска «террористический акт» не проработаны в методическом плане.

I. Для начала следует дать точное определение террористического акта, которым должны руководствоваться страховщики и органы управления, осуществляющие регулирование и надзор за страховой деятельностью.

В качестве такого определения можно взять формулировку из Федерального закона «О противодействии терроризму» от 6 марта 2005 г.:

> *террористический акт* — совершение взрыва, поджога или иных действий, связанных с устрашением населения и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления экологической катастрофы или иных особо тяжких последствий, в целях противоправного воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, а также угроза совершения указанных действий в тех же целях.

II. Далее нужен анализ статистики произошедших террористических актов. В табл. 1 приводится рейтинг самых крупных террористических актов на территории России (1993—2004).

Таблица 1:

№	Дата, место	Событие	Жертвы
1	14—19 июня 1995 г., г. Буденновск, Ставропольский край	Захват чеченскими террористами заложников и удержание их в больнице в течение шести дней.	Погибли 129 чел., были ранены 415 человек.

[1] См., например: Terrorism Risk in Property Insurance and Their Insurability after 11 September. 2001/Sigma. 2003. № 1; *Турбина К. Б., Мальковская М. А.* Организация страховой защиты на случай терроризма // Финансы. 2004. № 7.

Таблица 1 (продолжение)

№	Дата, место	Событие	Жертвы
2	9 января 1996 г., г. Кизляр, Дагестан	Захват больницы г. Кизляра чеченскими сепаратистами под руководством Салмана Радуева. В заложниках удерживались около 3000 чел.	Погибли 78 человек, были ранены несколько сотен.
3	16 ноября 1996 г., г. Каспийск, Дагестан	Взрыв девятиэтажного жилого дома для семей офицеров.	Погибли 68 человек.
4	19 марта 1999 г., г. Владикавказ	Взрыв на Центральном рынке.	Погибли 52, были ранены 168 человек.
5	4 сентября 1999 г., г. Буйнакск	Взрыв пятиэтажного жилого дома.	Погибли 62 человека, 146 были ранены.
6	8 сентября 1999 г., г. Москва	Взрыв девятиэтажного жилого дома по ул. Гурьянова.	Погибли 92 (94) человека, 164 были ранены.
7	13 сентября 1999 г., г. Москва	Взрыв восьмиэтажного жилого дома на Каширском шоссе.	Погибли 124 человека, 18 были ранены.
8	16 сентября 1999 г., г. Волгодонск	Взрыв девятиэтажного жилого дома.	Погибли 13 (18) человек, 28 (более 130) были ранены.
9	8 августа 2000 г., г. Москва	Взрыв в подземном переходе на Пушкинской площади.	Погибли 13 человек, были ранены 118 человек.
10	9 мая 2002 г., г. Каспийск, Дагестан	Подрыв фугаса на праздничном параде, посвященном Дню Победы.	Погибли 44, были ранены более 100 человек.
11	23 октября 2002 г., г. Москва	Захват около 800 заложников в Театральном центре на Дубровке во время представления мюзикла «Норд-Ост». Теракт осуществили более 50 чеченских боевиков, среди которых было 18 женщин.	Погибли 129 заложников.
12	27 декабря 2002 г., г. Грозный	Автомобили «КамАЗ» и «УАЗ» с террористами-смертниками за рулем взорвались напротив Дома Правительства Чечни.	Погибли 72, были ранены 110 человек.

Таблица 1 (продолжение)

№	Дата, место	Событие	Жертвы
13	12 и 15 мая 2003 г., с. Знаменское Надтеречного района и с. Белоречье Гудермесского района Чечни	Взрыв у зданий администрации и УФСБ.	Погибли 52, были ранены 199 человек.
14	1 августа 2003 г., г. Моздок, Северная Осетия	Террорист-смертник на грузовике «КамАЗ», груженном взрывчаткой, прорвался на территорию госпиталя и привел в действие взрывное устройство рядом с главным лечебным корпусом.	Погибли 50 человек, пострадали 132 (ранено 82) чел.
15	5 декабря 2003 г., Ставропольский край	Взрыв в вагоне электропоезда «Кисловодск — Минеральные воды».	Погибли 47, были ранены 180 человек.
16	6 февраля 2004 г., г. Москва	В поезде метро, следовавшем по направлению от станции «Автозаводская» к «Павелецкой», террорист-смертник привел в действие взрывное устройство, закрепленное на собственном теле.	Погиб 41 человек, получили ранения около 250.
17	22 июня 2004 г., Ингушетия	Нападения боевиков на ряд населенных пунктов.	Погибли 98, были ранены 104 человека.
18	24 августа 2004 г.	Взрывы на борту самолетов Ту-134 «Москва — Волгоград» и Ту-154 «Москва — Сочи».	Погибли 90 человек.
19	31 августа 2004 г., г. Москва	Взрыв у станции метро «Рижская».	Погибли 11 человек, ранен 41 человек.
20	1—3 сентября 2004 г., г. Беслан, Северная Осетия	Захват боевиками средней школы №1 г. Беслана. В течение двух суток в спортзале школы удерживались более 1200 человек. В результате взрыва, осуществленного террористами, произошло обрушение крыши спортзала.	Погибло 338 человек, в т. ч. 172 ребенка; 10 сотрудников спецназа и 2 сотрудника МЧС, были ранены 559 чел.

Из данных, приведенных в табл. 1, следует, что вопрос о компенсациях совершенно не отрегулирован. До сих пор не существует какой-либо системы в этом вопросе.

За счет государства и благотворительных организаций семьи погибших получали от 10 до 100 тыс. руб., а пострадавшие — от 3 до 50 тыс. руб.

Участие страховых организаций в возмещении ущерба носило эпизодический характер. Компанией «Ингосстрах» был возмещен ущерб от взрыва у гостиницы «Националь» 9 декабря 2003 г., а также в результате террористического акта у метро «Рижская» 31 августа 2004 г. (Универмаг «Крестовский» был застрахован «Ингосстрахом» по полному пакету рисков, включая риск терроризма).

Единичные случаи страховых выплат осуществлялись страховщиками гражданам после терактов на Дубровке (октябрь 2002 г.), в московском метро (6 февраля 2004 г.), а также, семьям погибших в авиакатастрофе Ту-134 и Ту-154 в августе 2004 г.

По числу жертв террористических актов Российская Федерация занимает одно их самых высоких мест в мире (см. табл. 2).

Таблица 2. Страны, наиболее пострадавшие от терроризма в 1994—2004 годах. Топ-10 (источник — `http://www.kommersant.ru/doc.html?DocID=504685&IssueId=18392`)

Место в рейтинге	Страна	Число погибших в терактах на территории страны в 1994—2004 годах	Число погибших в терактах (на 1 млн жителей страны)
1	США	3238	11,05
2	**Россия**	**2111**	**14,54**
3	Индия	1928	1,81
4	Израиль (без учета населения Западного берега реки Иордан и сектора Газа)	1274	219,28
5	Колумбия	1135	26,82
6	Ирак	1122	44,22
7	Алжир	869	27,05
8	Пакистан	783	4,92
9	Уганда	471	17,84
10	Шри-Ланка	409	20,55

Мировая тенденция такова, что число террористических актов и число пострадавших в результате совершения террористических актов растут. Согласно докладу Госдепартамента США за 2005 год в мире произошло более 10000 террористических нападений, жертвами которых стали 14602 человека. Большинство террористических нападений в 2005 году было совершено в Ираке.

III. Помимо главных вопросов: как предотвратить террористический акт, как уменьшить размер возможного ущерба, одной из ключевых проблем становится вопрос: как финансировать покрытие ущерба от террористических актов?

С позиции государства возможны три фундаментальных подхода к решению этой проблемы[1]:

1. Государство целиком обеспечивает компенсацию ущерба (что характерно для таких стран как: Израиль, Северная Ирландия, где совершаются хронические террористические акты существенной тяжести).
2. Государство делит страховой риск с частным сектором, что характерно для стран с относительно низким риском, но катастрофическим размером убытков, примером может служить США, где приняты соответствующие законы (TRIA (26.11.2002) и TRIEA (31.12.2005), предусматривающими участие государства в покрытии убытков до 100 млрд долл.
3. Государство полагается на частный бизнес в покрытии ущерба от террористических рисков (в странах, где террористические акты носят эпизодический характер).

В силу того, что террористические риски могут нанести катастрофический ущерб, для их страхования часто используется форма страхового пула.

Кроме того, такие риски перестраховываются, например: риски Всемирного торгового центра в Нью-Йорке были застрахованы и перестрахованы более чем в 100 компаниях, среди которых присутствовали глобальные страховщики и перестраховщики.

В некоторых странах государственные органы формируют гарантийные фонды для возмещения возможных убытков от террористических актов.

Возникают вопросы:

[1]Современный терроризм и борьба с ним: социально гуманитарные измерения. Научные проблемы безопасности и противодействия терроризму. М., 2007.

Может ли страховая система справиться с последствиями террористических актов? Какова должна быть роль государства? Должно ли быть страхование риска терроризма добровольным или обязательным?

В США и Великобритании страхование риска террористического акта добровольное.

Во Франции и Испании клиенты обязаны приобретать покрытие риска терроризма в качестве «нагрузки», покупая некоторые виды страховок.

Каждый из подходов имеет преимущества и недостатки.

Главный недостаток обязательного страхования — сложность регулирования тарифов (из-за отсутствия данных), вследствие чего владельцы собственности с низким риском будут вынуждены субсидировать владельцев собственности с высоким риском.

IV. Очевидно, что различные объекты и территории подвержены опасности террористических актов в разной степени. В табл. 3 приводится классификация наиболее привлекательных для террористов объектов.

Таблица 3. Классификация потенциальных объектов террористических угроз

Объект
Объекты атомной промышленности
Научно-исследовательские центры и испытательные полигоны по изучению опасных веществ
Промышленные объекты
Система водоснабжения
Система энергоснабжения
Места массового скопления людей
Высотные здания
Религиозные центры
Транспортная инфраструктура
Информационная система
Здания административного и федерального значения, посольств, штаб-квартир политических партий и организаций
Символические и исторические сооружения

По имеющимся оценкам, в Российской Федерации на сегодняшний день насчитывается: свыше 2,5 тысяч химически опасных объектов,

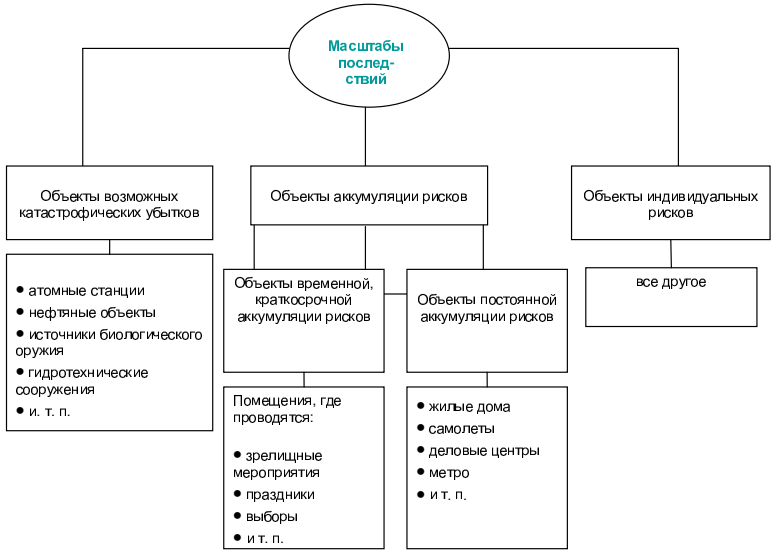


Рис. 1

1,5 тыс. радиоактивных опасных объектов, 8 тысяч пожаро- и взрывоопасных объектов, более 30 тысяч гидротехнических сооружений.

Наиболее уязвимы для террористических атак крупные города и мегаполисы, характеризующиеся большой плотностью населения и сосредоточением потенциальных объектов атак.

Повышенная угроза террористических атак существует в ряде регионов страны, например, в ЮФО.

Поэтому, при решении вопроса о страховании от риска террористического акта важна классификация территорий и объектов по критерию подверженности этим рискам.

Подходы к классификации объектов и видов деятельности, которые могут быть подвергнуты террористическим атакам, схематически можно изобразить в виде, показанном на рис. 1.

V. Далее важен анализ характеристики ущерба. Такой анализ необходим для оценки потенциального ущерба. Структура страховых выплат по возмещению ущерба гибели Всемирного торгового центра такова[1]:

- Имущество ВТЦ (два здания) — 11,1 %;
- остальное имущество — 18,5 %;

[1] Издание Information Insurance Institute.

- перерыв в производстве — 33,8 %;
- ответственность авиаперевозчиков — 10,8 %;
- страхование жизни — 3,1 %;
- фюзеляжи самолетов — 1,5 %;
- отмена мероприятий — 3,1 %;
- несчастные случаи на производстве — 5,8 %;
- другие виды ответственности — 12,3 %.

VI. На оценку риска террористического акта оказывает влияние возможность его профилактики и проведения превентивных мер (система безопасности, контроля и т. д.). По этому критерию степень уязвимости объектов также может быть классифицирована (см. рис. 2).

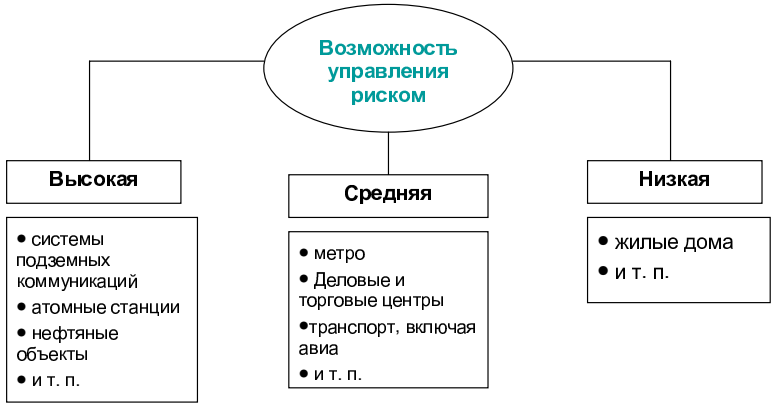


Рис. 2

Объекты высокого уровня управления рисками — закрытые от скопления людей места, в отношении которых можно организовать серьезные меры безопасности.

На объектах среднего и низкого уровня управления риском безопасность снижается.

Идеи обязательного страхования риска террористического акта содержатся в проектах Федеральных законов «Об обязательном страховании гражданской ответственности за причинение вреда при эксплуатации опасного объекта» и «Об обязательном страховании гражданской ответственности устроителей массовых мероприятий за причинение вреда в результате террористического акта». Однако идеи обязательного страхования риска терроризма не находят поддержки у регулярного страхового дела (Минфин), который считает, что страхование этих рисков можно

осуществлять в добровольной форме в рамках страхования имущества или ответственности за причинение вреда.

Целесообразность страхования риска террористического акта в Российской федерации определяется следующими факторами:

- стимулировать эксплуатантов опасных производств и объектов, а также устроителей массовых мероприятий снижать степень подверженности застрахованных объектов террористическим актам;
- определить гарантированные размеры компенсации жертвам и пострадавшим в результате террористического акта;
- унифицировать порядок компенсации убытков в результате террористического акта;
- определить порядок и источники компенсации ущерба экологии в результате террористического акта.

VII. Ключевым вопросом является оценка террористического риска.

Террористический риск в научной литературе определяется как функция угрозы, уязвимости и последствий:

$$\text{Риск} = \mathsf{P}(\text{атака произойдет}) \cdot \mathsf{P}(\text{возникнут убытки/атака произойдет}) \times \\ \times\, \mathsf{E}(\text{Убытки/произойдет атака и будет нанесен вред}).$$

Недостаток статистики не позволяет адекватно рассчитывать страховые тарифы, однако существуют разнообразные методики оценки риска террористических актов и размера ущерба. Так, например, в работе Willis и др.[1] приводятся два подхода к оценке риска терроризма в городских районах.

В моделях, использующих индикаторы населения (плотность населения) удается ранжировать мегаполисы и крупнейшие города США по степени уязвимости террористическим актам и потенциальному размеру убытков.

В другой работе La Tourette и др.[2] приводится RMS Terrorism Risk Model — детальный анализ последствий различных сценариев террористических атак в торговых центрах. Эта модель может быть использована как инструмент для страхового и перестраховочного бизнеса с целью оценки риска терроризма и определения страховых тарифов. В работе анализируются последствия свыше 200 террористических актов в крупнейших однотипных торговых центрах всего мира. Террористические акты классифицируются в зависимости от вида применяемого оружия нападения террористов (взрыв, распыление отравляющих веществ и др.) и метода осуществления теракта (у входа в здание, внутри здания, на подземной стоянке автомобилей и т. д.).

На основе анализа моделируются различные сценарии терактов, с помощью которых определяется экономическая целесообразность введения тех или иных мер безопасности, например: Установление металлоискателей.

Математические модели подобного типа было бы целесообразно разрабатывать в РФ с целью оценки размеров потенциального ущерба террористических актов и определения страховых тарифов.

[1] Estimating Terrorism Risk. Willis, Morral, Kelly, Medby. RAND Center for Terrorism (risk management policy, 2005, `www.rand.org`).

[2] Reducing Terrorism Risk of shopping centers. LaTourette, Howell, Masher, MacDonald. RAND, 2006.

Особенности перестрахования риска «террористический акт» в России

А. В. Щеголев

В последнее время в мире участились инциденты, вызывающие своей жестокостью и масштабом широкую негативную реакцию общества и часто называемые в СМИ террористическими актами. В связи с этим объективно появляется необходимость защиты от этого явления и защиты от его негативных последствий, которые подчас наносят больший ущерб по сравнению с самим терактом. События 11 сентября 2001 года в Нью-Йорке не были первым актом терроризма, они лишь послужили катализатором всплеска активности общественного мнения.

Терроризм, как явление, одной из основных содержательных, сущностных сторон которого является устрашение политических противников, известен человечеству с давних времен. Для мирового сообщества проблема терроризма стала особенно актуальной в XX веке, когда применение устрашающего насилия стало одним из действенных и часто применяемых орудий борьбы между преступными группировками, вооруженными формированиями, политическими партиями и даже государствами, а достижения науки и техники дали в руки террористов самые современные и эффективные средства реализации своих намерений. К началу 90-х годов возникли целые организации, готовившиеся к ведению вооруженной (по сути дела — террористической) борьбы.

Российское законодательство трактует терроризм как идеологию насилия и практику воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанную с устрашением населения и (или) иными формами противоправных насильственных действий. Террористический акт — совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения органами власти или международными организациями, а также угроза совершения указанных действий в тех же целях[1].

[1] Федеральный Закон «О противодействии терроризму» от 6 марта 2006 г. № 35-ФЗ, ст. 3.

Между тем, до сих ни в ученом мире, ни у юристов, ни у представителей правоохранительных органов не сложилось однозначного представления о феномене терроризма. Одни толкуют его расширительно, другие сужают это понятие до тех или иных конкретных действий. Многообразие подходов объясняется спецификой регионов, национальными и историческими традициями, уровнем демократии, степенью стабильности политической ситуации в той или иной стране, особенностями юридических школ, а также спекуляцией этого понятия в тех или иных целях. Проявлениями терроризма люди готовы называть все, что сделанное одними людьми против других вызывает ужас. Однако, различные точки зрения позволяют выделить содержащиеся в них общие признаки терроризма, комплекс которых и способен дать достаточно объективное представление о феномене терроризма. Эти признаки заключаются в следующем:

1. Терроризм предполагает достижение определенной политической цели определенным узким кругом лиц, группировкой. Если цель отлична от политической, то такое явление нельзя называть терроризмом, даже если оно очень похоже на террористический акт по способу осуществления и своим последствиям.
2. В отношении противостоящей стороны применяется насилие в той или иной форме либо угроза использования такового. Однако нет прямой вооруженной конфронтации с правительственными силами.
3. Объект террористического воздействия является двойственным: *непосредственный объект*, которым могут быть материальные объекты, некоторые категории граждан, определяемые по политическому, социальному, национальному, религиозному или иному принципу либо заранее конкретно не определенные случайные люди, — и *конечный*, или *стратегический объект*, которым является конституционный строй либо один из его элементов (территориальная целостность, порядок управления, экономическая мощь и т. д.). Таким образом, терроризм всегда направлен на достижение недовольства властью со стороны масс, мнение которых и решает в демократических странах вопросы власти.

Страхование катастрофических рисков, к которым в настоящий момент, без сомнения, принадлежит и риск терроризма, невозможно без надежной защиты страховщика. Наиболее эффективным и общепризнанным инструментом такой защиты на сегодня является перестрахование. В настоящее время при страховании катастрофических рисков компании вынуждены придерживаться условий перестрахования, поскольку, в конечном счете, именно от перестраховщика (как субъекта, обеспечива-

ющего выплату большей части убытка) и будет зависеть возможность страхования того или иного риска.

Еще одним способом передачи застрахованного риска может быть так называемый «альтернативный способ передачи рисков» — ART[1]. Однако ввиду современных сложностей на рынках ценных бумаг и специфики риска он практически не находит применения в отношении риска терроризма. Для вывода риска на рынок ценных бумаг риск должен быть оценен адекватным образом, но как оценить абсолютно непредсказуемый риск в условиях отсутствия какой-либо статистики и непонимания закономерности его проявлений никто пока не знает. Поэтому перспективы данного способа переноса риска на сегодняшний день весьма туманны.

Наконец, страховщики чувствуют себя более уверенно, если являются участниками и соответственно имеют поддержку пула, одним из участников которого может и должно также являться и государство. Сострахование также может быть выгодно страховщикам в защите от принятого риска терроризма.

Одним из критериев возможности страхования риска является вероятность его проявления и оценка величины этой вероятности. Здесь существуют определенные проблемы. Вероятность появления неблагоприятных экономических последствий в результате террористической атаки, безусловно, имеется, однако ее практически невозможно оценить в силу специфики этого риска. Поскольку масштабы его проявления все больше и больше увеличиваются, адекватная оценка данного риска играет ключевую роль в определении стоимости его покрытия для страховщика. Страховщик же в силу огромной величины потенциальных экономических последствий и соответственно покрытия данного риска, ориентируется на рынок перестрахования, который, в свою очередь, также не может адекватно оценить данный риск. Более того, масштаб убытков, понесенных в результате событий 11 сентября, явился сильнейшим напоминанием того, что риск имеет свою цену. Поэтому после осени 2001 г. цены на покрытие данного риска, которое существенно уменьшилось, возросли в десятки раз.

Неадекватность существующих моделей оценки ущерба от террористического акта подтверждается тем, что сразу после террористических атак страховые и перестраховочные тарифы резко увеличиваются (при одновременном увеличении числа страхователей), но в последующие годы наблюдается постепенное снижение числа страхователей и тарифов и так до нового теракта.

Важнейшим же фактором при страховании того или иного риска является страховой интерес, т. е. ответ на вопрос, кому реально необходимо

[1] Alternative risk transfer.

страхование от этого риска. Основное предназначение государства — обеспечить безопасность своих граждан и обеспечение удовлетворения их потребностей. Террористы как раз и добиваются изменения политики государства в нужную сторону с помощью невольной поддержки общества. Терроризм направлен, прежде всего, на изменение политики государства и транснациональных корпораций, чьи интересы опять же защищает государственная политика, поэтому логично утверждать, что иметь защиту от экономических последствий терроризма выгодно, прежде всего, тем, на кого такие действия направлены. Объекты административного и национального значения, опасные объекты, объекты инфраструктуры наиболее подвержены риску терроризма по причине большей вероятности широкой реакции общества.

Террористическая атака на ВТЦ 11 сентября 2001 г. подтвердила миру тот факт, что оценке риска при принятии его на страхование отводилась второстепенная роль. На протяжении более чем 10 лет страховщики занимались скорее управлением активами, чем управлением рисками. Террористический акт подчеркнул необходимость адекватной оценки риска страховщиком. Ведущие мировые страховщики и перестраховщики понесли огромные убытки именно из-за отсутствия надлежащего контроля и оценки принимаемых рисков, и эти убытки в настоящее время не могут быть компенсированы результатами инвестиционной деятельности. Все вышеперечисленное заставило акционеров страховых компаний и перестраховочных обществ серьезно задуматься о рентабельности страхового бизнеса.

Следствием вышеперечисленных факторов явился рост тарифов по большинству видов страхования для покрытия отрицательных результатов деятельности страховщиков. Террористический акт 11 сентября 2001 г. заставил по-новому взглянуть на оценку рисков, придерживаться более осторожной политики при их тарификации. Риск терроризма, как не подлежащий адекватной оценке в современных условиях и исключаемый большинством перестраховщиков, был исключен из покрытия, в свою очередь, и большинством прямых страховщиков, в один момент потерявших перестраховочную защиту своих портфелей от данного риска.

Повышение цен и исключение риска терроризма из перестраховочного покрытия являются причинами, в силу которых несколько усилился интерес к перестрахованию. В то же время, считается, что создание кэптивных страховых и перестраховочных компаний или соответствующих резервов будет все же недостаточным в сравнении с предполагаемым масштабом убытков в результате подобных нападений.

До теракта 11 сентября 2001 г. в мире уже существовали 4 организации, которые специализировались на предоставлении страховой защиты

от риска терроризма. По примеру этих организаций в ответ на события в Нью-Йорке стали создавать подобные структуры. На сегодняшний день созданы пулы во Франции, Германии, Австрии, Австралии, объявили о намерении создать таковые Швейцария и Швеция. Принят специальный закон о страховании риска терроризма в США. Появились авиационные пулы Equitime (США) и Eurotime (Европа), речь идет о создании мирового авиационного пула Globaltime. Отличительной чертой всех созданных организаций и схем организации страховой защиты от риска терроризма является участие государства в качестве перестраховщика «последней надежды/инстанции». Несмотря на интерес к альтернативам страхования, непосредственно после теракта также возрос спрос непосредственно на страховую защиту от риска терроризма. Ответом на растущий спрос послужило создание перестраховочных пулов во многих странах, одним из участников которых является государство в качестве перестраховщика «последней инстанции», т. е. выступает своеобразным «окончательным плательщиком» той части общего убытка, которая осталась неоплаченной всеми плательщиками (страховщиками и перестраховщиками), обязанными совершить выплату до государства[1].

Некоторые перестраховщики, такие как AXIS, Allianz AG, AIG, Berkshire Hathaway, Lloyd's of London[2], продолжали предоставлять перестраховочную защиту от риска терроризма во время отсутствия государственной поддержки. Однако цена такого перестрахования изначально была достаточно высокой. Так AIG предлагает страхование риска терроризма в отношении имущества с лимитами покрытия до 150 млн долларов по каждому случаю и агрегатно за период, обычно равный году, за минимальную премию 50 000 долл. с франшизой 2 % от страховой суммы, но не менее чем 100 000 долл. В рамках этой защиты покрываются также убытки от перерыва в деятельности, лимит покрытия которых ограничен 25 % общего лимита. В отношении убытков от перерывов в деятельности существует условная франшиза в 30 дней[3]. При этом тщательно анализируется географическое расположение страхователя. Подобного подхода придерживается специально созданная для страхования риска терроризма, военных рисков и рисков забастовок страховая компания SRIR, находящаяся в Люксембурге.

Террористические акты и нападения — риск, который технически трудно застраховать. Страховщик должен смоделировать непредсказуемый риск так, чтобы его можно было применить к большому числу страхователей в течение многих лет. Результатом этого является договор, определяющий размер покрытия и ставки. На текущий момент еще не существует единой модели оценки риска. Тем не менее, оценка риска терроризма — насущная проблема для страховщиков в настоящее время. Цены на покрытие, которые прокотировали различные страховщики непосредственно после 11 сентября 2001 г., различались во много раз, что свидетельствует об отсутствии адекватных подходов к оценке этого риска. В настоящее время три крупнейших мировых агентства по оценке рисков AIR Worldwide, Eqecat, Risk Management Solutions (RMS) разработали свои методики оценки риска, что, однако, не избавляет пользователей от интуитивных догадок относительно точной цены риска в ходе оценки его стоимости. Вообще процесс выработки цены покрытия риска терроризма может быть математическим лишь отчасти, в остальной части должно сыграть свою роль субъективное суждение, интуиция. Несмотря на то, что модели риска терроризма уже предлагаются на рынке, никто не может сказать, насколько они точны. Модели катастрофических рисков — ближайшие к ним по своей сути в мире моделей рисков — были не всегда оптимальны. И пока новый масштабный террористический акт не потрясет мир, разработанные модели не смогут быть протестированы, а значит, считаться адекватными.

В этой ситуации примечателен подход, практикуемый большинством отдельных перестраховщиков, принимающих риск терроризма в перестрахование без дальнейшей ретроцессии в тот или иной пул. При оценке риска уделяется внимание огромному количеству факторов, которые потенциально могут повлиять на степень риска или характеризуют подверженность ему конкретного объекта. Во внимание принимаются статистика убытков по данной местности, по подобным объектам в мире, общая политическая ситуация и т. п. Подход большинства андеррайтеров непосредственно к котировке риска терроризма следующий — за сублимит, оговоренный в договоре в отношении риска терроризма, взимается премия, приблизительно равная премии, уплаченной по страхованию данного имущества от риска огня и сопутствующих рисков, при условии довольно значительной безусловной франшизы. Конечно, данная цена высока, однако невелико и количество страхователей, желающих приобрести такое покрытие. Безусловно, цена на предоставляемое покрытие будет снижаться по мере наполнения портфелей договорами.

Интерес к предлагаемому страховщиками страховому продукту, включающему защиту от риска терроризма, выражающийся в платежеспособном спросе на страхование от этого риска за рубежом, в большинстве случаев возникает у следующих экономических субъектов:

[1] Reinsurer of last resort — перестраховщик «последней инстанции».

[2] Terrorism Insurance—UK Market Update // Marsh Adviser, December 2002, `http://www.marsh.co.uk`.

[3] AIA/AIG Response to Terrorism // `http://www.aiaa.com.au`, `http://www.aig.com`.

1. Государство (государственные объекты, национальные символы и т. п.).
2. Владельцы опасных объектов (ядерные объекты, химические заводы, токсичные производства).
3. Транспортные организации (авиакомпании, аэропорты).
4. Устроители мероприятий.
5. Корпорации — провайдеры коммуникаций.
6. А также субъекты, имеющие имущественный интерес в отношении объектов, находящихся в непосредственной близости с вышеуказанными.

Разрешить проблему организации страховой защиты от риска терроризма в отношении вышеназванных объектов призваны пулы с участием государства, а также некоторые другие механизмы реализации страховой защиты бизнеса от риска терроризма.

Тенденции после событий 11 сентября 2001 г. в США на мировом рынке страхования данного риска в разных странах схожи. Создаются пулы, в которых государство играет роль перестраховщика «последней инстанции». Обеспечивается также единообразие условий такого страхования путем запрета на какие-либо преимущества для любого участника рынка страхования риска терроризма. Отличительными чертами этих пулов являются также существенный размер премий, уплачиваемых пулу и ограничение удерживаемой прямыми страховщиками ответственности разумными лимитами, не ставящими под угрозу само существование компании в случае убытка.

Во многих государствах, на территории которых Страхователи заинтересованы в приобретении покрытия риска терроризма, образуются или функционируют в течение определенного периода соответствующие структуры, деятельность которых направлена на обеспечение удовлетворения потребности в покрытии данного риска.

Созданные структуры чаще всего имеют организационную форму перестраховочного пула. Страховщики во многих странах обязаны законодательством покрывать риск терроризма в случае возникновения потребности Страхователя в таком покрытии. Подобные пулы имеют поддержку государства в качестве последнего гаранта оплаты убытков. Государство декларирует возможность получения помощи в оплате убытков лишь в случаях катастрофических убытков для обеспечения выживания Страховщиков, а не сохранения их финансовой устойчивости. Участники пула имеют значительный размер собственного удержания по данным рискам.

В большинстве стран риск терроризма покрывается на ограниченной основе, т. е. покрываются в основном лишь риски пожара и взрыва, вызванных террористическим актом. По условиям большинства пулов не покрывается радиоактивное загрязнение. Во многих странах покрывается исключительно коммерческая недвижимость исключительно на территории государств, где функционируют пулы. В настоящий момент лимитируется сам размер покрытия риска терроризма, ранее предоставлявшегося на неограниченной основе.

Существует лишь 4 страны, Страховщики которых покрывают риск терроризма уже в течение достаточно длительного периода времени. Это Великобритания (Pool Re — 1993 г.), Франция (CCR — 1986 г., GAREAT — 2001 г.), ЮАР (SASRIA — 1976 г.), Испания (Consorcio — 1986 г.). Перестраховочные пулы, организованные для покрытия риска терроризма в остальных странах пока не выдержали проверку временем, поскольку не испытали серьезных убытков.

Во всех странах доступно альтернативное покрытие, предоставляемое крупнейшими мировыми перестраховщиками, однако зачастую оно весьма дорогое.

Необходимо отметить, что, несмотря на крайнюю сложность страхования риска терроризма, во многих странах делаются попытки организации страховой защиты, однако лишь время способно подтвердить их жизнеспособность. Нельзя не отметить также, и это является ключевым моментом, что ажиотажный спрос сразу после теракта на покупку покрытия риска терроризма имеет тенденцию к уменьшению по причине того, что за предложенную цену, которая является достаточно высокой во многом, по мнению автора, из-за спекуляции страховщиков на страхе общества перед террористами, покупаемое покрытие все же не полностью удовлетворяет потребностям страхователей в отношении требуемого размера, спектра покрытия, покрываемых объектов и территории.

Подверженность российской экономики риску терроризма в настоящее время не может быть оценена путем каких-либо стандартных подходов к данной проблеме. Анализ терроризма как политического риска в России имеет некоторую специфику. Во-первых, политическая традиция, несовершенство демократических институтов и переломный момент исторического развития обусловили значительную роль личностного фактора, которому необходимо уделять дополнительное внимание при оценке политического риска. Во-вторых, существенным фактором неопределенности является наличие множества разнотипных политико-территориальных образований, обладающих различным экономическим потенциалом, разнородных по национальному составу и опирающихся на разные исторические, политические, культурные и религиозные традиции. Региональные конфликты оказывают как прямое воздействие на общую политическую обстановку, так и косвенное влияние на ситуацию в других

регионах, поскольку решение региональных проблем требует дополнительных субсидий, что ведет к росту дефицита федерального бюджета, изменениям в налоговом законодательстве, сокращению социальных расходов, а, следовательно, возрастанию социальной напряженности. Недостаточный учет региональной специфики, пожалуй, является основным недостатком существующих зарубежных методик при их экстраполяции на Россию.

Риск терроризма, как риск, проявление которого зависит от общеполитической ситуации в мире, особенно возрастает в те моменты, когда его проявление целесообразно в качестве инструмента внешней политики. В настоящее время подверженность этому риску велика и продолжает расти. Это справедливо не только в отношении России, но и в отношении большинства стран мира, играющих сколько-нибудь значимую роль на мировой политической арене. Терроризм, по причинам, рассмотренным в первой главе, весьма удобен государствам в качестве инструмента осуществления не только внешней, а часто и внутренней политики.

Соответственно, рассматривая взаимоотношения России и США, в то время как последние являются главным игроком на мировой политической арене, можно понять, что любое противопоставление российских интересов интересам США гипотетически увеличивает вероятность совершения террористического акта в России. Назревание необходимости власти провести в жизнь те или иные решения, которые, скорее всего, вызовут негативную реакцию населения, также могут способствовать увеличению вероятности совершения террористического акта. Причем вероятность его совершения на территории РФ будет, скорее всего, выше в Москве, Санкт-Петербурге как городах, имеющих высокую плотность населения, т. е. наиболее подходящих террористам для осуществления их целей с точки зрения нанесения максимально возможного ущерба и вызова максимально возможной реакции, или на территориях, близких к Кавказу, как потенциальных районах базирования террористических группировок. Однако такой прогноз вовсе не исключает возможность совершения террористических актов в других российских городах.

Несмотря на все вышесказанное, подверженность риску терроризма страхового рынка РФ можно оценить как невысокую, поскольку покрытие данного риска пока приобретают немногие.

При этом спрос на страхование достаточно низок в России как со стороны физических, так и со стороны юридических лиц. Немногие покупают страховое покрытие традиционных рисков — пожар, залив водой, противоправные действия третьих лиц. Соответственно, лишь некоторые из этих немногих готовы уплачивать дополнительную премию за приобретение покрытия риска терроризма.

Российские страховщики оказались в определенной изоляции в части перестрахования риска терроризма в рамках тех возможностей, которыми они обладали до 2001 года — цена на страхование риска терроризма на международном перестраховочном рынке выросла в десятки раз, покрытие стало жестко сегментированным по страновому признаку — в отношении некоторых государств осуществить страхование от риска терроризма вообще не представляется возможным.

Российский рынок, даже при наличии определенной статистики убытков, связанных с террористическими актами на территории России, во всех отношениях представляет собой особенный с точки зрения андеррайтинга риск. В отличие от западных примеров, в России практически никто не брал на себя ответственность за совершенные террористические акты, а сами теракты были направлены скорее на запугивание населения, чем на подрыв устоев государства.

В РФ возмещение вреда, причиненного в результате террористического акта, подлежит возмещению государством в виде компенсационных выплат физическим и юридическим лицам в порядке, установленном Правительством Российской Федерации[1]. Данные отношения регулируются Гражданским Кодексом и специально принятым в марте 2006 г. Федеральным Законом «О противодействии терроризму». Однако в связи тем, что размер компенсаций пострадавшим зачастую является заниженным, страхователи, заключающие договоры страхования от огня и сопутствующих рисков и реально заинтересованные в покрытии риска терроризма, предпочитают включить этот риск в перечень застрахованных рисков по договору огневого страхования.

В конце 2001 г. шесть ведущих российских страховых компаний: «Ингосстрах», «Военно-страховая компания», «РЕСО-Гарантия», «Интеррос-Согласие», «Росгосстрах» и «РОСНО» — выступили учредителями Российского Антитеррористического Страхового Пула. Основная задача РАТСП — формирование Национальной емкости для страхования и перестрахования риска терроризм. По словам представителей объединения, идея создания подобной организации появилась еще в конце 1999 года после трагических событий в Москве и Волгодонске. Но главным катализатором процесса послужили теракты 11 сентября 2001 года.

Примером для создания РАТСП послужил Pool Re, с представителями которого были проведены переговоры. Было решено, что английские принципы принятия и передачи рисков, а также правила работы Pool Re лягут в основу деятельности российского аналога.

[1] Федеральный Закон «О противодействии терроризму» от 6 марта 2006 года № 35-ФЗ, ст. 18.

Классификация риска терроризма, признаваемая РАТСП, содержится в 205 статье УК РФ. Риски перестраховываются среди членов пула. В настоящее время емкости пула хватает для принятия рисков в перестрахование, однако, в том случае, если ее будет недостаточно, существуют договоренности о факультативном перестраховании превышения лимита над максимальной емкостью пула сначала среди компаний-участников, а при их отказе — на специализированных западных рынках, занимающихся страхованием риска терроризма. Максимальный лимит ответственности, принятый пулом по одному договору, равен максимальной емкости РАТСП. Ответственность участников пула не является солидарной.

По состоянию на 10 октября 2006 г. совокупная емкость РАТСП достигла более 1 396 728 310 рублей по каждому договору страхования от риска терроризм (или около 52 000 000 долларов США). В пул входят 38 страховых компаний.

Основным критерием для определения ставки страховой премии по страхованию риска терроризм является вид деятельности, осуществляемый предприятием (отраслевой принцип тарификации). Однако информация по всем существенным условиям обеспечения безопасности риска также является ценообразующей. Ставки колеблются в диапазоне от 0,0125 до 0,2 % от страховой суммы. Действуют лишь ограничения по территориальному принципу, которые, в частности, распространяются на Чечню.

Сейчас большинство рисков, переданных в пул, — предприятий непроизводственной сферы. Этот сектор потенциально является яркой иллюстрацией спроса на покрытие риска терроризма и, поскольку связан с предоставлением услуг и торговлей, как правило, связан с массовым скоплением людей, что может быть использовано террористическими организациями.

Риск терроризма включается в перечень застрахованных рисков при страховании имущества, строительно-монтажных рисков, грузов, средств водного и воздушного транспорта и, по сути, является причиной проявления стандартных рисков договора страхования «от огня и сопутствующих рисков» — пожара, взрыва и т. д. РАТСП не покрывает риски ядерной, химической, биологической и электронной атак.

Наиболее сложным вопросом сегодня вся еще остается вопрос о размещении рисков свыше максимальной емкости РАТСП на западном рынке на факультативной (или облигаторной в будущем) базе. Хотя с 2007 года появилась перестраховочная емкость до 150 000 000 долларов США для риска терроризм в Lloyds, причем по вполне умеренным тарифам, воспользоваться ее не всегда представляется возможным.

В то же время РАТСП предстоит решить несколько вопросов и проблем:

- Нет опыта в страховании подобных рисков. Основной аргумент представителей пула заключается в том, что риск терроризма по своей сути перекрывается другими рисками (например, риском противоправных действий третьих лиц). Такой подход говорит о том, что страховщики или не задумываются о последствиях того, чем может быть чревата недооценка этого риска, или попросту берут с клиентов дополнительные деньги в надежде на то, что платить не придется.
- Предстоит уточнить, кто и как будет определять, что имел место именно террористический акт, и не будут ли в случае нанесения ущерба предпочтения отдаваться признанию такого действия в качестве противоправных действий третьих лиц во избежание паники.
- Стоит вопрос и в отношении адекватности ставок пула — самых низких ставок по страхованию терроризма в мире, при существенной подверженности риску терроризма российской экономики. Большое значение здесь также имеет вопрос обслуживания клиентов.

Таким образом, страховая защита от риска терроризма предоставляется в рамках специально созданного по инициативе крупнейших российских страховщиков пула. Однако, в отличие от пулов, созданных с целью защиты от риска терроризма за рубежом, отечественный пул не имеет поддержки государства в качестве перестраховщика «последней инстанции». Тем не менее, это не играет большой роли, поскольку подверженность российского страхового рынка риску терроризма мала по причине невысокого уровня платежеспособного спроса на страхование данного риска со стороны страхователей. Причем такой уровень платежеспособного спроса не является в России особенностью исключительно данного риска — он характерен для страхования вообще. В отношении риска терроризма можно добавить и слабое осознание подверженности данному риску большинства населения, а соответственно и юридических лиц. Интерес в страховании данного риска проявляется, прежде всего, со стороны транспортных компаний и особенно авиации, организаторов различных мероприятий, гостиниц и некоторых других страхователей, деятельность которых связана с большими скоплениями людей в одном месте и подверженность которых данному риску в этой связи можно оценить как самую высокую. Таким образом, в отношении покрытия пула сохраняется антиселекция риска, т. е. пул покрывает лишь объекты, имеющие высокую подверженность данному риску. Ввиду того, что статистика убытков отсутствует, адекватный андеррайтинг данного риска невозможен в силу его специфики. Также наблюдается низкая наполняе-

мость портфеля данного риска, а тарифные ставки, даже максимальные, в несколько раз ниже, чем ставки, котируемые различными зарубежными пулами, то деятельность данного пула вызывает скептическое отношение к оценке его возможности адекватно возместить убытки, которые могут быть потенциально причинены застрахованному имуществу в результате террористического акта.

Теоретический анализ возможности страхования риска «террористический акт»

Е. Е. Смирнова

Риск «террористический акт» является одним из так называемых новых или возникающих видов рисков, с которыми сталкиваются страховые компании в современных условиях. Достаточно очевидно, что реалии сегодняшнего дня: вступление ряда стран в эпоху постиндустриального развития, изменение качества экономического роста, постепенная утрата ведущей роли физического капитала в обеспечении материальной базы развития и усиление роли интеллектуального капитала, возрастание значения нематериальных активов в деятельности компаний — не могут не порождать новых видов рисков. Поэтому вопросы возможностей страхования риска «террористический акт» необходимо рассматривать в контексте более общего вопроса: «Сумеют ли страховые компании или страховая отрасль в целом как институт современной рыночной экономики ответить на подобные вызовы современной эпохи?»

Первые вопрос, на который необходимо дать ответ, обладает ли «террористический акт» существеннейшими признаками страхового риска. Риск в данном случае рассматривается как событие, от наступления которого находится в зависимости выполнение страховщиком своей основной обязанности — осуществление страховой выплаты. В таком понимании риск должен характеризоваться рядом признаков, частично находящих выражение в нормах права, частично выдвигаемых страховой теорией и практикой.

Событие, на случай наступления которого проводится страхование, должно быть возможным и неизвестным. С точки зрения теории страхования, отчасти зафиксированной и в страховом праве, решающим для признания события неизвестным, является субъективная, а не объективная неизвестность. Достаточно, чтобы и страхователь, и страховщик считали наступление страхового случая не неизбежным, или, по крайней мере, для них оставалось бы неизвестным время наступления предусмотренного договором страхования события. Не случайно, как бы предваряя современные рассуждения о подобных вопросах, один из корифеев российской цивилистики Владимир Иванович Серебровский (1887—1971)

специально отмечал: «Страхование корабля действительно, если сторонам было неизвестно, что в трюме корабля спрятана адская машина, которая должна была с математической точностью через известное количество дней взорвать корабль»[1].

Таким образом, террористический акт — событие, характеризующееся признаками вероятности и случайности, необходимыми для признания события в качестве страхового риска. Признанием этого факта является хотя бы следующее обстоятельство: до трагических событий 11 сентября 2001 г. риск терроризм включался в перечни страховых рисков по договорам страхования имущества юридических лиц в США. Ситуация коренным образом изменилась после трагедии 11 сентября, которая продемонстрировала, возможно, не осознаваемые ранее последствия реализации этого риска — непредсказуемость, кумуляцию и взаимную зависимость убытков, их тяжесть. Как следствие, некоторые страховщики исключили риск «террористический акт» из перечня опасностей, либо стали отдельно выделять его в перечне застрахованных опасностей за отдельную (дополнительную) плату. Например, в декабре 2001 г. при возобновлении договора страхования, предусматривающего покрытие риска терроризм, аэропорт в Чикаго должен был бы уплатить страховую премию в размере 6,9 млн долл. при покрытии в 150 млн долл., в то время как годом раньше размер премии составлял лишь 125 тыс. долл., а покрытие — 750 млн долл.[2]

Используя различные критерии, можно выделить несколько «классических» признаков риска, принимаемого на страхование.

Первая группа признаков определяются техникой страхования, а соответствующие условия могут быть определены как актуарные ограничения. Риск должен быть измерим, т. е. должна существовать возможность оценки, измерения вероятности реализации опасности. Риски, принимаемые на страхование, не должны полностью коррелировать между собой, т. е. должна существовать независимость наступления ущерба. Страховая компания должна быть в состоянии возместить максимально возможный ущерб по любому из отдельных страховых событий. Классическое страхование ориентировано на умеренные/частные риски с умеренным/средним ущербом.

Следующие критерии связаны с асимметрией информации в страховых отношениях, а соответственно с феноменами морального риска (поведение страхователя меняется в результате приобретения страхового

[1] Цит. по: *Серебровский В. И.* Избранные труды по наследственному и страховому праву. М.: Статут, 2003. С. 499.

[2] Terrorism // CRO Position Paper. August 2007. P. 6.

полиса) и обратной селекции (больше страхования приобретают страхователи с высоким риском). Несоблюдение указанных принципов может приводить к андеррайтерским потерям. Моральный риск и обратная селекция неизбежны, но не должны быть чрезмерными.

Следующие критерии связаны с особенностями страхового рынка. Страховые премии должны быть адекватными и доступными для страхователей и страховщиков. Страховщикам они должны обеспечивать отдачу на капитал, достаточный, чтобы нести принятые на себя риски. Страхователи должны иметь возможность получить страховое покрытие, соответствующее их потребностям и ожиданиям. Иными словами, на страховом рынке должно существовать предложение, адекватное как с точки зрения необходимых покрытий, так и их конкретных условий и исключений. Емкость страхового, или точнее, финансового рынка в целом, должна быть достаточна для принятия рисков.

И, наконец, общее положение, касающееся всех видов рисков — страховой интерес и покрываемый риск должны соответствовать общественным интересам и законодательству.

Как можно характеризовать риск «террористический акт» с точки зрения выделенных критериев? Достаточно очевидно, что некоторые существенные признаки риска «террористический акт» не позволяют классифицировать его как вид риска, принимаемого на страхование.

Террористический акт является тщательно спланированным, продуманным действием. Такая характеристика вызывает желание отнести его к умышленным, преднамеренным актам разрушения, которые обычно ассоциируются с преступлениями или военными действиями, которые являются исключенными опасностями по большинству видов договоров страхования иного, чем страхование жизни. Стремление страховщиков включить риск «терроризм» в перечень военных (исключенных) рисков достаточно отчетливо проявилась в США до момента принятия TRIA (Terrorism Risk Insurance Act) в ноябре 2002 г.

Сознательный характер действий террористов позволяет изменять характер, время и место каждой новой террористической атаки, делая ее все менее и менее предсказуемой. Террористы, стремясь преодолеть существующие и возможные системы защиты, действуют не по определенной логике, а вопреки ей. Необходимо также учитывать, что терроризм начала XXI века имеет ряд принципиально новых характеристик. Для современного терроризма характерен выбор более широких целей атак — «под риском» оказываются практически все жизненно важные объекты инфраструктуры, места скопления людей, любые гражданские объекты (больницы, школы, супермаркеты и т. п.). Последнее десятилетие характеризуется и наиболее серьезными по последствиям террористи-

ческими актами. Отечественные и зарубежные исследователи проблем терроризма указывают на особую опасность применения химического, бактериологического и ядерного оружия в ближайшие 10—15 лет. В этой связи достаточно упомянуть попытки использования террористами биологических и химических веществ в США в 2001 г., в Марокко в 2007 г. и т. д.

Процессы моделирования риска «террористический акт» находятся на начальных этапах своего развития, отсюда, естественно, огромное множество различных сценариев развития событий, попытки оценить ущерб в зависимости от способа и места реализации террористического акта: с использованием обычного взрывного устройства или «грязной бомбы (ядерное, химическое или биологическое оружие), захват самолета в воздухе или заложников на земле и т. д.

Множественность сценариев и оценок, отсутствие неких признанных стандартов затрудняет измерение риска. Риск террористической атаки — риск, характеризующийся низкой вероятностью, но значительными потерями (low probability—high consequence event). Моделирование подобных событий в принципе затруднено, для террористических атак оно еще больше осложняется ограниченным характером открытой и доступной, в том числе для страховщиков, информации. Этим, в частности, риск терроризм отличается от рисков природных катастроф, имеющих подобные качественные характеристики частоты/размера ущерба. Однако природные катаклизмы являются физическим феноменом, исследования ученых, инженеров и экономистов позволяют создавать все более адекватные модели природных катастроф, что позволяет страховщикам предлагать страхование подобных рисков по адекватным тарифам. В отличие от «классических» принимаемых на страхование рисков, для риска терроризм характерно симметричное отсутствие необходимой информации, как у страхователя, так и у страховщика.

Потенциальный ущерб в результате реализации страхового случая должен рассматриваться как неограниченный. Естественно, что при моделировании риска специалисты всегда анализируют возможность реализации наиболее пессимистического варианта развития событий, наступление катастрофического (тотального) ущерба. Однако, как свидетельствует опыт 11 сентября 2001 г., многие существовавшие в тот момент сценарии даже не предполагали возможность такого исхода, который имел место в действительности.

Террористический акт означает кумуляцию различных видов потерь, связанных со страхованием жизни, имущества, перерывов в хозяйственной деятельности, ответственности, что было подтверждено событиями 11 сентября в США. Например, общеизвестно, что страховые выплаты в

связи с событиями 11 сентября 2001 г. составили порядка 37 млрд долл., однако, необходимо учитывать, что сразу после событий 11 сентября в США был создан специальный фонд для выплаты компенсации пострадавшим (Victim Compensation Fund), который существовал до 15 июня 2004 г. За это время было удовлетворено 7400 требований родственников погибших и пострадавших в результате теракта на общую сумму 7 млрд долл. Убытки по террористическому акту 11 сентября 2001 г. были оплачены примерно 150 страховыми и перестраховочными компаниями.

Размер ущерба в результате террористической атаки может быть столь значительным, что он будет превосходить финансовую емкость рынка страхования и перестрахования. По имеющимся оценкам Insurance Information Institute, размер свободных активов американских страховых компаний, занимающихся страхованием имущества и ответственности, составляет в настоящее время 414 млрд долл., примерно половина этих активов может быть использована для покрытия ущербов юридических лиц.

Чтобы обеспечить выплаты по наступившему страховому случаю, страховые компании будут вынуждены распродать значительную часть своих активов, однако, после крупного террористического акта естественным является спад на финансовых рынках, что приводит к росту трансакционных издержек проведения всех сделок и резко обостряет риск рыночной ликвидности (достаточно вспомнить, что после 11 сентября 2001 г. американский рынок акций упал на 12 %). Осуществление значительных выплат может сказаться и на будущей способности страховщиков привлекать заемный капитал на финансовых рынках, равно как и увеличивать собственный капитал.

В последние годы были предприняты различные попытки оценить потенциальный ущерб в связи с террористическими актами. Например, по оценкам Risk Management Solutions, ожидаемый ущерб от террористического акта с использованием 5-килотонной «грязной» бомбы оценивается в 630 млрд долл., верхний предел — до 1,9 трлн долл. American Association of Actuaries оценивает средний ущерб от возможной крупной террористической атаки в 778 млрд долл., что значительно превосходит ущерб от урагана Катрина (66 млрд долл.), что в настоящее время расценивается как самый крупный застрахованный ущерб. По оценкам Towers Perrin, общие застрахованные убытки по одному террористическому акту могут превышать 250 млрд долл. Приведенные выше оценки последствий террористических атак строятся с учетом использования ядерного, химического или биологического оружия, однако, один крупный или несколько одновременных террористических актов с применением обычного ору-

жия, также, несомненно, могут приводить к катастрофическим потерям, сопоставимым или превосходящим финансовые возможности страхового рынка.

Последствия террористических актов сказываются на различных видах бизнеса страховой компании: страховании имущества, страховании от перерывов в производстве, страховании ответственности, страховании жизни, страховании от несчастных случаев и т. п. Кроме того, возможна кумуляция по объектам и географическим регионам. Подобная ситуация значительно сокращает возможности диверсификации рисков в портфеле страховой компании.

Обследования рынка страхования терроризма, проводимые Marsh& McLennan с 2003 г., отмечают рост процента компаний, приобретающих страхование от терроризма: 2003 г. — 27 %, 2004 — 49 %, 2005 — 58 %. Основными покупателями являются крупные компании, средняя страховая сумма по договору превышает 1 млрд долл. По отраслям основными покупателями страховых полисов являются владельцы недвижимости — 79 %, финансовые институты, промышленность, строительство, энергетика и строительство — порядка 43—45 % компаний в этих отраслях или видах деятельности имеют полисы страхования по риску терроризм. С точки зрения географии распределения полисов — лидирует северо-восток США[1]. А ведь именно на северо-востоке сосредоточены критически важные объекты с точки зрения уязвимости для террористических атак (т. е. объекты, характеризующихся наиболее высоким уровнем риска). Таким образом, очевидно наличие проблемы обратной селекции.

Некоторые приведенные выше соображения позволяют сделать вывод о том, что риск «террористический акт» не полностью соответствует всем классическим определениям риска, принимаемого на страхование.

Одной из естественных реакций на подобное положение стало использование во многих странах различных форм государственно-частного партнерства при страховании риска «террористический акт». Почему подобное партнерство является естественным, или, иными словами, почему именно взаимодействие с государством выглядит в данном случае естественным?

Во-первых, государство обладает в силу особенностей своего положения, уникальными возможностями по финансированию, в том числе катастрофических, потерь. Следовательно, государство может выступать в качестве страховщика/перестраховщика последней инстанции. Во-вторых, государство может вводить обязательное страхование, что позволяет автоматически распределять дополнительную страховую премию по данному риску на всех участников страхового фонда, отчасти снимать проблему обратной селекции.

[1] Marketwatch: Terrorism Insurance 2006. P. 7, 9.

Не случайно, в ряде стран, которые раньше других ощутили последствия действий террористических организаций, уже достаточно давно появились подобные формы взаимодействия государства и частных страховщиков. Достаточно вспомнить Испанию (Consorcio de Compensación de Seguros создан в 1941 г.), Израиль (Property Tax and Compensation Fund создан в 1973 г.), Великобританию (POOL Re создан в 1993 г.), ЮАР (South Africa Special Risks Insurance Association создана в 1979 г.), Намибию (Namibian Special Risk Insurance Association создана в 1988 г.). После 11 сентября 2001 г. различные формы взаимодействия государства и частных страховых компаний на постоянной или временной основе сложились в США (Terrorism Risk Insurance Act 2002, Terrorism Risk Insurance Extension Act 2005), Германии (EXTREMUS создан в 2002 г.), Франции (GAREAT 1 — 2002, GAREAT 2 — 2005), Австралии (Australian Reinsurance Pool Corporation создана в 2003 г.), Австрии (Austrian Terrorism Pool создан в 2003 г.), России (Российский антитеррористический страховой пул создан в 2001 г.) и ряде других стран.

К настоящему времени накоплен значительный опыт взаимодействия государства и частных страховщиков: государство может выступать в качестве администратора соответствующего денежного фонда, спонсировать некоторые программы страхования, выступать гарантом или перестраховщиком. Иными словами, в цепочке управления риском терроризм: страхователь — первичный страховщик — перестраховщик — финансовые рынки — появляется новое дополнительное звено — государство (правительство) как страховщик/перестраховщик/гарант последней инстанции.

Накопленный к настоящему времени опыт функционирования подобного государственно-частного партнерства позволяет говорить об определенных преимуществах: большей прозрачности с точки зрения финансовой ответственности участников партнерства (основания возникновения и размер ответственности); повышения адекватности оценки риска страховщиками и перестраховщиками; возможности снижения страховых тарифов за счет расширения числа страхователей; повышения надежности финансовых рынков, поскольку присутствие государства снижает риск кризисных явлений на рынках капитала как следствия террористических актов.

Следует, однако, иметь в виду, что в данном случае речь идет не просто о финансовой помощи государства коммерческим страховщикам в связи с фундаментальным характером рассматриваемого риска или в связи с недостаточностью финансовой емкости рынка, но в значительно боль-

шей степени об осознании государством своей роли в противодействии современным формам терроризма.

Безопасность, стабильность, уважение к частным правам, отсутствие насилия — признанные, краеугольные камни современного общества и демократического государства. Участие в их обеспечении является непосредственной обязанностью любого государства, поскольку речь идет о создании общественных благ, что никогда не являлось прерогативой рыночного механизма.

Более того, современный терроризм политизирован и часто является ответом на действия самого государства, что определяет дополнительную ответственность государства по террористическим рискам.

И, наконец, наличие партнерства с государством не просто помогает страховым компаниям осуществлять страхование террористических рисков, оно предполагает, а подчас и требует осуществления подобного страхования. Тем самым снижается вероятность негативных тенденций разбалансирования на страховом рынке, когда при наступлении страховых случаев, естественно, увеличивается спрос на страховую защиту от терроризма и одновременно снижается ее предложение. Отсутствие страхового покрытия по тем или иным рискам может оказывать весьма негативное влияние на макроэкономическую ситуацию в стране.

Таким образом, участие государства в страховании рисков, связанных с терроризмом, осуществляется по нескольким направлениям. Государство должно оказывать помощь в быстром восстановлении финансовых возможностей страховой отрасли. В качестве страховщиков/перестраховщиков последней инстанции только государство способно обеспечить достаточный капитал для финансирования наиболее значительных последствий террористических атак. В качестве регулятора государство может обеспечить адекватное правовое регулирование соответствующего вида страхования.

Вместе с тем, говоря о государственно-частном партнерстве, не следует забывать, что страховщики и перестраховщики призваны играть в нем активную роль, обеспечивая необходимую емкость рынка, используя имеющийся опыт организации страховой защиты.

Характеристика риска как не принимаемого или с трудом принимаемого на страхование является относительной. Опыт развития мирового страхования показывает, что риски, считавшиеся не подлежащими страхованию, начинают с течением времени приниматься на страхование и наоборот, страховые компании начинают отказываться от страхования некоторых видов рисков. Возможности принятия риска на страхование различаются по странам в силу различий в национальном законодательстве, по страховым рынкам в силу различий в их финансовых характеристиках, по страховым компаниям в силу их отношения к риску, особенностей финансового менеджмента, возможностей и готовности принимать от страхователей те или иные риски.

В современных условиях вопрос приемлемости или неприемлемости страхования рассматривается не только по отношению к риску «террористический акт». Такие же «проблемные» или «трудные» риски — это риски новых технологий, например нанотехнологий, риски природных катастроф, ядерные риски, риски ответственности директоров и управляющих. Можно вспомнить и о печально знаменитых рисках, связанных с применением асбестосодержащих материалов. Соответственно, те инновационные решения, которые находят страховые компании при страховании этих рисков, могут и должны использоваться при страховании риска «террористический акт».

На наш взгляд, анализ опыта развития мирового рынка страхования позволяет утверждать, что более широкие возможности для принятия рисков на страхования открывает разработка новых страховых продуктов (покрытий), использование мультипродуктов, сочетающих разные виды страхования.

При страховании риска «террористический акт» возможно использование различных методов «справедливого» распределения риска между участниками страховых отношений, что позволяет управлять моральным риском, снижать ответственность страховщика (самострахование, в том числе с использованием кэптивных страховых компаний, установление лимитов ответственности, использование системы франшиз и т. д., использование механизмов сострахования, перестрахования).

Далее, необходимо взвешенное, аккуратное составление правил страхования и условий конкретных договоров страхования, отбор и оценка рисков, обеспечивающие установление приемлемой и адекватной цены страховой услуги. На наш взгляд, современный страховой рынок в состоянии удовлетворить спрос на страховое покрытие в большинстве террористических актов с использованием обычных видов вооружения. Некоторые виды террористических атак, в частности массированные атаки или атаки с применением химического, биологического, ядерного оружия или «грязных» бомб должны рассматриваться как исключения из покрытия. Этому соответствует и существующая в настоящий момент практика развитых страховых рынков: в большинстве стран ядерные, химические, биологические и радиоактивные риски (NBCR) исключены из покрытий по имущественным видам страхования, но включены в число страхуемых рисков по страхованию жизни, здоровья, компенсаций работникам (на развивающихся рынках подобные риски исключены из покрытий по договорам личного страхования). В морском страховании

исключение NBCR рисков применяется ко всем видам договоров, кроме договоров страхования ответственности судовладельца. По оценкам зарубежных специалистов, вряд ли следует ожидать включения NBCR рисков в страховые покрытия в обозримом будущем.

В качестве дополнительного механизма возможно использование секьюритизации, т. е. непосредственного переноса риска на рынки капитала, что может, как и в случаях с рисками природных катастроф, оказаться одним из решений для расширения перечня рисков, принимаемых на страхование.

Наконец, достаточно очевидно, что механизм страхования являются лишь одним из возможных способов управления риском «террористический акт». Не менее важны различные способы обеспечения безопасности, разработка планов действий на случай чрезвычайных ситуаций, разработка и претворение в жизнь превентивных мер по пресечению и предотвращению террористических актов.

Терроризм как угроза социальной и экономической стабильности общества. Страхование террористических рисков

Е. И. Ярмизина

В последние годы российские законодатели предпринимали несколько попыток введения обязательного страхования террористических рисков. Одна их них касалась обязательного страхования от терроризма граждан, выезжающих за рубеж, и была оформлена в виде поправки к закону «О туризме и туристской индустрии» в 2005 г. Еще две попытки были связаны со страхованием гражданской ответственности в результате теракта.

1. Впервые идею о том, чтобы «устроители всех массовых мероприятий в обязательном порядке страховали всех их участников от возможного ущерба в результате терактов» в сентябре 2003 г. высказал Борис Грызлов, занимавший в то время пост главы МВД. И в апреле 2004 г. зам. председателя комитета Госдумы по безопасности Валентин Бобырев подготовил и внес в Государственную Думу *поправки к федеральному закону «О борьбе с терроризмом»*.

Однако тогда депутаты не поддержали его инициативу и возвратили проект автору в связи с несоответствием Конституции Российской Федерации.

Представленный документ не был лишен недостатков и неясностей, а отдельные положения требовали гораздо более детальной проработки. В частности, не были обоснованы лимиты ответственности, и осталось непонятным, почему возможные выплаты жертвам и пострадавшим от терактов были ограничены предлагавшимися рамками. Также в предложенном документе не были установлены тарифы на услуги страховщиков, как в остальных законах об обязательном страховании. Кроме того, у страховой компании, понесшей серьезные убытки в результате теракта, не было права обратиться с регрессным иском к государству.

Несмотря на недостатки и отклонение предложенного проекта, в целом попытка законодателя была оценена положительно. Инициатива депутата не осталась незамеченной, и ровно через год в Госдуму был внесен

2. *Законопроект «Об обязательном страховании ответственности за вред, причиненный в результате террористической акции, совершенной в местах массового пребывания людей».*

Авторы законопроекта предлагали обязать организаторов массовых мероприятий и владельцев мест их проведения страховать посетителей от последствий теракта, а в случае уклонения от страхования — призывать к административной ответственности.

Места массового пребывания людей определялись как торговые, спортивные, развлекательные, транспортные сооружения и другие, используемые в коммерческих целях объекты, на территории которых могут одновременно находиться 200 и более человек. Страхователями должны быть выступать владельцы мест массового скопления людей или организаторы массовых мероприятий, проводимых с целью получения коммерческой выгоды. Ответственность предлагалось страховать в пользу физических лиц, жизни, здоровью или имуществу которых в результате теракта мог быть причинен ущерб. Страховая сумма, в пределах которой страховщики должны были бы возмещать потерпевшим причиненный вред, составляла:

- для мест массового пребывания людей, на территории которых могут одновременно находиться от 200 до 1000 человек — не менее 42 млн руб.;
- для мест массового пребывания людей, на территории которых могут одновременно находиться 1000 человек и более — не менее 210 млн руб.

При этом в законопроекте устанавливался лимит ответственности по одному пострадавшему: в части возмещения вреда, причиненного жизни или здоровью, — 160 тыс. руб., в части возмещения вреда, причиненного имуществу, — 50 тыс. руб. Тарифы на этот вид страхования должны были устанавливаться Правительством России.

Согласно законопроекту, страховой договор заключался между страховой компанией и организатором мероприятия или владельцем сооружения. Название страховщика и реквизиты, с помощью которых пострадавший мог бы получить страховые выплаты, должны были указываться на входном билете на мероприятие.

Вторая попытка введения в России обязательного страхования гражданской ответственности устроителей массовых мероприятий снова оказалась неудачной: меньше чем через 2 недели после внесения Совет Госдумы вернул законопроект авторам законодательной инициативы.

Законопроект «Об обязательном страховании ответственности...» также не был лишен недостатков.

Главным камнем преткновения стал вопрос о том, кто, по сути, должен нести ответственность за произошедший теракт: государство или

устроители зрелищных мероприятий. Ясно, что терроризм — явление, направленное не против какого-либо конкретного мероприятия, а событие более крупного масштаба, провоцирующее страх, панику и нестабильность. Поэтому за действия террористов ответственность должна возлагаться на государство, на силовые ведомства, в ведении которых находятся противодействие и борьба с терроризмом. В свою очередь, предложенный законопроект устанавливал обязательный порядок страхования ответственности лица, не являющегося причинителем вреда. Что, впрочем, не противоречило действующему законодательству, поскольку по закону обязанность возмещения вреда может быть возложена на лицо, не являющееся его причинителем.

Вторым спорным вопросом снова оказались размеры установленных лимитов ответственности: в очередной раз осталось неясным, чем именно обоснованы предложенные в законопроекте размеры компенсаций.

Наконец, в представленном проекте закона был не ясен порядок определения численности людей, которые могут находиться в местах массового пребывания или участвовать в массовых мероприятиях. Предлагалось распространить страховую защиту только на убытки, возникшие в местах проведения массовых мероприятий, на территории которых могут находиться не менее 200 человек. Вместе с тем террористические акты в местах массового скопления людей могут совершаться не только в связи с проведением массовых зрелищных или культурных мероприятий и не только на объектах, используемых в коммерческих целях (как подразумевалось проектом закона).

Законопроектом устанавливалось, что страхователями по обязательному страхованию являются организаторы массовых мероприятий или владельцы мест массового пребывания людей, заключившие договор обязательного страхования. При этом не было четко определено, в каких именно случаях страхователями должны являться организаторы массовых мероприятий, а в каких случаях — владельцы мест массового пребывания людей, от чего, соответственно, зависит, к кому должны были бы предъявлять требования о компенсации ущерба пострадавшие.

Также в случае принятия предложенного законопроекта необходимо было бы введение нового для законодательства института ответственности владельцев мест массового скопления людей и организаций, использующих такие места в коммерческих целях, за обеспечение безопасности посетителей и обязанности возмещать вред, причиненный в результате террористических акций на их территории.

Практика последних лет показала, что государство оказалось не готовым к терактам на всех стадиях — профилактики, пресечения, мини-

мизации последствий, расследования, возмещения пострадавшим ущерба и компенсации морального вреда. В такой ситуации идея переложить затраты на компенсацию ущерба от терактов из госбюджета на организации, занимающиеся массовыми мероприятиями, и упорядочить процедуру получения возмещений потерпевшими лицами казалась значительным шагом в решении давно назревшей проблемы. Законодательная инициатива по введению обязательного страхования гражданской ответственности устроителей массовых мероприятий была положительно воспринята страховым рынком, хотя организаторы развлекательных мероприятий и владельцы мест массового пребывания людей отнеслись к ней настороженно. Тем не менее, законопроект не прошел стадию рассмотрения Советом Госдумы и был возвращен авторам всего через несколько дней после внесения. Очевидно, документ содержал слишком серьезные недостатки и противоречия, поскольку он не был отправлен на доработку, а был возвращен с формальной формулировкой об отсутствии заключения Правительства РФ.

Проблемы и перспективы развития страхования от терроризма

В настоящее время страхование террористических рисков в России находится на начальной стадии развития. Накоплен первый опыт, но в то же время многие вопросы остаются нерешенными.

Основными задачами, которые совместными усилиями предстоит решить российским страховщикам и законодателям в ближайшие годы, являются:

1. Унификация определения риска «терроризм», используемого в страховой практике. В настоящее время существует около двухсот определений этого явления, ни одно из которых не признано общепринятым.
2. Разработка комплексной системы оценки и управления рисками терроризма, а также прогнозирования вероятности совершения террористических актов.
3. Создание статистических баз данных; расширение возможностей обмена информацией о деятельности международных террористических организаций на территории стран Содружества с целью количественной оценки террористических рисков.
4. поиск дополнительных финансовых возможностей для покрытия возможных убытков в результате наступления страхового случая.

Реализация этих задач позволит российскому страховому сообществу разработать и применять более гибкую тарифную политику, а в конечном итоге в значительной степени минимизировать террористический риск и обеспечить надежную защиту населения России от проявлений террористической активности.

Государством должны быть предприняты меры по обеспечению финансовой защиты пострадавших от террористических рисков. Решением сложной задачи обеспечения прав жертв террористических атак может стать, к примеру, принятие отдельного закона, регулирующего страхование всех рисков, связанных с терактами, а не только гражданской ответственности устроителей массовых мероприятий. Разработка подобного закона должна проводиться органами законодательной и исполнительной власти совместно со страховщиками.

Литература

[1] Федеральный закон Российской Федерации «О борьбе с терроризмом» от 25.07.1998 г. № 130-ФЗ.
[2] Проект федерального закона № 38877-4 «О внесении изменения в статью 17 ФЗ «О борьбе с терроризмом».
[3] Проект Федерального закона № 156166-4 «Об обязательном страховании ответственности за вред, причиненный в результате террористической акции, совершенной в местах массового пребывания людей».
[4] Кто будет выплачивать компенсации пострадавшим во время терактов. Поправка к законопроекту по борьбе с терроризмом. Интервью В. Бобырева радиостанции «Эхо Москвы», `http://echo.msk.ru/guests/8898/`.
[5] *Тишкин О.* Насколько проработанным и жизнеспособным является предложенный депутатами вариант закона о страховании от терактов? `http://corporate.renins.com/news_2_1_656_0.html`.

Превентивные мероприятия в системе управления риском «террористический акт»

О. Г. Корягина

В последние годы очень актуальной стала проблема борьбы с терроризмом. Несмотря на то, что в период с 1980 по 1999 годы ежегодно в мире происходило от 182 (в 1997 году) до 1272 (в 1998 году) террористических актов[1], только после 11 сентября 2001 года, когда погибло более 3000 человек из более 90 стран мира[2], все государства активно включились в борьбу с терроризмом, стали вырабатывать меры по пресечению и предотвращению действий террористов, по управлению рисками террористических актов.

Опыт показывает, что предотвращение нестабильности всегда обходится дешевле, чем устранение последствий, особенно, если это касается человеческой жизни. Поэтому на пути борьбы с терроризмом важным этапом становится проведение превентивных мероприятий, позволяющих либо устранить риски, либо минимизировать их, либо снижать ущерб.

Только после выплаты страховыми компаниями огромных сумм по искам, стала очевидна необходимость использования страхования для снижения рисков террористических актов, а не только для устранения их последствий. Поэтому нельзя отделять страховые инструменты от комплекса по реализации превентивных мероприятий в рамках системы управления рисками террористических актов.

В системе управления рисками террористических актов можно выделить следующие методы:

- превентивные мероприятия, позволяющие предотвратить или уменьшить риски;
- превентивные мероприятия, позволяющие снизить величину ущерба;
- передачу риска через страхование (включая создание страховых пулов) и не страховыми методами;

[1] RAND-MIPT, Terrorism knowledge Base (Incident data), источник: `www.rand.org`.

[2] „Policy watch: challenges for terrorism risk insurance in the United States“, Howard Kunreuther, Erwann Michel-Kerjan, October, 2004, источник: `www.nber.org`.

- метод самострахования, то есть создание кэптивов или специальных фондов.

Ключевым методом в системе управления рисками, конечно, является проведение превентивных мероприятий.

Еще в 1999 году в России было принято Постановление Правительства РФ «О мерах по противодействию терроризму»[1], совсем недавно, 6 марта 2006 года был принят закон «О противодействии терроризму»[2], который заменил действовавший с 1998 года закон «О борьбе с терроризмом»[3]. Во всех документах одним из основных принципов противодействия терроризму является приоритет мер предупреждения терроризма, что опять-таки подчеркивает значимость мер управления рисками.

Исходя из фактов терроризма, их предпосылок и последствий каждое государство должно строить свою систему превентивных мероприятий по борьбе с подобными рисками. Приведем приблизительный перечень превентивных мер, требуемых при управлении рисками террористических атак:

- Разработка комплексной системы оценки и управления рисками террористических атак совместными усилиями всех структур и стран, а также стратегии борьбы с терроризмом.
- Создание статистических баз данных и расширение обмена информацией о деятельности террористических групп между государствами.
- Усиление координации между всеми ветвями власти и организациями по противодействию терроризму (включая и международное взаимодействие).
- Постоянный анализ природы террористических групп, то есть особенностей террористических лидеров, их сторонников, окружающей среды, в которой они действуют, структуры террористических организаций и методов их работы.
- Постоянное проведение мероприятий, направленных на выявление и пресечение деятельности террористических групп.
- Определение отраслей, наиболее подверженных атакам, и выработка мероприятий по обеспечению устойчивости деятельности объектов промышленности, транспорта, связи, ядерного, топливно-энергетического и продовольственного комплексов. Наиболее часто террористические атаки совершаются на транспортных путях, поэтому в

[1] Постановление Правительства РФ от 15 сентября 1999 года № 1040 «О мерах по противодействию терроризму» (Собрание законодательства РФ, 20.09.1999, № 38, ст. 4550).

[2] Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» (Собрание законодательства РФ, 13.03.2006, № 11, ст. 1146).

[3] Федеральный закон от 25.07.1998 № 130-ФЗ «О борьбе с терроризмом» (Собрание законодательства РФ, 1998, № 31, ст. 3808).

первую очередь необходимо принять соответствующие рекомендации и требования по эксплуатации транспортных путей, повысить меры безопасности. В качестве конкретных рекомендаций, можно привести следующие, сделанные после исследования причин взрывов в Лондонском метрополитене: установка надежных ограждений, усиление освещенности, использование взрывостойких контейнеров для мусора, монтаж камер наблюдения, увеличение численности охранников[1].

- Меры по усилению безопасности жилых районов, мест массового пребывания людей, в том числе образовательных учреждений, учреждений культуры и спортивных объектов; к таким мерам можно также отнести ужесточение наказания за несоблюдение мер безопасности и невыполнение работниками своих обязанностей по охране объектов.
- Работа по разъяснению населению необходимости бдительности, готовности к действиям в чрезвычайных ситуациях. Очень интересны точки зрения психологов на проблему борьбы с терроризмом: речь в основном идет о формировании определенного психологического состояния у людей, позволяющего сопротивляться влиянию терроризма и о выработке идеи «коллективизма». Учитывая тот факт, что терроризм очень сильно влияет на душевное состояние человека, необходимо повышать психологическую устойчивость граждан, проводя «подготовку к экстремальным ситуациям».
- Меры по усилению регистрационного учета граждан, контроль за миграционными потоками (включая информационное взаимодействие между государствами).
- Усиление работы и обеспечения служб, занимающихся борьбой с преступностью (в том числе в финансовой сфере) и терроризмом.
- Производство и закупка специальных технических средств для структур, ведущих борьбу с терроризмом; разработка и создание мобильных, оперативно разворачиваемых комплексов специальных средств обеспечения безопасности (технической и физической защиты) населения и персонала объектов.
- Принятие мер по недопущению незаконных поставок оружия и боеприпасов, по ограничению и устранению незаконного оборота химических и ядерных материалов, что создает «ресурсную базу» для террористических групп.
- Контроль и анализ финансовых потоков должен стать первоочередной задачей в борьбе с терроризмом. Необходимо определить перечень дополнительной информации для выявления подозрительных финансовых операций. Для уменьшения рисков финансирования террористов необходимо разработать и усилить механизмы и способы обмена информацией. По признанию экспертов ФАТФ (Межправительственной комиссии по борьбе с отмыванием денег), безналичные переводы средств через границы позволяют террористам блокировать доступ к информации, в связи с чем, необходимо устанавливать единые требования к раскрытию информацией во всех странах. Важно выявлять и пресекать потенциальную незаконную деятельность влиятельных политических лиц, используя процедуры повышенного контроля.
- Работа со средствами массовой информации, общественными и религиозными организациями в направлении сплочения населения в борьбе с терроризмом (таковым может являться запрет на распространение информации, которая вызывает межнациональные волнения). Анализ последствий терроризма позволяет утверждать, что в основном задачей террористических групп является дестабилизация в обществе, запугивание людей, которое осуществляется посредством СМИ, поэтому главной задачей в борьбе с террористами должна стать разработка грамотной политики освещения событий через Интернет и СМИ, необходимо также противодействовать распространению экстремистской литературы. Влияние средств массовой информации (СМИ) на развитие терроризма в современном мире постоянно усиливается. Влияние на массовую аудиторию является основным оружием террористов. В связи с этим можно утверждать, что СМИ невольно оказывают поддержку террористическим группам, поэтому работа со средствами массовой информации должна вестись в ключе разработки этических правил освещения террористических событий, развития журналистской этики и наложения запретов на распространение информации, которая вызывает межнациональные волнения. Кроме того, необходимо на законодательном уровне закрепить требования к освещению террористических событий (в настоящий момент они прописаны в ст. 15 закона «О борьбе с терроризмом»[1], который утратит силу с 1 января 2007 года, а в новом законе «О противодействии терроризму»[2] статьи, посвященной «информированию общественности о террористической акции», нет).
- Повышение мер безопасности по защите компьютерных программ, систем и баз данных. Компьютерный терроризм в последние годы с развитием информационных систем, Интернета приобретает все большие масштабы, поэтому необходимо вести разработки по усилению

[1] Jack Riley, Terrorism and Rail Security, 2004, `www.rand.org`.

[1] ФЗ от 25.07.1998 № 130-ФЗ «О борьбе с терроризмом» (Собрание законодательства Российской Федерации, 1998, № 31, ст. 3808).

[2] ФЗ от 06.03.2006 № 35-ФЗ «О противодействии терроризму» (Собрание законодательства РФ, 13.03.2006, № 11, ст. 1146).

систем безопасности информации, чтобы избежать несанкционированного проникновения в базы данных, в другие компьютерные системы. В настоящее время компьютерный терроризм пока остается скорее угрозой, чем большой проблемой, но, не предпринимая необходимых шагов для борьбы с ним, можно опасаться за сохранность многих информационных систем, например, за работу диспетчеров в аэропортах, что создает уже явную угрозу жизни и здоровью людей.

- Проведение политики, направленной на сглаживание внутренних конфликтов в стране, межэтнических противоречий; осуществление систематического анализа социальных и политических волнений и пресечение нарушения прав человека. Нельзя допускать смешения понятий и навешивания ярлыков «терроризм» на религиозные, расовые и этнические группы.
- Принятие и совершенствование законодательных актов по нескольким направлениям: регулирующих антитеррористическую деятельность (включая правила борьбы, структуры и органы, противодействующие терроризму); предусматривающих наказание за преступление; регулирующих финансирование превентивных мероприятий; обеспечивающих работу страховых механизмов.
- Усиление внимания к программам поддержки молодежи, для предоставления им возможности нахождения работы и получения достойного качественного образования.
- Повышения внимания к людям, живущим за чертой бедности (решение социальных проблем позволит избежать социальных конфликтов, недовольства правительством).
- Постоянное пребывание и работа наблюдателей в склонных к конфликтам регионах и странах.
- Решение проблемы воспитания детей; обучения педагогов не только преподаванию соответствующих дисциплин, но и воспитанию. Самой главной проблемой для человечества, лежащей в основе терроризма, является проблема воспитания. Именно от него зависят поступки людей, которые под влиянием различных обстоятельств становятся террористами. Необходимо с детства воспитывать в людях доброту, человечность и любовь к окружающему миру, учить их радоваться успехам других, а не завидовать, а силу направлять в мирное русло.
- Использование страховых механизмов для снижения риска террористических атак. Страхование рисков возникновения террористических атак можно и нужно рассматривать не только с точки зрения его роли при устранении последствий, но и как инструмент, предотвращающий риски и частично уменьшающий величину потерь. Так, принятие законов об обязательном страховании объектов повышенной опасности и страховании людей в местах массового пребывания должно послужить не только инструментом покрытия ущерба, но и предупредительным мероприятием, позволяющим повысить ответственность за соблюдение мер предосторожности на опасных объектах и в местах массового скопления людей и бдительность, позволит избежать халатного отношения к работе.

Хотелось бы подчеркнуть, что приведенный перечень мероприятий не является закрытым. Кроме того, в каждом конкретном случае необходимо продумывать детальный план проведения превентивных мероприятий. Однако, только использование всех мер безопасности в комплексе может дать положительный эффект.

На сегодняшний день очевидна потребность в дальнейшей разработке системы управления рисками, в том числе превентивных мероприятий. Страхование также можно рассматривать как превентивное мероприятие, которое косвенно снижает риски, заставляя страхователей с повышенной внимательностью относиться к охране застрахованных объектов. Поэтому осуществление комплекса превентивных мероприятий и страхования позволит с большей уверенностью смотреть в будущее.

Программно-целевой подход к обеспечению безопасности критически важных объектов от чрезвычайных ситуаций и террористических угроз

В. П. Авдотьин, А. А. Таранов, Ю. С. Авдотьина, С. А. Кададов

В последние годы уделяется особое внимание оценке воздействия по жизненно важным объектам промышленно развитых стран поражающих факторов чрезвычайных ситуаций и террористов обладающих современными средствами поражения и возможных последствий этих воздействий для политической, экономической, экологической и других сфер деятельности государства. В условиях интенсивного развития инфраструктуры промышленно развитых стран существует множество так называемых критически важных объектов (далее — КВО), таких, например, как крупные гидротехнические сооружения, нефте-, газо-, продуктопроводы, сети АЭС, пункты хранения стратегических запасов нефти и газа, вредные химические производства, транспортные узлы и т. п., выведение из строя которых может привести к непредсказуемым тяжелым и даже катастрофическим последствиям в жизнеобеспечении населения. В ряде государств большая часть КВО находится в собственности не государства, а различных фирм и корпораций (например, в Великобритании доля таких объектов достигает 70 %). Список КВО в США включает более 33 тыс. объектов. Из этого списка выделены 1 700 КВО, которые рассматриваются в качестве критически важных с точки зрения национального масштаба.

При рассмотрении критической важности объектов учитывается не только масштаб эффекта нарушения его функциональности, но и такие факторы, как время на его восстановление, например нарушение работы важного объекта в течение короткого времени может иметь меньшие последствия в сравнении с остановкой на продолжительное время менее значимого объекта, кроме того средства на восстановление могут быть различными. Другим важным фактором является взаимное влияние одного объекта на другой, прекращение работы которого имеют большие последствия. В частности, вывод из строя объектов энергоснабжения приводит к прекращению работы телекоммуникационных средств или водоснабжения. Потеря связи к нарушению работы, управления и контроля других объектов, например автоматических аппаратов в банках и т. д.

Наибольшую опасность, по мнению руководства ведущих государств в настоящее время представляет терроризм. Опыт последних событий в мире показывает, что опасность терроризма постоянно возрастает.

Трудности борьбы с терроризмом определяются следующими факторами:

- обычные боевые действия являются полной противоположностью асимметричных действий террористов;
- как правило, организационная структура террористических организаций не позволяет ее быстро обнаружить и оперативно ликвидировать;
- идентификация правонарушителей часто затруднена;
- доктрина терроризма межнациональная и оппозиционна государственной власти;
- цепочка связей внутри террористических организаций запутана и аморфна;
- масштабы материально-технического снабжения террористов относительно невелики, что затрудняет их отслеживание;
- требования по обнаружению отдельных бойцов и разведке баз террористов в различных условиях могут значительно отличаться.

Наиболее развитая система борьбы с терроризмом и защиты КВО создана в США. Она включает разработку необходимой законодательной и юридической основы, весьма значительный объем финансирования, образование необходимых органов управления и подчинение им чрезвычайных служб, оснащение необходимыми техническими и программными средствами. Во многом система обеспечения безопасности КВО становится объектом изучения и примера для других государств, создающих аналогичные системы с учетом национальных особенностей, традиций и особенностей государственного устройства.

В условиях сохранения угроз создаваемых поражающими факторами чрезвычайных ситуаций и террористами обладающими современными средствами поражения одной из важнейших задач становится повышение безопасности населения и защищенности КВО от этих угроз.

По результатам анализа событий 11 сентября 2001 г. в США были сделаны соответствующие выводы. Если в 2001 г. Федеральному агентству по чрезвычайным ситуациям (ФЕМА) на борьбу с терроризмом было выделено около 34 млн долл., при этом 2/3 всех расходов приходились

на органы местной власти, то в 2002 г. расходы выросли более чем на порядок и оцениваются не менее, чем в 3,5 млрд долл. Министерству обороны США выделяется до 8 млрд долл. на решение задач внутренней безопасности и организации помощи, гражданским органам власти. В январе 2003 г. решением администрации президента США в разведывательном сообществе был создан Интеграционный центр террористических угроз. На защиту КВО в 2001 г. выделялось около 2 млрд долл., а после 2001 г. — 25—30 млрд долл.

Существо проблемы для Российской Федерации состоит в том, чтобы, обеспечить повышение уровня защищенности КВО от угроз не только природного и техногенного характера, но и террористического характера, создать в стране необходимые условия для устойчивого развития государства путем координации совместных усилий и финансовых средств федерального центра и субъектов Федерации.

В Российской Федерации в 2006 году принята федеральная целевая программа «Снижение рисков и смягчение последствий чрезвычайных ситуаций природного и техногенного характера в Российской Федерации до 2010 года» (далее — Программа) которая является инструментом, как межведомственной координации, так и координации усилий федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации. Программа обеспечила базовые условия, необходимые для реализации неотложных мер в отношении защиты КВО в соответствии с решениями совместного заседания Совета Безопасности Российской Федерации и президиума Государственного совета Российской Федерации (протокол от 13 ноября 2003 г. № 4).

Применение программно-целевого метода позволит обеспечить комплексное решение задачи по защите КВО на основе:

- определения целей, задач, состава и структуры мероприятий и запланированных результатов;
- концентрации ресурсов по реализации мероприятий, соответствующих приоритетным целям и задачам;
- повышения эффективности государственного управления защитой КВО;
- повышения результативности государственных и муниципальных инвестиций, использования материальных и финансовых ресурсов.

Дополнительные эффекты от применения программно-целевого метода достигаются за счет:

- развития и использования научного потенциала страны в исследовании защиты КВО;

- информационной поддержки и создания инфраструктуры для ситуационного анализа рисков влияющих на защиту КВО;
- координации действий по поддержанию в необходимой готовности сил и средств поддержания устойчивости функционирования КВО в условиях чрезвычайных ситуаций создаваемой террористами;
- реализации комплекса практических мер, исключающих причины снижающие защиту КВО;

обеспечения оперативного реагирования на нарушение функционирования КВО путем оптимизации размещения сил и средств.

При разработке Программы использовались следующие принципы, обеспечивающие обоснованный выбор мероприятий Программы:

- системный подход, комплексность, концентрация на самых важных направлениях и наличие вариантов;
- оценка потребностей в финансовых средствах мероприятий Программы с учетом порядка разграничения расходных обязательств между органами управления всех уровней;
- оценка результатов и социально-экономической эффективности Программы, которая осуществляется на основе расчета целевых показателей.

Системный подход к разработке Программы предусматривает:

- охват всех видов опасностей, влияющих на КВО;
- использование всех способов снижения рисков нарушения работы КВО, в том числе организационных, методических, технических и других, и повышение уровня защиты объектов.

Комплексность мероприятий Программы предусматривает:

- выбор и реализацию мероприятий по повышению защищенности КВО на основе прогнозирования рисков влияющих на их функционирование;
- социальное, техническое, экологическое и экономическое обоснование мероприятий Программы.

Концентрация финансовых средств и организационных усилий Программы на значимых направлениях предусматривает:

- включение в состав мероприятий, в первую очередь межведомственного и межотраслевого характера, реализация которых относится к компетенции и расходным обязательствам федеральных органов исполнительной власти;
- повышение защиты КВО, находящимся полностью под управлением федеральных органов исполнительной власти, а также управляемым совместно с другими органами власти и управления;

- развитие систем, технических средств и технологий, признанных наиболее значимыми и перспективными для решения проблемы снижения рисков нарушения функционирования КВО;
- повышение готовности органов управления, сил и технических средств по выполнению основных функциональных задач, направленных на реализацию мероприятий Программы.

Каждое мероприятие Программы и ожидаемые результаты отобраны из имеющихся альтернативных вариантов достижения цели при различных объемах финансирования.

Альтернативные варианты мероприятий отличаются техническими решениями (использование альтернативных видов технических средств, применение альтернативных технологий и другие), потребностями различных объемов финансовых ресурсов и продолжительностью по времени их реализации.

По каждому мероприятию Программы даны конкретные количественные и качественные оценки социальных и экономических результатов реализации этих мероприятий. При этом под результатами понимаются снижение рисков нарушения работы КВО.

Механизм реализации Программы базируется на принципах партнерства федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления, хозяйственных и общественных организаций, а также разграничения полномочий и ответственности всех участников Программы. Решение задачи по формированию и эффективному управлению реализацией Программы осуществляется путем обоснованного выбора форм и методов управления на основе разграничения уровней управления и распределения функций между органами управления реализацией Программы.

Управление реализацией Программы будет осуществляется на основе смешанного метода управления на 3 уровнях:

- стратегический уровень, включающий Правительство Российской Федерации, Министерство экономического развития и торговли Российской Федерации;
- тактический уровень, включающий государственного заказчика-координатора, государственных заказчиков;
- оперативный уровень, включающий органы управления реализацией Программы (МЧС России и другие органы исполнительной власти Российской Федерации), осуществляющие текущее управление.

Использование такого метода предполагает разделение на тактическом уровне функции по координации деятельности государственных заказчиков между государственным заказчиком-координатором (МЧС России) и специально создаваемым коллегиальным совещательным органом управления, основной задачей которого является координация решений государственного заказчика-координатора и государственных заказчиков по наиболее значимым вопросам (ежегодное планирование и корректировка планов, оценка хода реализации Программы и достигнутых результатов и другое), а также по любым острым проблемам, возникающим при реализации мероприятий Программы.

Соответственно на тактическом уровне управления обеспечивается учет мнений всех государственных заказчиков и не допускается потеря управляемости процесса реализации Программы со стороны государственного заказчика-координатора.

На оперативном уровне управления государственные заказчики самостоятельно осуществляют текущее управление реализацией Программы. При этом выполнение комплексных мероприятий, в реализации которых принимают участие 2 и более государственных заказчика, осуществляется государственным заказчиком-координатором.

Использование этого метода представляется оптимальным, поскольку имеется ряд преимуществ, основными из которых являются:

- обеспечение управления реализацией Программы без излишней бюрократизации;
- учет интересов государственных заказчиков при принятии важных решений на тактическом уровне при одновременном обеспечении высокой эффективности процесса управления реализацией Программы;
- предоставление государственным заказчикам необходимой и достаточной самостоятельности в процессе текущего управления реализацией Программы при одновременном осуществлении государственным заказчиком-координатором оперативного контроля за реализацией комплексных мероприятий.

Программа является важнейшим звеном в построении системы по повышению защищенности КВО. Реализация Программы позволила придать системность, организованность и управляемость деятельности по повышению защищенности КВО в субъектах Российской Федерации.

Программа востребована не только в сфере государственного регулирования и управления, но и обеспечивает прозрачные механизмы и процедуры взаимодействия с бизнесом и общественностью в области повышения защищенности КВО.

Важным целевым приоритетом Программы является разработка механизмов привлечения и расширения участия институтов бизнеса и граж-

данского общества в реализации конкретных проектов и программ в области повышения защищенности КВО.

С учетом уровня угроз для безопасного развития страны эффективное повышение защищенности КВО не может быть обеспечено только в рамках основной деятельности органов государственной власти и органов местного самоуправления. Характер проблемы требует долговременной стратегии и организационно-финансовых механизмов взаимодействия, координации усилий и концентрации ресурсов субъектов экономики и институтов общества.

Распределение сфер ответственности и построения организационной структуры на этапе повышение защищенности КВО основывается на учете их генезиса.

В системе действий по повышению защищенности КВО существенное значение имеют система мер и их технологическое обеспечение, которые могут быть общими для разных по своей природе явлений.

Для повышения у населения уровня подготовленности, сознательности и убежденности в необходимости и важности правильных действий по повышению защищенности КВО, уверенности в эффективности применяемых средств и методов внедрения норм безопасного поведения в окружающей обстановке, а также для оперативного оповещения и информирования населения в чрезвычайных ситуациях с учетом постоянного увеличения потока информации о различных опасностях активно используются современные информационные и телекоммуникационные технологии.

Эти технологии позволяют оповещать, информировать и обучать людей, находящихся в местах массового пребывания (с использованием электронных наружных и внутренних табло коллективного пользования), а также вне зависимости от места их нахождения (с применением различных типов оконечных устройств индивидуального пользования — мобильных телефонов, портативных компьютеров с беспроводным выходом в сеть Интернет, теле- и радиоприемников и др.). Важную роль в прогнозировании опасных ситуаций и своевременности реагирования играют также современные средства профилактического видеонаблюдения в местах массового пребывания людей, а также устройства, обеспечивающие обратную связь населения с персоналом дежурных служб.

Указанные задачи решаются путем создания и функционирования общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей (далее — ОКСИОН), представляющей собой совокупность федеральных, региональных и местных информационных центров, технически объединенных в единую вертикаль приема и передачи информации.

Указанная система по характеру и режиму использования предназначена для государственных нужд. Работы по определению мест размещения, оснащению и разработке регламента использования терминальных комплексов общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей проводятся МЧС России с МВД России и ФСБ России. В соответствии с концепцией и программой создания ОКСИОН в местах массового пребывания людей предполагается ее использование в трех режимах.

Первый режим (повседневное функционирование) ОКСИОН в местах массового пребывания людей используется для подготовки населения по вопросам гражданской обороны, защиты населения и территорий, обеспечения пожарной безопасности и охраны общественного порядка, а также доведения до граждан необходимой информации об основах безопасности жизнедеятельности. Одновременно производится комплексный сбор в местах размещения терминальных комплексов информации о состоянии правопорядка и о поведении отдельных категорий граждан с архивированием результатов наблюдений.

Второй режим (угроза возникновения и возникновение чрезвычайных ситуаций и массовых нарушений общественного порядка) ОКСИОН в местах массового пребывания людей используется для доведения до граждан оперативной информации о параметрах опасностей и угроз, направлениях и скорости их распространения, мерах по защите жизни и здоровья, организации помощи окружающим. В это же время осуществляется комплексный сбор информации для подготовки органами управления МЧС России, МВД России и ФСБ России управленческих решений в целях локализации и ликвидации чрезвычайных ситуаций.

Третий режим (после чрезвычайных ситуаций) общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей задействуется для выполнения комплекса мероприятий, направленных на социальную реабилитацию, оказание психологической помощи населению, всестороннее информационное обеспечение граждан.

Коммерческое использование общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей нецелесообразно и не предполагается.

Принятие общих решений о реализации тех или иных мер по предотвращению чрезвычайных ситуаций и ликвидации их негативных последствий основывается на оценке экономической и общественной эффективности сценариев реагирования.

Исходя из изложенного, при применении программно-целевых механизмов используются следующие алгоритмы действий:

- развитие и использование научного потенциала при исследовании причин возникновения чрезвычайных ситуаций влияющих на устойчивое функционирование КВО;
- информационная поддержка и создание инфраструктуры для непрерывного мониторинга и ситуационного анализа рисков нарушения работы КВО;
- координация действий по поддержанию в необходимой готовности сил и средств реагирования с учетом особенностей технологического содержания и технического обеспечения мероприятий и реализация сценариев реагирования на угрозы устойчивости функционирования КВО на основе оценки экономической и социальной эффективности этих действий;
- реализация практических мер, исключающих возникновение чрезвычайных ситуаций на КВО и или уменьшающих возможный ущерб.

Наиболее проблемной частью единой вертикали реагирования на чрезвычайные ситуации является «зона контакта» научного сообщества и государственного управления. При отсутствии постоянного администрирования процесса такого взаимодействия повышение его эффективности возможно путем применения программных механизмов.

Требует совершенствования взаимодействие федеральных и региональных структур различных ведомств для комплексного решения основных проблем, связанных с защитой КВО.

Необходимый уровень координации действий и концентрации ресурсов при решении задач связанных с защитой КВО и может быть достигнут только при использовании программно-целевых методов. Реализация Программы позволит обеспечить переход к единой системе целевого управления в области связанных с защитой КВО и на базе единых методических подходов.

Снижение рисков чрезвычайных ситуаций всех типов и масштабов и их негативных последствий, а также защита КВО обеспечено реализацией следующих основных направлений Программы:

- системные исследования и совершенствование нормативных правовых, методических и организационных основ государственного управления в области повышения безопасности населения и защищенности критически важных объектов от угроз природного и техногенного характера;
- совершенствование систем мониторинга и прогнозирования чрезвычайных ситуаций, в том числе обусловленных сейсмической опасностью и цунами;

- создание общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей;
- разработка и реализация практических мер по повышению безопасности населения и защищенности критически важных объектов;
- развитие и совершенствование технических средств и технологий повышения защиты населения и территорий от опасностей, обусловленных возникновением чрезвычайных ситуаций, а также средств и технологий ликвидации чрезвычайных ситуаций;
- развитие инфраструктуры информационного обеспечения и ситуационного анализа рисков чрезвычайных ситуаций;
- развитие и совершенствование системы подготовки руководящего состава и специалистов, спасателей и населения к действиям в чрезвычайных ситуациях.

Основными целями Программы являются последовательное снижение рисков влияющих на устойчивость функционирования КВО, повышение безопасности населения и защищенности критически важных объектов от угроз природного и техногенного характера, а также обеспечение необходимых условий для безопасной жизнедеятельности и устойчивого социально-экономического развития страны.

Основные задачи Программы:

- совершенствование научно-методических основ и развитие механизмов координации управления в сфере снижения рисков чрезвычайных и кризисных ситуаций, повышения безопасности населения и защищенности критически важных объектов от угроз природного и техногенного характера;
- совершенствование научных основ анализа опасных природных явлений, возникновения техногенных аварий и катастроф, оценки и прогноза рисков чрезвычайных и кризисных ситуаций, а также оптимизации мер по управлению этими рисками;
- создание общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей, создание научно-методических основ, методов и средств формирования культуры безопасности жизнедеятельности на основе применения современных информационно-телекоммуникационных технологий и технических средств массовой информации;
- прогноз рисков чрезвычайных ситуаций на критически важных объектах и разработка основных элементов государственной политики и комплекса мер по обеспечению необходимого уровня их защищенности;
- совершенствование системы государственного управления и экстренного реагирования в чрезвычайных и кризисных ситуациях;

- совершенствование организационной основы сил ликвидации чрезвычайных ситуаций, тушения пожаров и гражданской обороны;
- развитие и совершенствование системы сейсмологических наблюдений и оповещения о цунами;
- создание национального центра управления в кризисных ситуациях;
- развитие и совершенствование автоматизированной информационно-управляющей системы единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций;
- совершенствование системы подготовки руководящего состава и населения в области предупреждения и ликвидации чрезвычайных ситуаций;
- внедрение системы обязательного страхования гражданской ответственности за причинение вреда при эксплуатации опасных объектов;
- концентрация организационно-технических, финансовых, материальных и информационных ресурсов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации при решении проблемы снижения рисков чрезвычайных ситуаций.

Программа реализуется в течение 5 лет в 2 этапа.

На первом этапе (2006—2007 годы) проведены научно-исследовательских и опытно-конструкторских работ, обследование и паспортизация территорий и объектов, разработана стратегия реализации мероприятий по повышению защищенности критически важных объектов, а также выполнение следующих первоочередных мероприятий:

- реализация существующих и разработка новых целевых программ в субъектах Российской Федерации, осуществление мероприятий, которые позволят повысить безопасность населения и защищенность критически важных объектов, эффективность мониторинга и прогнозирования чрезвычайных ситуаций, уровень информирования и оповещения населения в интересах личной и общественной безопасности;
- систематизация и дальнейшее развитие нормативно-технической и правовой базы в сфере снижения рисков чрезвычайных ситуаций;
- создание первой очереди общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей;
- создание национального центра управления в кризисных ситуациях;
- разработка методических, экономических, организационных основ и механизмов реализации программных мероприятий в полном объеме.

На втором этапе (2008—2010 годы) планируются:

- завершение работ по созданию системы сейсмологических наблюдений и системы оповещения о цунами;
- создание второй очереди общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей;
- создание в федеральных округах центров управления в кризисных ситуациях как структурных элементов национального центра управления в кризисных ситуациях;
- обеспечение требуемого уровня безопасности населения и защищенности критически важных объектов от угроз природного и техногенного характера.

Для проведения оценки эффективности использования средств, выделяемых на реализацию мероприятий Программы как из федерального бюджета, так и из бюджетов субъектов Российской Федерации, проведено разделение показателей Программы по соответствующим финансовым источникам.

Отношение размера средств, направляемых на предупреждение чрезвычайных ситуаций, к размеру предотвращенного ущерба составляет 14 процентов.

Реализация Программы может быть прекращена Правительством Российской Федерации, если величина риска чрезвычайных ситуаций на территории Российской Федерации достигнет приемлемого уровня. Приемлемый уровень риска чрезвычайных ситуаций на территории Российской Федерации устанавливается Правительством Российской Федерации.

Программные мероприятия по решению приведенных выше задач сформированы по следующим направлениям:

1. Системные исследования и совершенствование нормативных правовых, методических и организационных основ государственного управления в области повышения безопасности населения и защищенности критически важных объектов от угроз природного и техногенного характера.
2. Совершенствование систем мониторинга и прогнозирования чрезвычайных ситуаций, в том числе обусловленных сейсмической опасностью и цунами.
3. Создание общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей.
4. Разработка и реализация практических мер по повышению безопасности населения и защищенности критически важных объектов.

5. Развитие и совершенствование технических средств и технологий повышения защиты населения и территорий от опасностей, обусловленных возникновением чрезвычайных ситуаций, а также средств и технологий ликвидации чрезвычайных ситуаций.
6. Развитие инфраструктуры информационного обеспечения и ситуационного анализа рисков чрезвычайных ситуаций.
7. Развитие и совершенствование системы подготовки руководящего состава и специалистов, спасателей и населения к действиям в чрезвычайных ситуациях.

В рамках первого направления решаются задачи связанные с разработкой научно-методических основ возникновения и развития кризисов и катастроф в основных сферах жизнедеятельности государства, формирование научных основ и обоснование приоритетных направлений развития технологической базы в сфере защищенности КВО, развитие и совершенствование научно-методических основ управления рисками чрезвычайных ситуаций, в том числе интегральными рисками, в основных сферах жизнедеятельности государства и др.

В рамках второго направления решаются задачи оптимизации функций, задач и организационной структуры систем мониторинга и прогнозирования чрезвычайных ситуаций, включая контроль состояния источников возникновения чрезвычайных ситуаций, обстановки в зонах чрезвычайных ситуаций, а также в зонах возможного применения средств поражения и на территориях (объектах), в пределах которых (на которых) введен правовой режим контртеррористической операции и др.

В рамках третьего направления решаются задачи гарантированного и своевременного информирование и оповещение населения при угрозе и возникновении чрезвычайных и кризисных ситуаций, профилактика чрезвычайных ситуаций и правонарушений, а также сбор информации о предпосылках возникновения кризисных ситуаций, формирование культуры безопасности жизнедеятельности населения, его подготовка по вопросам гражданской обороны, защиты от чрезвычайных ситуаций, пожарной безопасности и охраны общественного порядка и др.

Создание и введение в эксплуатацию общероссийской комплексной системы информирования и оповещения населения в местах массового пребывания людей осуществляется в 3 этапа:

- 1 *этап* — в городах, в которых размещены региональные центры Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий;
- 2 *этап* — в промышленных центрах, обеспечивающих функционирование базовых секторов экономики и транспортных коммуникаций;
- 3 *этап* — в городах и других населенных пунктах, расположенных в зонах с высокими уровнями природных и техногенных рисков.

Приоритетными территориями для создания и введения в эксплуатацию этой системы являются города и другие населенные пункты, имеющие важное социально-экономическое и оборонное значение, наибольшую плотность населения и концентрацию потенциально опасных объектов, а также характеризующиеся высокими рисками чрезвычайных ситуаций, повышенными угрозами террористических проявлений и проблемами, связанными с охраной общественного порядка. Это обеспечит высокую результативность использования средств федерального бюджета в целях своевременного и качественного информирования и оповещения населения об угрозе и возникновении чрезвычайных и кризисных ситуаций.

В рамках четвертого направления решаются задачи по концентрации усилий и финансов федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и организаций на повышении безопасности населения и защищенности КВО, развитие и совершенствование системы технической диагностики КВО промышленности и инфраструктуры, разработка и реализация при проектировании, строительстве и эксплуатации комплекса специальных инженерно-технических мероприятий и решений, направленных на снижение рисков чрезвычайных ситуаций, разработка специальных инженерно-технических решений, обеспечивающих повышение защищенности КВО при техногенных авариях и катастрофах, стихийных бедствиях, обеспечение защищенности информационных систем КВО, проведение научных исследований и опытно-конструкторских разработок, направленных на создание эффективных средств пожаротушения, развитие и совершенствование специализированных сил и средств для проведения подводных работ специального назначения, связанных с идентификацией и обезвреживанием подводных КВО, повышение защищенности населения и КВО от опасностей, возникающих при террористических актах.

В рамках четвертого направления решаются задачи разработки и внедрения информационных и прогнозно-аналитических систем, в том числе геоинформационных экспертных систем, проведения комплексных исследований с использованием методов математического моделирования для выявления закономерностей в области обеспечения техногенной безопасности, выработки вероятных сценариев развития ситуаций и поддержки принятия необходимых решений, создание условий, исключа-

ющих или в максимальной степени снижающих негативное техногенное воздействие на население, производственную и социальную инфраструктуры и экологическую систему, внедрение более эффективных методов и технических средств мониторинга и оценки состояния обстановки в зонах чрезвычайных ситуаций и др.

В рамках пятого направления решаются задачи повышения оперативности реагирования единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций на чрезвычайные и предкризисные ситуации, как на федеральном, так и на региональном уровнях, обеспечение автоматизированной информационной и интеллектуальной поддержки управленческих решений единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, создание национального центра управления в кризисных ситуациях и др.

В рамках шестого направления решаются задачи развития и совершенствования системы подготовки руководящего состава и специалистов единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, развитие системы информационного обеспечения подготовки и переподготовки специалистов единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций и др.

Седьмое направление традиционное и решает традиционные задачи.

Литература

[1] Постановление Правительства Российской Федерации от 6 января 2006 г. № 1 «О федеральной целевой программе „Снижение рисков и смягчение последствий чрезвычайных ситуаций природного и техногенного характера в Российской Федерации до 2010 года“» (в ред. Постановлений Правительства РФ от 14.07.2006 № 425, от 28.07.2006 № 465, от 12.06.2007 № 370)

[2] Цыгичко В. Н., Смолян Г. Л., Черешкин Д. С. Обеспечение безопасности критических инфраструктур в США (аналитический обзор). Труды ИСА РАН, 2006, т. 27.

[3] Распоряжение Правительства Российской Федерации от 31 октября 2007 г. № 1532-р Концепция федеральной целевой программы «Пожарная безопасность в Российской Федерации на период до 2012 года»

[4] Закон о стихийных бедствиях (P.L. 93-288) от 22 мая 1974 г.

[5] Закон Стаффорда о стихийных бедствиях и чрезвычайных службах (P.L. 93-288) от 23 ноября 1988 г.

[6] Федеральный закон о реформе в области информационной безопасности (GISRA—Government Information Security Reform Act), 2000 г.

[7] Оперативный план взаимодействия правительственных ведомств при борьбе с терроризмом (CONPLAN), директивы президента США № 39 и 62, январь 2001 г.

[8] Директива Президента США № 63 о критически важной инфраструктуре и развертывании Национального центра защиты инфраструктуры (N1PC—National Infrastructure Protection Center) от 22 мая 1998 г.

[9] Национальная стратегия внутренней безопасности, июль 2002 г.

[10] Закон о внутренней безопасности (P.L. 107-296) от 25 ноября 2002 г.

[11] Определение критически важной инфраструктуры, приоритеты и защита. Директива Президента США по внутренней безопасности № 7 от 17 декабря 2003 г.

[12] Указ Президента США 13010 от 15 июля 1996 г. об учреждении комиссии по защите критически важной инфраструктуры при президенте.

[13] Указ Президента США 13228 от 8 октября 2001 г. о централизации системы национальной и внутренней безопасности.

[14] Указ Президента США 13231 от 16 октября 2001 г. о Совете по защите КВИ.

[15] Директива Президента США № 39 от 21 июня 1995 г. по контртерроризму и мерах по обеспечению продовольственной безопасности.

[16] Директива Президента США № 62 от 22 мая 1998 г. по терроризму и защите критически важных объектов инфраструктуры.

[17] Директива Президента США № 5 от 28 февраля 2003 г. по внутренней безопасности МВБ.

[18] Закон о морской транспортной безопасности (P.L. 107-295) от 25 ноября 2002 г.

[19] Закон о береговой охране и морском транспорте (P.L. 108-293) от 9 августа 2004 г.

[20] Закон о безопасности в области здравоохранения, готовности к биотерроризму и реагировании на него (P.L. 107-188) от 2002 г.

[21] Директива МО США 3025.15 об операциях по поддержке гражданских органов управления и помощи населению внутри страны от 1 июля 1993 г.

Часть V

СЕМИНАР-КРУГЛЫЙ СТОЛ «СМИ И ТЕРРОРИЗМ: ВЗАИМООТНОШЕНИЯ, СТРАТЕГИЯ АНТИТЕРРОРА»

Терроризм и СМИ: симбиоз или противостояние? К вопросу о природе современных взаимоотношений

Е. Л. Вартанова, Н. В. Ткачева

Терроризм — не новое явление. Терроризм — плод цивилизации, порождение целого ряда обстоятельств. Обращение к истокам терроризма убеждает, что современный терроризм не является новым социальным явлением, не имеющим прецедента в истории.

Практически у каждого террористического течения имеется исторический аналог, прототип. Характер терроризма в целом, как и смысл отдельных террористических актов, определяется не только сегодняшними социально-политическими, национальными и иными реалиями и противоречиями. Формирование его уходит своими корнями вглубь человеческой истории. Терроризм, как и другие формы протеста, определяется мироощущением и психологией человека, его отношением к обществу и самому себе, его вечным поиском защиты и справедливости.

Глобализация открыла не только новые горизонты демократизации современного мира, но и привела к возникновению новых узлов общественных противоречий, болевых точек демократической системы. Кроме того, она способствовала активизации агрессивного, экстремистского начала в движениях социального протеста, утверждению в нем приверженности тактике насильственных, радикальных действий. Одним из ярких свидетельств этой тенденции стал международный терроризм.

После событий 11 сентября мировое сообщество всерьез столкнулось с публичным характером современного терроризма. Современные террористы организуют массовые убийства, делая их, благодаря современным СМИ, публичными и потому все более шокирующим.

Сегодня однозначно можно назвать одним из важнейших влияние, оказываемое телевидением, радио, периодическими печатными изданиями и Интернетом на общественное мнение. Террористы активно этим пользуются в своей разрушительной деятельности. Особенностью современного терроризма является использование информационно-психоло-

гического воздействия как важного элемента манипуляции сознанием и поведением людей, с помощью возможностей глобальных коммуникаций. 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.

Практически всякому террористическому течению свойственна некая идеология, которая оправдывает жестокость террористического действа, мифологизирует его.

Воздействие террористов на СМИ становится еще более массированным, глубоким и эффективным, если они находятся «в руках» профессионалов, владеющих пером и словом, умело сочетающих в процессе контакта со своей аудиторией рациональную и эмоциональную составляющие преподносимой информации. В этой ситуации последняя воспринимается не только на уровне сознания, но и на более тонком, глубинном, психологическом подсознательном уровне, что гарантирует более полное ее усвоение и длительное управление мировосприятием и поступками человека. Сегодня средства массовой информации являются главным инструментом политического влияния в современном обществе.

Вместе с этим перед ними стоит непростая задача — найти баланс между свободой слова и безопасностью человека и общества, правом общества и его граждан на информацию и гражданской ответственностью СМИ. Составными частями последней в демократическом обществе являются такие часто противоречащие друг другу элементы, как:

- предоставление гражданам объективной и сбалансированной своевременной информации;
- предоставление основным политическим силам и движениям доступа к СМИ;
- обеспечение плюрализма и разнообразия в содержании СМИ;
- использование разнообразных источников информации;
- подотчетность обществу;
- защита общества от паники;
- сохранение эмоционального и морального спокойствия аудитории.

Результаты исследований материалов российских масс-медиа по проблеме терроризма демонстрируют опасное разногласие в вопросах, касающихся общей безопасности, отчужденность и даже враждебность многих СМИ по отношению к государству, правоохранительным и силовым органам в условиях опасности международного терроризма. Невозможность консолидации власти, СМИ и общества в чрезвычайных обстоятельствах стала одной из центральных проблем информационной безопасности в России. Именно поэтому сегодня становится необходимым рассматривать информационную безопасность самым широким образом, не только вводя в это понятие безопасность электронных сетей, связи банков данных, но и обязательно 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.

Как отмечалось выше, современный терроризм немыслим без СМИ. Многие зарубежные исследователи отмечают, что терроризм сегодня имеет симбиотическую связь со СМИ. И задача широко понимаемой нами информационной безопасности — не преградить информации о терроре доступ в СМИ, не ввести цензуру или ограничить свободу слова, а разорвать именно эту симбиотическую связь, без которой террористы не смогут вызывать страх у широкой аудитории. Нельзя согласиться с утверждением о том, что само развитие современных СМИ породило современный терроризм в его нынешнем виде. Напротив, террористы на протяжении всей истории существования этого явления стремились использовать существующие каналы масс-медиа для распространения своих взглядов и информации о своей деятельности. Более того, террористы преследовали целью не только добиться распространения информации о своих деяниях, но и пытались получить у СМИ признания легитимности или моральности своих действий для того, чтобы завербовать сторонников и новых участников.

Французский социолог М. Вивиорка, осмысливая связи СМИ и террора, выделил 4 типа отношений между ними. Первый он обозначил как *полное равнодушие*, причем в этом случае именно террористы не считают нужным запугивать население или пропагандировать свои действия. Второй тип отношений, названный *относительным равнодушием*, предполагает, что террористы не стремятся попасть в заголовки новостей или на первые полосы массовых СМИ, но происходит это потому, что они опираются на собственные медиаканалы для объяснения своей точки зрения. К таким каналам могут относиться проплаченные газеты, некоммерческое вещание из подконтрольных террористам политических или религиозных центров, сайты в интернете. Однако все эти СМИ носят характер альтернативных и не адресуются широкой аудитории. Третий тип отношений — *медиаориентированные стратегии* — направлены на то, чтобы создать террористам максимальное присутствие в СМИ. Террористы в данном случае прибегают к инструментальному использованию СМИ, что стало основной современной формой терроризации

широкого населения. Четвертая форма отношений была определена как «*тотальный разрыв*», и это значит, что террористы относятся к медиаорганизациям, редакторам и журналистам СМИ как к врагам, которых надо наказывать и уничтожать. В этом случае сами журналисты становятся объектами воздействия террористов.

Вовлечение СМИ как социального института и журналистов как профессионалов и граждан в сферу влияния экстремистов происходит под воздействием определенных обстоятельств. Причем в обоих случаях они несколько различны. Можно выделить несколько основных факторов вовлечения журналистов в сферу влияния террористических группировок. Это:

- отсутствие в обществе ясных представлений о национальных интересах, его дезинтеграция и дезориентация, проявляющиеся в отсутствии внутренних этических принципов, потерях перспектив и социального оптимизма;
- отсутствие общих и разделяемых всеми журналистами правил профессиональной деятельности, в том числе и при освещении терактов и деятельности террористических групп, преобладание узкокорпоративных интересов над общенациональными, что является следствием отсутствия системы принципов профессиональной деятельности, профессиональных стандартов и норм, а также отсутствие понимания и критериев оценки вреда, наносимого национальным интересам;
- корпоративная зависимость и незащищенность журналиста от работодателя (страх остаться без работы, власть редактора, собственника издания, групповое давление);
- внутренние причины: психологическая некомпетентность, непонимание собственных психических процессов (неконтролируемая эмпатия, сочувствие «угнетенным»), неспособность к эмоциональному самоконтролю и саморегуляции («стокгольмский синдром»), недостаточно развитые способности логического мышления, неструктурированная, диффузная система ценностей (тщеславие, стремление играть влиятельную роль, желание получить эксклюзив любой ценой и т. д.);
- физическая и правовая незащищенность журналиста (страх мести со стороны экстремистов, лоббистских группировок);
- принадлежность к группам с экстремистской и маргинальной ориентацией (этническим, социальным, референтным).

Деструктивные последствия деятельности СМИ могут стать результатом их вовлечения в сферу интересов террористических группировок, которые стремятся превратить СМИ в инструмент собственного продвижения. Сами СМИ могут вовлекаться в сферу влияния террористических группировок по многим причинам. В их числе наиболее важную роль играют размытая система представлений о содержании национальных интересов; лоббирование интересов групп или политических партий; неограниченная власть главного редактора или владельца СМИ; непрозрачность источников финансирования изданий и программ; отсутствие контроля над СМИ со стороны гражданского общества.

Остановимся подробней на каналах распространения контента террористической направленности. К ним могут быть в принципе отнесены все СМИ, правда, формы взаимодействия создателей контента и самих каналов существенно различаются.

Во взаимодействии с *традиционными печатными СМИ* можно выделить следующие особенности. Самым простым для террористических группировок является издание пропагандистской книжной продукции. В условиях удешевления и децентрализации издательского бизнеса, появления современной множительной техники такая деятельность легко осуществляется самими террористическими группировками. Однако реальную трудность представляет широкое распространение такой продукции, поскольку оно запрещено в конституциях практически всех стран.

Использование террористическими группировками периодической печати предполагает публикацию журналистских материалов — как новостных, так и аналитических — в газетах и журналах. Вполне логичным в этой связи выглядит создание партийных изданий или собственных органов террористических группировок, а также сотрудничество с печатными СМИ, принадлежащими «сочувствующим». Правда, часто такая деятельность часто имеет гипотетический характер: при запрете самих террористических организаций возможности для такой «партийной» журналистики исчезают, и СМИ, «отлученные» от своих идеологов, прекращают свою деятельность.

Более сложная ситуация возникает при освещении проблемы терроризма общеполитическими — непартийными, независимыми — печатными СМИ, создание которых в большинстве стран мира не контролируется государством и его правоохранительными структурами. В этом случае мы видим непосредственное взаимодействие журналистов и источников, находящихся в руках или в связи с террористами, на основе чего журналисты и создают свои материалы. Именно здесь возникает первый узел проблем, связанных с пособничеством терроризму. В условиях актуальности террористических угроз материалы независимой прессы на тему терроризма могут оказывать весьма неоднозначное воздействие на аудиторию, которая пребывает в уверенности, что пресса во всех случаях нейтрально, непредвзято и объективно освещает проблемы терроризма. В большинстве случае так и происходит, однако встречаются и приме-

ры того, как террористы манипулируют журналистами для дальнейшей манипуляции аудиторией.

Важнейший для современной журналистики принцип объективности обязывает журналистов представлять позиции всех упоминающихся в материале сторон. Проявлением этого же принципа во многих журналистских культурах является нейтральность в изложении материала, нежелательность высказывания собственного отношения к происходящему. С другой стороны, и сам этот принцип таит определенные «подводные камни»: журналист может подробно излагать позицию террориста, мотивируя это необходимостью ответного слова «другой» стороны. Он также может, пренебрегая принципом нейтральности, создавать позитивный образ террористов. Играя на естественной в условиях рынка конкуренции СМИ за сенсацию или на противоречиях внутри медиасообщества, террористические группировки умудряются получить доступ к массовой аудитории через практику «вброса»/утечки сенсаций, подкупа или идеологической «обработки» журналистов, декларирующих принципы объективности и нейтральности.

Здесь мы уже сталкиваемся с проблемами журналистского профессионализма, журналистской этики и ответственности журналистов, что должно решаться на уровне журналистского сообщества, но при обязательном участии гражданского общества.

В более жесткие условия террористы попадают при взаимодействии с *аналоговым радио- и телевещанием*. «Старые» электронные СМИ существуют по-прежнему в условиях редкости частот вещания, следовательно, они попадают в сферу особого внимания государственных органов. Создание террористами собственных радио- и телестанций невозможно, так как в большинстве стран аналоговое вещание лицензируется государственными органами. Для трансляции передач иностранных телеканалов на массовую аудиторию в большинстве стран созданы определенные барьеры, преодолеть которые оказывается довольно сложно. Такая ситуация на зарубежных телерынках характерна для катарского канала «Аль-Джазира», предоставляющего право обращения к телезрителям лидерам исламистских террористических организаций. У канала существуют очень серьезные сложности и с вещанием на территории США, и с созданием англоязычной версии, которую заранее отказываются транслировать практически все крупные вещатели и даже кабельные телесети. Однако попадание интервью или телеобращений террористических деятелей международного масштаба в эфир крупных каналов все-таки возможно по упомянутым выше причинам — коммерциализации СМИ, стандартам профессиональной объективности, просто по человеческим симпатиям.

Теоретически возможность проникновения материалов террористической направленности в *рекламные материалы* СМИ значительно выше, чем в журналистские материалы: как правило, журналисты не принимают участие в создании текста рекламы, оставляя его на усмотрение рекламных отделов или рекламных агентств. Вероятность публикации террористических материалов на полосах рекламы, таким образом, выше, чем на полосах редакционных, однако во многих странах мира кодексы рекламных ассоциаций запрещают публикацию материалов, нарушающих законодательство или нравственные, этические и культурные нормы страны. Несмотря на то, что размещение рекламы в СМИ преследует откровенный коммерческий интерес, осознание рекламными сообществами многих зарубежных стран недопустимости определенного типа содержания стимулирует появление кодексов рекламной деятельности. А если, как говорят японские рекламисты, «покупатель — это божество», то и содержания, оскорбляющего или травматизирующего покупателя, реклама допускать не может. Это уже вопрос экономический.

Мы видим, что как в редакционных, так и рекламных материалах СМИ важнейшую роль при публикации материалов террористической направленности играет наличие или отсутствие определенных «фильтров». Они присутствуют как на уровне самих редакций (критерии профессиональной деятельности журналистов, кодексы их поведения, информационные приоритеты СМИ), так и на уровне «сырьевых» поставщиков медиаиндустрии — информационных агентств. На этом уровне мы сталкиваемся с необходимостью анализа принципов отбора информационного «сырья» для журналистов, а также факторов, определяющих формирование «повестки дня» для традиционных СМИ.

Ситуация радикально меняется, если мы обратимся к новой области современного медиапространства — к сектору интерактивных онлайновых СМИ.

Благодаря компьютерным технологиям и телекоммуникационной инфраструктуре доступ террористов к СМИ существенно упростился. Создать материал террористической направленности и сделать его одновременно доступным миллионам людей во всем мире сегодня не сложно. Цифровые СМИ, не попадающие под прежние жесткие формы государственного контроля, в руках террористов становятся новым пластичным и эффективным инструментом воздействия на глобальное общественное мнение.

Кабельное или спутниковое телевидение, не подлежащее государственному регулированию, усиливает вероятность того, что материалы террористического содержания могут транслироваться этими каналами. Исходя из западного опыта, появление «контента террористической

направленности» возможно в эфире отдельных каналов в рамках реализации концепции равного доступа.

Интернет-ресурсы представляют практически неограниченные возможности для пропагандистской и информационной деятельности, для распространения текстовых и мультимедийных материалов, для создания и трансляции сигнала онлайновых радиостанций или даже видеоканалов, для электронной коммерции и коммуникации, как через собственные ресурсы организаций, так и через сайты или блоги отдельных членов сетевого сообщества, сочувствующих экстремистам. Онлайновые представительства крупных СМИ также несколько более свободны в обращении к специфической тематике, чем офлайновые редакции, и могут размещать собственные материалы, полученные текстовые и мультимедийные файлы, а также давать ссылки на ресурсы радикальных и террористических организаций или связанных с ними групп и отдельных активистов.

Возможности электронной коммуникации позволяют проводить структурные изменениях в террористических группах, обеспечивая отказ от обязательной иерархической структуры, переход к сетевому децентрализованному построению организации и делегированию многих функций, в том числе, и пропагандистских, и популяризаторских — на индивидуальный уровень.

Впрочем, отсутствие ограничений в законодательстве многих стран периодически компенсируется инициативами или законодательных органов, или провайдеров доступа к сети, которые могут блокировать тот или иной ресурс. Подобные действия могут предприниматься как в отношении откровенно террористических ресурсов, так и заподозренных в сочувствии группам экстремистов. Например, временные сайты, которые создаются после каждого крупного теракта, в США быстро блокируются властями, в чьих руках сосредоточенно управление доменными адресами Интернета. А Европейская ассоциация провайдеров доступа в качестве важнейшей меры саморегулирования считает лишение доступа в Сети тех производителей контента, которые нарушают закон или общественные порядок и нравственность.

Часто создается впечатление, что СМИ забывают о своей социальной ответственности в обществе, хотя они, несомненно, должны работать для развития правового просвещения людей, выполнять образовательную и воспитательную функцию. В процессе противодействия терроризму конструктивная позиция СМИ не менее важна, чем действия антикриминальных и антитеррористических силовых структур. СМИ должны стать одним из эффективных каналов деятельности институтов гражданского общества, донося до властей независимое экспертное мнение по вопросам борьбы с терроризмом.

Найти тонкую грань, между свободой слова и безопасностью человека и общества, правом на информацию и гражданской ответственностью — это сложная задача, решить которую можно, лишь объединив интеллектуальный потенциал гражданского общества, практиков и теоретиков СМИ и профессионалов силового блока. В поиске баланса между соблюдением свободы слова и необходимостью борьбы с терроризмом многие международные организации — ООН, ЮНЕСКО, Совет Европы — в своих документах сходятся в том, что ограничения свободы слова и информации в рамках кампаний по противодействию терроризму недопустимы, так как это нарушает одну из фундаментальных свобод человека, которую стараются низвергнуть террористы. Свобода слова рассматривается как основной ресурс для борьбы с экстремизмом и терроризмом, однако при соблюдении важнейшего профессионального принципа — социальной ответственности СМИ перед гражданским обществом. В то же время некоторые документы ограничиваются достаточно расплывчатыми формулировками в отношении пределов допустимых ограничений. Это связано с различными политическими культурами в разных странах, что не позволяет выработать универсальных механизмов гарантирования свободы слова и условий соблюдения социальной ответственности.

Каждая страна должна найти свои решения, опираясь на свои традиции в сфере масс-медиа и свободы слова, в области взаимодействия государства — гражданского общества — СМИ. С другой стороны, очевидно, что необходимые решения всегда лежат в сфере информационной политики, и набор «действующих сил» во всех национальных контекстах остается одним и тем же.

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 (до сих пор не принят закон о защите молодежи от деструктивной информации). Общественный контроль является главным условием начала процессов самоорганизации и саморегулирования в структурах СМИ.

Саморегулирование в свою очередь придает смысл и стержень деятельности журналистов и медиаинститутов, служит естественным иммунитетом против террористических и антиобщественных идей. Внутренний контроль способствует саморазвитию системы, повышает её жизнеспособность и адекватность. Саморегулирование и самоорганизация способны восстановить нормальное функционирование СМИ в российском обществе.

Как показывает опыт развитых демократий, внутренний самоконтроль журналистского сообщества помогает существенно упростить и удешевить необходимый внешний контроль со стороны государства. Но вместе с тем внутренний контроль только дополняет единственную возможную форму внешнего контроля — контроля со стороны гражданского общества, то есть самих читателей, слушателей, зрителей и пользователей. Именно этот контроль призван осуществлять обратную связь общества со СМИ. Сегодня в российских условиях только развивающееся гражданское общество — в сотрудничестве с государством и профессионалами антитеррористических структур — должно инициировать создание механизма и рычагов 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.

СМИ в условиях террористической угрозы: медиапсихология против политтехнологии

Е. Е. Пронина

Терроризм в его современных масштабах не может существовать без активного вовлечения СМИ. В условиях глобального информационного общества СМИ многократно увеличивают «поражающую силу» любой технологии воздействия, начиная от актов устрашения до целенаправленной дезориентации: лжи, лести, подкупа, запутывания, подрыва базовых убеждений и ценностей и т. д. Речь идет не только и не столько о беспрецедентной массовости «поражения», обусловленной сетевым характером электронных СМИ, сколько о глубинном изменении, направленной трансформации культурного кода и ментальности общества, становящихся главной мишенью воздействия.

Информационные политические технологии, разрабатываемые сегодня террористами и соответствующими лобби, носят запланировано «вирусный» характер: их отличает продуманная режиссура, рассчитанная на внешнюю эффектность и широкий резонанс, интенсивная сетевая поддержка в виде интернет-сайтов, форумов, теле- и радиостанций, а основная цель состоит в том, чтобы провоцировать дискуссии и сомнения, создавать фобии, называя черное белым, смешивая потребность в самоопределении и стремление к господству (односторонним привилегиям), стирая различие между справедливостью и произволом, оправдывая насилие «благородными» целями, выдавая информационный террор за свободу слова и т. д.

Специфическая особенность и основная опасность внедрения политтехнологических «вирусов» состоит в том, что присоединяясь к наиболее важным понятиям и ценностям, составляющим основу идентичности и самоопределения общества, вирусы затемняют и искажают их значение, постепенно блокируя этим жизненно важные функции социальной системы. Подобно биологическим вирусам, вирусы информационные стремятся захватить контроль над системой, подавив аутентичные механизмы регуляции собственной программой. «Это — самая настоящая битва за

управление клеткой, которую ведут генетическая программа самой клетки (её ДНК) и вирусный код-захватчик»[1].

Вирусный характер хорошо просматриваются в нашумевших террористических актах последних десятилетий. Самый крупный из них — теракт 11 сентября был продуман до мельчайших подробностей, не только в отношении подготовки и организации, но и в том, что касается сопряженных и отсроченных эффектов. Удар был направлен непосредственно в символ западной культуры и экономики, падение башен-близнецов должно было сокрушить веру в неколебимую мощь западной цивилизации, неуязвимость её адептов и сторонников. Гигантские башни были видны отовсюду. Это означало тысячи снимков и видеозаписей, сделанных невольными свидетелями в самых разных точках города и с самых разных ракурсов. И каждый из снимков, переданных затем по сети Интернет и СМИ, обладал жуткой «картинностью», вызывая одновременно мистическое и эстетическое потрясение. Мистический и символический эффект свершившегося должен был найти дополнительное подтверждение в мистических «совпадениях», сакрализирующих смысл произошедшего. Так, спустя несколько дней после теракта как бы случайно открылось, что обозначение одного из рейсов, использованных террористами, при отображении в символьном шрифте Wingdings достаточно однозначно указывает на фатальные события:.

Q33 NYC — ✈🗎🗎 ☠✡🕯

Примечательно, что информация эта распространилась первоначально по неофициальным каналам, среди интернет-пользователей и лишь затем была опубликована в печати:

Название рейса Нью-Йорк — Бостон содержало зашифрованную информацию о катастрофе

В конце прошлой недели Интернет вновь запестрел паническими сообщениями из Америки. Десять дней спустя после терактов, аккурат перед окончанием национального траура, поднялась новая волна истерии. Аббревиатура рейса Нью-Йорк — Бостон «Q 33 NY» оказалась ПРЯМЫМ предупреждением об уничтожении двух небоскребов-близнецов. Более того, любой желающий может убедиться в этом лично.

Если «Q 33 NY» набрать в любом текстовом редакторе, а затем перевести надпись в шрифт Wingdings, получится следующая картинка:

✈🗎🗎 ☠✡

[1] *Рашкофф Д.* Медиавирус! Как поп-культура тайно воздействует на ваше сознание. М.: Ультра. Культура, 2003. С. 14.

Невооруженным глазом виден самолет, два прямоугольника, напоминающих небоскребы, потом знак смерти и мистическая гексаграмма — Соломонова звезда, знак макрокосма. С первыми четырьмя символами все понятно. Пятый же — гексаграмма — согласно энциклопедии оккультизма, обозначает не только принадлежность к иудейству, но и рассматривается как общая схема хода феноменов в природе. А в самом широком смысле подчеркивает судьбоносную подоплеку события вообще.

Строго говоря, получается какая-то безумная мистика. Компьютерный шрифт предсказал катастрофу?

Шрифт Wingdings является набором значков (...) *Он используется крайне редко, в основном при издании узкоспециальной литературы и входит в обязательный стандартный набор шрифтов Windows. Кто первый придумал перевести аббревиатуру нью-йоркского рейса в режим этих символов, неизвестно. Однако весть об этом впечатляющем открытии тут же облетела весь Интернет. Мистически настроенные пользователи утверждают, что и обычные буквы по одиночке ничего не значат. Однако будучи сложены в сочетания, образуют слова...*[1]

«Пророчество», передаваемое пользователями друг другу по сети и изустно, очень быстро и широко *самораспространилось* в Интернете и за его пределами, повсеместно сея тревогу и возбуждая мистический трепет. Весьма характерная особенность. Именно эта способность самораспространяться, используя активность зараженных элементов системы, составляет специфическую особенность вирусов как таковых и вирусных сообщений, в частности. Самораспространению способствует яркая, привлекающая внимание, пугающая или завлекающая «оболочка» вирусов. По мнению известного американского специалиста в области средств массовой информации Д. Рашкоффа, медиавирусы «распространяются тем быстрее, чем сильнее они пробуждают наш интерес... Чем более провокационна «картинка» или знак — будь то заснятые на видео бесчинства полиции или новый текст известного рэппера — тем дальше и быстрее они путешествуют по инфосфере»[2]. Сегодня это специфическое свойство медиавирусов целенаправленно используется в рекламных

[1] Цит. по: *Ткачук О. В.* Слух и СМИ: альтернатива или контрапункт? // Проблемы медиапсихологии-2. М.: РИП-холдинг, 2003. С. 56—57.

[2] *Рашкофф Д.* Медиавирус! Как поп-культура тайно воздействует на ваше сознание. М.: Ультра. Культура, 2003. С. 15.

стратегиях (так называемая вирусная реклама и маркетинг), шоу-бизнесе и политтехнологиях, что позволяет достигнуть сразу три цели: сэкономить средства на распространение и продвижение идеи, максимально широко внедрить нужное послание, и, самое главное, сделать это настолько незаметно, «спонтанно», что поражаемая система, не подозревая о вирусной интервенции, не оказывает никакого сопротивления. В этом ослаблении защитных сил, иммунной системы общества — одно из самых опасных последствий успешной атаки вирусов.

Современные стратегии политической борьбы, в том числе стратегии, используемые террористами, все более приобретают вирусный характер. В глобализирующемся мире соединение методов политической борьбы с новыми информационными возможностями привело к возникновению самого, должно быть, зловещего феномена конца XX–начала XXI века: политтехнологии.

И что характерно, четкой дефиниции этой самой политтехнологи до сих пор нет, словно ни ученым, ни идеологам, ни правозащитникам просто не хватает духу прямо взглянуть на грозное объективное явление.

«Политтехнология — это какое-то странное слово, которое непонятно что обозначает» — кокетничает профессиональный политтехнолог, небезызвестный директор «Фонда эффективной политики» Г. Павловский[1].

«Если брать расхожее определение политтехнологии как искусства разводить массы, — дает оценку явление профессиональный публицист Максим Соколов, — то при таком циническом взгляде на вещи 9 (22) января, именуемое также Кровавым воскресеньем, может считаться профессиональным праздником политтехнолога»[2].

Но ни умолчание, ни кокетливая самоирония не скроют уже того факта, что *политтехнология* сегодня — не конкретный прием и не частный случай, а системное явление, стремящееся использовать сетевую структуру общества, чтобы проникнуть во все поры социума, стать способом существования его институтов, социальных групп и индивидов.

В противоположность спонтанным и суверенным формам социально-психологической самоорганизации социумов, как например, «общественное мнение», «личная безопасность», «национальные интересы» и т. п., политтехнология целенаправленно создается как вирусная программа, по которой достигается полный контроль над жизнеобеспечивающими функциями системы и в требуемом режиме задействуются информационные, финансовые, административные и людские ресурсы, чтобы получить вполне конкретный и, главное, материальный результат.

[1] `http://www.newizw.ru/news/2005-08-26`.

[2] `http://www.exprt.ru/columns/205-01-24`.

Противодействие разрушительным политтехнологиям становится первоочередной задачей, идет ли речь об антитеррористической борьбе, разделении сфер влияния в международной политике или вмешательстве внешних сил во внутренние дела суверенного государства. Однако трудность состоит в том, что в полном соответствии с русской пословицей: «Волк волком не травится», — *политтехнология политтехнологией не вышибается*. Опасность использования политтехнологий не снимается, даже если политтехнология применяется не извне, конкурирующей системой, а изнутри определенными структурами общества в отношении другой части общества с целью «стабилизации обстановки» или дезактивации внешних вирусов. Но с какой бы стороны ни применялись политтехнологии, общество в любом случае проигрывает и платит, как показал опыт преодоления последствий терактов, стокгольмским синдромом, разочарованием в национальных лидерах, диффузией идентичности, безнадежностью и депрессивным раптусом[1] масс.

Деструктивную роль играют попытки манипулировать общественным мнением в обход интересов самого сообщества, когда оно рассматривается в качестве условия или средства решения тех или иных «стратегических задач». Подобный подход часто считается само собой разумеющимся и тогда необходимость «стабилизации обстановки» ставится выше решения конкретных проблем пострадавших (так как требует меньших затрат). Характерными особенностями взаимодействия официальных структур с населением в чрезвычайных обстоятельствах являются, по наблюдениям одного из ведущих отечественных специалистов в области психологии катастроф, д. психол. н. А. У. Хараша, следующие:

- «Успокоительные» манипуляции органов управления. Попытка преуменьшить опасность.
- Апелляция к закону больших чисел, «допустимых жертв».
- Нравственная дискредитация пострадавших путем интерпретации их действий, направленных на самосохранение, как стимулируемых потребностью в комфорте и дополнительных благах.
- Отсутствие институтов контроля, законности (защиты и компенсации) и добровольности[2].

Работая в составе экспертных групп по оценке психологических и гуманитарных последствий крупных катастроф, экологических кризисов и вооруженных действий, в том числе в регионах радиоактивного зара-

[1] *Ханыков В.* Кому будет польза, если народ впадет в депрессивный раптус? // Комсомольская правда. 1992, 1 февраля.

[2] *Хараш А. У.* Гуманитарная экспертиза в экстремальных ситуациях: идеология, методология, процедура // Введение в практическую социальную психологию. М.: Смысл, 1999. С. 110.

жения на Украине и в Белоруссии, местах проживания вынужденных переселенцев, в зоне Юго-Осетинского конфликта и других, исследователь заметил, что информационные и интерактивные стратегии власти, используемые в экстремальных обстоятельствах, «могут служить ничуть не менее травмирующим фактором, чем сама по себе природная или техногенная угроза»[1]. Это обусловлено тем обстоятельством, что «органы управления в оценке риска в экстремальной ситуации ориентированы, как правило, на интересы ведомств, фирм и государственных институтов, тогда как население руководствуется восприятием реальности»[2]. Свою задачу официальные структуры понимают как «успокоение» населения, а не решение проблемы, вызывающей тревогу. Отсюда замалчивание, искажение фактов, призывы сохранять спокойствие ради блага страны в целом. «Примером, — пишет А. У. Хараш, — могут служить эксперты Минздрава, неуклонно проводившие в зоне чернобыльской катастрофы «успокоительную» пропаганду, но питавшиеся при этом исключительно привезенными с собой продуктами и оставлявшие в зоне одежду, которую они там носили»[3].

Весьма травмирующим для населения оказывается и негласно подразумеваемый властью приоритет количества (малое число людей должно поступиться своими интересами ради большего числа), преимущество одних групп перед другими — «принуждение к жертве» одних ради других. В соответствии с этим неписаным правилом высшие представители государства считают возможным призывать людей, пострадавших от вооруженного налета, потерявших своих детей, родных и близких, к примирению и спокойствию во имя мира в данном регионе и даже (!) грозить наказанием ослушавшимся. Понятно, что для государства это важная цель, но насколько в конечном итоге будет эффективна такая стратегия? Ведь заставить больного молчать и не двигаться, чтобы не тревожить остальных, не только жестоко по отношению к больному, но и в высшей степени недальновидно. Болезнь, если её не лечить по-настоящему, может превратиться в эпидемию.

Подобные стратегии государственных структур разочаровывают и деморализуют население. Последующие денежные вливания в пострадавшие районы не только не компенсируют нанесенного психологического ущерба, но даже усугубляют его, усиливая пассивность пострадавших, формируя синдром «выученной беспомощности», обращая праведный гнев в деструктивную агрессию в том числе против самого государства.

[1] *Хараш А. У.* Цит. соч. С. 110.
[2] Там же, с. 108.
[3] Там же, с. 121.

Иной подход можно видеть в ряде западных стран, также становившихся жертвами террористических атак. Центральным моментом психологически выверенной речи Президента США Дж. Буша, прозвучавшей на следующий день после теракта 11 сентября, было обещание неотвратимого наказания виновным: «Мы найдем, мы покараем и террористов, и их укрывателей»[1]. Только при этом условии президент мог позволить себе заявить, и имел право надеяться, что: «Террористы разрушили наши здания, но им не удастся разрушить духовные устои нашей нации».

Помимо публичных заявлений, государством были предприняты активные действия по обеспечению защиты населения от возможной новой угрозы, широко освещавшиеся всеми средствами массовой информации: беспрецедентные меры безопасности в аэропортах, на дорогах, в общественных местах. Ничто не казалось власти чрезмерным. Вскоре последовали удары по базам террористов. Пусть постфактум, но была раскрыта террористическая сеть, связи и соучастники заговорщиков. По всему миру разыскивались (и были арестованы) сообщники террористов-смертников. Любой сигнал об опасности принимался во внимание. Спустя несколько месяцев был объявлен общенациональный день психического здоровья, с тем чтобы выявить всех нуждающихся в эмоциональной и иной поддержке, дойти до каждого, заглянуть в каждый дом. Людей призывали внимательнее посмотреть друг на друга, оказать помощь, если это по силам, или привлечь соответствующие социальные службы.

Однако в дальнейшем администрация США поспешила использовать удобный момент для решения экономических и политических задач определенной группы лиц, близкой к власти. Сопровождаемая не слишком убедительными фактами и наспех скомпилированной риторикой о необходимости искоренения терроризма, началась затяжная война в Ираке. И сама война, за которой изначально стояла быстро обнаруженная ложь и подтасовка фактов относительно якобы имеющихся у Ирака лабораторий по производству химического оружия и баз террористов, и пафосные речи политиков о защите американских интересов и демократии во всем мире привели в конце концов к хорошо знакомому синдрому снятия вины с агрессора и поиску виноватых в собственном стане. Так в самой Америке (!) неожиданно нашла поддержку и активно стала муссироваться в Интернете и СМИ идея, которую ранее осмеливались высказывать только самые оголтелые противники «американского империализма». Согласно этим ожившим подозрениям, башни Всемирного торгового центра

[1] Подробнее речь см.: *Пронин Е. И.*, *Пронина Е. Е.* Архетипы тотальной войны в локальном конфликте // Государственная служба. № 4 (14), декабрь 2001—Январь 2002.

взорвали сами спецслужбы[1]! Вот мнение члена Американского института архитекторов, одного из инициаторов петиции архитекторов к Конгрессу США, Ричарда Гэйджа: «Шок, в который повергли нас террористические атаки, помешал тогда рационально оценить случившееся. Мы поверили в миф о том, что башни-«близнецы» обрушились из-за самолетов. Теперь же нам очевидно, что имел место профессиональный демонтаж с использованием взрывчатки. Всем известно, что подобная операция требует сложной системы минирования. С учетом существовавшей в Торговом центре системы контроля и безопасности трудно представить, что все эти работы могли беспрепятственно осуществить террористы. Так мы приходим к ужасному выводу: теракт мог быть «срежиссирован» в правительственных кругах США»[2].

Подобные противоестественные идеи могли бы показаться просто случайным завихрением человеческой мысли, вызванной состоянием фрустрации, если бы точно такие же подозрения не возникли бы за несколько лет до этого в другом полушарии, в другой стране с иной ментальностью, с иным анамнезом, иным стилем управления, но в сходной ситуации. Речь идет о взрыве домов на Каширском шоссе, породившем обвинение ФСБ в причастности к трагедии.

Совершенно очевидно, что подобное сходство не может быть объяснено случайностью, тем более родством душ. Это симптом болезни, вирусного заражения, вызванного ослаблением иммунной системы общества. Весьма вероятно, что вирус был разработан одновременно с терактами и распространен непосредственно после их исполнения. Возможно, вирус самозародился, подобно спонтанной мутации под воздействием неблагоприятных факторов. Но каким бы образом он ни возник, вряд ли кто-либо воспринял бы столь противоестественную идею всерьез, если бы не травмогенные, манипулятивные и потому неправомерные информационные стратегии самой власти. Неважно, что в каждой из двух стран эти стратегии были неправильны по-разному. В России власть избегала называть и преследовать подлинных виновников случившегося из-за боязни «дестабилизировать ситуацию». В США власть искала виновных там, где ей было выгодно. И в том и в другом случае, результат был один — аутоагрессия: обращение гнева населения на нерелевантный объект, какую-либо важную структуру внутри самого общества, что, с одной стороны, пугает людей еще больше, с другой, подрывает национальное единство и способность к мобилизации. Политтехнологические ухищрения власти,

[1] Башни 11 сентября Америка взорвала сама! `http://www.kp.ru/daily/23965/72873` (26.10.2007).

[2] Там же.

таким образом, привели к обратным (от желаемых) эффектам, создав благоприятную почву как для внедрения патогенных вирусов, так и для самопроизвольных мутаций «природного кода» общества.

Другой проблемой становится неспособность власти и общества вовремя распознавать и купировать вирусные технологии, поражающие СМИ. Неинформированность общества, некомпетентность и неповоротливость органов управления приводит к бесконтрольному обращению информации, наносящей прямой ущерб национальным интересам и морально-психологическому состоянию общества.

Наиболее частотной «вирусной инфекцией», сопровождающей освещение терактов в СМИ, является дискредитация действий спасателей и силовых подразделений, то есть именно тех, кто олицетворяет надежду населения на защиту и справедливость. Посеять сомнения в надежности, честности, бескорыстии спасателей значит блокировать способность к сопротивлению, лишив людей веры в то, что общество в состоянии защитить их. Несмотря на очевидность этого психологического факта, российские СМИ зачастую преподносят действия властей и спасателей так, как будто именно власть, силовые структуры и спасатели являются истинными виновниками терактов, то есть фактически воспроизводят вирус стокгольмского синдрома. Весьма типичным в этом смысле является материал, помещенный спустя год после трагедии в Беслане в одной из центральных газет: «Беслан: 10 вопросов, на которые нет ответа»[1]. Само название статьи призвано возбудить обиду у читателя. Далее следуют риторические вопросы, сопровождаемые расхожими слухами и домыслами:

- Можно ли было предотвратить захват школы?
- Сколько боевиков захватили школу и удалось ли кому-нибудь уйти после штурма?
- Было ли оружие заранее спрятано в школе?
- Почему боевики сделали исключение для Аушева?
- Почему загорелась крыша спортзала?
- Сколько раз стрелял танк и по каким целям?
- Почему взорвались бомбы в спортзале?
- От чего погибли заложники?
- Был ли спланирован штурм 3 сентября?
- Возможен ли был мирный уход террористов?

Девять из десяти поставленных вопросов переводят внимание читателя с заказчиков и исполнителей теракта на оценку действий служащих школы, спасателей и силовиков. Подразумевается, что действия эти были неправильные: захват школы можно было предотвратить (правда,

[1] Беслан: 10 вопросов, на которые нет ответов // Известия. 1 сентября 2003 г.

автор не сообщает, как именно), оружие можно было отыскать (хотя в действительности было установлено, что оружие боевики принесли с собой), крыша спортзала загорелась из-за неосторожных провокационных действий силовиков и т. д. Таким образом, постепенно вырисовывается «истинный виновник» произошедшего. Журналист старательно ищет любой намек на действия тех, кого менее всего можно было бы обвинять, людей, которые были виновны только в том, что жили мирной жизнью в мирное время и даже не могли вообразить подобного зверского преступления. При этом не приводится ни одного реального факта или доказательства. Ограничиваясь предположениями («если допустить, что среди неустановленных 66 трупов тоже были заживо сожженные, напрашивается вывод о десятках сгоревших, которых можно было спасти при эффективно организованном пожаротушении...»), слухами («говорят, что наряду с боевиками в камуфляже 1 сентября у школы видели боевиков в балахонах...») и домыслами («Разумеется, Хучбаров перед походом на Беслан готовился к встрече с Аллахом...»), силясь оправдать агрессора и возложить вину на всех остальных, автор создает питательный бульон для вируса стокгольмского синдрома. Действия боевиков описываются зачастую бравурно-высокой лексикой (так, например, преступление Басаева против человечности в Буденновске называется «триумфальным возвращением террориста № 1...»). Заключительная фраза оставляет впечатление, что именно несговорчивость и имперская гордость «Москвы» причина негативного развития событий: «Поход на Беслан преследовал не менее амбициозные цели (имеется в виду захват Басаевым больницы в Буденновске), согласиться на которые Москва вряд ли смогла бы».

Среди поставленных вопросов есть только один, ответ на который мог бы вскрыть подлинные мотивы преступления, дезавуировать заказчиков и исполнителей теракта: «Почему боевики сделали исключение для Аушева?». Однако здесь журналист обходится самыми общими и обтекаемыми фразами, скорее запутывая, нежели проясняя суть вопроса.

Распознавание вирусов и вирусных технологий затрудняется их мимикрией под спонтанную, бескорыстную активность индивидов: утверждение справедливости, защиту демократии, прав человека, а также другие наиболее актуальные и значимые идеи и ценности современности. Присоединяясь к наиболее важным понятиям, вирусы тем скорее поглощают и разлагают их, превращая в труху или полную противоположность. Триумф бархатных революций в Югославии, Грузии, на Украине обернулся ползучим политическим кризисом, социальным расколом, экономическими потрясениями, извращением демократии, деградацией национальных лидеров. Гуманистическое «принуждение к миру» послужило прикрытием этнических чисток и прямой военной поддержки своих союзников (Косово). Борьба с мировым терроризмом стала удобной ширмой для начала раздела сырьевых ресурсов (Ирак).

Но каков бы ни был практический результат вирусных технологий, духовный и моральный урон превосходит все возможные материальные и территориальные потери, поскольку грозит утратой самой возможности регенерации и самостоятельного аутентичного существования социума.

Учитывая специфику вирусных поражений, можно констатировать, что единственной радикальной защитой от всевозможных политтехнологий является активизация способности к сопротивлению самого общества.

Все, что усиливает способность к самодетерминации, все, что повышает уровень самоосознания, все, что расширяет возможности самореализации — все это ослабляет возможность вирусной модификации коллективной ментальности, усиливает иммунную защищенность, автономность и суверенность общества. Основной формой самоосознания общества и средством становления национальной ментальности является массовая коммуникация. Психодинамика взаимодействия и развития индивидуального и коллективного сознания в системе массовой коммуникации является предметом специальной отрасли науки — медиапсихологии. Медиапсихология рассматривает массовую коммуникацию как форму коллективного мышления, определяющую образ жизни, ментальность социума и способ самоопределения индивидов. Но в отличие от политтехнологий, использующих научные достижения исключительно для манипуляции общественным мнением и рассматривающих аудиторию в качестве средства достижения внешних (политических, экономических, групповых) целей, для медиапсихологии аутентичность аудитории — цель, поскольку саморазвитие и самоопределение общества составляет условие существования массовой коммуникации, за пределами которого и массовая коммуникация и журналистика вырождаются в вирусный алгоритм программирования общественной жизни.

Ориентируясь на саморазвитие и самоопределение общества как единственно возможную непатологическую модель массовой коммуникации, медиа-психология играет роль естественной антиивирусной программы в ситуации массированных информационных атак. Необходимость информационно-психологической самозащиты как условие существования массовой коммуникации на современном этапе обуславливает развитие трех взаимосвязанных направлений медиапсихологии: *медиааналитики*, *медиатерапии* и *медиаобразования*. В задачи *медиааналитики* входит прежде всего анализ контента массовой коммуникации с точки зрения соблюдения принципов информационно-психологической безопасности, выявление психотехнологий массовых

информационных кампаний и их последствий, психологические, юридические и этические аспекты журналистской деятельности. В настоящее время классифицированы возможные патогенные факторы журналистского воздействия, разработаны основные категории экспертизы контента массовой коммуникации[1]. Недавние исследования работы прессы по освещению последствий террористических актов и чрезвычайных ситуаций свидетельствуют, в частности, о том, что «журналисты зачастую не учитывают динамику развития психических состояний пострадавших»[2], усиливая деструктивное воздействие события. Между тем для освещения каждого этапа ЧС должны применяться адекватные информационно-психологические приемы. «Непосредственная передача экстремальных переживаний порождает массовое заражение и приводит к всеобщей травматизации социума»[3].

Отсюда вытекает необходимость разработки систем и способов психологической защиты от патогенных информационных технологий, что составляет предмет второго направления медиапсихологических исследований — *медиатерапии*. В задачи *медиатерапии* входит профилактика и реабилитация информационных травм аудитории[4], психологическое восстановление после чрезвычайных ситуаций посредством массовой коммуникации[5], стабилизация психических состояний, формирование адекватных контролируемых реакций, содействие национальной самоидентификации[6] и личностному самоопределению индивидов. Реальный опыт медиатерапевтического воздействия был реализован в разгар информационно-психологической атаки «оранжевых» с целью микшировать остроту информационной травмы, укрепить устойчивость к стрессу

[1] *Пронина Е. Е.* Психологические особенности творческой работы репортера. М.: Пульс, 2001.

[2] *Рыбалко О. М.* Динамика изменения психолингвистических характеристик текстов СМИ в чрезвычайных ситуациях: компенсаторные возможности // Материалы IV Всероссийского съезда Российского психологического общества. Ростов-на-Дону, 18—21 сентября 2007 г.

[3] Там же.

[4] «Информационная травма — воздействие, осуществляемое СМИ, которое вызывает деструктивное изменение базовых структур личности, аффективных и когнитивных систем на всех уровнях, начиная с физиологических механизмов и заканчивая картиной мира и образом «Я» индивида» (см. *Рыбалко О. М.* Динамика изменения психолингвистических характеристик текстов СМИ в чрезвычайных ситуациях: компенсаторные возможности // Материалы IV Всероссийского съезда Российского психологического общества. Ростов-на-Дону, 18—21 сентября 2007 г.).

[5] *Чудова Н. В.* Журналистика и социотерапия // Проблемы медиапсихологии-2. М.: РИП-холдинг, 2003.

[6] *Пронин Е. И., Пронина Е. Е.* Архетипы тотальной войны в локальном конфликте // Государственная служба. 2001. № 4.

массового избирателя. «В течение двух месяцев в «Крымской правде» публиковались психологические обозрения типа: «Выключите телевизор», «Оранжевый сценарий обернулся диагнозом», «Толпа превращается в племя» «Почем оранжевый адреналин» и др., — раскрывающие приемы и уловки «социальной инженерии», манипулятивных психотехник и тотального напора»[1]. Инициатива не осталась незамеченной. Аналогичные антиманипулятивные материалы стали публиковать и другие газеты Крыма. Ретроспективный анализ предпринятой акции показал, что медиатерапевтические тексты реально помогают конкретным людям преодолеть стресс.

Этот опыт также убедительно показал, что медиатерапевтические методы по самой своей природе антиманипулятивны, их невозможно приспособить для антиобщественных или своекорыстных пропагандистских акций. Отвечающие исключительно собственным потребностям индивида в самоопределении и ориентации, соблюдающие все принципы психологической безопасности, они эффективны в условиях массированной психической атаки и вирусных технологий, когда традиционные контрпропагандистские приемы, ориентированные на дискредитацию противника и продвижение альтернативной политической силы, оказываются беспомощными и бессильными. Эффективность медиапсихологических методов обусловлена их способностью повышать уровень самоосознания и психологической компетентности, содействовать личностной зрелости и инициативе в противоположность ориентации на сужение сознания и формирование неконтролируемых аффективных и фобических реакций, что составляет главный механизм воздействия политтехнологий.

Расширение знаний аудитории об основных приемах воздействия СМИ и современных коммуникативных технологиях повышает информационно-психологическую защищенность участников массовой коммуникации и в этой связи является основной задачей *медиаобразования* — третьего направления медиапсихологии. Как известно, политтехнология действует до тех пор, пока остается скрытой от сознания объекта воздействия, а также пока объект воздействия не превращается в субъекта, реализующего хорошо осознанные собственные интересы. Медиаобразование обращено ко всему обществу, включая и самих журналистов, которые зачастую первыми подвергаются деструктивному воздействию манипулятивных технологий, и, не имея возможности в полной мере оперативно осмыслить происходящее, транслируют соб-

[1] *Вербицкая Ю. А.* Попытка социотерапии в разгар психической атаки // Ломоносов-2005. Материалы международной научной конференции студентов, аспирантов, молодых ученых. В 2 ч. Ч. 1. М.: МГУ, 2005.

ственные травматические переживания и неадекватные реакции по каналам массовой коммуникации[1].

Медиааналитика, *медиатерапия* и *медиаобразование* вкупе образуют элементарную стратегию *медиапсихологической* защиты, отвечающей важнейшим тенденциям развития социума и человека в направлении самодетерминации и индивидуации и поэтому способной противостоять политтехнологическим попыткам тотального контроля над сознанием и поведением участников массовой коммуникации.

[1]Подробнее об этом см.: *Трубицына Л. В.* Средства массовой информации и психологическая травма // Проблемы медиапсихологии. М.: РИП-холдинг, 2002.

О роли государственного патернализма в деятельности СМИ в рамках построения системы противодействия терроризму

Н. Н. Литвинова

В эпоху смены постиндустриального общества информационным, отмечается *высокая динамика протекания различных процессов*. Смена ценностей и моделей поведения воспринимается в первую очередь гражданскими институтами, культурной и научной общественностью.

Происходящие изменения формируют *новый диапазон отношений* в различных отраслях права, выходящих за рамки регулирования правового поля. Отсутствие адекватного, последовательного механизма законодательного реагирования на вновь образуемые общественные отношения приводит к отставанию и системы противодействия государства.

Принципиально новые процессы призывают на службу и *новые инструменты трансформации*. В современный период главным преобразователем является *информация*, которая выступает *стратегическим ресурсом нового века*. Посредством информации выстраиваются процессы воздействия на различные системы, а также осуществляются функции управления и контроля.

Личность и ее внутренний облик формируется путем усвоения информации о жизни общества и его ценностных ориентациях. *На основе доступной информации* субъект выбирает *способ действия* при достижении какой-либо цели. Для *позитивной* социально-психологической адаптации личности необходимо получение *в достаточном объеме* данных, ориентирующих в происходящих изменениях. *Положительно протекающая* адаптация способствует *снижению психического напряжения* у человека, социальной напряженности в обществе и уменьшает степень подверженности личности информационно-психологическому воздействию. Нарушение социальной адаптации ведет к возможной немотивированности социальных требований.

Степень свободы личности в социальном пространстве находится в прямой зависимости от *объема и качества* освоенной культурно-значимой информации.

Человечество учится жить в режиме постоянного нарастания информационных потоков, интенсификация которых проявляется: в возрастании *скорости передачи* информации, *увеличение объема* вновь образуемой информации, ускорение *обработки* информации, ускорение *внедрения* новой информации в глобальные социальные процессы, интенсивном росте технической оснащенности труда, увеличение уровня гипнабельности.

Традиционные *формы диалога между государством и обществом* демонстрируют *высокую степень деформации* двусторонней связи. Крайним выражением этого является терроризм. Государство вынуждено обратиться к институтам гражданского общества за расширенным анализом данного явления и поиском путей его ослабления с дальнейшей нейтрализацией. Только солидарно осознанная совместная работа может выработать упреждающие и адекватные пути выхода из проблемного комплекса, венцом которого стал терроризм. Предлагаем на рассмотрение *социально-политическое определение терроризма* как метода воздействия на органы государственной власти через мотивированное насилие в отношении произвольных субъектов, не являющихся сторонами конфликта.

В результате террористического акта появляется статистически неопределенный круг лиц, имеющих те или иные психологические девиации. *Физическое и психическое здоровье населения — один из ключевых элементов безопасности*, в связи, с чем необходимо рассматривать терроризм как преступление против мира и безопасности человечества. Представляется целесообразным ст. 205 «Терроризм» поместить в раздел XII УК РФ «Преступления против мира и безопасности человечества».

Также, учитывая высокую степень опасности терроризма, целесообразно внести в перечень ч. 5 ст. 78. «Освобождение от уголовной ответственности в связи с истечением сроков давности» ст. 205 УК РФ.

Терроризм — *вершина пирамиды из комплекса противоречий* всех сторон жизнедеятельности. При безусловной важности адекватного законодательного регулирования всех сторон жизнедеятельности необходимо выделить и законодательно закрепить *приоритет рассмотрения и принятия законов, касающихся нарушения общественной безопасности*.

Любое деяние представляет собой акт работы сознания по переработке социально-значимой информации, в связи, с чем *ведущим звеном системы противодействия терроризму должна стать информационно-психологическая сфера*.

Сегодня общество стоит на пороге исторической переоценки роли государства. Меняется понимание сути данного института и философии

его деятельности. Государство должно научиться защищать человека как носителя созидательной силы. Прошла пора абстракций, необходимо четко и конкретно определить круг реальных, возможных и срочных мер по гармонизации информационной среды российского общества. *Основной задачей государства становится* обеспечение безопасности в удовлетворении жизненно важных потребностей направленных на прогрессивное развитие личности. Необходимо создать государственную систему востребования и эффективного использования отечественной мысли. Интеллект сегодня первооснова любой конкурентоспособности. Ведущие игроки глобальной геополитики, понимая это, интегрируют свои интересы методом культурного сотрудничества через свои стандарты образования, мировоззренческие ценности. «Культурный империализм» проявляет себя тем, что подчиняет себе сознание, образ мышления и, как следствие, образ жизни. Изменение общественного строя наиболее результативно «через молекулярную агрессию»[1] в общественное сознание и разрушение культурного ядра.

Информационное вторжение представлено достаточно комплексно:

- целенаправленное создание, внедрение и поддержка в СМИ массива информации, пропагандирующего геноцид, насилие, культ денег, универсального эквивалента ценностей Запада;
- создание и финансирование различного рода «демократических институтов;
- поддержка изданий трудов западных философов и политиков, пропагандирующих ценности западного мира;
- концентрация массмедиа вокруг интересов узкого круга лиц;
- деятельность прозападных фондов культурного сотрудничества;
- использование коррупции с целью оказания давления на работу различных госструктур.

Любое воздействие явно или опосредованно преломляется в сознании, что влечет цепную реакции внутренних перестроек социума. Кризис общественного менталитета оказывается главным разрушителем социума.

Информационное воздействие на социум стало самостоятельной индустрией, где основными средствами выступают: СМИ, литература, искусство, образование, система воспитания. В результате формируется информационное поле, разрушающее основу адекватного состояния сознания по переработке информации, что ведет к трансформации менталитета.

Одной из ключевых проблем российского государства является прогрессирующее отторжение граждан от управленческого воздействия го-

[1] См. *Лопатин В. Н.* Информационная безопасность России.

сударственных институтов посредством *формирования интеллектуальной анемии* через деструктивное воздействие различных субъектов информационной экспансии (религиозные секты, идеологии радикальных политических партий и движений, криминальная субкультура, разрушающее воздействие СМК...). *Основной задачей жизнедеятельности является самопознание. Различные деструктивные идеологии нарушают процесс самопознания*, *следовательно*, *препятствуют осуществлению самопознания как основы созидания*. Созидание является предназначением духовной силы человека. Потеря смысла является благоприятной основой нигилизма, анархии, уничтожения любых обязанностей перед обществом.

На современном этапе СМИ, как основные субъекты информационного пространства, игнорируют положение Концепции национальной безопасности РФ об интересах человека и гражданина в духовном и интеллектуальном развитии, а также положения Доктрины информационной безопасности запрещающей распространение информации направленной на девальвацию и снижение духовного, нравственного и творческого потенциала страны.

Вызывает острую обеспокоенность формирование нового поколения в условиях агрессивной информационной среды. В процессе социализации человек с детства должен усваивать сложные объемы культурно-значимой информации, развивая способность оперировать ей и порождать новые смыслы. От того, каким образом и с какими социальными и психологическими характеристиками сформировалось новое поколение, как в массовом масштабе произошла трансляция социокультурного опыта, зависит, каким стало общество, его взаимодействие с государством и процессы обеспечения безопасности личности.

В научной литературе различают криминальную идеологию, террористическую идеологию, созрела острая необходимость в появлении государственной идеологии и распространении ее во все сферы жизни. Комплексной *программе противодействия терроризму необходимо идеологическое сопровождение*, которое направлено на:

- предотвращение интеллектуальной деградации населения страны как основного субъекта системы профилактики;
- пресечение вовлечения граждан в преступную деятельность через принятие ценностей криминальной субкультуры широко представленных СМИ;
- недопустимость использования средств массовой коммуникации как ресурсов криминальной субкультуры, в частности, террористической деятельности.

Динамичный рост социальной базы, несущей посттравматические стрессовые реакции, говорит о необходимости *корректной информационной среды*, в связи с чем, следует изменить существующую редакцию ст. 3 Закона «О СМИ» от 1993 года о недопустимости какой-либо цензуры.

В каждом явлении, даже самом разрушительном, есть положительная сторона. Опасность в любой момент и в любой точке потерять жизнь свою и близких, вне зависимости от национальной, религиозной, профессиональной и иной принадлежности, вовлекает в естественный переход от «культуры войны» к «культуре мира».

Стратегии деятельности СМИ в контексте локальных войн и терроризма

С. Э. Некляев

Информационная составляющая локальной войны

Национальные системы безопасности стран-лидеров, достаточно эффективные в прошлом веке, обнаруживают свою уязвимость при столкновении с угрозами нового века. Потенциал угрозы международного терроризма стал очевидным после террористического акта против США 11 сентября 2001 года. Характер и тактика самой операции выявили недостатки старой системы национальной безопасности.

Терроризм и порождаемые им угрозы — явление отнюдь не новое. Тактическая составляющая имеет много общего с тактикой партизанских движений.

Партизанское движение квалифицируется как вид борьбы народа за свободу и независимость своей родины на территории, занятой противником и в отношении войск противника[1]. Главной и основной целью является деморализация войск противника, нарушение коммуникаций, создание атмосферы страха внутри подразделений противника. Действия партизанских отрядов ведутся по двум направлениям: боевые действия[2] и информационная работа. Издание газет и журналов, вещание в радиоэфире, направленное на войсковые части, становится эффективным инструментом влияния на психологическое состояние противника[3]. Эффективность информационно-психологического воздействия подтверждается историческим опытом — деятельностью советских партизан во время Великой Отечественной войны, действиями С. Бендеры при развертывании сопротивления войскам НКВД, Че Гевары при ведении революционной борьбы на Кубе и в Южной Америке[4].

[1] Советский энциклопедический словарь. М.: Советская энциклопедия, 1998.

[2] Сюда входят подготовка партизан, проведение диверсий на железных дорогах, автомобильных трассах, аэродромах; диверсии в расположении противника — засады; налеты; поиски; поднятие бунтов против оккупационных войск и т. д.

[3] *Ткаченко С.* Повстанческая армия: тактика борьбы. Минск; М.: Харвест-АСТ, 2000.

[4] *Гевара Э. Ч.* Партизанская война // Малая война. Хрестоматия. Минск: Харвест, 1998.

Информационно-психологическое противоборство в условиях малой войны приобрела решающее значение в последние десятилетия. Афганская война (1977—1989 гг.) и первая чеченская война (1994—1996 гг.) обнаружили полную неготовность органов психологической защиты государства (подразделения психологической борьбы Вооруженных сил, специальных подразделений ФСБ и МВД) к противодействию информационным атакам боевиков[1].

В *информационно-психологическом противоборстве* акцент делается на манипуляции страстями, желаниями и страхами людей. Информационно-психологическая работа в условиях партизанской войны ориентирована на создание атмосферы страха посредством демонстрации особой жестокости и унижений. У личного состава противника возбуждаются самые низменные желания[2]. В результате информационного прессинга противник вынужден заниматься наведением порядка в своих рядах, а партизаны в этот момент наносят боевые удары. Результативной формой информационно-психологической работы стала подделка СМИ под издания и каналы радио-телевидения противника. Таким образом запускается любая дезинформация и создается возможность манипулировать настроениями солдат противника, провоцировать бунты и дезертирство. Психологическая атака позволяет партизанам формировать среди личного состава вооруженных сил противника и населения страны-противника группы сочувствующих, что приводит к переходу войск противника на сторону повстанцев[3].

Современные информационные технологии расширяют арсенал средств информационно-психологической войны. Используя ценности демократии, в частности, плюрализм мнений, партизаны стремятся апеллировать к общественному мнению стран противника. Доступ к национальным и глобальным СМИ обеспечивает влияние на общественное мнение, дает возможность вести направленную пропаганду, способную вызывать чувство презрения и откровенное недовольство политикой, проводимой в регионе вооруженными силами.

Важным элементом работы современных партизан являются ресурсы сети Интернет, с помощью которых можно безопасно координировать действия и рекрутировать добровольцев, широко пропагандировать свои идеи. Особенностью современных информационных (компьютерной, сетевой и телекоммуникационной) технологий стала возможность мультимедийной передачи информации аудитории. Теперь респондент знакомит-

[1] *Брудер Г.* Афганская война. Франкфурт-на-Майне: Посев, 1988.

[2] *Макнаб К.* Психологическая подготовка подразделений специального назначения. М.: Гранд, 2002.

[3] *Крысько В.* Секреты психологической войны. Минск: Харвест, 1999.

ся не только с текстовыми и графическими материалами, но и способен просмотреть и прослушать аудио-видео записи бесчинств противника[1]. Партизаны используют информационное пространство в качестве самостоятельного театра военных действий.

Террористическая деятельность. Деятельность террористических организаций имеет существенные отличия. Первое отличие связано с тем, что целью для атаки могут быть как войска, так и мирные граждане, зачастую не имеющие никакого отношения к выдвигаемым требованиям. Второе отличие — террористические организации преследуют исключительно политические или экономические требования. Третья отличительная черта обусловлена особым типом отношения в группе. Партизаны действуют как военная организация. В террористических организациях принята идеологически-иерархизированная модель управления, где руководитель является абсолютным лидером, а ее члены — ближайшими учениками и соратниками. Есть еще одно важное отличие. Террористические организации не используют свои собственные СМИ. Они паразитируют на глобальных и национальных средствах массовой информации, хотя иногда создают свои собственные средства массовой информации, не предназначенные для длительной деятельности[2]. В последние десятилетия отчетливо проявляется важнейшая задача практически любого теракта: наравне с предъявлением требований стоит и привлечение общественного мнения, или, точнее сказать, запугивание его[3].

Анализируя процесс освещения в СМИ террористических актов, можно выделить ряд этапов этого процесса. Главная приманка всей прессы, как известно, — сенсация. В момент совершения теракта на место прибывают съемочные группы всех телекомпаний, газетные и радиожурналисты. Им нужна горячая новость. Террористы на это и рассчитывают. За считанные минуты об их акции узнает и национальная аудитория, и весь мир. На этом этапе террористы даже не стремятся получить прямой эфир и огласить свои требования. Им нужно создать атмосферу страха, заставляющую людей бояться и сомневаться в компетентности властей обеспечить безопасность общества.

Первый шаг сделан. О маленькой агрессивной группке узнали миллионы. Событие широко обсуждается, говорят о несостоятельности правоохранительных органов, бессилии правительства, самих террористах, от которых следует поскорее избавиться.

Следующий этап можно назвать «шоу ужаса». Нет такого СМИ, которое не сделает теракт главной новостью дня. Нет такого СМИ, которое

[1] *Крысько В.* Секреты психологической войны. Минск: Харвест, 1999.
[2] *Жаринов К. В.* Терроризм и террористы. Минск: Харвест, 1999.
[3] *Ольшанский Д. В.* Психология терроризма. СПб: Питер, 2002.

откажется от обсуждения события с участием экспертов и специалистов. Будут обговорены особенности проведения теракта, вооружение террористов, затронуты геополитические вопросы, аудиторию просветят во всех аспектах и тонкостях идеологии террористов. Если кто-то из комментирующих теракт обмолвится об исламском следе, то на аудиторию польются потоки невнятной аргументации вековой агрессивности исламского фундаментализма. Если же представители власти будут говорить о национализме, то аудитории придется погрузиться в темные стороны истории как своей страны, так и мирового фашизма в целом[1].

Третья фаза характеризуется активными кампаниями по раздуванию темы терроризма. Возможно, до этого этапа сами террористы, совершившие теракт, не доживут, но обсуждение будет идти еще как минимум неделю. Если же террористы смогут уничтожить хотя бы несколько ни в чем неповинных граждан, то тема растянется не менее чем на месяц.

Новые угрозы заставили задуматься о необходимости перестройки всех систем безопасности. Она осуществлялась на основе принципа самостоятельной работы всех сфер обеспечения, но при их четкой координации.

США — одно из первых государств, которому удалось сформировать *доктрину информационно-психологического обеспечения локального военно-политического конфликта*. Пентагон опробовал ее во время первой войны в Ираке. Поскольку эта доктрина была самой современной в контексте локальных военных конфликтов того периода, необходим ее анализ.

«Буря в пустыне» была первой операцией коалиционных войск Европы и США, где информационно-психологическая составляющая воспринималась как самостоятельный вид боевой активности. Здесь были применены и опробованы на практике многие современные методы. Основной формой работы со СМИ стали информационные «пулы», через которые распространялась информация во все страны мира[2]. При всем желании ни один журналист не мог работать вне тотального контроля военных. Информационные потоки содержали только нужную и определенным образом поданную информацию. Такая форма работы с журналистами в очень скором времени принесла плоды. Население стран Западной Европы и Америки были твердо убеждено в правильности действий своих войск и выражало полную поддержку командования во всех его действиях. Вместе с ведением информационно-психологических операций

[1] *Joett G. S., O'Donnell.* Propaganda and Persuasion. Newbury Park etc., 1992.
[2] *Young P., Jesser P.* The Media and the Military. From the Crimea to Desert Strike. Houndmills etc., 1997.

ведомства, занимающиеся информационной безопасностью, отлаживали свою организационную и функциональную структуру и схему действий в тех или иных условиях развития конфликта.

Свое развитие модель ведения информационно-психологических операций в новых условиях получила во время косовского кризиса в 1998—1999 годах. Югославия — многонациональная страна с очень непростыми межнациональными отношениями. Основной состав населения представляли три народа: хорваты, сербы и албанцы. Распад Варшавского договора и развал СССР привели к череде внутриполитических кризисов, приведших страну к нескольким конфликтам: в 1994—1995 годах конфликт между Боснией и Герцеговиной, затем в 1998 вспыхнул косовский кризис. Оба конфликта порождены как межрелигиозной, так и межэтнической напряженностью. Но если боснийский кризис был решен достаточно безболезненно за счет активной роли в его решении ООН, то косовский оказался чрезвычайно сложным для правового международного регулирования.

США вступили в конфликт в крае Косово под эгидой проведения гуманитарной операции по разведению сторон. В результате сложилась ситуация, при которой народы, жившие вместе на протяжении многих столетий, стали врагами. Одновременно нарастал и религиозный конфликт. Страны НАТО поддерживали албанскую освободительную армию (костяк армии состоял из исламских фундаменталистов).

В таких условиях от НАТО потребовалось обеспечить эффективную информационно-психологическую работу с общественным мнением Европы. Освещение конфликта шло по заранее подготовленному сценарию. Была введена предварительная цензура на материалы из районов боевых столкновений. Особым приемом информационного обеспечения кампании стала деятельность журналистов в зоне конфликта, работавших во взаимосвязи с войсками альянса, что и позволяло расставлять нужные акценты в информационной картине событий. Подобная тактика обеспечила США и НАТО информационное превосходство как в регионе конфликта, так и благоприятное отношение общественного мнения в странах альянса, сочувствующих и зависящих стран.

Если раньше военные говорили о превосходстве в воздухе, радиоэфире, на море или на плацдарме, то теперь прибавился новый вид превосходства — информационный. Это превосходство в современных условиях можно расценивать как важнейший фактор успешных боевых действий. СМИ превратились в инструмент достижения чисто военных целей.

Структурно-функциональный подход к *тактике информационно-психологической работы* в период локальной войны дает основание выделить следующие этапы:

Этап I. Подготовительный период (от 6 месяцев до 2 лет).

1. Поиск врага.
2. Создание образа врага.
3. Укоренение образа врага в общественном мнении, через СМИ.
4. Создание резонанса в общественном мнении.
5. Убеждение населения в единственно возможном варианте решения конфликта.
6. Давление на врага (угроза введения экономических санкций, введение экономических санкций, организация контроля со стороны лояльных международных организаций над территорией и политической жизнью внутри страны).
7. Создание напряженности на этнической или религиозной почве в сопредельных странах по отношению к населению и правительству противника.
8. Дестабилизация обстановки внутри страны противника (сомнения, поддержка враждующих сторон, манипулирование общественным мнением).

Этап II. Проведение военной операции.

1. Воздушная война:
   a) поддержка благоприятного общественного мнения внутри страны к проводимой операции;
   b) поддержка образа врага в общественном мнении;
   c) обеспечение поддержки проводимых боевых действий в зоне конфликта общественным мнением;
   d) деморализация войск и населения противника проведением ударов с использованием высокоточного оружия;
   e) дестабилизация политической и экономической ситуации внутри страны;
   f) давление на лидеров противника с целью навязывания своего варианта развития событий;
   g) активное информационно-психологическое противодействие информационной политике дружественных или сочувствующих противнику стран;
   h) фильтрация информации для предотвращения появления альтернативной точки зрения на проводимую политику;
   i) контроль за деятельностью СМИ специальными военными органами.
2. Вторжение на территорию противника (возможно только при полной уверенности в отсутствии жертв среди личного состава своих войск):

a) подавление информационного противодействия сил противника с применением всех возможных сил и средств, вплоть до полного физического уничтожения;
b деморализация войск и населения противника;
c ведение пропагандистской работы с населением на захваченных территориях;
d поддержание благоприятного общественного мнения внутри страны для проведения военной операции;
e активная контрпропаганда на информацию, поступающую из дружественных или сочувствующих стран;
f полный контроль за информационными потоками со стороны органов ведения информационно-психологической борьбы;
g свержение политического режима противника, угрожающего национальным интересам.

Этап III. Установление лояльного режима и включение страны бывшего противника в зону национальных интересов:

1. Уничтожение истоков возможных опасностей информационного характера.
2. Создание лояльного правительства.
3. Проведение всенародных выборов для легитимизации лояльного правительства.
4. Внедрение информационных стереотипов стран Запада через создание лояльных СМИ.
5. Полное подчинение внешней и внутренней политики бывшего противника интересам США[1].

Данная тактика явилась результатом многолетних исследований. Эти результаты положены в основу наставлений для войск специальных операций США. Первым в этой серии было разработано «Наставление по проведению психологических операций: техники и методы»[2]. Оно появились 5 мая 1994 года, когда американские войска начали военную

[1] См.: FM 41-10 Civil affair operations — http://155.217.58.58/cgi-bin/atdl.dll/fm/41-10/toc.htm, FM 3-19-30 Psychological security — http://155.217.58.58/cgi-bin/atdl.dll/fm/3-19-30/toc.htm, FM 3-61.1 Public affairs tactics, techniques and procedures, Psychological operations: techniques and procedures, FM 7-98 Operations in a low-intensity conflict — http://155.217.58.58/cgi-bin/atdl.dll/fm/3-61.1/toc.htm.

[2] FM 33-1-1 Psychological operations: techniques and procedures — http://155.217.58.58/cgi-bin/atdl.dll/fm/33-1-1/toc.htm.

кампанию против Ирака. Затем последовало «Наставление по связям с общественностью»[1], которое включало принципы и технологии деятельности отделов по связям с общественностью, а также методы проведения информационных кампаний в обществе. Окончательное формирование технологической базы психологической войны произошло в 2000 году, когда было утверждено сразу четыре инструкции: «Наставление по ведению массовых публичных мероприятий: тактика, техники и методы»[2], «Психологическая безопасность»[3], «Психологические операции»[4], «Информационные операции в обществе»[5]. Разработка и появление этих наставлений-методик продиктованы необходимостью скорейшего перевооружения с целью отражения нового типа информационно-психологических угроз, а также особенностями современного информационного пространства.

С тактической стороны в период локальных войн, вызванных внутренними или внешними политическими кризисами, доктрина информационно-психологического обеспечения локального военно-политического конфликта себя оправдала полностью, но она оказалась не в состоянии противостоять информационном угрозам, порождаемым терроризмом.

Информационное обеспечение в условиях «сетевой войны»

Теракт в Нью-Йорке 11 сентября 2001 года поставил под сомнение всю эффективность имеющихся моделей обеспечения национальной безопасности. Особая сложность отражения новой угрозы — международного терроризма связана с типом организации международных террористических групп. Группа, атаковавшая Всемирный торговый центр, «Аль-Каида», за счет сетевой модели организации управления может мобилизовать до 4—5 тысяч бойцов, со всей необходимой экипировкой, имеющих боевой опыт и проживающих в десятках стран мира[6]. Она

[1] FM 46-1 Public affairs operations — http://155.217.58.58/cgi-bin/atdl.dll/fm/46-1/toc.htm.

[2] FM 3-61.1 Public affairs tactics, techniques and procedures — http://155.217.58.58/cgi-bin/atdl.dll/fm/3-61.1/toc.htm.

[3] FM 3-19-30 Psychological security — http://155.217.58.58/cgi-bin/atdl.dll/fm/3-19-30/toc.htm.

[4] FM 33-1 Psychological operations: techniques and procedures — http://155.217.58.58/cgi-bin/atdl.dll/fm/33-1/toc.htm.

[5] FM 41-10 Civil affair operations — http://155.217.58.58/cgi-bin/atdl.dll/fm/41-10/toc.htm.

[6] *Трунок С. Г.* Информационно-коммуникационная революция и новый спектр военно-политических конфликтов // ПОЛИС. 2003. № 1.

состоит из более чем десятка локальных центров, разбросанных по всему миру и действующих в рамках единой идеологической среды.

В классических военизированных организациях с иерархичной структурой самым уязвимым звеном является командование — по двум причинам: во-первых, оно располагается в одном месте, во-вторых, вся власть сосредоточена в руках одного человека. При сетевом же принципе организации лидеры могут находиться в постоянном движении и в любом уголке земного шара, при этом они способны управлять всеми силами и средствами за счет использования современных телекоммуникационных систем. Сама же организация не имеет ни четкой внешней организационной структуры, ни определенной территории деятельности. У нее, как правило, несколько равноправных лидеров, которые принимают решение консолидированно. В случаи гибели одного из лидеров другие способны продолжать управление организацией. Это высшее звено ответственно за стратегическое планирование, идеологию и финансирование локальных отделений. Непосредственный выбор целей теракта, его планирование и исполнение полностью отдано в компетенцию локальных отделений. Их инициатива ограничена рамочными условиями и системой ценностей, формирующей систему координат «свой-чужой». Это позволяет организации осуществлять асинхронизированные и непредсказуемые акции[1].

Сетевая модель управления усиливает опасность, исходящую от террористических организаций. Ответом на эту угрозу стала разработка Пентагоном доктрины «сетевой войны» (network-centrik-warfare-NCW)[2]. Переход к подобной доктрине предполагает трансформацию всего силового блока государства в «силы национальной безопасности», включающие и военные, и гражданские компоненты. Так, *военный компонент* включает в себя *разведывательный*, *военно-воздушный*, *космический*, *военно-морской*, *информационно-психологический* блоки, а также войска специального назначения и силы быстрого развертывания, представленные силами и средствами вооруженных сил, специальными агентствами, службами и министерствами. *Гражданский компонент* представлен такими блоками, как *политический* (*дипломатический*), *экономический* (*электронный банковский обмен*), *информационно-телекоммуникационный*, *медийный*, в которых задействуются силы и средства всех невоенных министерств и ведомств государства, а также банками, средствами массовой информации, телекоммуникационными компаниями и т. д. Каждый из компонентов независим друг от друга, но одновременно они координируют свою работу друг с другом.

[1] *Ronfeldt D., Arquilla J.* Networks and Netwars. Santa Monika, 2001.
[2] *Гриняев С.* «Сетевая война» по-американски // НВО. 2002. № 5.

Силы и средства гражданского компонента призваны обеспечить долговременное, кооперативное, ненасильственное присутствие в зонах национальных интересов. Их основная задача — развивать партнерские связи и взаимоотношения, а также обеспечить проникновение в сознание потенциального противника за счет размещения определенных ценностных ориентаций и поведенческих моделей в контексте локальных культур. Вооруженные силы должны быть готовы, при необходимости, произвести шок, посеять ужас, нанести, с помощью показательного применения войск, «неожиданный удар во внешнем мире в целях дезориентации противника в его «мире внутреннем»[1].

Технология «сетевой войны» предполагает постадийное развитие. На *начальном этапе* из военного компонента задействуется только разведывательный блок. Гражданский компонент берет на себя основную нагрузку, которая распределена между политическим, информационно-телекоммуникационным и медийным блоками.

На *разведывательный блок* возлагаются задачи по детальному изучению районов предстоящей войны, просчет возможных сценариев и поиск наиболее подходящих мест для размещения своих войск и войск коалиции вокруг страны-противника, поиск и разработка среди личного состава войск и населения противника развитой агрессивной оппозиции и перетягивание ее на свою сторону, проведение глубокого изучения особенностей политического и экономического управления; организации системы обороны, жизнеобеспечения, умонастроения личного состава вооруженных сил противника и населения страны-противника, разработка действий по устранению и дискредитации лидеров противника; выявление скрытых союзников и связей с диаспорами и организациями на территориях других стран. Разведка также должна представить возможные маршруты снабжения противника и методы их ликвидации.

Политический блок ответственен за работу: по убеждению мировой политической элиты в абсолютности зла, в неразрешимости проблемы невоенными мерами; по переубеждению возможных союзников противника в нецелесообразности его поддержки противника; по перетягиванию союзников противника в свой лагерь; по созданию единой коалиции в рамках союза из наиболее сильных сочувствующих стран, даже с учетом того, что союзники могут не принимать непосредственного участия в боевых действиях; заключение договоров с другими странами о предоставлении территории и акваторий для размещения военных баз и флотов. Одновременно проводится работа по отчуждению страны противника от

[1] *Ronfeldt D., Arquilla J.* In Athena's Camp: Preparing for Conflikt in the Information Strategy. Santa Monika, 1997. P. 408.

близлежащих государств и диаспор по всему миру. Тем самым достигается эффект «отчужденности» и усиление образа «абсолютного зла» по отношению к противнику.

Информационно-телекоммуникационный блок призван поставить под контроль все возможные каналы связи противника; выявить и подавить все альтернативные каналы передачи информации на территориях третьих стран и внутри страны. Не менее важной задачей является обнаружение во всех имеющихся базах данных информации о ресурсах страны-противника и возможности доступа к этим ресурсам. Решается и задача блокирования доступа противника к мировым ресурсам телекоммуникационных сетей, аппаратным средствам компьютерной и телекоммуникационной техники, базам данных и системам жизнеобеспечения.

Цели и задачи деятельности *медийного блока* по сути схожи с политическим сектором, однако он работает с большими аудиториями. В общественном мнении поэтапно формируется устойчивый образ страны-противника как абсолютного зла. Для этого используются такие формы и методы, как псевдообсуждение и псевдоанализ; внушение мысли о скорейшем и полном уничтожении противника, необходимости всеобщего участия в борьбе со злом; внушение представлений о справедливой бескровной войне; активизация деятельности общественных движений в поддержку правящей элиты и принимаемых решений; нейтрализация диаспор через формирование чувства стыда за действия своих соотечественников, ставших противником. На глобальном уровне в рамках ответственности медийного блока осуществляются: поддержка общественных движений, выступающих за немедленное уничтожение абсолютного зла; убеждение в невозможности решения проблемы; формирование благоприятного отношения к действиям сил коалиции; снижение неприязни к войскам коалиции в районах сосредоточения; возбуждение отвращения к действиям, подобным действиям страны-противника по всему миру; активизация обсуждения вопроса национальной безопасности в контексте угроз глобального терроризма.

Важнейшим элементом информационно-психологической работы становится создание псевдореальности — иллюзорных представлений о географической близости конфликта. Основными характеристиками этого процесса выступают *скорость информационного обмена* внутри телекоммуникационных сетей, позволяющая вести репортажи о событиях практически в режиме реального времени, и *иллюзия мирового единства* в борьбе с «абсолютным злом».

Сама же кампания по подготовке аудитории к новому конфликту может развиваться по двум сценариям снежного кома и информационного

взрыва[1]. Сценарий «информационного взрыва» рассчитан на масштабное событие-катастрофу. Огромные объемы информации, адресованные аудитории, должны вызвать чувства праведного гнева и ненависти по отношению ко всем, кто мог оказаться причастным к трагедии. Первая волна подавляет сферу рационального, стирает все ценностные установки. На таком восприятии создается образ врага. Общество подготавливается к требованию отмщения путем немедленного вооруженного решения проблемы. Проблема постоянно присутствует в повестке дня средств массовой информации.

Сценарий «снежного кома» требует больших усилий. Основой этого метода является два элемента — контроль за источниками информации и шумовой метод подачи информации. Информационная повестка дня начинает аккумулировать трагические события, связывая их при помощи рефлексии экспертов, мнения которых призваны убедить аудиторию во взаимосвязи происходящего. В рамках общественного обсуждения происходит лавинообразный сброс информации, построенной по правилам манипулятивной и убеждающей технологии. В результате аудитория теряет способность принимать решения самостоятельно и принимает навязываемые решения. Находясь в состоянии полной дезориентации, аудитория видит выход из ситуации в силовом решении проблемы. Для того чтобы в «снежный ком» не попали мнения, комментарии, не соответствующие генеральной линии обсуждения, события должны освещаться только с одной стороны. Для этого необходим полный контроль за источниками. Так создается иллюзия объективности — информация комментируется представителями институтов государства, общественности, но точки зрения на события практически полностью совпадают.

После информационной обработки общественного мнения наступает следующий этап проведения «сетевой войны» — *этап проведения военной операции*. На этом этапе ведущая роль принадлежит таким блокам военного компонента, как военно-морской, воздушный, космический, информационно-психологический и войскам специальных операций. Политический, экономический, информационно-телекоммуникационный, медийный блоки, входящие в гражданский компонент, обеспечивают работу «вне зоны конфликта». Задачи политического блока претерпевают изменения. Если до этого этапа политикам следовало убеждать всех в абсолютном зле и создавать коалицию, то теперь они разоблачают террористов и предостерегают страны коалиции о недопущении деятельности террористов на их территории.

[1] *Тоффлер Э.* Метаморфозы власти. М: АСТ, 2002.

Военные блоки (*военно-морской*, *воздушный*, *космический*, *информационно-психологический и войска специальных операций*) призваны обеспечить абсолютное превосходство над противником. Версия сетевой войны, в отличие от классических сценариев абсолютного перевеса над противником, предполагает наличие не трех театров военных действий, а четырех. Четвертым театром становится *информационный*. Здесь происходят события, схожие по своему характеру с действием органов пропаганды в годы войны. Информационно-психологическая работа рассматривается, как полностью самостоятельный вид и обладает развитым арсеналом средств для ведения как оборонительных, так и наступательных операций. Новый театр военных действий, в сравнении с классическим, не только не имеет линии фронта, но и реально видимого противника. Противник виртуален — это умонастроения населения и солдат противника, их мнения и чувства, их ценности и устои. Только теперь стало возможным разрушать ментальные структуры людей.

В основу технологии деятельности информационно-психологического блока в информационном пространстве региона конфликта положены технологии жесткой пропаганды или манипулятивные технологии. Подробно их виды и типы будут проанализированы в следующем параграфе. Отметим только, что эти технологии применяются без каких-либо оглядок на нормы этики и морали.

В задачу частей *информационно-психологического воздействия* или *psychological warfare* входит: подавление деятельности местных и военных СМИ, вплоть до их физического уничтожения; дискредитация деятельности военного руководства как внутри войск, так и среди населения противника; создание полной информационной блокады внутри страны; направленное вещание на территорию противника специально созданных СМИ, копирующих национальные радио и телеканалы. Для обеспечения максимального доступа к этим СМИ на территорию противника доставляются и бесплатно раздаются населению радио и телеприемники с прошитой фиксированной частотой приема.

Как уже подчеркивалось, особую роль в концепции «сетевой войны» играет *медийный блок*. В отличие от военного информационно-психологического блока, выполняющего работу по контролю и управлению общественным мнением, умонастроениями и ценностными установками непосредственно в зоне конфликта, медийный блок, решая схожие задачи, развертывает деятельность на территориях всех стран, кроме территорий государства (государств), где непосредственно происходят боевые действия. Этот блок несет ответственность за управление общественным мнением на глобальном уровне.

Современные СМИ способны навредить и своим собственным войскам, допустив в эфир информацию другой стороны линии фронта, которая может радикально изменить вектор общественного мнения о войне. Для предотвращения подобных ситуаций был разработан целый комплекс мер по работе с журналистами. Прежде чем попасть в зону конфликта, журналист обязан преодолеть целый ряд бюрократических барьеров, чтобы оказаться в зоне расположения частей своего государства или коалиционных сил. В целях безопасности журналиста его будет постоянно сопровождать офицер по информационной работе. Для этого военные разработали систему пулов. Она во многом напоминает экскурсии для журналистов на военные полигоны. Утром все желающие собираются у палатки информационной службы армии, садятся в автобусы и под прикрытием бронетехники доставляются на относительно безопасные участки линии фронта. Там журналисты получают указания, что можно снимать и с кем говорить. Работать на передовой во время боев журналисту крайне сложно. Ведь помимо физической опасности существует и военная тайна. Все комментарии и документальные кадры возможно получить в штабе в отделе информационно-психологической работы. Когда материал готов, журналист еще раз должен согласовать содержание текста с офицером по информационной работе. Таким образом появление в эфире или на страницах печатных СМИ фактов, относящихся к военной тайне не возможно[1].

Однако на любом театре военных действий можно найти журналистов, желающих получить эксклюзив. Такие журналисты готовы пренебречь опасностью быть задержанными военными властями или попасть в плен к противнику. Зачастую журналисты нелегально пересекают линию фронта и начинают работать с лидерами и подразделениями противника. Под прикрытием статуса независимого журналиста работают и специалисты военной разведки. Подобная деятельность почти маргинальна с точки зрения закона: журналист может быть обвинен в пособничестве террористам. Для редакторов крупных СМИ, которые финансируют работу журналистов, информация — козырь при работе с военными. В нужный момент они могут спровоцировать скандал, который привлечет внимание аудитории и одновременно побудит военных быть более открытыми для СМИ.

Нельзя недооценивать информационные возможности современных террористов. Международные террористические организации придают не меньшее значение масс-медиа, чем и противостоящие им антитеррори-

[1] FM 3-61.1 Public affairs tactics, techniques and procedures — `http://155.217.58.58/cgi-bin/atdl.dll/fm/3-61.1/toc.htm`.

стические силы. В первую очередь, медийные возможности противника представлены различными Интернет-сайтами, обладающими развитой внутренней структурой и способные пересылать видео и радиоматериалы. Вторым проверенным средством являются радиостанции, вещающие из зоны конфликта и создаваемые наиболее агрессивно настроенными членами диаспор. Специфическим звеном передачи информации являются политические, религиозные и культурные деятели, эмигрировавшие из зоны конфликта, а, правильнее говоря, бежавшие от «бесчеловечных зверств» антитеррористических сил. Они получают возможность распространять свои идеи через общенациональные СМИ, когда редакторы пытаются представить объективную картину событий, дать двусторонний комментарий[1].

Террористы стараются представлять себя «непреклонными борцами за свободу своей родины», или «несчастными жертвами мировой агрессии»[2]. СМИ, поддерживающие террористов, представляя их аудитории в виде «непреклонных борцов за свободу своей родины», пытаются показать решимость террористов вести войну до полной победы путем осуществления террористических актов. Лучшим средством проведения подобного сценария является предоставление аудитории данных об «истинных» потерях коалиционных сил, информации о некомпетентности и откровенной безграмотности командиров коалиционных сил при проведении спецопераций, «реальном» числе повстанческих сил и их возможностях, о готовности нанести удар по любому объекту в глубоком тылу Альянса и другой информации подобного толка. Но когда шансы выиграть информационное противостояние уменьшаются или террористы начинают терять союзников, то остается возможность использовать образ «несчастных жертв мировой агрессии» и таким образом спровоцировать внутреннюю нестабильность внутри общественного мнения стран антитеррористической коалиции. Для такого приема особых усилий не потребуются. Надо только помочь мировым СМИ увидеть «реальную деятельность» миротворческих или контртеррористических сил: зачистки, проверки документов, жуткие условия жизни мирного населения, голодных и раненых детей; услышать душещипательные рассказы пленных боевиков об издевательствах над ними.

Противодействовать этим сценариям сложно, хотя приемы известны — разоблачение дезинформации и вывод в информационное поле полной картины событий, обязательное публичное расследование фактов

[1] Tactical Use of Psyop, `http://call.army.mil/call/ctc_bull/90-0/9092c14.htm`.

[2] FM 7-98 Operations in a low-intensity conflict — `http://155.217.58.58/cgi-bin/atdl.dll/fm/7-98/toc.htm`.

и событий, усиление освещения гуманитарной работы. Такие средства используются сейчас в контрработе.

Завершающий этап можно назвать *этапом гуманитарной операции*[1]. Его главная особенность состоит в том, что он может начаться еще до полного прекращения боевых действий. Основной задачей этого этапа является формирование власти в стране: рушится террористический режим и власть переходит к «законно избранному» правительству, лояльному стране/коалиции-победителю. Политический сектор должен подготовить мировое сообщество к принятию нового государства и оказанию ему помощи на начальном периоде становления.

Изменяется характер работы *военных блоков*. Они переходят от прямых военных и специальных операций по уничтожению боевиков к организации контроля над территорией и препятствованию возникновения любого объединения, неугодного или оппозиционного проводимой политике. Осуществляется тотальное «прочесывание» территории для обнаружения оставшихся бандитов. Есть еще одна задача — сбор доказательной базы по связям боевиков с террористическими организациями других стран и раскрытие полной картины преступлений боевиков за время правления в стране. На военные власти совместно с различными гуманитарными организациями возлагаются задачи по построению в стране системы здравоохранения и неотложной помощи. Также формируются спасательные и пожарные подразделения, которые возглавляют офицеры коалиционных сил, но служат в них жители страны.

На первой стадии проведения гуманитарной операции, т. е. до формирования лояльного правительства, полицейские органы состоят исключительно из коалиционных сил, на второй стадии, т. е. до формирования всех необходимых институтов гражданской и государственной власти, — полицейские органы находятся под командованием коалиционных сил и лишь потом они обретают самостоятельность, но продолжают зависеть от коалиции по вопросам снабжения оружием, спецсредствами и другим необходимым для несения службы, а также подготовки необходимых кадров личного состава. Похожая ситуация складывается практически во всех отраслях обеспечения безопасности государства. Тем самым военные могут сохранять контроль над территорией долгие годы.

Особое место в проведении гуманитарной операции занимает *экономический блок*. На него возлагается задача по втягиванию территории в сферу жизненноважных интересов США. Это означает перестройку экономики с ориентацией на торговые и экономические каналы США и с жесткой привязкой экономики к курсу доллара. В экономических

[1] *Wohlforth W.* The Stability of a Unipolar World // International Security. 1999, Summer.

преобразованиях акцент делается на реформе банковской и денежной системы страны, создании совместных предприятий и дочерних фирм крупных промышленных корпораций[1].

Обратим внимание на события, происходящие в *медийном блоке*. Очевидно, что народ жаждет информации, он хочет увидеть черты мирной жизни, где важная роль отведена национальным СМИ. На территории страны создаются новые газеты. Их редакции состоят из местных журналистов и специально приглашенных из числа эмигрантов на родину. Несмотря на то, что средства массовой информации в основном существуют на производственной базе контртеррористической коалиции, они начинают формировать национальное информационное поле. СМИ получают доступ к вещанию глобальных и транснациональных СМИ, у них появляется выход в интернет. Мировые информационные агентства открывают свои корпункты и не препятствуют созданию национальных информационных агентств. Таким образом, в мировом информационном поле появляется еще одно национальное информационное поле. Главной темой новых СМИ является послевоенное восстановление в стране и развлечение аудитории. Через эти СМИ начинается и культурная экспансия, при помощи универсального набора ценностей демократических идей и транснациональных ценностей массовой культуры и мировой демократии. Еще одной стороной медийной работы является и восстановление в стране развлекательной отрасли. В первую очередь, это всевозможные праздники и спортивные соревнования, от которых полностью отвык народ за время войны. Вместе с тем на них очень удобно показывать образцы новой культуры, новые ценности.

Теперь о том, как меняется характер освещения проблемы в транснациональных СМИ для своей аудитории. Период войны закончился, и для «победителя» важно, чтобы все видели, что военные и политики, ввязавшись в войну по уничтожению террористов, поступили правильно. В этот период может появляться информация о том, что боевики живы. Очевидно, такая информация только на руку военным, стремящимся сохранить свое присутствие в регионе. Но в целом тема войны выводится из повестки дня. Теперь освещение событий в зоне прошедшего конфликта ведется по правилам информации о международной жизни.

[1] *Renwick N.* America's World Identity. The Politics of Exclusion. New York: St. Martin's Press, 2000.

Борьба с терроризмом и свобода слова (опыт США)

М. И. Макеенко

Тема терроризма, безусловно, далеко не нова, однако рассмотрение актуальных реалий, скорее всего, подразумевает современную политическую ситуацию в мире и ее преломление в условиях европейского и американского законодательного климата. Борьба с терроризмом в информационной среде может рассматриваться через призму европейских ограничений на ультрарадикальную деятельность и традиции законодательства в области средств информации, которые предусматривают запреты на пропаганду через различные СМИ ряда идей радикальной и экстремистской направленности.

Однако американская модель отношений государства и экстремистских организаций, государства и СМИ, и соответственно экстремистских организаций и СМИ несколько отличается, что обусловлено всем известным либерализмом законодательства и гарантированными Конституцией правами в сфере свободы мнений, слова и прессы, а также интересами государства и особенно спецслужб. Последние при большей открытости информационных потоков, проходящих через прессу или интернет-ресурсы, получают возможность мониторить, отслеживать настроения в обществе. Это особенно важно в ситуациях с относительно маргинальными идеями и течениями, которые развиваются в небольших группах или сообществах, при этом носят достаточно радикальный характер и способны спровоцировать действия, подпадающие под определение террористических.

Исходя из этого, обращение к опыту Соединенных Штатов позволяет говорить не только о *взаимодействии* государства и законодателей со СМИ, но и о *непосредственной деятельности* в сфере СМИ. И деятельности не только террористических группировок, но и любых организаций радикальной или экстремистской направленности, способных на совершение террористических актов разной степени тяжести. К подобным организациям можно отнести, к примеру, движения или отдельные группы зеленых или антиглобалистов.

Рассмотрим возможности использования различных каналов СМИ для распространения материалов экстремистской направленности:

Печатные каналы. Издание пропагандистских и популяризаторских книг, брошюр, газет и журналов, распространение PDF файлов на CD: а) как официальных публичных органов организации, б) лидерами, идеологами или отдельными членами организации с акцентом на индивидуальных усилиях или интерпретациях. Получение доступа к аудитории через печатные источники, принадлежащие «сочувствующим». Получение доступа к аудитории через освещение отдельных акций или мероприятий, как в рамках принципа объективности (должны быть представлены позиции всех упоминающихся в материале сторон), так и, например через, практику подкупа или идеологической «обработки» журналиста. Последние варианты допустимы, но маловероятны. Подобные материалы могут пройти теоретически, так как на них не наложено законодательных ограничений, однако практика саморегулирования и «фильтрования» тем и материалов в различных газетах и журналах — от общенациональных до «общинных» — развита на высоком уровне.

Радио и телевещание. Создание собственных радио и телестанций невозможно, так как вещание в отличие от издательской деятельности, лицензируется, что налагает на вещателей обязанность работать в общественных интересах, определяемых государством. Возможна запись или съемка пропагандистской программы, но в эфир она тоже не попадет. Кабельное или спутниковое телевидение не подлежат подобному регулированию, но кабельные операторы не станут включать в свои пакеты подобные каналы, а кабельные и спутниковые телесети не будут ставить соответствующие программы. Появление «контента террористической направленности» возможно в эфире отдельных каналов в рамках реализации концепции равного доступа. Самый заезженный пример с каналом «Аль-Джазира», предоставляющим право обращения к широким аудиториям лидерам исламистских террористических организаций. Однако у канала существуют очень серьезные сложности с вещанием на территории США и с созданием англоязычной версии, которую заранее отказываются ретранслировать практически все крупные операторы. В рамках вышеупомянутой концепции возможно попадание интервью или обращений фигур международного масштаба в эфир и более крупных каналов, как это произошло, к примеру, с интервью Басаева Бабицкому, показанным общенациональной телесетью Эй-би-си. Правда в данном случае необходимо все же констатировать политику двойных стандартов в саморегулировании канала.

Интернет-ресурсы. Представляют практически неограниченные возможности для пропагандистской и информационной деятельности, для

дистрибуции текстовых и мультимедийных материалов, для создания и трансляции сигнала онлайновых радиостанций или видеоканалов, для электронной коммерции и коммуникации как через собственные ресурсы организаций, так и через сайты или блоги отдельных членов террористических организаций или сочувствующих. Онлайновые представительства крупных медиаобразований также несколько более свободны в обращении к специфической тематике, чем офлайновые редакции, и могут размещать собственные материалы, полученные текстовые и мультимедийные файлы, а также давать ссылки на ресурсы радикальных и террористических организаций или аффилированных с ними групп и отдельных активистов.

Возможности электронной коммуникации приводят к структурным изменениям в террористических организациях, отказу от обязательной иерархической структуры, переходу к сетевому децентрализованному построению структуры и делегированию в том числе и пропагандистских и популяризаторских функций на индивидуальный уровень.

Отсутствие законодательных ограничений периодически компенсируется инициативами провайдеров доступа к сети, которые могут блокировать тот или иной ресурс, в особенности зарубежный. Подобные действия могут предприниматься как в отношении откровенно террористических ресурсов, так и заподозренных в сочувствии отдельным группам, что иногда случалось с сайтом той же «Аль-Джазиры».

После 11 сентября главным документом, созданным американскими законодателями и оказывающим наибольшее влияние на деятельность органов исполнительной власти и функционирование общественных и коммерческих институтов и отдельных граждан в стране, стал *USA PATRIOT Act* (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of* 2001). Этот закон был подписан президентом уже 26 октября 2001 года, и продлен в марте 2006 г. с одобрения обеих палат конгресса. В разделах документа содержатся определения внутреннего и международного терроризма, ставшие на сегодняшний день наиболее близкими к статусу государственного определения этого явления.

Внутренним терроризмом признается (section 802) деятельность (A) включающая в себя действия, представляющие опасность для жизни людей и нарушающие законы уголовного права США или любого другого государства, (B) явно направленная на (i) устрашение или запугивание гражданского населения, (ii) попытку воздействия на политику государства через устрашение или силовое принуждение, (iii) нарушение нормального функционирования правительства путем массовых разрушений, убийств и похищения людей, (C) ведущаяся

непосредственно на территории Соединенных Штатов. Международным терроризмом считается (section 2331) выше перечисленная деятельность вне определенных географических границ.

В США также наиболее часто ссылаются на определения, сформулированные в рамках Национальной стратегии безопасности, разработанной Министерством обороны и Национальным центром по борьбе с терроризмом, а также используют ряд неофициальных определений, предложенных экспертами Организации объединенных наций.

В последние годы национальная безопасность и противостояние международному терроризму остаются важнейшими приоритетами внутренней и внешней политики США, однако PATRIOT Act, один из программных документов этой политики, является по мнению общественности и одним из наиболее противоречивых законов. Общественность страны пытается решить дилемму о том, насколько национальная безопасность может ограничивать индивидуальные права и свободы и может ли вообще, исходя, в частности, из предпосылки о том, что либеральная республика ставит принципы свободы выше безопасности. Один из самых объемных законодательных актов в истории Америки стал объектом критики с самых разных сторон, в том числе и с позиции сторонников свободы слова и свободы информации. Главными аргументами критиков стали тезисы о том, что Закон вторгается на территории, защищаемые Первой и Четвертой поправками, касающимися свободы слова и защиты частной жизни.

Вообще, необходимо подчеркнуть, что и свобода прессы, и свобода слова в США пока достаточно защищены для того, чтобы не иметь проблем с воздействием внешних факторов. После 11 сентября также ни PATRIOT Act, ни ряд других шагов правительства не создали реально ощутимых инструментов для регулирования СМИ, или для влияния на основные принципы саморегулирования журналистов. Гораздо более ощутимой стала для журналистского сообщества проблема снижения транспарентности и открытости государственного сектора в Америке, но это уже тема иного дискурса.

Профессиональные кодексы, не являющиеся обязательными (в отличие от Европы) ни к принятию, ни к исполнению за последние годы, не претерпели никаких изменений. Что касается кодексов, принятых ведущими профессиональными (Общество профессиональных журналистов) и коммерческими (издательские или вещательные компании) организациями, то в них наряду с традиционными принципами правдивости, аккуратности, объективности, независимости, честности и ответственности перед обществом обнаружить какие-то специальные дополнения, связанные с контентом террористической направленности не удалось. Если и можно

установить какие-либо связи с этой областью, то скорее опосредованные. К примеру, содержащийся в большинстве кодексов постулат о неэтичности ситуаций, когда журналист оказывается втянутым в конфликт интересов. Он предполагает, что журналист не может состоять членом каких-либо организаций или работать на различные политические и общественные образования, в том числе, можно предположить, и террористического или экстремистского толка. Соответственно, в своих материалах он не должен способствовать распространению или популяризации каких-либо политических или мировоззренческих идей и показывать свою политическую позицию. Последнее в СМИ является прерогативой специальных отделов, которые заполняют полосы мнений и редакционных статей, и им уже никто запретить высказывать самые разные мнения не может. Кроме владельца, коммерческого расчета и здравого смысла, которые и способствовали тому, что за последние десятилетия коммерческие средства информации не становились каналом для особенно радикальных или экстремистских взглядов (по крайней мере, с позиции американского общества). Что же касается журналистов и редакторов специализированных медиа, представляющих именно радикальные силы, то, условия их деятельности не были и не стали отягощены инструментами жесткого саморегулирования.

В целом, за последние годы практически не появилось областей, которые можно было бы включать в сферу саморегулирования как нечто новое. То же касается и проблемы терроризма. В US PATRIOT Act можно найти минимум рычагов для прямого или косвенного воздействия на сферу саморегулирования. Если и есть отдельные положения, то они, скорее, апеллируют в нашем случае к самоконтролю. Как, например, параграф в разделе 805 (a), в котором экспертная поддержка и советы террористам приравниваются к предоставлению им материальной помощи и ресурсов. По мнению большинства экспертов, это положение стало одним из наиболее явно противоречащих Конституции страны, так как оно предоставляет поле для самых вольных трактовок данных определений, налагает ограничения и приравнивает к преступлению свободные высказывания, а случаи непосредственного влияния каких-либо высказываний на террористические действия должны быть доказаны. По Конституции такие высказывания преступлением не являются, но из-за несовершенства закона они могут привести к судебным разбирательствам, вроде тех, которые пришлось пережить студенту из Айдахо, оказывавшему такую «экспертную поддержку» в записях на своем сайте.

В принципе, концептуальные вопросы саморегулирования в условиях повышенного внимания к национальной безопасности решаются, как и большинство этических противоречий, не столько на уровне пропи-

санности в отдельных кодексах, сколько через публичную дискуссию, обсуждение наиболее показательных прецедентов и достижения в профессиональной среде некоего консенсуса в их оценке. Хотя и тут остается пространство для индивидуальных решений в рамках подразумеваемых, но не закрепленных нигде, профессиональных представлений о том, что такое хорошо и что такое плохо. В последние 5—6 лет такие этические дилеммы обнаруживались в разных направлениях. В общем, всем понятно, что контент террористической направленности (в рамках общепринятых представлений) в традиционных средствах информации появляться не должен, хотя и не запрещен (правда за действия не в общественных интересах можно, допустим, лишится лицензии). Однако есть более тонкие моменты, связанные, например, с теми ситуациями, когда приходится решать, этично или нет передавать или печатать информацию, которая важна для граждан страны, но в то же время может потенциально использоваться террористами для достижения ими каких-либо целей. В этом контексте могут обсуждаться и не приводить к однозначным выводам например вопросы, стоит ли общенациональным телевизионным сетям показывать записи обращений Усамы бен Ладена или допускать ли представителей прессы к военным на самой линии фронта. Еще более полярные оценки вызывают отдельные прецеденты, например, такие публикации, основанные на утечках материала в Los Angeles Times, затрагивающие вопросы ядерной стратегии США, или сюжет на канале CNN, в котором приводились примеры американских городов, наиболее уязвимых для террористических атак, или сайты в интернете, на которых специальные некоммерческие исследовательские группы описывали сценарии последствий возможных химических атак. Определения и трактовки в подобных случаях далеко не столь однозначны, чтобы их можно было применять в контексте некоей конкретной концепции саморегулирования, однако приоритетным остается подход, при котором информирование граждан ставится выше задачи сокрытия информации от террористов.

Что же касается не только журналистского, но и медийного сообщества в целом, то тут можно остановится на вопросах саморегулирования в организациях, обеспечивающих средствам информации каналы доступа к аудитории. У кабельных операторов письменно сформулированных, закрепленных в форме кодексов и широко признанных стандартов саморегулирования практически нет. Их положение как контролера, который бы мог снять с трансляции канал, допускающий в эфир материалы террористической направленности, тоже не оговорено, да и не подвергалось в особым испытаниям. Все, что может вызвать неудовольствие потребителей, отфильтровывается уже на стадии заключения договоров, как это

происходит, к примеру, в последние месяцы с англоязычной версией арабского новостного канала «Аль-Джазира», который до сих пор не может заключить договор на трансляцию ни с одной кабельной или спутниковой компанией.

Для провайдеров услуг доступа и хостинга в интернете ситуация складывается несколько иная, предполагающая большую активность в контроле за содержанием сайтов и деятельностью в сети. Для контролирующих организаций, скажем, Министерства внутренних дел, существуют отдельные сферы деятельности, в том числе защита авторских прав и сетевой инфраструктуры, борьба с детской порнографией и незаконным игорным бизнесом, когда предпринимаются попытки привлечь провайдеров к ответу за действия подписчиков. Инициатив государства по созданию более жесткого законодательства для регулирования деятельности провайдеров в рамках борьбы на вышеупомянутых фронтах и на ряде других, в том числе и с терроризмом, насчитывается довольно много, но большинство из них неудачных. Тем не менее, провайдеры ведут себя достаточно ответственно, и часто включают в договоры на оказание услуг пункты о возможности блокирования или разрыва отношений в случаях осуществления деятельности не одобряемой государством. Так упоминавшаяся «Аль-Джазира» уже несколько раз вынуждена была менять хостинговую компанию.

Японская практика борьбы с терроризмом в СМИ

М. В. Блинова

Современная Япония — страна стабильного миропорядка, довольно демократичных законов и законопослушных граждан с высоким уровнем правосознания. Однако, помня террористические акты боевиков секты Аум-Синрикё в токийском метро в марте 1995 г., в результате которых погибли 12 человек и более трех тысяч получили травмы различной степени тяжести, правительство страны всячески стремится предотвратить. Тотальная компьютеризация страны в последние годы и понимание того факта, что Сеть может быть использована для нанесения серьезного удара по критически важным объектам инфраструктуры (компьютерные сети и интернет играют ключевую роль в управлении хозяйственной инфраструктурой страны, и в силу этого растет угроза кибертерроризма), побудили правительство Японии принять спешные защитные меры по борьбе с терроризмом в Сети.

Еще в 1996 году японский Электронный Сетевой Консорциум — коммерческая организация при Новой Ассоциации Развития СМИ, которая, в свою очередь, было учреждена Министерством Международной Торговли и Промышленности, начала внедрять использование фильтрующих программ. Новая Ассоциация Развития СМИ участвовала в разработке совместимого с фильтрами программного обеспечения, нацеленного на контроль Сетевого контента. С 2001 г. Электронный Сетевой Консорциум был слит с Интернет-Ассоциацией Японии (*IAJapan*). Сегодня IAJapan — одна из наиболее влиятельных некоммерческих организаций, развивающих сетевую экономику и сетевой контент страны. В последние годы в Японии широко используются фильтрующие программы, особенно в школах, офисах, библиотеках и других общественных институтах. В качестве оснований для введения запрета на свободное использование Интернета большинство компаний называют ущерб от компьютерных вирусов, которые проникают в киберпространство через электронную почту и скачиваемые программы. Среди других причин указываются помехи, причиняемые корпорационным коммуникациям чрезмерным трафи-

ком, утечка важной служебной информации, а также случаи насилия, клеветы, угроз.

В 2000 г. Национальным управлением полиции Японии разработана программа создания интегрированной общегосударственной системы «раннего предупреждения» об угрозе несанкционированного доступа к сетевым компьютерным системам критического значения и противодействия кибертерроризму. В соответствии с этой программой активизируется деятельность государственных ведомств по совершенствованию организационно-технической системы защиты от несанкционированного доступа к сетевым информационным ресурсам. По замыслу разработчиков, такая система должна осуществлять постоянный мониторинг за потоками электронных данных в наиболее важных узлах национальной коммуникационной инфраструктуры, обладать способностью в реальном масштабе времени распознавать аномальные явления, являющиеся признаками возможной кибератаки, точно определять источник подозрительных электронных сигналов, обеспечивать эффективную защиту баз данных и локализовать развитие потенциально опасной ситуации в Сети.

На втором этапе, с июля 2000 г. Управлением полиции, комитетом по безопасности сетевых ресурсов Министерства экономики, торговли и промышленности (МЭТП) и рабочей группой по противодействию кибертероризму министерства почт и телекоммуникаций (МПТ) проводилась интенсивная совместная работа по углубленному анализу внутренних и внешних угроз информационной безопасности государственных организаций с целью выработки общих подходов защиты информации на национальном уровне и конкретных планов действий отдельно для каждого из ведомств. Повышенное внимание уделялось также определению принципов государственной политики информационной безопасности наиболее важных областей национальной инфраструктуры, связанных с обеспечением бесперебойной работы кредитно-денежной системы, транспорта, связи и энергоснабжения. Для выработки стратегии информационной безопасности в частном секторе была создана специальная комиссия при кабинете министров, к работе в которой привлечены эксперты ведущих коммуникационных компаний, банковских учреждений и энергетического комплекса. В качестве основной задачи указанной комиссии определена выработка эффективной системы налоговых льгот, стимулирующей частные предприятия к самостоятельному совершенствованию корпоративных систем защиты информации.

Одной из главных целей третьего этапа программы стала разработка новых высокоэффективных технологий выявления, анализа несанкционированного доступа к сетевым ресурсам, а также создание комплексной

организационной системы противодействия компьютерным преступлениям на общенациональном уровне в плане подготовки к внедрению в стране единой системы поддержки административной деятельности и электронного документооборота государственных учреждений (так называемого «электронного правительства»).

Для осуществления эксплуатации общенациональной системы информационной безопасности коммуникационной инфраструктуры и организации эффективного противодействия преступлениям в Сети создано специальное подразделение «киберполиции» численностью 150 человек. На новую организацию возложены также задачи регулярной проверки уровня защищенности государственных и корпоративных информационных сайтов, сбор информации о потенциальных правонарушителях, координация деятельности различных ведомств в области разработки прогрессивных технологий защиты информации.

В свою очередь в апреле 2000 г. группой японских компаний, производителей продуктов и услуг в области защиты информации в компьютерных коммуникационных сетях учреждена специализированная организация Japan Network Security Association. Членами ассоциации стали 55 крупных фирм, включая NTT Communications, Cisco Systems KK, VeriSign Japan, Microsoft Japan, Toyo Information Systems и др. Деятельность ассоциации направлена на дальнейшее укрепление системы информационной безопасности страны.

В Японии деятельность по предотвращению терактов ведется особыми отделами всех министерств.

Японское Управление национальной обороны планирует создать спецподразделение по борьбе с терроризмом в Сети, которое будет пресекать потенциальные попытки электронных взломщиков проникнуть в компьютерные системы, имеющие важное значение с точки зрения обеспечения безопасности страны. В проекте госбюджета уже выделено на эту задачу свыше 25 млн долларов.

В октябре 2005 г. Министерство внутренних дел и коммуникаций Японии приняло решение провести общенациональные учения по противодействию кибертерроризму, организацию и финансирование которых оно берет на себя. В ходе учений заранее спланированным кибератакам подвергнутся серверы крупных компаний и правительственных организаций по всей стране. Главная цель учений — выявить слабые места в системах защиты компьютерных сетей и принять соответствующие меры по их устранению. Первое мероприятие намечено на начало 2006 г., далее учения планируется проводить каждые три года. Частные компании, играющие ключевую роль в функционировании экономики Японии, планируют принять в этом участие. Кроме того, будет проверяться надежность интернет-сайтов центральных и местных органов власти. Впервые аналогичное мероприятие было организовано в США в 2003 г.

Япония является также активным участником международной борьбы с терроризмом. Так, в октябре 2005 г. Япония в числе более 14 стран-участниц (Канады, Китая, Евросоюза, США, Индонезии, Южной Кореи, Лаоса, Малайзии, Пакистана, Филиппин, Сингапура, Таиланда, Вьетнама, России и др.) была представлена на 2-м ежегодном Семинаре стран участниц ASEAN по вопросам борьбы с кибертерроризмом и защиты важнейших национальных инфраструктур, проходившем на Филиппинах. Основными темами, которые обсуждались на семинаре были темы — «Кибертерроризм как региональная угроза», «Защита национальных инфраструктур», «Кризис-менеджмент в ходе возможных кибертеррористических инцидентов».

На встрече в Токио, в ноябре 2005 г. Владимир Путин и Дзюнъитиро Коидзуми подписали программу действий Российской Федерации и Японии в области сотрудничества в борьбе с терроризмом. В числе прочих документ содержит статью по сотрудничеству в борьбе с кибертерроризмом. Япония и Россия планируют изучать в рамках «Большой восьмерки» способы пресечения подстрекательства к терроризму, в том числе с использованием Интернета.

Часть VI

СЕМИНАР-КРУГЛЫЙ СТОЛ «СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ ФАКТОРЫ РАЗВИТИЯ ТЕРРОРИЗМА»

Психологический портрет терроризма: истоки терроризма как социальной формы идентичности

Ю. П. Зинченко

Тема нашего сегодняшнего заседания: «Психология терроризма». Терроризм, казалось бы, далекая, на первый взгляд, от университетской фундаментальной науки тема. Ею в основном занимались политологи, конфликтологи и военные специалисты. Но сейчас эта тема является первой в перечне из шести приоритетных направлений научных исследований в нашей стране. Необходимо вспомнить, что ровно 5 лет назад, 23 октября 2002 года, всю страну потряс один из самых жестоких терактов: чеченские террористы захватили Театральный центр на улице Дубровка. В заложниках оказались 912 человек. Три дня длилась эта трагедия, и 26 октября в результате штурма все 40 террористов были уничтожены, но это стоило жизни 130 заложникам. Сегодня утром состоялась панихида и минута молчания по погибшим. Предлагаю почтить память погибших.

Мы, как представители университетской науки, обязаны включиться во всемирный проект по борьбе с терроризмом. Терроризм как явление геополитического масштаба многолик, многоаспектен и не имеет государственных границ. Более того, этот феномен «ускользает» от точных определений. Еще в 1973 году на заседании Специального комитета ООН по вопросам международного терроризма была сделана попытка создать определение «существа» и «основы» терроризма как явления международного масштаба. Многочисленные усилия в прошлом не нашли удовлетворительного решения. Было предложено три вида определений: общее определение абстрактного характера — «гнусный международный акт варварства»; определение в форме перечисления актов терроризма с последующим анализом аналитическое определение — был составлен перечень преступлений, носящих признанный террористический характер. Затем список был подразделен на категории и выявлены общие характерные особенности и составные элементы терроризма. Пример — «акт, совершенный отдельными лицами против невинных лиц в целях их соб-

Исследование выполнено при поддержке РГНФ (проект № 06-06-184а).

ственной личной выгоды или эмоционального удовлетворения». Смешанное определение должно было содержать описание причин терроризма, их целей и мотивов, изложение характерных особенностей этого явления, и перечень конкретных актов терроризма — «акт насилия, направленный против иностранных граждан по причине их национальной принадлежности к той или иной стране, в целях провоцирования войны или создания международных осложнений или по обычным уголовным мотивам».

В 2000 году в «Законе о борьбе с терроризмом», принятом Парламентом Великобритании, к террористическим актам относятся «любые действия или угроза совершения тяжкого насилия над личностью, причинение ущерба частной собственности в крупных размерах, а также вмешательство в работу или нарушение деятельности разных систем по идеологическим или политическим мотивам».

Терроризм является одной из наиболее острых проблем современного общества, ставящих под сомнение фундаментальные основы самого его существования. События последних десятилетий показали его тотальный, всепроницающий характер, практически изменивший современный мир. Если ранее террор был достаточно локальной проблемой, касавшейся либо географически, либо экономически ограниченных областей, социальных страт, этносов, то в настоящий момент ни один человек не может ощущать себя достаточно защищенным от действий вездесущих террористов.

Термин «терроризм» стал широко употребляться со времен Французской буржуазной революции 1789 года. В 1789 году, в словаре Французской Академии Наук терроризм был определен как система страха или в английском варианте «правление ужаса». В толковом словаре С. И. Ожегова терроризм определяется политика и практика террора, под которым в свою очередь мыслится устрашение политических противников, выражающееся в физическом насилии вплоть до уничтожения. Использование силы с целью запугивания и распространения паники, вызов политических изменений, дестабилизация государственного режима или даже свержение правительства.

Я позволил себе так много времени посвятить проблеме определения терроризма, чтобы показать, что суть данного явления непосредственно смыкается с понятийным аппаратом психологической науки. Мы можем выделить несколько аспектов, актуальных для психологической науки:

- исследование идеологических и культурологических истоков терроризма — это аспект политической психологии;
- выявление индивидуально-личностных основ терроризма и проблемы ненависти и агрессии как способа решения социальных задач — это аспект возрастной психологии и психологии личности;
- изучение особенностей функционирования террористических организаций — это аспект социальной психологии;
- исследование психологических причин, толкающих человека на участие в террористической деятельности — это аспект клинической психологии;
- изучение использования террористами современного глобального информационного пространства как всемирной сцены для своих действий — это аспект психологии массовых коммуникаций.

Современные исследования показывают, что терроризм — отнюдь не новое явление в человеческой истории. Террористы обладают высокой мотивацией. К террористическим методам борьбы часто прибегали люди и организации, которые не имели иных инструментов для достижения своих целей. Терроризм силен, потому что террористам, как правило, нечего терять. В подавляющем большинстве случаев они находятся под влиянием религии или иных идеологий, прославляющих мученичество и самопожертвование.

Хорошо известно, что лидеры исламских террористических организаций убеждают своих сторонников, что они ведут священную войну против неверных. Лидеры исламских террористов утверждают, что они не являются пророками, они лишь точно выполняют волю Аллаха.

Терроризм стал стилем жизни для многих людей. Террористические организации дают своим членам социальный статус, самоуважение, власть, влияние, чего они могут быть лишены, живя в обычных условиях.

Пол Пилар, бывший исполнительный директор конттеррористического центра ЦРУ, сформулировал четыре ключевых элемента, отличающих террористическую организацию от любой другой.

Во-первых, террористы действуют не импульсивно, а по заранее разработанному плану.

Во-вторых, они преследуют политические, а не криминальные цели. В отличии от мафии они стремятся изменить существующий порядок вещей, а не просто получить деньги.

В-третьих, их целью являются гражданские лица, а не войска.

В-четвертых, они действуют в составе межнациональных групп, в большинстве случаев не обращая внимания на государственные границы.

Но лицо терроризма очень изменчиво. Например, опыт борьбы с террористами в Чечне показывает, что целью их нападения могут быть и войска. Это свидетельствует о том, что в России есть своя специфика у явления терроризма, которую надо изучать.

В настоящее время наиболее компетентными экспертами по психологии терроризма являются:

Джеррольд Пост, личный консультант нескольких американских президентов, специалист по политической психологии. Он более 20 лет возглавлял Аналитический центр по изучению политического поведения в ЦРУ. Он инициировал принятие государственной программы США по изучению психологии терроризма.

Согласно его концепции, среди террористов существует два типа личности: «анархист-идеолог» и «националист-сепаратист». «Анархист-идеолог» в детстве, как правило, становится жертвой серьезных ссор между родителями, и это приводит его к бунту против семьи, прежде всего против отца. Поскольку родители зачастую отождествляются с преданностью существующему политическому порядку, бунт против отца легко превращается в бунт против государства. «Анархист-идеолог» всегда находит основания для бунта, даже если цели его уже достигнуты, ибо бунт есть не что иное, как выплескивание наружу неприятия любой власти. Что же касается «националиста-сепаратиста», то он в принципе не выступает против власти собственного государства; его действиями руководит желание поднять бунт против внешних врагов. Проблема «националистов-сепаратистов» состоит в патологической невозможности отличить себя от других. Поэтому они восстают против общества и мстят ему за те страдания, какое оно некогда причинило их родителям. Оба — и «анархист-идеолог», и «националист-сепаратист» — обретают внутреннее равновесие, только присоединяясь к группе террористов-мятежников со сходным прошлым и сходными проблемами.

Чарльз Руби, клиницист, автор книги «Являются ли террористы душевнобольными?» 2002 года издания, долгое время занимался уголовными преступниками и контрразведчиками, служил в ВВС США. Исследовал ролевые отношения в террористических организациях. В частности, он указывает на то, что люди становятся террористами скорее по причине своих психологических потребностей, чем из желания улучшить социополитическое положение масс. Он описывает портрет основных участников террористической организации. «Лидер» — интеллектуальный мотор группы. Мотивирует он свои действия тем, что общество не справляется со своими обязанностями, и его нужно изменить. Лидер недоверчив и предан делу самым иррациональным образом. Вторая важная роль — «оппортунист», он обеспечивает техническую подготовку группы и ее силовые действия. Эту роль исполняют антисоциальные элементы, люди с криминальным прошлым. Третья роль — «идеалист» — человек молодой, не удовлетворенный существующим положением дел и смотрящий на проблемы общества с наивной точки зрения.

Абрахам Каплан — философ, международный эксперт по терроризму. Он предлагает различать основания терроризма и его причины; к первым

он относит социальные условия, которые побуждают индивида к рационализации своих террористических действий, ко вторым — особенности личности террористов.

Энтони Купер придерживается мнения, которое основывается на теории социальных рефлексов. Террорист — это не душевно больной человек, а субъект, который в период социальной адаптации испытывает опыт, отклоняющийся от норм. Этот опыт обусловливает основы его характера и способы поведения в конфликтных ситуациях. Так, Э. Купер утверждает, что «с точки зрения психической патологии нет никакой разницы между террористом и солдатом; эти двое просто избирают разные способы достижения своей цели с оружием в руках». Те, кто лишен официальных и законных способов достижения военных и политических целей, прибегают к незаконным способам.

Тед Гурр, американский политолог, специалист по этнополитическим конфликтам, рассматривает самоидентичность террориста как плод влияния группы на индивида. Молодые люди с бунтарскими наклонностями тянутся к террористическим организациям. Пережив негативный опыт в общении с представителями власти, они ищут поддержку у подобных себе и часто оказываются в рядах террористической группировки, где они получают моральную поддержку и сочувствие. Они начинают разделять идеологию группы и стремиться к достижению ее специфических целей. Чем более опасны действия террористов, тем сильнее их убежденность в законности и важности этих действий. Согласно Теду Гуру, чем большее удовлетворение доставляют индивиду агрессия и насилие, тем чаще он будет прибегать к ним для решения любых вопросов. Проблемы же, волнующие террористов, носят по преимуществу, политический характер.

Таким образом, можно заключить, что террорист — это человек, преследующий цель внушить всем безграничный ужас, и тем самым представителей власти изменить политику, которую террористы считают несправедливой. Мы с Александром Шамилевичем Тхостовым в последнее время предприняли попытку анализа особенностей социальной идентичности террориста как человека, принимающего решения о вступлении в такую организацию. Результаты этой работы опубликованы в журнале «Вестник Московского университета. Серия 14. Психология.»

Нам важно понять логику действий этих людей, чтобы выработать психологические меры защиты и способы профилактики террористического поведения. Надеюсь, что заседание нашего круглого стола послужит решению этой задачи.

Я предлагаю такой порядок работы. Мы заслушаем доклады участников, а затем проведем дискуссию в режиме «мозгового штурма» и в рамках обсуждения следующих вопросов:

1. Терроризм как социально-психологическое явление.
2. Психологическая суть терроризма, Психологические особенности террориста.
3. Мотивация терроризма и террориста.
4. Снятие межэтнической напряженности как фактор снижения террористической активности.
5. Психологические механизмы влияния СМИ на поведение людей в условиях опасности возникновения террористических актов.
6. Публикации в СМИ как способ профилактики терроризма.
7. Психологические механизмы вовлечения в террористические организации.
8. Психологическая реабилитация людей, переживших различные формы насилия, в том числе террористические акты.
9. Психологическое сопровождение антитеррористических мероприятий.
10. Психологическая подготовка специалистов по противодействию терроризму и ликвидации последствий террористических актов.

Методологические проблемы психологической подготовки специалистов по ведению переговоров для преодоления террористических актов

Р. С. Шилко

Одной из проблем современного развития общества являются социальные конфликты, которые зачастую сопровождаются отчетливыми проявлениями экстремизма. Пожалуй, наиболее крайняя форма социальных конфликтов с проявлениями экстремизма — это феномен терроризма. Поэтому разработка мер и способов предотвращения и, главное, профилактики терроризма представляется в настоящее время особенно актуальной. Среди этих мер и способов особое место занимают методы переговоры. Научные достижения в области психологии межличностных коммуникаций позволяют провести методическое обеспечение переговорного процесса для повышения его эффективности.

Первостепенной по важности задачей для повышения эффективности переговоров представляется разработка системы подготовки специалистов, предназначенных для проведения переговоров как с террористами так и с представителями экстремистских групп.

Это, в свою очередь, требует подготовки и реализации порядка подготовки, прежде всего психологической, специалистов по ведению переговорного процесса.

В общем виде этот порядок должен содержать следующие этапы работы:

- методическое обеспечение: разработка, апробация, обоснование, адаптация методов и техник ведения переговоров с террористами;
- методическое обеспечение отбора кандидатов в специалисты по ведению переговорного процесса;
- отбор кандидатов в специалисты по ведению переговорного процесса, обладающих необходимыми профессионально важными качествами;

Исследование выполнено при поддержке РГНФ (проект № 06-06-184а).

- обучение кандидатов в специалисты по ведению переговорного процесса: методам и техникам переговоров, методикам экспресс-диагностики актуальных психических состояний и личностных свойств;
- формирование навыков ведения переговоров и психологического воздействия;
- практическая отработка умений и навыков в модельных и реальных условиях.

Как показывают исследования, опыт подготовки специалистов свидетельствует о том, что подобный порядок оправдывает себя и дает неплохие результаты. Осмысление и методическое наполнение перечисленных этапов, однако, вызывает множество вопросов, которые в настоящее время еще не имеют готовых и однозначных ответов.

Принципиальным вопросом, требующим разрешения в первую очередь, является определение необходимых переговорщикам профессионально важных качеств. С одной стороны, перечень профессионально-важных качеств можно было бы выявить путем оценки личностных и профессиональных свойств специалистов, успешно проводивших переговоры с террористами. Но, поскольку таких специалистов очень немного, подобный подход малоэффективен, чтобы получить надежные и репрезентативные результаты. Поэтому более адекватным подходом будет анализ специфики ситуаций, возникающих во время террористических актов, с последующим прогнозированием тех профессионально важных качеств, которые обеспечивающих решение поставленных перед переговорщиком задач. На основе анализа профессионально важных качеств отдельных специалистов можно сделать обобщение, чтобы сформулировать перечень общих, частных и специфических качеств для переговорщиков. Анализ специфики террористических актов осуществляется обычно post factum, с участием представителей силовых структур и выживших очевидцев. Восприятие и интерпретация произошедших событий теми и другими имеют определенную степень субъективизма, что следует учитывать в ходе психологического анализа террористического акта.

Наиболее важными моментами, связанными с анализом террористического акта и имеющими отношение к подготовке переговорщиков, вероятно, следует считать: мотивы террористического поведения, социальные представления, цели террористического акта; способы подготовки и реализации; личностные качества лидеров экстремистской группы; степень психологической подготовки террористов и методы их психологического воздействия на окружающих. Выяснение этих факторов может помочь спрогнозировать эффективность методов воздействия переговорщика на террористов.

Для точного выяснения перечня необходимых переговорщику психологических качеств и свойств необходимо провести профессиографическое исследование.

Продолжением этапа формирования перечня профессионально-важных качеств является выбор или разработка в случае их отсутствия валидных и надежных (необязательно стандартизированных) методик их выявления. При этом объективирование критерия, определяющего эффективность отбора и подготовки переговорщиков, может оказаться не всегда возможным.

Экспресс-диагностика личностных свойств террориста (экстремиста) столь же актуальна, сколь и оценка собственных психических состояний. Переговорщик обязан уметь регулировать уровень качество эмоционального состояния. Идеальной следует считать способность наблюдать за происходящим как бы со стороны, одновременно оценивая и себя, и оппонента. Подобное качество обеспечивает возможность предугадывать ход событий и выбирать те стратегию и тактику переговоров, которые будут наиболее эффективными.

Подготовка переговорщиков не может быть совершенной без обучения разнообразным приемам и способам психологического воздействия. Техники установления и поддержания психологического контакта, создания позитивного впечатления, привлечения внимания и инициации интереса, создания адекватных ситуации имиджа и ролевых моделей с учетом этнических и конфессиональных качеств террориста, поддержания диалога, убеждения и даже подчинения, очевидно, должны составить ядро этого этапа подготовки. Приведенный перечень можно считать открытым, особенно с учетом быстро меняющейся специфики чрезвычайных ситуаций.

Практическая отработка полученных знаний, умений и навыков реального взаимодействия с террористами представляется наиболее сложным этапом подготовки переговорщиков. Сложность состоит не только в том, что трудно моделировать кризисную ситуацию как таковую, но и в том, что практически невозможно предугадать ее реальный ход. Важным элементом прикладного этапа подготовки должны стать семинары, в ходе которых действующие опытные переговорщики будут передавать свой психологический опыт.

Система подготовки переговорщиков, вне всякого сомнения, должна носить комплексный характер с привлечением различных специалистов, при этом важная роль отводится именно психологам.

Динамика восприятия фактора неопределенности в управлении экстремальными ситуациями в имитационной игре «Координация»

Е. Ю. Лихачева, А. В. Зайкова

Нарастание природных и социальных рисков влечет за собой необходимость осознания и принятия индивидами и группами людей ответственности за настоящие и будущие результаты своей деятельности. Обучение управлению рисками, принятию решений в условиях нехватки времени, недостатка информации и неопределенности выходит на первый план. Имитационные игры имеют коридор возможного предвосхищения событий, позволяют моделировать деятельность человека по решению задачи, и могут использоваться в качестве «штабных учений»[1]. Реализации этих целей служит имитационная игра «Координация».

Имитационная игра «Координация» была разработана на факультете государственного управления МГУ им. М. В. Ломоносова группой студентов и аспирантов под руководством заведующего кафедрой управления природными ресурсами профессора Д. Н. Кавтарадзе на базе междисциплинарного проекта МГУ по теме «Гуманитарные методы противодействия терроризму»[2]. В игре моделируется экстремальная ситуация террористической активности в условной стране. Цель игры — подготовка участников к выработке стратегии противодействия терроризму — сложному виду групповой управленческой деятельности с периодической обратной связью.

Апробация игры, в которой приняли участие студенты, аспиранты и сотрудники четырех факультетов МГУ (государственного управления, журналистики, психологии и экономического факультета), была осуществлена 30 сентября 2006 года на ФГУ. Вторая игровая сессия игры

[1] *М. М. Крюков.* Уроки военной игры. Доклад на V Международной конференции «Государственное управление в 21 веке: традиции и инновации», Москва, 31 мая–2 июня, 2007; *Kavtaradze Dmitri.* Simulation Games: Limits of Impact. 37th Annual Conference of International Simulation and Gaming Association (ISAGA). St. Petersburg, 3—7 July 2006.

[2] См. описание игры.

Рис. 1. Параметры экстремальной ситуации (ЭС)

состоялась 9 декабря 2006 года с участием студентов и аспирантов факультета мировой политики, государственного управления, психологии и журналистики МГУ. Во второй сессии также приняли участие эксперты: участник разрешения нескольких военных конфликтов и преподаватель МГИМО. Во время апробации и второй сессии игры авторы статьи выступали в качестве наблюдателей.

Игра «Координация» представляет психологическую модель групповой деятельности по разработке стратегии и принятию решений в экстремальной ситуации. Экстремальная ситуация (ЭС) характеризуется длинным перечнем признаков[1], проанализировав которые мы выделили представленные на причинно-следственной диаграмме (рис. 1) взаимосвязанные параметры (неопределенность; ограниченность ресурсов, в первую очередь, проявляющаяся во временном лимите; повышенная ответственность; эмоциональный и когнитивный стресс). Многомерность предмета моделирования может быть полноценно отражена каузальными диаграммами по методу системной динамики Джея Форрестера[2].

На рис. 1 представлена взаимосвязь параметров экстремальной ситуации в виде причинно-следственной диаграммы, где «+» соответствует

[1] Социология: Энциклопедия / Сост. *Грицанов А. А., Абушенко В. Л., Евелькин Г. М., Соколова Г. Н., Терещенко О. В.* Мн., 2003.

[2] *Дж. Форрестер.* Мировая динамика. АСТ, Terra Fantastica. 2003.

прямо пропорциональным отношениям, «–» — обратно пропорциональным отношениям. Следует отметить, что параметры усиливают друг друга по типу порочного круга (маниакальная петля по Д. Медоузу).

В нашем исследовании мы приняли следующее *рабочее определение неопределенности*:

> Неопределенность — это отсутствие у субъекта ситуации ее целостного видения, контекста, ее значения, возможностей и тенденций ее дальнейшего развития.

Ситуация неопределенности включает внешнюю (объективные характеристики) и внутреннюю (психологическое переживание) стороны. Проблемная ситуация предъявляет человеку требования, реализуя которые, он преобразовывает или преодолевает ее: уменьшение степени неопределенности требует навыков планирования деятельности в условиях оперирования *вероятностными данными и управления рисками*[1]. Имитационные игры (simulation games) обучают действиям в условиях неопределенности с помощью освоения модели возможного будущего, модели проблемы[2]. Общей мерой неопределенности принято понятие риска. Возможность в интерактивном обучении работать с этими понятиями приводит к осознанию своей и общей ответственности за настоящие и будущие действия.

В игре «Координация» моделируются и наблюдаются следующие виды неопределенности:

- *информационная неопределенность* — недостаток информации (как самой информации, так и знаний, где ее можно найти — источников). Средства моделирования в игре: через генератор случайных событий, изолированность всех групп друг от друга и опосредованность коммуникации (либо через администраторов игры, либо через Интернет и телефон). Информация часто поступает с запаздыванием или искажается в ходе игры.
- *смысловая неопределенность* — заложена в самой игре, проявляется в обсуждении или через некоторое время после игры (смыслообразование происходит после осознания участником процессов, происходивших с ним в игре, соответственно, для выявления процессов смыслообразования необходимы интервью, либо опрос после игры). В «Координации» достаточно четко заданы функции игроков и поставлена задача игры, но размыты цели участника (или им не осознаются).
- *ролевая неопределенность или проблемы с ролевой самоидентификацией*. В игре ролевая неопределенность вызывалась недостаточным инструктажем и лимитом времени, что, в целом соответствует реальности, поскольку должностные обязанности зачастую недостаточно прописаны.

[1] *Солнцева Г. Н.* Определение неопределенности. В сб. Управление риском, 1997, № 2; *Солнцева Г. Н., Корнилова Т. В.* Риск как характеристика действий субъекта. М., 1999.

[2] *Кавтарадзе Д. Н.* Обучение и игра. М., 1998

Взяв за основу анализа возможную динамику смены Президентов и их политики («либерал», «военный», «демократ» — соответственно, в первом, втором и третьем игровом периодах)[1], мы построили график возможной динамики восприятия неопределенности в игре в течение игрового периода, послеигрового обсуждения и времени после игры.

Мы предположили, что ролевая неопределенность возникает каждый раз в начале каждого игрового периода (1-й период — в связи с вхождением каждого участника в роль; 2-й и 3-й периоды — в связи с перемещением некоторых игроков групп экспертов и министров). При инструктаже ролевая неопределенность достигает своего максимума (вследствие непривычности ситуации в целом и неясности ее контекста).

Информационная неопределенность возникает в начале игры и нарастает к ее окончанию; причины — отсутствие информации, неожиданные события, искажение информации, когнитивный стресс. Мы допустили, что информационная неопределенность частично снижается в ходе пресс-конференции или выходит на уровень плато (в связи с обменом информацией между всеми игровыми группами — общением по вертикали — и редуцированием острого временного лимита). В ходе послеигровой дискуссии информационная неопределенность снижается вследствие обсуждения участниками заложенной в игру модели, обмена мнениями и т. п. Резкое нарастание информационной неопределенности также возможно при инструктаже (как реакция на переизбыток новой непривычной информации).

Предполагается, что смысловая неопределенность возникает во втором игровом периоде вследствие осознания участниками низкой продуктивности применения силы («военный» президент), роста количества жертв террористических актов и эмоционального стресса. У играющих возникает внутреннее противоречие: расхождение между желаемым результатом, реальными результатами деятельности и непониманием причин результатов собственной деятельности. В третьем периоде смысловая неопределенность нарастает (вследствие нехватки времени на осознание происходящих процессов в игре) и снижается только в послеигровой дискуссии или после окончания всей игровой сессии (происходят процес-

[1] Отчет по теме «Социально-психологические методы повышения эффективности антитеррористических мероприятий». МГУ, ИПИБ, 2006.

сы смыслоосознания — построение внутренних связей между увиденным, осуществленным и потребностями, личностными ценностями, мировоззрением каждого из участников; значения превращаются смыслы (значения-для-меня[1])). Фактически обучение продолжается спустя много дней после проведения игры.

Для проверки сделанных предположений относительно динамики неопределенности в игре «Координация» специально для второй игровой сессии нами был разработан опросник (по типу САН[2]), нацеленный на оценку участниками текущей игровой ситуации, оценку уровня неопределенности и самооценку. Наше исследование носит качественный характер, и, несмотря на всю трудоемкость качественного подхода к изучению, позволяет получить целостную картину процессов. Опираясь на данные наблюдения, отзывы участников, полученные в ходе апробации игры, а также на разработанную модель параметров экстремальной ситуации, мы включили в опросник следующие вопросы:

1. Испытывали ли Вы неопределенность, связанную со своей ролью, в отношении своей роли?
2. Испытывали ли Вы неопределенность, связанную с информацией, ее недостатком, избытком, искажением?

Верны ли следующие высказывания в отношении Вас:

3. Я понимал смысл происходящих в игре событий.
4. Я понимал цели своей/нашей деятельности (подгруппы).
5. Я понимал смысл игры в целом.

Участники должны были оценить себя (или согласиться/не согласиться с утверждениями) по 10-тибалльной шкале, где 1 — слабо выраженный признак (абсолютно нет), 10 — сильно выраженный признак (абсолютно да). Опросник раздавался 2 раза: во время перерыва после первых двух игровых периодов и после окончания игры для оценивания третьего периода и послеигрового обсуждения. В опросе приняли участие 9 участников второй игровой сессии. При анализе данных учитывались также письменные отзывы игроков.

Для построения простейшего графика динамики самооценки участников нами был проведен анализ средних баллов, полученных по каждому из вопросов (рис. 2).

[1] *Леонтьев Д. А.* Психология смысла. М.: Смысл, 1999.

[2] САН — тест для оперативной оценки самочувствия, активности и настроения; название опросника — по первым трем буквам этих функциональных состояний. Альманах психологических тестов. М., КСП, 1996.

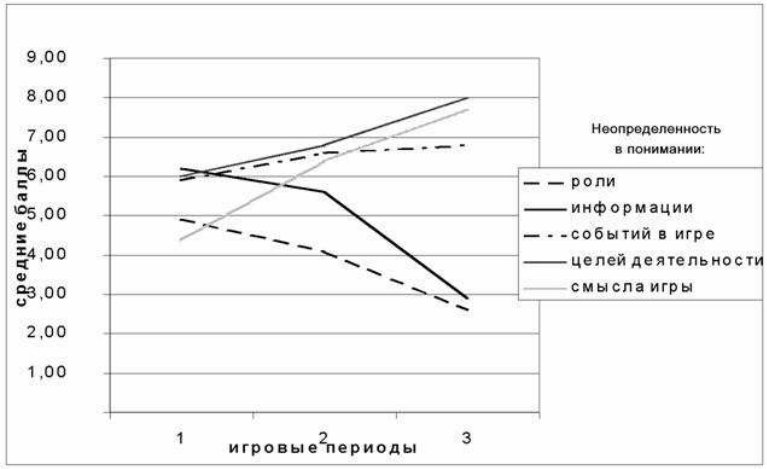


Рис. 2. График динамики самооценки участников и оценки ими наличия разных видов неопределенности в игре «Координация» (вторая игровая сессия)

Оказалось, что для участников второй игровой сессии «Координации» уровень информационной неопределенности достаточно высок в начале игры (причем, как из-за недостатка информации, так и от ее переизбытка — отзыв участников) и постепенно снижается к ее окончанию. Возможно, это снижение объясняется тем, что в первом игровом периоде участники в условиях извне созданной информационной неопределенности действуют, не опираясь на информацию, а применяя свой опыт и умения, — информационная неопределенность «не замечается» игроками, происходит «привыкание» к постоянной нехватке или искажению информации.

Ролевая неопределенность, как и информационная неопределенность, снижается к концу игры, причем уровень информационной неопределенности действительно находится выше уровня ролевой. О том, что участники испытывали ролевую неопределенность, свидетельствуют наблюдения во время игры (вопрос наблюдателю во втором игровом периоде: «Что делает эксперт?»), а также отзывы участников после игры: «В каждой группе должен присутствовать профессионал, который подскажет верный путь решения», «Я недоволен — слишком быстро, слишком мало людей. У меня интерес пропал. Недоволен и понижением» (в должности — *авт.*).

Неопределенность в отношении понимания происходящих в игре событий, наоборот, возрастает к концу игры. Мы предполагаем, что это происходит вследствие нехватки времени на принятие решений и оценку

игровой ситуации в целом, а также вследствие изолированности групп друг от друга, несопряженности совместной деятельности и недостатка информации.

Наибольшей неопределенностью обладают для участников понимание целей своей деятельности в группах и понимание смысла всей игры в целом. Во-первых, в субъективном опыте участников отсутствуют умения, знания и навыки, необходимые для управления страной в условиях террористической активности и для выработки антитеррористической стратегии. Во-вторых, у участников отсутствуют возможности и время для осознания мотивов своей деятельности в игре. Кроме того, перемещение участников из групп экспертов и министров влияет на восприятие и осознание ими целей и смысла их деятельности («Слишком много информации, да, есть бумаги, Интернет, но организованности никакой!! Поэтому смысла играть нет... Меня разжаловали за то, что я подсказал, что сделать Президенту!!»).

Используя полученные данные, мы построили график динамики восприятия неопределенности во второй игровой сессии.

Полученные результаты необязательно описывают жесткий сценарий развития процессов восприятия и понимания участниками событий, но, скорее, могут свидетельствовать о возможных тенденциях. Для обеспечения надежности результатов (а также валидности методики) необходимо неоднократное проведение опроса участников игры «Координация» и продолжение наблюдения.

В целом данный метод опроса позволяет получить моментальный срез самооценки и оценки участниками игровой ситуации. Изучение восприятия фактора неопределенности участниками экстремальной ситуации — при помощи опроса и психологической реконструкции имитационной игры — позволяет проанализировать возможные способы его переживания, освоения и преодоления[1]. Полученные данные могут быть использованы как для изучения внутриигровых процессов и явлений, так и для корректировки самого игрового метода как инструмента освоения управления экстремальными ситуациями.

[1]Выявление групп риска, представляющих ресурсы развития терроризма, и обоснование принципов антитеррористической деятельности на этом направлении (Глава 2). В кн.: Современный терроризм и борьба с ним: социально-гуманитарные измерения / *С. Афонин и др.* Под ред. *В. В. Ященко.* М.: МЦНМО, 2007; *Е. Ю. Лихачева*, *А. В. Зайкова*. Психологический анализ игровой имитации экстремальной ситуации. Сб. научных работ студентов и аспирантов ФГУ МГУ, 2007.

СМИ и психологические последствия терроризма

С. Н. Ениколопов, А. А. Мкртычян

Существующие психологические исследования в основном, направлены на изучение типологии терроризма, мотивов и строение личности террориста. И практически незатронутыми остаются вопросы, связанные с последствиями. Между тем, это не только физические жертвы. Очевидно, что основной целью терроризма являются более масштабные и имеющие долгосрочный характер социальные и психологические последствия. Именно они являются эффективным инструментом террористов для достижения наибольшего внимания общества к себе [*McCauley C.*, 2001; *McCormick H. C.*, 2003].

Прежде всего, к последствиям терроризма относится посттравматическое стрессовое расстройство (*Далее — ПТСР*). Оно возникает отсрочено и длится около шести месяцев [*Robin P.*]. Люди с ПТСР, могут испытывать постоянное чувство страха, ужаса и беспомощности. У них наблюдается бессонница и кошмары, в которых они возвращаются в психотравмирующую ситуацию и снова переживают ее. Постоянное напряжение приводит к физическим расстройствам: головным болям, гипертонии, язве. Начинаются проблемы не только со здоровьем, но и семьей, работой. В подобном состоянии отмечаются попытки суицида [*Terry L.*, *Bradley M.*; *Keinan G.*, *Sadeh A.*, 2002]. Необходимо отметить, что ПТСР возникает не только у непосредственных участников событий, но и у сторонних наблюдателей, в частности, у телезрителей.

Как последствие теракта, можно охарактеризовать и процесс групповой сплоченности, способный перерасти в патриотизм, стремление к взаимовыручке и т. д. [*Arndt J.*, *Goldenberg J. L.*, 2005]. Но последствиями групповой сплоченности могут стать и такие отрицательные явления как национализм, ксенофобия и нетерпимость. После очередного теракта у обывателя разрушаются представления о собственной безопасности, и усиливается мнение о степени уязвимости и беззащитности перед террористами. Для того, чтобы сохранить свое мировоззрение и уверенность в собственной защищенности человек стремится идентифи-

цировать себя с некой группой, в рядах которой он будет чувствовать себя в безопасности. Для этого необходимо «слепо» принять правила группы и следовать им. Подобная сплоченность, основанная на групповых принципах, схожем мировоззрении ее членов, представляется способом редуцировать свой страх и эффективно реагировать на угрозу. И любое нападение или угроза нападения извне, сплачивают группу. Но, непременным условием однородности является отсутствие противоречий и разногласий, в том числе и со стороны. В кризисные моменты, такие как теракты, любые альтернативные мнения начинают трактоваться носителями данного мировоззрения как угроза не только своим принципам, но и своему существованию. Следствием этого являются крайне негативные и агрессивные реакции [*Solomon S.*, *Greenberg J.*, *Pyszczynski T.*, 2000]. Таком образом, обратной стороной подобной сплоченности является эскалация враждебности и агрессивности к тем, кто не является членом группы, а значит, автоматически воспринимается как носитель угрозы для ее существования и нормального функционирования [*Goldenberg J. L.*, *Pyszczynski T.*, *Greenberg J.*, *Solomon S.*].

Еще одним опасным социально-психологическим последствием теракта является процесс легитимизации насилия. Демонстрация сцен насилия приводит к снижению чувствительности и привыканию к нему. Люди воспринимают насилие спокойно, без осуждения и, что самое опасное, допускают возможность его применения для достижения собственных целей. Трансляция насилия, его эффективности, приводит к тому, что оно начинает восприниматься как оправданное, справедливое и полезное средство.

С легитимизацией насилия связан процесс изменения в моральной сфере человека, принятие насилия как способа достижения своих целей. Эффективное, результативное применение способов самооправдания способствует стремлению снова и снова использовать насилие в своих целях, его закреплению в поведении. Группа американских психологов во главе с А. Бандурой сформулировали основные способы самооправдания, к которым прибегают террористы, сотрудники силовых ведомств и обыватели в процессе легитимизации насилия [*Bandura A.*, *Zimbardo P.*, *Osofsky M.*, 2005]:

1. *Моральное самооправдание*

   При совершении противоправных поступков или насильственных действий, санкционированных государством, человек начинает трактовать свое поведение как необходимое для нации, или совершаемое в защиту религии или идеологии группы, к которой он принадлежит.

2. *Утилитарное* (*экономическое и юридическое*) *самооправдание*

   Данный способ скорее относится к насильственным действиям, которые санкционированы государством. В частности, смертная казнь или диверсионные акции. В первом случае речь идет о, экономически невыгодном, пожизненном заключении смертников и их потенциальной опасности даже за стенами тюрем, во втором — о превентивных необходимых акциях, устраняющих потенциальную угрозу национальной безопасности.
3. *Сравнение своих действий с другими*, *более жестокими* — «*Выгодное сравнение*»

   При совершении насильственных действий, для самооправдания, человек прибегает к сравнению своих поступков с другими. Но, при этом, в качестве эталона для сравнения намеренно выбираются более жестокие поступки [*Bandura A.*, 1999].
4. *Смещение ответственности*

   Террорист или солдат начинают объяснять свои действия со ссылкой на каких-либо внешних авторитетов, отрицая собственную активность в процессе совершения насильственного действия. Человек характеризует себя как пассивного исполнителя, но не организатора, ссылаясь на закон, субординацию, приказ лидера группы и т. д. [*Bandura A.*, 2004].
5. *Диффузия ответственности*
   - разделение обязанностей между членами группы;
   - дробление процесса на множество мелких частей, где каждый отдельный этап видится исполнителю безвредным и обыденным;
   - групповое принятие решения, где анонимность и раздробленность способствует минимизации ответственности и самоосуждения отдельного члена группы.
6. *Дегуманизация жертвы и атрибуция вины*

   Дегуманизация жертвы происходит путем искаженной оценки человеческих качеств. О ней говорят не как о личности, живом человеке, а как о неодушевленном объекте насилия. Если процесс обезличивания не эффективен, то жертве начинают приписывать различные низменные, отрицательные качества.
7. *Искажение и пренебрежение последствиями*

   Агрессор старается не замечать последствий совершенных им действий, избегает их, игнорирует или искажает. Особенно эффективно данный способ работает в тех случаях, когда агрессор не имеет объективной возможности наблюдать страдания жертвы, когда последствия несут отсроченный характер.

Наличие в обществе симпатий или антипатий к террористам, принятие их идеологии и оправдание методов и способов — также можно отнести к психолого-социальным последствиям терроризма. Очевидно, что значительное большинство воспринимает террористов как преступников. Но существует и другая группа людей, которая в своих оценках не столь однозначна и радикальна. Данная референтная группа чрезвычайно важна для террористов, так как является базисом для формирования положительной, сопереживающей позиции. Она же — благоприятная среда для рекрутирования новых членов в террористическую организацию. Масштаб ее незначителен по сравнению с большинством. Но для террористов численность референтной группы не является приоритетом. Для них важен сам факт ее существования в обществе. Наиболее радикальным и опасным результатом положительного отношения к терроризму является желание человека стать частью какой-либо террористической группы или перенять методы борьбы и применять их в одиночку, оправдывая свое поведение, ссылаясь на террористов [*McCormick G. H.*, 2003].

Следует отметить, что современный терроризм имеет явную направленность на СМИ. В качестве одного из основных этапов планирования теракта выделяется активное участие прессы в освещении преступления. Это делает его более заметным и значимым [*McCormick G. H.*, 2003; *Bruno S.*, *Dominik R.*, 2006]. Последствия теракта распространяются на широкую аудиторию телезрителей, минуя географические и временные барьеры, увеличивая многократно количество жертв. Роль СМИ в формировании психологических последствий терроризма чрезвычайно велика. Она может быть как положительной, так и отрицательной. Непрофессиональное освещение способствует искажению информации, повышению степени страха и паники, легитимизации насилия [*Cohen R.*, 2005]. Но, естественно, речь не идет о том, чтобы запретить трансляцию в СМИ. Проблема заключается в нахождении ее оптимальной формы, которая будет способствовать минимизации негативных последствий, а не их развитию. Обмен информацией между правительственными структурами и населением (до теракта, в течение его и после) чрезвычайно важен. Людям необходимо подготовиться к долговременной ситуации угрозы, научиться эффективно реагировать на возникшую опасность. Немаловажной функцией СМИ является и препятствие возникновению в обществе идеализированных представлений о террористах, устранение слухов и мифов. На данный момент существуют рекомендации освещать теракт максимально оперативно и не искажать при этом факты. Речь не идет о подробном освещении, но о том, что не стоит пренебрегать или намеренно искажать последствия преступления. Дефицит информации в СМИ вынуждает население с недоверием относиться к ней и обращаться к другим источникам — слухам и мифам, которые лишь усугубляют негативные последствия теракта. А непосредственное интервьюирование террористов может приводить к их восхвалению и популяризации через подмену понятий и превратное истолкование ситуации и фактов [*Risk communication during a terrorist attack // US Department of Health and Human Services*, *September* 2005].

В настоящее время единственным способом контроля СМИ являются различного рода уставы этических требований к представителям СМИ. Речь идет о регламентировании лишь поведения журналистов, нежели материала, который они транслируют. Но очевидно, что последствия террористических актов можно редуцировать не только через запретительные меры, ограничивающие поведение журналиста или объем информации, но и с помощью моделирования характеристик самого предъявления, содержательной стороны и стиля комментариев, образа коммуникатора.

От того, как будет предъявляться информация о теракте, зависит и степень восприятия риска обывателем данного происшествия и субъективная оценка вероятности повторения подобных преступлений в будущем. Под субъективным восприятием риска понимается степень угрозы теракта для человека, то, что американские психологи формулируют как «личная угроза» в противовес «угрозе национальной». Характер риска, его субъективная значимость и степень во многом определяют дальнейшие поведенческие и эмоциональные реакции человека: страх, подозрительность, повышенная агрессивность по отношению к незнакомым людям, беспокойство, чувство беспомощности, вины, ограничительное поведение [*Huddy L.*, *Feldman S.*]. В связи с этим специалисты в области коммуникаций с населением в кризисных ситуациях (*Risk communication*, *далее — RC*) предположили возможность контролировать или прогнозировать степень риска, а значит — и дальнейшие реакции аудитории [*Fischhoff B.*, *Durodie W.*, *Wesseley S.*, *Cohen R.*, *Feldman S.*, *Jenkin C. M. и др.*]. Предлагается следующая рекомендация к составителям информационных программ: не стоит злоупотреблять фактами, «сухими» цифрами в процессе трансляции, так как ошибочным будет рассчитывать на хладнокровие аудитории в подобной ситуации [*Fischhoff B.*, 2002]. Соответственно, и рекомендации относительно характера трансляции:

- не углубляться в рассуждения по поводу перспектив происшествия;
- первостепенная задача любой трансляции не сенсация, а стремление облегчить участь заложников и жертв;
- при дефиците и неопределенности информации настаивать на том, что это следствие не некомпетентности, а неповторимости и неизвестности

характера преступления, что приводит к отсутствию шаблонов, как в ответных мерах, так и в рекомендациях населению.
- следует избегать частой смены экспертов из одной области. Это создает у аудитории впечатление их некомпетентности и несерьезности (возможно наличие экспертов из разных областей, но в рамках одной области их менять не стоит).

Предлагается ряд вопросов, на которые обыватель обязательно должен получить ответы в течение короткого репортажа:

- что случилось?;
- в безопасности ли я и мои родные?;
- какие меры предпринимаются для моей защиты и кем?;
- срок устранения последствий?

Barnett и *Breawell* предполагают, что прошлые сообщения о чрезвычайных ситуациях вполне могут влиять на восприятие подобной информации в будущем, а значит, и на ответные реакции населения. Серия прошлых оповещений об опасности может способствовать тому, что последующая информация будет восприниматься более уравновешенно, что положительно скажется на эффективности ответных действий. Подобный механизм авторы объясняют шаблонами, которые формируются на основе прошлых сообщений в СМИ. Речь идет о шаблонах поведения в схожих ситуациях. Для понимания и прогнозирования реакции населения на будущие происшествия необходимо прояснить какой именно шаблон был сформирован в результате предыдущих сообщений [*Barnett J.*, *Breakwell G. M.*, 1995].

Субъективное восприятие риска у человека основывается больше на интуиции и эмоциях, нежели на фактах и хладнокровном анализе [*Slovic P.*, 1992]. Совсем недостаточно фактически обеспечить безопасность страны и населения, важно еще и убедить людей в этой безопасности. Специалисты в области RC предлагают некоторые условия потенциально «успешного» (в плане минимизации негативных последствий) освещения теракта на ТВ:

- продуманный образ коммуникатора: тип, узнаваемость, авторитетность;
- признание серьезности события и его последствий;
- четкое представление целевой аудитории;
- эмоциональность сообщения: сострадание (в разумных рамках).
- апеллирование к госструктурам, к их компетентности;
- избегание негативных прогнозов;
- информировать о текущих экстренных мероприятиях;
- ссылки на экспертов из разных научных областей;

- если отсутствует возможность предъявления объективной и проверенной информации, то не стоит додумывать ее. Необходимо аргументировано объяснить дефицит информации;
- информированность о возможных слухах и мифах.

Таким образом, можно выделить как минимум две важные функции СМИ в процессе сообщения населению об угрозах или фактах терроризма. Первая — информирование о предполагаемом риске. В данном случае основная задача — инструктаж населения, повышении степени стрессоустоичивости. Вторая — работа с населением после теракта, контроль эмоционального состояния посредством грамотно представленной информации. Для эффективной борьбы с терроризмом недостаточно обладать знаниями о типах терроризма, его целях и т. д. Необходимо рассматривать данный вид преступлений и с точки зрения его психологических последствий, их динамики и факторов.

Профайлинг как метод выявления потенциально опасных пассажиров в целях авиационной безопасности

О. В. Деснянская

Терроризм является одной из острейших проблем нашего времени, в частности, касающейся гражданской авиации (ГА). Угроза террористических актов на воздушном транспорте оказывает существенное воздействие на эффективность и деятельность гражданской авиации, ставит под угрозу жизнь пассажиров и экипажей воздушных судов. Тем не менее, несмотря на актуальность данной проблемы и существующий запрос на ее решение, как со стороны государства, так и со стороны общества сегодня налицо явное доминирование теоретического подхода к феномену терроризма и крайняя скромность в изложении базового фактологического материала.

Суть социального заказа психологической науке сегодня распадается на два основных направления: объяснить природу терроризма и предложить обществу (конкретным структурам — силовым, например) эффективные средства противостояния террористическому вызову.

Профайлинг является единственным на данный момент существующим методом борьбы с терроризмом на воздушном транспорте, совмещающим в себе, с одной стороны, теоретические познания в области психологии терроризма, а, с другой, — многолетний практический опыт противостояния терроризму.

Профайлинг — это метод выявления потенциально опасных пассажиров путем специального опроса в ходе предполетного обслуживания, который включает в себя проверку и исследование предъявленных документов в ходе активного диалога сотрудника авиационной безопасности и досматриваемого лица. Знание метода профайлинга и использование его в процессе обслуживания пассажиров совместно с использованием технических средств досмотра, позволяет повысить эффективность досмотра и уровень обеспечения мер авиационной безопасности.

В рамках работы были рассмотрены различные как отечественные, так и зарубежные подходы к феномену терроризма (Руби Ч., Сейджман М., Поуст Д., Бодрийяр Ж., Ениколопов С. Н., Вершинин М. В., Ольшанский Д. В., Решетников М. М., Юрьев А. И. и т. д.). Личность террориста рассмотрена как с точки зрения теорий человеческой агрессивности (теория Dollar — Miller), так и в рамках концепций, объясняющих психопатологические варианты развития личности. Отдельно нами был проведен анализ террористической деятельности на воздушном транспорте и существующих в разных странах направлений в профайлинге.

Целью исследования стало выявление тех особенностей вербального и невербального поведения пассажиров аэропорта, которыми руководствуется профайлер при принятии решения об отнесении их к группе риска.

Всего было обследовано 970 пассажиров. В исследовании принимали участие 39 профайлеров.

Эмпирическая программа исследования включала в себя использование методики выявления потенциально опасных пассажиров путем специального опроса в ходе предполетного обслуживания и разработанного нами анкетного опроса, позволяющего выявлять те поведенческие характеристики, на основании которых происходит выделение пассажира из пассажиропотока и отнесение его к группе риска.

В результате мы составили список тех параметров, которые являются критическими для отнесения пассажира к группе риска («демонстрируемая агрессия», «скрытая агрессия», «тревожность», «возбужденность», «отрешенность», «ореол смерти», «алкогольное опьянение»). В случае выявления данных параметров необходим более углубленный досмотр как самого пассажира, так и его вещей. Ценность и значимость данных параметров в том, что они, с одной стороны, тесно связаны с теоретически выведенными личными особенностями членов террористических организаций, а, с другой, отражают особенности реальной деятельности профайлеров. Таким образом, основываясь на этих данных, можно проводить обучение профайлеров, а также они могут служить критерием оценки деятельности профайлеров со стороны проверяющих структур.

Также к каждому из параметров мы составили список тех ключевых признаков в невербальном и вербальном поведении пассажира, которые позволили профайлерам выявить пассажира в пассажиропотоке и отнести его к категории потенциально опасных по тому или иному параметру. Причем мы не просто выделили эти признаки, но и определили их эффективность и частоту, с которой они встречаются. Эти данные также чрезвычайно полезны, так как позволяют проанализировать сам процесс деятельности профайлера.

Таким образом, в ходе своего исследования мы, с одной стороны, подробно исследовали психологию терроризма и выделили те моменты, которые могут быть значимы для выявления террористов. С другой сторо-

ны, мы исследовали реальную деятельность профайлеров и те признаки, которыми они руководствуются при выборе потенциально опасных лиц, что, несомненно, очень важно для практической стороны антитеррористической деятельности. Анализ показал, что профайлеры учитывают многие психологические особенности террористов, адаптируя их к специфике своей деятельности. Дальнейшая работа в этом направлении, на мой взгляд, должна все больше двигаться в сторону слияния теоретических знаний и практических навыков, поскольку именно профайлинг является той областью антитеррористической деятельности, которая позволяет наиболее четко реализовать данный принцип.

В заключение, хотелось бы остановиться еще на одном важном моменте внедрения профайлинга с точки зрения анализа общей концепции безопасности. Система профайлинга является хорошей прогностической базой для превентивных мер по предупреждению терроризма в гражданской авиации. В рамках данной концепции тщательно изучаются общие вопросы, связанные с современным терроризмом, с существующими экстремистскими организациями и основными тенденциями их деятельности, а также составляется описательная модель участника террористической угрозы. Такая информация является, можно сказать, бесценным материалом для создания модели террористической деятельности, опираясь на которую можно с достаточно высокой степенью вероятности прогнозировать осуществление новых террористических атак. Знать психологию терроризма — значит получить лишний шанс на свою собственную безопасность.

Литература

[1] Авиационная безопасность / Под общ. ред. Ю. М. Волынского-Басманова. М.: НОУ «АБИНТЕХ», 2005.
[2] *Антонян Ю. М.* Терроризм. М., 1998.
[3] *Введенская Т. Ю.*, *Дзигумская Е. А.* Международный терроризм: психологический аспект // Проблемы политической психологии. Материалы научной конференции. Киев, 1997.
[4] Психология и психопатология терроризма. Гуманитарные стратегии антитеррора // Сб. статей под ред. М. М. Решетникова. СПб., 2004.
[5] *Лукабо Р.*, *Фукуа Х. Э.*, *Кенджеми Д. П.*, *Ковальски К.* Терроризм — психологические и политические аспекты // Иностранная психология. 1998. № 10.
[6] *Ольшанский Д. В.* Психология терроризма. СПб.: Питер, 2002, 288 с.
[7] *Поуст Д.* Мы против них: групповая динамика политического терроризма // Социальные конфликты: экспертиза, прогнозирование, технологии разрешения. 1993. № 4.

[8] Психологи о терроризме («круглый стол») // Психологический журнал. 1995. № 4.
[9] *Сейджман М.* Сетевые структуры терроризма. Презентация в «Президент-отеле», 26 января 2005 г. // Источник: `http://www.inop.ru/files/Sageman PPP rus.ppt`.
[10] *Чаленко Н. В.* Адаптация методики выявления потенциально опасных пассажиров аэропорта. Дипломная работа, научный руководитель И. Ц. Грыженко. Новомосковск: НФ УРАО, кафедра психологии и педагогики, 2006.
[11] *Schneier B.* Beyond Fear: Thinking Sensibly about Security in an Uncertain World. Copernicus Books, 2003.
[12] *Schneier B.* Behavioral Assessment Profiling // Boston Globe. 24.11.2004.

Kultur und kulturspezifische Probleme in der globalen Informationsgesellschaft

A. W. Sokolowa

Die heutige Phase der Zivilisationsentwicklung wird zu Recht als Anfangsphase der Entstehung einer globalen Informationsgesellschaft bezeichnet. Die Mittel der Informatik, neue Informations- und Computertechnologien setzen sich immer mehr praktisch in allen Bereichen des Lebens von Hunderten Millionen Menschen durch, ändern ihre Arbeits- und Alltagsbedingungen, werden zu Merkmalen der neune gesellschaftlichen Informationskultur. Heute tritt das Problem der Wechselwirkung zwischen der Kultur und rasantem wissenschaftlich-technischem Fortschritt.

Die Frage nach dem Einfluss der Technik auf die Kultur hat in der Entstehungsphase der Informationsgesellschaft besonders an Aktualität gewonnen, da Rundfunk und Telefon, Fernseher und Tonbandgeräte, Drucker und Scanner, Taschenrechner und Computer, das World Wide Web und andere Informationsnetze im zunehmenden Maße einen komplizierten Einfluss nicht nur auf den Bereich der materiellen Produktion und das sozial-politische Leben der Gesellschaft ausüben, sondern auch auf ihr geistiges Leben.

D. Bell unterscheidet in der modernen Gesellschaft drei Bereiche: öffentliche Strukturen, politische Organisationen und kulturelle Orientierungen. Die Kultur selbst bezieht den existierenden sozialen Instituten und Gesetzen gegenüber eine feindliche Position, sie setzt sich gegen die Allmacht und Standardisierung der politischen und technisch-ökonomischen Tendenzen der gesellschaftlichen Entwicklung ein. José Ortega y Gasset, der die These von dem negativen Einfluss der Technik auf die Kultur vertritt, bemerkt, dass „die Technik für den Menschen einerseits im Prinzip eine grenzenlose Fähigkeit ist, anderseits verwüstet sie das Menschenleben, indem sie die Menschen zwingt, ausschließlich vom Glauben an die Technik zu leben, und deshalb ist unsere Zeit — wie niemals die technische — äußerst gedankenarm und leer“[1].

Die Technik ist ein materieller Träger der sozialen Erblichkeit. In die Geschichten der menschlichen Gesellschaft wird die Verbindung zwischen

[1] José Ortega y Gasset. Brevier. Moskau, 1997.

den Generationen durch die Technik realisiert. Mit Hilfe der Technik unterwirft sich der Mensch die Natur, schafft um sich herum ein künstliches Umfeld, nach Worten Ju. A. Zhdanows die zweite Form der objektiven Realität, die neuen kulturellen Werte, bildet die neuen kulturellen Ideale. Dadurch geht die Technik ins Fleisch und Blut der modernen Kultur, des Lebens, des Alltags, der Bräuche, der Gefühle und der Stimmungen des modernen Menschen über. Nicht zufällig schrieb G. Grant, dass die Technologie unsere Gedanken über die Welt und über uns selbst durchdringt. Das Aufkommen der Technologie veränderte unsere Vorstellungen darüber, was gut ist, was man unter Wahnsinn und die Vernunft verstehen soll, die Gerechtigkeit und die Ungerechtigkeit, die Rationalität und die Irrationalität, die Schönheit und die Hässlichkeit. Die Technik beeinflusst indirekt die Weise, auf die wir die Welt und sich selbst verstehen. Sie öffnet uns die Schönheit der technischen Erzeugnisse, schafft riesige Möglichkeiten für die Erweiterung der Wahrnehmung der Welt von Mikro-, Makro- bis zu Megawelt. Auf keine Weise steht die Technik im Gegensatz zur Kultur. Anderseits, ist sie ihr Element, das Ergebnis der kulturellen Entwicklung, das vielseitig das kulturelle Potential der Gesellschaft beeinflusst[1].

In seinem Buch „Die Qualität des Menschen“ schreibt der Gründer des Römischen Klubs Aurelio Piccei, dass das vom Menschen geschaffene technische Umfeld den Menschen körperlich schwächte, seine biologische Aktivität abstumpfte. Je zivilisierter der Mensch wurde, desto schlechter konnte er auf die Schwierigkeiten der grausamen Umwelt reagieren und desto notwendiger wurden die Medikamente. In der letzten Zeit ist das Gleichgewicht zwischen dem wissenschaftlich-technischen und kulturellen Fortschritt, zwischen dem Fortschritt und den biophysikalischen Fähigkeiten des Menschen ernsthaft gestört. Das heutige Problem der Menschengattung besteht darin, dass der Mensch sich kulturell als unfähig erwies, mit den Veränderungen Schritt zu halten, die er selbst an seiner Umwelt vorgenommen hat, und sich an diese Veränderungen vollständig anzupassen. Niemand von uns hat sich weder psychologisch noch funktional der veränderten Welt und der veränderten Stellung des Menschen in dieser Welt angepasst. Der Kern des Problems liegt nach Aurelio Piccei in der Diskrepanz zwischen der vom Menschen geschaffenen Wirklichkeit und der Weise, auf die er diese Wirklichkeit wahrnimmt und in seinem Verhalten berücksichtigt[2]. Der Ausweg aus der entstandenen Situation sieht A. Picchei in der kulturellen

[1] *Negodaev I. A.* Na putach k informazionnomu obschestvu (Auf dem Weg zur globalen Informationsgesellschaft). Rostow-na-Donu, 1999.

[2] *Peccei Aurelio.* Die Qualität des Menschen. Moskau, 1985.

Evolution als wichtigstem Zweck und der Grundlage der menschlichen Entwicklung, in der Veränderung der menschlichen Qualitäten im Laufe der Revolution im Menschen. Wenn wir die technische Revolution zügeln und der Menschheit den Weg zu einer würdigen Zukunft zeigen wollen, so A. Piccei, müssen wir uns zuerst über die Veränderung im Menschen selbst, über die Revolution im Menschen selbst Gedanken machen[1].

Die Kultur ist ein kompliziertes soziales Phänomen, das eine Reihe gesellschaftlicher Phänomene beinhaltet. Es ist natürlich, dass auf diese Phänomene das jeweilige kulturelle Klima einen großen Einfluss hat. Nicht weniger bedeutsam ist die Einwirkung der Wissenschaft auf diese Kultur. So hat die Entstehung der papierlosen Informationstechnologien große Bedeutung für diese Kultur gewonnen. Heute kommt eine neue Generation, die Computergeneration, auf. Junge Leute, die am Computer arbeiten können, haben die Möglichkeit, am Tag 8 Bücher im Umfang von jeweils 300 Seiten zu lesen, dank der wahrnehmungsfreundlichen audio- und visuellen Darstellung, Lesegeschwindigkeit, Auswahl und Präsentation der Information. In erster Linie findet die papierlose Technologie Anwendung in der Bearbeitung bei schnellem Erhalten von Informationen, deren Inhalt sich schnell ändert und veraltet, was langfristige Aufbewahrung von Informationen einfach überflüssig macht. Viele vertreten die Meinung, dass die Tageszeitung bald von einer Rund-um-die-Uhr-Nachrichtensendung im Fernsehen abgelöst werden soll. Die elektronischen Verlage erleben einen echten Boom. Die Archivmaterialien, Raritätsbücher, die über das Internet, Satellitenkanäle oder Telefax auf die CDs übertragen werden, werden allen zugänglich.

Der Einfluss der modernen Informationstechnologie auf die Kunst erfolgt in zwei Richtungen. Einerseits setzen Maler und Bildhauer, Künstler und Komponisten diese Technologie in ihrer schöpferischen Arbeit ein. Anderseits machen die modernen Informationsmittel die hohe Kultur allgemein zugänglich.

Die meisten Versuche, die Rechentechnik in der Kunst einzusetzen, werden im Bereich der Malerei und zeichnerischen Kunst unternommen. Man kann zwei Ansätze bei der Verwendung des Computers in diesen Bereichen unterscheiden. Für einen Fall spielt der Computer einfach die Rolle eines Werkzeugs, in anderem gibt der Künstler der Maschine ein Programm vor, und der Computer erstellt das Kunstwerk selbst. Manchmal ist das Ergebnis erfolgreich, manchmal nicht. Die Informationstechnik bringt dem Menschen die Kunst nahe und spielt dabei eine sehr große Rolle, da sie die hohe Kultur allgemein zugänglich macht. Die Informationstechnik

[1] *Peccei Aurelio*. Die Qualität des Menschen. Moskau, 1985.

hat die einzigartigen Errungenschaften der Weltkultur den Massen nahe gebracht. Um die Sixtinische Madonna zu sehen, muss man heute nicht mehr die Dresdener Gemäldegalerie besuchen, die Gemälden von Rubens oder Kramskoj, die Opern des Bolschoi-Theaters kann man zu Hause vor dem Fernseher genießen. Louvre oder Eremitage besuchen, eine Theater- oder Ballettaufführung sehen, Beethovens Sinfonien anhören kann man im Videorecorder oder über einen Multimedia-Computer im Internet.

Neue Massenmedien

Von der Kultur der Schrift wendet sich die Menschheit heute der Bildschirm-Kultur zu. Sie entsteht aus der Synthese des Computers mit der Videotechnik. Die bedeutenden Veränderungen vollziehen sich im Bereich der Massenmedien. Der Inhalt wird in digitale Form umgesetzt, in dieser Weise funktionieren das Druckwort und das bewegte Bild nebeneinander, entgegen allen Prognosen darüber, dass Kino, Rundfunk und Fernsehen die Zeitungen und Zeitschriften ablösen werden. Die Massenmedien sind so vielfältig geworden, dass es mit der Zeit schwierig wird, zu verstehen, um welches Medium es sich jeweils handelt: Rundfunk im Internet, Enzyklopädie auf CD oder im World Wide Web, Post, die man über ein Pocket PC oder ein Mobiltelefon empfangen kann.

Die Übertragung der Funktionen von den einen Massenmedien auf die anderen hat die Rolle des Publikums grundsätzlich verändert. Aus der Masse, die früher die ihr angebotenen Inhalte geduldig konsumierte, heben sich nun konkrete Gruppen hervor, mit ganz präzisen Informationsbedürfnissen und Gewohnheiten. Die neuen Medien gewähren dem Publikum die Möglichkeit, den Inhalt selbst auszuwählen, so wird das Publikum nun zu Redakteuren, und manchmal zu Schöpfern der neuen Produkte. Heute kann praktisch jeder „Zuschauer“ seine Nachrichten veröffentlichen, seine Meinung über die neuen Informationskanäle äußern, was Aktivität und Interesse steigert.

Außerdem hat die technische Konvergenz nicht nur zu Veränderungen im Bereich der Massenmedien geführt, sondern auch zu den Veränderungen in der Einstellung der Politiker und Staatsorgane zu den sich vollziehenden Wandlungen. So hat sich der Wortschatz um Wörter wie „elektronische Regierung“, „Digitaldemokratie“ und andere bereichert. Die staatlichen Organe benutzen Informationstechnologien zur Bildung des demokratischen, informationsoffenen und transparenten Staates sowie zur Erhöhung der Effektivität der Tätigkeit staatlicher Organe durch große Ablagen der staatlichen Daten, wie, zum Beispiel, die Statistik oder Gesetzessammlung.

Kultur Vielfältigkeit in der globalen Informationsgesellschaft

Jedes Volk schafft und pflegt seine eigene Kultur. Die Kultur eines Volkes zeigt sich in verschiedenen Bereichen: in Bräuchen, in Werteorientierungen, in seiner Sprache und Schrift, in Kunst und Dichtung, im Gerichtswesen, in der Religion, usw. Die Kultur der Pflege nationaler Besonderheiten wird reicher, wenn sie mit vielen anderen Völkern der Welt in Wechselwirkung steht.

Heute ist unsere Welt global. Dies bedeutet, dass in politischer, ökonomischer, rechtlicher u. a. Hinsicht Systeme aller Länder der Welt einander angeglichen werden, und die gegenseitige Abhängigkeit der Länder die bisher ungeahnten Ausmaße erreicht. Bisher waren Völker und Kulturen niemals so stark voneinander abhängig. Probleme, die an einem Ort der Welt entstehen, bekommt die restliche Welt sofort zu spüren. Der Globalisierungs- und Homogenisierungsprozess führt zur Bildung der einheitlichen Weltgesellschaft, in der sich einheitliche Normen, Institute und kulturellen Werte bilden. Die Welt erscheint dabei als zusammenhängender Ort. Deshalb wacht das nationale Bewusstsein heute weltweit auf. Es zeugt von der Verschmelzung der Nationen und davon, dass die Menschen ihre nationale Identität nicht verlieren wollen. Gleichzeitig kennen wir Beispiele erfolgreicher mehrkultureller Gesellschaften, ob Nation, Bündnis, Föderation oder Union eng zusammenhängender Staaten, wo der Unterschied zwischen den Kulturen (sei es das Essen, die Religion, die Feiertage, die Sprache oder politische und ideologische Überzeugungen) die Stabilität und den Wohlstand nicht bedrohen.

Wie die Geschichte zeigt, ist eine erfolgreiche Beseitigung kultureller Widersprüche und der Aufbau eines Staates, der ein Zuhause für viele Menschen mit verschiedenen kulturellen Traditionen, Konfessionen, ideologischen Weltanschauungen wäre, sehr wohl möglich, obwohl die Konstruktion einer bestimmten sozialen Basis, der Annahme der Gesetze und der Bildung der bestimmten Institute bedarf. Beispiele dafür sind die Europäische Union, die USA, die Russische Föderation, Indien, Südafrika. Niemand sagt, dass die Situation in diesen Ländern ideal ist, aber das System funktioniert. Das bedeutet, dass Toleranz und Verständnis für fremde Kulturen den Menschen helfen, Konflikte zu verhindern und Harmonie zu erreichen.

Selbstverständlich beeinflussen die Informationstechnologien die Lebensweise, Religion, Sprache und andere Komponenten der Kultur. Die Informationstechnologien ändern die moderne Welt, ermöglichen den Menschen aus den verschiedenen Ecken der Welt mehr über die Kulturen

anderer Länder zu lernen. So sehen sich die Russen lateinamerikanische Seifenopern an, in den afrikanischen Ländern kann man CNN oder BBC empfangen. Und im Internet findet man Informationen über alle Länder und ihre kulturelle Traditionen.

Sprachliche Probleme

Ein bedeutendes Hindernis bei der Herausbildung der globalen Informationsgesellschaft sind sprachliche Barrieren. Die moderne Kultur der Informationsgesellschaft geht von einem hohen Niveau ihrer sprachwissenschaftlichen Kultur aus. Vor allem muss man eine immer größere Verbreitung der englischen Sprache in der Welt hervorheben. Die englische Sprache ist heute nicht nur eine am meisten verbreitete Sprache der internationalen Kommunikation, sondern wird auch als Basissprache der globalen Informationsgesellschaft bezeichnet. Denn 90 % des wissenschaftlichen Gedankenguts und mehr als 80 % der elektronischen Datenbanken liegen heute auf Englisch vor. Ob es jemandem gefällt oder nicht, wird sich jeder Fachmann ohne gute Englischkenntnisse in der Informationsgesellschaft nicht wohl fühlen, ein Wissenschaftler oder eine gesellschaftspolitische Persönlichkeit werden ohne Englischkenntnisse nicht effektiv arbeiten können.

Nach Angaben der UNO, beherrschen heute ca. 500 Mio. Menschen in der Welt (8,5 % der Bevölkerung unseres Planeten) die englische Sprache fließend, noch 1200 Mio. (20 % der Erdbevölkerungen) lernen bzw. können Englisch als erste Fremdsprache. In den nächsten Jahrzehnten, dank Globalisierungs- und Informatisierungsprozessen in der Gesellschaft, bleibt die Tendenz zur weiteren Verbreitung der englischen Sprache nicht nur bestehen, sondern wird aller Wahrscheinlichkeit nach anwachsen. Schon heute fällt auf, dass der große Teil der Informationen im Internet auf Englisch vorliegen, doch auch in den anderen Sprachen sind im World Wide Web wichtige und durchaus interessante Informationen vorhanden. Daher wird die Möglichkeit zwischensprachlicher Kommunikation eine Frage von großer Wichtigkeit. Damit das Internet zu einem echten internationalen Kommunikationsmedium wird, muss ein Instrumentarium entwickelt werden, der den Benutzern nicht nur die Verständnis von Informationen ermöglicht, sondern auch die Möglichkeit gibt, Informationen in einer Vielzahl von Sprachen zu präsentieren. In dieser Richtung werden heute intensive Forschungen geführt, die hoffen lassen, dass sich die bestehende Situation in den nächsten Jahren ändern wird. So ermöglicht ein Projekt der EU, OTELO, die Dienstleistungen der Übersetzer mit maschinellen Übersetzungsprogrammen zu kombinieren. Den Partnern aus Frankreich, Italien und Deutschland gehört

das Projekt des neues Informationssuchsystems MULINEX (Multilinguale Indexierungs-, Navigations- und Editier-Extensionen für das WWW)[1], das auf dem Internet basiert, und einen selektiven Zugriff auf die Information, Ansicht von Informationen und Navigation im vielsprachigen Umfeld ermöglicht[2].

Die intensive Nutzung globaler Netze macht jedoch vielen Sorgen, dass die Gefahr, die nationale und kulturelle Eigenständigkeit und vor allem sprachliche Eigenständigkeit zu verlieren, dabei zunehmen wird. Konkretes Individuum, Gesellschaft, Ethnos identifizieren sich vor allem mit der Sprache als Grundpfeiler der nationalen Kultur. Die Sprache ist nicht nur ein Mittel zur Informationsübertragung, d.h. sie ist nicht nur Kommunikationsmittel, in der Sprache spiegelt sich auch die Weltanschauung- bzw. Wahrnehmung, in der Sprache ist die gesamte Biografie eines Volkes enthalten, die Sprache wurde von den Vorfahren verwendet. Die Sprache ist untrennbares Merkmal eines Volkes: es gibt keine Nationalität ohne Sprache. Deshalb befürchten viele Menschen in letzter Zeit die Amerikanisierung des Informationsraums.

Amerikanisierung

In der modernen Welt ist die militärische, politische, wirtschaftliche und finanzielle Hegemonie Amerikas offensichtlich geworden. Aber die Überlegenheit der USA zeigt sich nicht nur in dem politischen, militärischen, ökonomischen oder finanziellen Bereich, die USA sind der Hauptdarsteller im Bereich der Informationstechnologien. Nach U.S. National Science Foundation ist der Anteil Amerikas an der Produktion der Hochtechnologien von 25 % im Laufe von 25 Jahren auf 42 % in 2003 gestiegen. Die Produktion der Hochtechnologien in einigen Ländern zum Beispiel in China und Südkorea ist viel schneller gewachsen, aber sie haben ihr Wachstum bei Null angefangen (1 % in jedem Land). Daher ist ihr Anteil an der globalen Produktion im Vergleich zu den USA sehr gering — 9 % (USA) und 4 % (China und Südkorea). Die USA sind am meisten unabhängig von den Systemen für Datenübertragung und von den Telefonnetze, aber sie haben dabei fast alle anderen Länder der Welt, einschließlich ganz entwickelte Länder, in ihre Abhängigkeit gestellt[3]. U.a. wie es bereits oben erwähnt

[1] `http://mulinex.dfki.de/index-d.html`.

[2] *Tschernov A. A.* Stanovlenije globalnogo informazionnogo obschestva: probleme i perpektivi (Die Herausbildung einer globalen Informationsgesellschaft: Fragestellungen und Perspektiven). Monographie. Moskau: Daschkov & Co, 2003.

[3] Nauka mira. Washington ProFile (Unanhängige Information und Analytik aus den USA). `http://www.washprofile.org/ru/node/5164`.

wurde, sind fast 70 % der Software, die heute in der Welt verkauft werden, in den USA hergestellt[1].

Nachdem die Amerikaner versucht hatten, in die Televisionsmärkte Europas einzudringen, haben die Länder Westeuropas in den 80er angefangen, die Schutzmechanismen gegen die äußere Informationsaggression zu entwickeln. In 1986 waren acht von zehn größten Monopolen in der westlicher Welt auf dem Gebiet Massenmedien amerikanisch, das neunte Monopol war australisch, aber an seinem Spitze stand ein Amerikaner R. Merdok. Und nur ein großes Unternehmen, das nichts Gemeinsames mit den USA hatte, war Firma „Bertelsmann“ aus der BRD[2].

Viele europäische Zeitungen schrieben über den „kulturellen Genozid“ und über die „amerikanische Fernsehinvasion in Europa“. Zugleich in Frankreich und dann auch in den anderen Ländern hat man angefangen, eine protektionistische Politik in Bezug auf das nationale Kino und TV auszuüben. Auf den verschiedenen westeuropäischen Foren wurden die Maßnahmen der Gegenwirkung der amerikanischen Fernsehinvasion besprochen. Verschiedene internationale europäische Projekte waren aufgefordert, der billigen amerikanischen Fernsehproduktion die europäische Produktion entgegenzusetzen, die preislich konkurrenzfähig ist und die viel qualitativer und traditioneller für die Kultur der alten Welt ist.

Allerdings wurde die Einheitlichkeit der europäischen Staaten, die ihren Fernsehmarkt vor dem amerikanischen Eingriff zu beschützen wollten, nach und nach verschwommen. Die Versuche Frankreichs „die europäische kulturelle Identität“ aufzubewahren, waren von den Ländern attackiert, die den Verdacht hatten, dass Frankreich seine „hoch intellektuellen“ Filme statt amerikanischen aufdrängen wollte. Die Debatten wurden geführt, als die Filme aus den USA, die in 1995 in Europa gezeigt wurden, schon auf 82 % belaufen haben. Das kommerzielle Denken Europas hat das geistige Denken besiegt, und dieses Verhältnis konnten die europäischen Länder wesentlich nicht ändern[3]. Der Hauptstrom der Fernsehmaterialien kommt heute aus den USA. Die USA verkaufen jährlich den Fernsehorganisationen

[1] *Penkov I. A.* Ob aktualnich problemach razvitija voenno-promischlennogo komplexa Rossji (Über aktuelle Entwicklungsprobleme des Militär-Industrie komplex Russlands). Analiticheskij Vestmik Soveta Federaziji RF. 2005. № 09 (261).

[2] *Michaltschenko I. A.* Informatzionnije vojni i konflikti ideologij v usloviach sovremennich geopolititcheskich izmenenij (Informationskriege und Ideologiekonflikten unter Bedienungen der moderne geopolitische Veränderungen). `http://mihalchenko1.narod.ru/html/disser.html`.

[3] *Michaltschenko I. A.* Informatzionnije vojni i konflikti ideologij v usloviach sovremennich geopolititcheskich izmenenij (Informationskriege und Ideologiekonflikten unter Bedienungen der moderne geopolitische Veränderungen). `http://mihalchenko1.narod.ru/html/disser.html`.

anderer Länder die Fernsehmaterialien für 100–200 Tausend Sendestunden.

Mit neuen technischen Mitteln für die Informations- und Unterhaltungsproduktion steigt die amerikanische Dominanz auf diesem Markt noch mehr. Insbesondere übertrifft heute der Vertrieb von Videospielen schon den Vertrieb von Hollywoodfilme[1]".

Die Computerethik

Die globale Informalisierung der Gesellschaft führt unausweichlich zur Herausbildung einer neuen gesellschaftlichen Kultur sowie zur weltweiten Verbreitung. Diese Kultur zeigt sich äußerst aggressiv gegenüber den traditionellen Kulturen der Gesellschaft. Die neue Kultur bringt mit sich nicht nur eine neue Sprache und neue Verhaltensstereotype, sondern auch neue moralische Werte. Sie bildet eine neue Weltanschauung des Menschen auf die Gesellschaft, die Ziele und den Sinn seines Lebens. Es ist zu erwarten, dass auch eine neue Ethik, die Ethik der globalen Informationsgesellschaft dabei gebildet wird.

Die Computerethik ist die Gesamtheit der moralischen Prinzipien und Normen, die die Beziehungen zwischen den Menschen regeln, die sich aufgrund ihrer Arbeit mit den Computern herausgebildet haben. Der Mensch programmiert den Computer, und der Computer „programmiert" in hohem Maße sein Denken. Diese neue Ethik wird in hohem Maße die Vorlieben, die Regeln, die moralischen Normen und die Beschränkungen bestimmen, nach denen sich Millionen von Menschen unseres Planeten richten werden.

Der Wechsel der moralischen Normen unter dem Einfluss der Informationstechnologien wird heutzutage von vielen Forschern anerkannt. Außerdem wurde versucht die bestimmten Verhaltensregeln bei der Arbeit mit dem Computer zu erarbeiten. So wurde zum Beispiel eine Anforderung formuliert: „Machen Sie mit Hilfe eines Computers das nicht, was Sie für amoralisch ohne ihn halten würden. Keine Handlung wird moralischer nur deswegen, weil für ihre Erledigung ein Computer verwendet wurde". Ein Mensch ohne Moral beginnt sich selbst als eine kluge Maschine wahrzunehmen, überträgt den technischen Umgang mit dem Computer auf die Beziehungen zwischen den Menschen, was zu den weit gehenden Folgen führt. Nicht von ungefähr hat R.Wyden in seiner Rede vor den Kongressmännern der USA erklärt, dass „einige der vollkommen würdigen jungen Menschen die ethischen und moralischen Folgen ihrer Handlungen nicht bewerten können. Ich bin

[1] Washington ProFile (Unanhängige Information und Analytik aus den USA). `http://www.washprofile.org/ru/node/5715`.

sicher, dass viele wenn nicht alle jungen Hacker in unserem Land nicht mal auf die Idee kommen, einer alten Frau auf der Straße mit Gewalt Geld wegzunehmen. Aber andererseits ist es äußerst wahrscheinlich, dass sie per Mausklick ihr alle Ersparnisse wegnehmen"[1].

Die Notwendigkeit die Computerethik zu schaffen, wurden in vielen Aspekten durch die Probleme verursacht, auf die die Menschheit in der ersten Etappe der Entwicklung der globalen Informationsgesellschaft gestoßen ist. Die Computerisierung der Gesellschaft hat zu dem ernsten Informationsmissbrauch, der Computerkriminalität wie Datenbeschädigung im Computer, dem Diebstahl mit Hilfe eines Computers, der Gefahr der Monopolisierung von Massenmedien, der Manipulation der öffentlichen Meinung und der Computerpiraterie geführt.

Viele Seiten des Lebens und der Tätigkeit der Menschen werden in der Informationsgesellschaft immer mehr „transparent" und verwundbar für die Einflusse von außen. Schon heute in den Computernetzen und elektronischen Datenbanken werden die verschiedenen Informationen über die Tätigkeit von Unternehmen, staatlichen und gesellschaftlichen Organisationen oder einzelner Personen gespeichert. Analyse und unbefugte Benutzung dieser Informationen schaffen die realen Möglichkeiten für die politische und industrielle Spionage, die Manipulation der öffentlichen Meinung und für die Gesamtkontrolle über die Person. Es entstehen die neuen Arten der Informationsverbrechen gegen die Persönlichkeit, die Gesellschaft, die einzelnen Organisationen.

In Zukunft je nach der Entwicklung der Informalisierung und Globalisierung der Gesellschaft werden diese Möglichkeiten breiter. Doch wird nicht nur die Tätigkeit der Menschen in der Informationsgesellschaft immer mehr „transparenter", sondern auch die Gesellschaft wird immer enger durch die modernen Informationskommunikationen verbunden[2]. Besonders fördern es solche Faktoren wie die wachsende Verbreitung der elektronischen Bezahlung von Waren und Dienstleistungen, die Entwicklung der E-Mail-Kommunikation und der Internettelephonie sowie des Mobilfunks. Alle diesen neuen Kommunikationsmittel sind vor dem unbefugten Zugang zu den Informationen nicht geschützt und deshalb können von den Konkurrenten, den politischen Gegnern und Krimineller leicht benutzt werden.

Unter diesen Bedingungen können viele Errungenschaften der Demokratie solche wie der Schutz des Privatlebens, das Postgeheimnis, Arztgeheimnis oder Berufsgeheimnis und andere zum bloßen Gerede werden, das

[1] *Baturin U. M.* Pravo i politika v komputernon kruge (Recht und Politik im Computerkreis). Moskau, 1987.

[2] *Kolin K. K.* Globalisazija i kultura (Globalisierung und Kultur) // Vestnik Bibliotetschnoj Assambleji Evraziji. 2004, № 1. S. 12–15.

nichts Gemeinsames mit der Realität haben wird. Es wird doch möglich die fremden Geheimnisse zu erfahren, ohne das Haus zu verlassen. Man muss nur entsprechende Fertigkeiten haben, um die Computer-, Informations- und Telekommunikationsnetze anwenden zu können.

Dieses Problem kann komplett mit technischen oder öffentlichen und rechtlichen Mitteln nicht gelöst werden. Hier müssen die moralischen Beschränkungen ins Spiel kommen. Wir vertrauen doch unseren Schriftwechsel den Postmitarbeitern und verstehen dabei, dass der wirkliche Garant des Postgeheimnisses nicht die Stabilität des Briefumschlages ist, sondern die ethischen Prinzipien, die, wie wir hoffen, die Postmitarbeiter einhalten. Deshalb ist es äußerst wichtig, der neuen Generation, die in der globalen Informationsgesellschaft leben und arbeiten wird, die gleichen Prinzipien beizubringen. Dabei müssen die uns aus der Kindheit gut bekannten moralischen Kategorien wie „gut“, „schlecht“, „erlaubt“, „verboten“, „beschämend“ einen neuen Informationsinhalt bekommen, der der neuen Realität der Informationsgesellschaft adäquat entsprechen würde. Nur dies kann zum Garant der Informationssicherheit des Menschen und der Gesellschaft in der Informationsepoche werden. Deshalb ist die Herausbildung der neuen Ethik der Informationsgesellschaft heute eine aktuelle und wichtige Aufgabe, um die Informationssicherheit zu gewähren[1].

[1] *Kolin K. K.* Informatzionnaja besopasnost kak gumanitarnaja problema (Informationssicherheit als geistwissenschaftliche Problem) // Otkritoje obrazovanije. 2006. № 1 (54). S. 86–93; *Kolin Kolin K. K.* Stanovlenije informatzionnogo obschestva v Rossiji i natzionalnaja besopasnost (Informationsgesellschaft Herausbildung in Russland und nationale Sicherheit). Im Buch „Iskustvennij intellekt: megdisziplinarnij podchod“ („Künstliche Intillegenz: interdisziplinäres Herangehen“. Hrsg. *Kolin Dubrovskij D. I.*, *Lektorskij V. A.* Moskau: IInteLL, 2006. S. 379–391.

МАТЕРИАЛЫ ТРЕТЬЕЙ МЕЖДУНАРОДНОЙ НАУЧНОЙ КОНФЕРЕНЦИИ ПО ПРОБЛЕМАМ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ

Московский государственный университет им. М. В. Ломоносова,
25—27 октября 2007 г.

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