Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Санкт-Петербургский государственный
инженерно-экономический университет»

# АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник научных трудов



**Санкт-Петербург**
**2012**

УДК 004.056
ББК 32.973
А43

*Утверждено редакционно-издательским советом СПбГИЭУ*



Одобрено к изданию научно-техническим советом СПбГИЭУ

А43 **Актуальные** проблемы информационной безопасности : сб. науч. тр. / редкол.: Е. В. Стельмашонок (отв. ред.) [и др.]. – СПб. : СПбГИЭУ, 2012. – 272 с.

ISBN 978-5-9978-0586-9

В сборнике рассмотрены вопросы развития и применения информационных технологий в сфере образования и бизнеса, проблемы информационной безопасности, методы и средства защиты информации, а также подходы к экономической оценке и управлению информационной безопасностью предприятия.

Издание предназначено для преподавателей, аспирантов, магистров, бакалавров и студентов, а также для всех, кто интересуется проблемами развития современных информационных технологий и обеспечения их безопасности.

УДК 004.056
ББК 32.973

ISBN 978-5-9978-0586-9

# ПРЕДИСЛОВИЕ

Переход к информационному обществу вызвал бурное развитие технологий обработки и передачи информации во всех сферах жизнедеятельности. При этом неизбежно возникают проблемы обеспечения надежности и безопасности информационных систем, особенно при использовании сетевых информационных технологий и виртуальных сред.

Основу сборника составили доклады, представленные на научно-практической конференции «Информационная безопасность и непрерывность бизнеса», прошедшей 8 ноября 2012 г. в СПбГИЭУ. В сборнике рассматриваются теоретические и практические аспекты обеспечения безопасности современных информационных технологий, методы и средства защиты информации, подходы к корпоративному управлению и экономической оценке информационной безопасности, обеспечение непрерывности бизнеса.

Сборник состоит из трех разделов.

Первый раздел посвящен применению информационных технологий и моделированию в сфере образования и бизнеса.

Во втором разделе анализируются угрозы информационной безопасности, рассматриваются особенности обеспечения безопасности различных информационных технологий, предлагаются методы и анализируются средства защиты информации.

Третий раздел посвящен вопросам корпоративного управления и оценке информационной безопасности предприятия. Рассматриваются имитационные модели, предназначенные для оценки рисков, подходы к оценке затрат и экономической эффективности информационной безопасности.

Статьи сборника могут представлять интерес для преподавателей, аспирантов, магистров, бакалавров и студентов, а также для всех, кто интересуется проблемами развития современных информационных технологий и обеспечения их безопасности.

Ответственный редактор
*Е. В. Стельмашонок*

## *Раздел 1*

# ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ И БИЗНЕСЕ

УДК 378

**Т. В. Дмитриева, М. О. Сайманова**

Санкт-Петербургский государственный инженерно-экономический университет

## РОЛЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ В ПОВЫШЕНИИ КОНКУРЕНТОСПОСОБНОСТИ ВУЗА

Повышение конкурентоспособности – одна из основных задач, стоящих перед крупным вузом, успех решения которой лежит в рациональном управлении портфелем программ и специальностей, обеспечении эффективного использования преподавательских кадров и материальных ресурсов, построении внутривузовской системы контроля качества, формировании приоритетов в деятельности вуза, планировании и мониторинге достижений стратегических целей и напрямую зависит от тех инструментов и возможностей, которые используются сотрудниками вуза. Очевидно, что без использования информационных систем в современных условиях выполнение вышеперечисленных задач не представляется возможным. Специфика информационных систем для образовательных учреждений в целом и высших профессиональных образовательных учреждений в частности заключается в том, что помимо хранилищ данных и построенных на их основе системы поддержки принятия решений и аналитических приложений, блоков стратегического планирования и управления система должна помогать в решении целого ряда проблем, связанных с повышением качества обучения и контроля знаний.

Таким образом, внедрение информационных систем в вузе должно способствовать:

- повышению качества обучения и контроля знаний;
- получению более рациональных вариантов решения научных и управленческих задач;
- освобождению работников от рутинной работы за счет ее автоматизации;
- обеспечению достоверности информации;
- замене бумажных носителей данных информационными потоками, что приводит к более рациональной организации переработки информации и снижению объемов бумажной документации;
- совершенствованию структуры потоков информации, ее анализа и системы документооборота;
- уменьшению затрат на подготовку выпускников вуза при повышении качества образования;
- предоставлению потребителям (студентам и работодателям) уникальных услуг;
- отысканию новых рыночных ниш.

Информационные технологии на сегодняшний день становятся одним из основных приоритетов в планировании развития высшего образования. Включенность информационных технологий в учебный процесс оказывается для поступающих тем привлекательным моментом, на основании которого они выбирают, в какой институт пойти. Кроме того, в высшем образовании важны не только для успешной конкуренции различных вузов на рынке высшего образования. Без использования информационных технологий сегодня становится невозможным эффективно управлять образовательным процессом.

В высшем образовании наиболее приоритетными становятся направления использования таких информационных технологий, как:

- дистанционное образование;
- сетевые технологии;
- управление безопасностью;

• повсеместное использование компьютеров/универсальный доступ;

• стратегии преподавания и обучения;

• подготовка персонала для информационных технологий и управление человеческими ресурсами;

• стратегии финансирования информационных технологий;

• онлайновые услуги для студентов;

• расширенные способы связи;

• административные системы.

В целом многие аналитики выделяют следующие основные направления, в рамках которых применение информационных систем и технологий в высшем образовании играет центральную роль.

1. Учебный процесс. Это главная область использования информационных систем и технологий. В рамках ее ключевыми проблемами являются обеспечение сетевого неограниченного доступа к учебным материалам, электронное копирование и рассылка документов, доступ к базам данных, электронные публикации, цифровые библиотеки, интерактивное взаимодействие через скоростные локальные сети, передача голосовой и визуальной информации и многие другие.

2. Научные исследования. Коммуникация с коллегами и исследователями по всему миру: электронная почта, интернет-конференции, форумы, свободный доступ к научной информации – вот лишь небольшое количество технологических решений, которые позволяют значительно повысить уровень исследовательской работы в университете. Распространение коммуникационных технологий ведет к тому, что сегодня вполне реально существование научных сообществ, включающих ученых из многих стран, объединенные усилия которых дают качественно новые результаты.

3. Административный процесс. Сегодня управление высшим учебных заведением сложно представить без ин-

формационных систем и технологий. Начиная с простой компьютеризации процесса поступления (обработка анкет абитуриентов, онлайновая регистрация и др.) и заканчивая обеспечением оперативного обмена информацией между административными работниками.

4. Электронная коммерция. К этому направлению можно отнести электронную оплату за обучение, рекламу и продажу производимых в вузах товаров и услуг через Интернет и др.

Проблема обеспечения комплексной информационной поддержки развития управления учебным процессом по-прежнему является одной из актуальных задач информатизации вуза. Ее значение, требования, предъявляемые к решающим эту задачу средствам, еще более усиливаются в связи с созданием в университетах системы управления качеством. Разработка современной автоматизированной информационно-аналитической системы управления большим университетом является исключительно сложной задачей, требует привлечения больших материальных и интеллектуальных ресурсов, применения самых современных информационных технологий.

**Литература**

1. *Третьякова И. В.* Конкурентоспособность современного образования // Образование в информационную эпоху: Сб. науч. ст. – Ярославль, 2001. – С. 83.

2. *Москвичев Ю. А., Разумов С. В.* Повышение эффективности деятельности вуза – комплексный подход // Образование в информационную эпоху. – Ярославль, 2001. – С. 59.

3. Новые педагогические и информационные технологии в системе образования: Учеб. пособие для студ. пед. вузов и системы повыш. квалиф. пед. кадров / Е. С. Полат и др.; Под ред. Е. С. Полат. – М.: Изд. центр «Академия», 2001. – 272 с.

УДК 378

**М. М. Мгебришвили**
Санкт-Петербургский государственный
инженерно-экономический университет

# ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ИННОВАЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ РАЗРАБОТКАХ

В настоящее время все большее внимание в сфере образования уделяется активным методам обучения (АМО), которые позволяют по-новому взглянуть на процесс обучения, сделать его интересным, живым, активным, приносящим удовольствие как преподавателю, так и студентам.

Методы активного обучения характеризуются высокой степенью включенности обучающихся в учебный процесс, активизируют их познавательную и творческую деятельность при решении поставленных задач. Отличительными особенностями активных методов обучения являются:

- целенаправленная активизация мышления, когда учащийся вынужден быть активным независимо от его желания;
- вовлечение учащихся в учебный процесс в течение всего занятия, так как их активность должна быть устойчивой и длительной;
- самостоятельная творческая выработка решений, повышенная степень мотивации и эмоциональности обучаемых;
- постоянное взаимодействие субъектов учебной деятельности (обучаемых и преподавателей) посредством прямых и обратных связей, свободный обмен мнениями о путях разрешения той или иной проблемы.

Одним из прогрессивных и действенных методов обучения, который можно и нужно применять в вузах, являются деловые игры (ДИ) и тренинги.

На Западе ДИ уже давно стали непременным элементом университетских учебных программ в сфере экономики и управления. Однако мало кому известно, что родились они в нашей стране. В 1930 г. в Ленинградском инженерно-экономическом институте была организована «группа пуска новостроек». В результате исследований, проведенных этой группой, было установлено, что одной из важнейших причин неудач и задержек в запусках крупных заводов являлась нехватка опыта у руководящих кадров. Мария Мироновна Бирштейн предложила обучать руководителей на примере условных ситуаций, моделирующих реальные ситуации еще до пуска объекта. Первая такая игра была успешно проведена в июне 1932 г. Впоследствии автор первой деловой игры, М. М. Бирштейн, писала об их значении: «Аналогично тому, как проекты технических новшеств обязательно проходят испытания в лабораторных условиях до их запуска в производство, так и проекты новшеств организационного характера в социально-экономической сфере могут и должны до их внедрения испытываться методом ДИ на качество и прочность, на пригодность их в данных конкретных условиях». Здесь подчеркнуто значение ДИ не только для процесса обучения, но и для организационно-исследовательских целей – например, испытания новых методов управления и организации производства.

Первая компьютерная деловая игра (КДИ) была создана в США в 1956 г. и моделировала деятельность фирм-производителей и их конкуренцию на рынке готовой продукции. В нашей стране также предпринимались попытки создания такого рода программных продуктов. Сегодня стало общепринятым делить КДИ на два типа – коллективные и индивидуальные.

Прекрасной возможностью получить знания по основам экономики и управления, а с применением информационных технологий и усилить эти знания и практические навыки, является применение компьютерных деловых игр (КДИ) и тренингов в учебном процессе СПбГИЭУ.

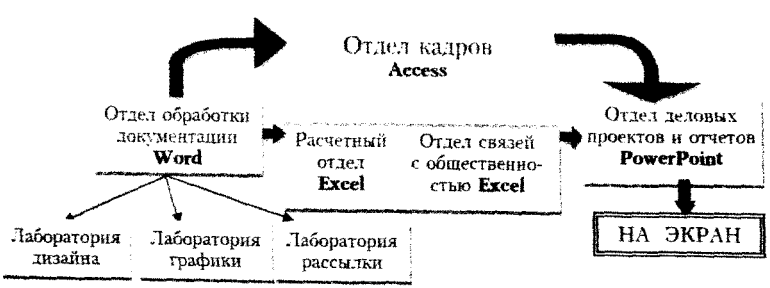
Данная форма обучения позволяет применять полученные теоретические знания в практической деятельности, связать «технологический» аспект управленческой подготовки с психологическим аспектом.

Тренинги в области информационных технологий (ИТ) также могут быть использованы в учебном процессе для:

- обучения технике общения;
- обучения технике переговоров;
- создания рабочей команды;
- повышения эффективности деятельности руководителя;
- развития коммуникативных навыков;
- позитивного настроя для дальнейшей деятельности и т. д.

Тренинги могут применяться по различным ИТ, таким как Информатика, Компьютерная графика, ИТ в экономике и др., для эффективного закрепления знаний, формирования умений, навыков и личностных качеств, которые не могут формироваться никакими другими методами обучения.

Хочется обратить особое внимание на компьютерную деловую игру (рисунок) по предмету «Информационные технологии в экономике», в основе которой лежит прогрессивная технология обучения, основанная на активном диалоге «человек-компьютер».




Функциональная структура деловой игры «Виртуальное предприятие»

В виртуальной модели данной деловой игры можно использовать материал всего блока учебной программы или ее части по выбору преподавателя. Игра позволяет, проигрывая возможные варианты поведения, принятия решений, разрешения конфликтов, формировать и развивать управленческие умения и навыки в условиях, максимально приближенных к реальной практической деятельности.

Деловая игра является коллективным мероприятием, где взаимодействие игроков, принимающих решения, моделирует конкретную экономическую ситуацию, а эксперт, направляющий игру, анализирует и оценивает их действия. В коллективной компьютерной деловой игре предусматривается обмен ролями, появляется возможность изучить проблему с разных сторон. При этом процесс обучения идет очень эффективно – каждый участник наблюдает развитие проблемы в динамике, сам принимает решения (правильные и неправильные) и может быстро увидеть их результаты, обретая, таким образом, свой собственный опыт.

Эта форма обучения позволяет применять полученные теоретические знания в практической деятельности, связать «технологический» аспект управленческой подготовки с психологическим.

Деловая игра «Виртуальное предприятие» моделирует структуру фирмы, состоящей из пяти отделов и трех лабораторий в определенной ситуации делового общения. Ее можно отнести к разряду учебных социально-экономических игр, назначение которых заключается в приобретении ее участниками основных навыков совместной работы в различных отделах и лабораториях, использующих различные информационные технологии.

Сотрудники фирмы (участники игры) приходят на работу и приглашаются на совещание работников фирмы, где им подробно докладывается план работы на текущий день, разъясняются их задания и конечный результат их работы за день. Эта игра создана в качестве итоговой по дисциплине, но может выступать и формой проведения зачета. Ее можно использовать после изучения участниками

игры разделов информационных технологий, необходимых для выполнения заданий. Задания деловой игры можно менять, подстраивая их под пройденный материал и направляя на выявление полученных знаний. Команды общаются посредством локальной сети, пересылая созданные документы из отдела в отдел. В результате проделанной работы «работники» всех отделов собираются на отчетное собрание, где представляется презентация с использованием мультимедийной техники и вывода презентации на экран аудитории. Производится обсуждение деятельности всех «лабораторий» и «отделов» виртуального предприятия, использующих в своей работе различные информационные технологии, а работники предприятия получают поощрительные зачетные баллы.

За обслуживанием сети следит преподаватель, выполняющий роль администратора сети.

Мотивация участников игры складывается из набранных баллов, а также из штрафов и поощрений, присуждаемых участникам «отделов» и «лабораторий», во время игры.

Общая цель: произвести всю заданную работу качественно и в срок.

Успешность проведения деловой игры зависит от собранности и дисциплины всех участников игры. Деловая игра «Виртуальное предприятие» построена как обучающая система открытого типа, функциональная структура которой гибко модифицируется в соответствии с требованиями пользователя. Структурно в ней выделяются относительно самостоятельные элементы трех уровней: подсистемы, модули и виды расчетов. Каждый из элементов может использоваться в едином цикле расчетов как часть деловой игры или как самостоятельная лабораторная работа учащегося.

Таким образом, применяя современные активные методы обучения в учебном процессе, можно еще более активизировать мышление учащихся, направляя его на интерактивность, мотивацию и эмоциональное восприятие

учебного процесса. АМО в области ИТ позволяют активизировать и развивать познавательную и творческую деятельность учащихся, повышать результативность учебного процесса, формировать и оценивать профессиональные компетенции, особенно в части организации и выполнения коллективной работы.

**Литература**

1. *Жуков Р. Ф.* Основные мероприятия по развитию активных методов обучения в академии // Проблемы повышения качества и эффективности подготовки специалистов: Учеб-метод. конф. 26–28 января 2000 г.: Тез. докл. / Отв. ред. П. Д. Шимко. – СПб.: СПбГИЭА, 2000. – С. 148–149.

2. *Мгебришвили М. М.* Информационные технологии в экономике: Методические указания по выполнению и проведению деловой игры «Виртуальное предприятие» в среде Microsoft Office 2007 для студентов всех форм обучения, для всех специальностей. – СПб.: СПбГИЭУ, 2011 г.

3. *Жуков Р. Ф.* Как научиться учиться: Практикум по использованию активного социологического тестированного анализа и контроля для студентов младших курсов обучения в вузе (Начинающий студент). – СПб.: СПбГИЭА, 1994.– 62 с.

4. *Сапунова В. Д.* Компьютер в экономическом образовании. – М.: Изд. дом «Новый век», 1999. – 232 с.

УДК 338.24

**Д. Ю. Федоров**

Санкт-Петербургский государственный
инженерно-экономический университет

## ОБЛИК АВТОМАТИЗИРОВАННОЙ СРЕДЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ОБЕСПЕЧЕНИЮ НЕПРЕРЫВНОСТИ И УСТОЙЧИВОСТИ БИЗНЕСА

Одной из целей вступления России в ВТО являлось привлечение западных инвестиций. Но иностранные инвесторы не будут вкладывать деньги в предприятия, которые

могут оказаться ненадежными бизнес-партнерами, в частности неустойчивыми к воздействию различных чрезвычайных обстоятельств [1].

Решение подобных задач на предприятиях возлагается на специалистов по обеспечению непрерывности и устойчивости бизнеса. Вузы РФ имеют определенный опыт в подготовке ИТ-специалистов, однако их количество, сроки и качество подготовки не удовлетворяют возросшим потребностям бизнеса. Среди известных причин – рост сложности и объема знаний о предметной области [2], несистемный подход, недостаточная научно-методическая квалификация профессорско-преподавательского состава, слабая учебно-материальная база системы подготовки.

Совершенствование существующей системы подготовки специалистов по обеспечению непрерывности и устойчивости бизнеса лежит в плоскости автоматизации ее элементов и, в частности, среды подготовки.

Рассмотрим облик автоматизированной среды подготовки специалистов по обеспечению непрерывности и устойчивости бизнеса. Для этого зададим комплекс координат, характеризующий текущее состояние системы подготовки во времени ($t$) и пространстве состояний ($S$), а также допустимые ограничения ($L$) и необходимые условия ($C$) перевода системы из состояния $S_i$ в состояние $S_j$. Таким образом, задача построения автоматизированной среды подготовки специалистов может быть сформулирована как задача управления изменением состояния сложной системы с условиями и ограничениями.

Объективно можно измерить входные и выходные показатели системы ($W$), т. е. требуемый начальный уровень знаний ($W_а$) абитуриента и уровень знаний выпускника ($W_в$).

Рассматриваемый подход может обеспечить непрерывность процесса обучения специалиста при переходе на следующий курс (между дисциплинами) за счет технологии структуризации знаний.

В дальнейшем «знанием» будем называть множество понятий и связей между ними (семантическую сеть понятий).

Методологическая база технологии представления передаваемых знаний основана на трудах профессора В. Я. Розенберга. Согласно этой модели, процесс обучения представляет собой управляемый переход от «входного» состояния (знания, алфавита) абитуриента к «выходному» состоянию выпускника. Процесс перехода осуществляется итерационно. Шаг обучения (итерация) заключается в модификации «входного» алфавита, который в общем случае является «выходным» для предыдущего шага.

Препятствием к внедрению компьютерных технологий служит слабая формализация процесса подготовки специалистов.

Таким образом, можно сформулировать следующие требования к автоматизированной среде:

- непрерывность процесса подготовки ($L$);
- структуризация знаний ($C_1$);
- формализация процесса подготовки ($C_2$).

С учетом введенных понятий процесс подготовки специалистов в автоматизированной среде можно представить как задачу перевода системы из состояния $S_а$ (с уровнем знаний $W_а$) в состояние $S_в$ (с уровнем знаний $W_в$) за время обучения $T$ с соблюдением ограничений на непрерывность процесса $L$, структуризацию знаний ($C_1$) и формализацию процесса подготовки ($C_2$).

Обучение пользователя автоматизированной среды сводится к получению необходимого набора услуг.

Важной особенностью применения автоматизированной среды обучения является эмуляция таких ситуаций, как «пожар (затопление) в серверном помещении», недоступность персонала, поскольку они препятствуют нормальному осуществлению бизнес-процессов, связанных со складом, и создают угрозу простоя в работе организации [3].

**Литература**

1. *Седов О.* Непрерывность бизнеса и ВТО [Электронный ресурс] // Директор информационной службы. 2004. № 12. URL: http://www.osp.ru/cio/2004/12/173604 (дата обращения: 01.11.2012).

2. *Петренко С.* Стандарты управления непрерывностью бизнеса [Электронный ресурс] // Открытые системы. 2012. № 01. URL: http://www.osp.ru/os/2012/01/13012922 (дата обращения: 01.11.2012).

3. *Баранов Д.* Обеспечение непрерывности деятельности организации [Электронный ресурс] // Управление рисками. 2008. № 8(66). URL: http://www.rcb.ru/dep/2008-08/14195 (дата обращения: 01.11.2012).

УДК 378

**Ф. Ф. Павлов**

Санкт-Петербургский государственный инженерно-экономический университет

# УПРАВЛЕНИЕ КОНТЕНТОМ «ТЕСТЫ» В СИСТЕМЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

**Дистанционное обучение** – совокупность технологий, обеспечивающих доставку обучаемым основного объема изучаемого материала, интерактивное взаимодействие обучаемых и преподавателей в процессе обучения, предоставление обучаемым возможности самостоятельной работы по освоению изучаемого материала, а также в процессе обучения[1].

В России датой официального развития дистанционного обучения можно считать 30 мая 1997 г., когда вышел Приказ Минобразования России № 1050, позволяющий проводить эксперимент дистанционного обучения в сфере образования.

На сегодняшний день самой распространенной системой дистанционного обучения с самым большим количеством пользователей и разработчиков является Moodle.

Moodle – это система управления содержимым сайта (Content Management System – CMS), специально разработанная для создания онлайн-курсов. Такие системы часто называются системами управления обучением (Learning



[1] *Зайченко Т. П.* Основы дистанционного обучения: Теоретико-практический базис: Учеб. пособие. – СПб.: РГПУ им. А. И. Герцена, 2004. – С. 4.

Management Systems – LMS) или виртуальными образовательными средами (Virtual Learning Environments – VLE)[1].

Moodle достаточно просто устанавливается на любую поддерживающую PHP платформу (Linux/Windows/MacOS/Solaris) и обеспечивает работу с базами данных MySQL, MSSQL, Oracle, PostgreSQL, Interbase, Foxpro, Access, ADO, Sybase и ODBC. Сохранность контента гарантируется многоуровневой системой защиты. Moodle распространяется как программное обеспечение с открытыми исходными кодами (http://www.opensource.org/docs/definition_plain.html) под лицензией GPL (http://www.gnu.org/copyleft/gpl.html). Это обеспечивает широкое распространение этой системы, быстрое развитие, высокое качество и защищенность.

Moodle (англ. *Modular Object-Oriented Dynamic Learning Environment*) – это система управления обучением, разработанная для создания электронных курсов преподавателями, это модульная объектно-ориентированная динамическая учебная среда – свободная система управления обучением (LMS), распространяющаяся по лицензии GNU GPL.

Система дистанционного обучения (СДО) имеет широкие возможности для поддержки процесса дистанционного обучения – разнообразные способы реализации учебного процесса с планированием курса, проверкой знаний и контроля успеваемости.

СДО реализует главные задачи организации системы дистанционного обучения:

- полный и качественный состав электронных УМК;
- интерактивный процесс обучения;
- оперативный контроль и мониторинг;
- программная поддержка.

Функциями СДО могут быть:

- разработка структуры учебных курсов;

---

[1] *Анисимов А. М.* Работа в системе дистанционного обучения Moodle: Учеб. пособие. 2-е изд., испр. и доп. – Харьков: ХНАГХ, 2009. – 292 с.

• настройка пользовательского интерфейса с инструментами создания и настройки элементов курса;

• реализация операций дистанционного обучения с интерактивным общением;

• тестирование и обучение знаний.

Основным средством проверки знаний в СДО является **тестирование**, которое позволяет с наименьшими затратами преподавателя оценить знания большого количества слушателей.

В современной литературе тест рассматривают как форму контроля знаний. Оценим тест с двух точек зрения: как форму контроля и как форму обучения.

Тест как форма контроля – это комплекс заданий, ориентированных на определение уровня усвоения содержания обучения. Тест как форма контроля характеризуется следующими показателями:

• действенность, т. е. полнота, всесторонность проверки всех изучаемых элементов знаний;

• надежность, т. е. стабильность, устойчивость показателей при повторных измерениях;

• дифференцируемость, т. е. способность определить тех, кто усвоил и не усвоил материал на заданном уровне.

При составлении тестов как формы контроля необходимо придерживаться следующих правил:

• однозначность заданий, т. е. не должно допускаться произвольное толкование;

• однозначность ответов, т. е. должна быть исключена возможность формулирования многозначных ответов;

• соответствие изученному материалу;

• подбор дистракторов, т. е. неправильные ответы должны быть правдоподобными и на основе типичных ошибок.

Тест как форма обучения – это комплекс заданий, ориентированных на определение уровня усвоения содержания обучения с предоставлением слушателю возможности анализа и исправления ошибок.

По сравнению с тестами контроля тесты как форма обучения имеют большие настраиваемые возможности:

- обучающий режим, т. е. возможность ответить несколько раз в рамках одной попытки;
- просмотр результатов (свои ответы, баллы, комментарии);
- комментарии для каждого ответа и вопроса ко всему тесту;
- обучающие тесты различного рода (тест самоконтроля, тренинг).

В системе Moodle имеется два разных понятия: банк вопросов и тест.

Банк вопросов – это совокупность вопросов данного курса. Вопросы в банке распределены по категориям (обычно по темам курса).

Тест – это элемент курса, содержащий конкретный набор вопросов, с которым работает слушатель. Банк вопросов не привязан к тестам.

**Управление контентом «Тесты»** содержит следующие этапы:

- добавление теста и настройка его параметров;
- добавление категорий;
- добавление вопросов в категории банка вопросов;
- просмотр результатов и анализ вопросов.

Главными параметрами теста являются следующие.

- Название.
- Вступление: короткая информация для слушателей.
- Начать тестирование: дата и время открытия теста.
- Закончить тестирование: дата и время закрытия теста.
- Ограничение времени: время выполнения одной попытки.
- Вопросов на одной странице: максимальное количество вопросов.
- Случайный порядок вопросов: изменение очередности вопросов.
- Количество попыток.

• Метод оценивания: метод вычисления итоговой оценки по попыткам (лучшая оценка, средняя, первой попытки, последней попытки).

• Обучающий режим.

• Начислять штрафы.

• Студент может просматривать: ответы, баллы и т. д.

• Наличие пароля.

На **этапе добавления теста и настройки его параметров** надо в списке-меню «Добавить элемент курса» выбрать «Тест». Откроется форма для заполнения параметров теста.

Пример этапа добавления теста и настройка его параметров показан на рис. 1.

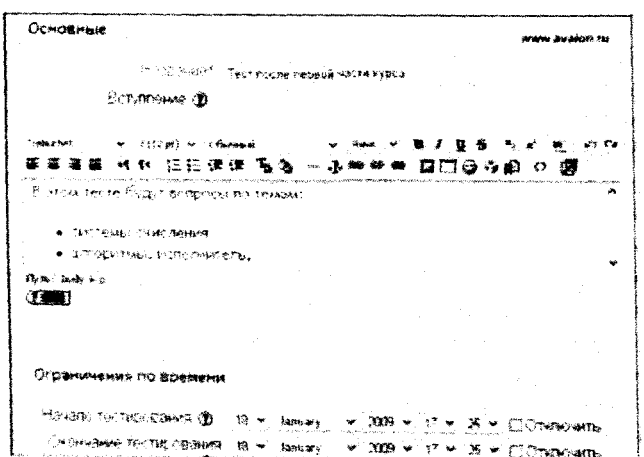



Рис. 1. Добавление теста

Дальнейшие этапы создания теста представлены на рис. 2.

1. Добавление категорий.
2. Добавление вопросов в банк вопросов.
3. Добавление вопросов в тест.

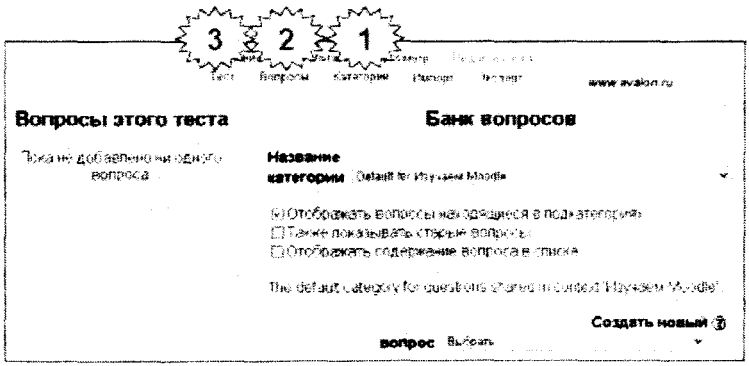



Рис. 2. Дальнейшие этапы создания теста

Тесты в банке вопросов разделяются на группы, называемые категориями, согласно темам курса. Категории могут иметь иерархию, т. е. вложенность.

Страницы для выполнения этапа 1 **(Добавление категории)** и этапа 2 **(Добавление вопросов)** показаны на рис. 3.

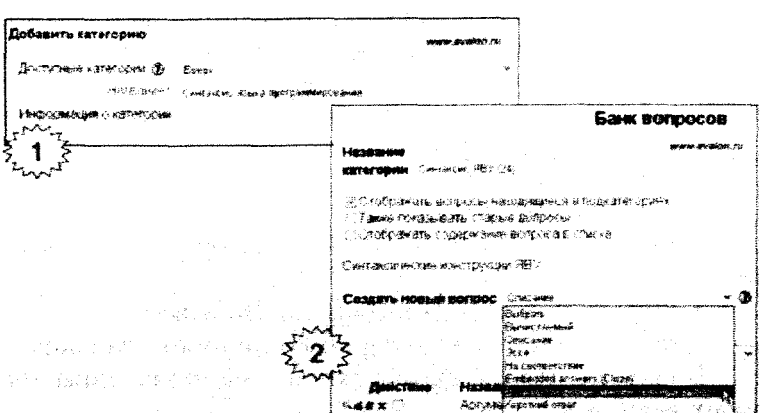



**Рис. 3. Добавление категории и вопросов**

Чтобы добавить/редактировать категорию, можно воспользоваться двумя способами:

- в блоке «Управление» нажать ссылку «Вопросы» и выбрать вкладку «Категории»;
- в блоке «Элементы курса» нажать ссылку «Тесты», затем на открывшейся странице нажать кнопку «Редактирование вопросов», а затем – вкладку «Категории».

В верхней части страницы имеются средства для добавления новой категории, в нижней части – для редактирования существующих категорий.

Главными параметрами категории являются следующие:

- доступные категории: родительская категория;
- название категории;
- информация о категории.

Чтобы добавить/редактировать вопросы, можно воспользоваться двумя способами:

- в блоке «Управление» нажать ссылку «Вопросы»;
- в блоке «Элементы курса» нажать ссылку «Тесты» и в открывшейся странице нажать кнопку «Редактирование вопросов».

В списке «Название категории» необходимо выбрать категорию вопросов, к которой относится добавляемый вопрос, затем необходимо выбрать тип вопроса в списке «Создать новый вопрос».

Главными параметрами вопроса являются следующие:

- название категории;
- название вопроса;
- содержание вопроса;
- оценка для вопроса по умолчанию: вес вопроса в тесте;
- штраф: от 0 до 1 за неправильный ответ;
- общий отзыв: комментарий после ответа на вопрос.

В системе Moodle применяются следующие **типы тестовых вопросов**.

**Альтернативный вопрос Верно/Неверно:** выбор их двух вариантов, пример – на рис. 4.

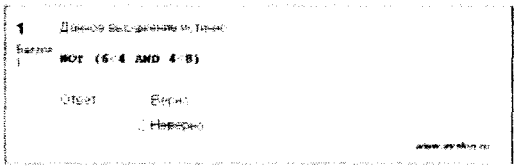



Рис. 4. Типы вопросов: Верно/Неверно

**Числовой вопрос:** ответ в виде числа, возможна единица измерения (кг, г, м, км...) (рис. 5).

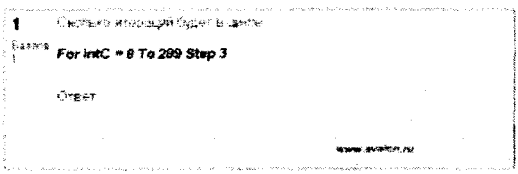



Рис. 5. Типы вопросов: числовой или короткий ответ

**Короткий ответ (вопрос в открытой форме):** ответ – слово или короткая фраза (см. рис. 5).

**Множественный вопрос (вопрос в закрытой форме):** задается вопрос и предлагается либо несколько вариантов ответов, есть два варианта: только с одним ответом либо с несколькими, пример – на рис. 6.

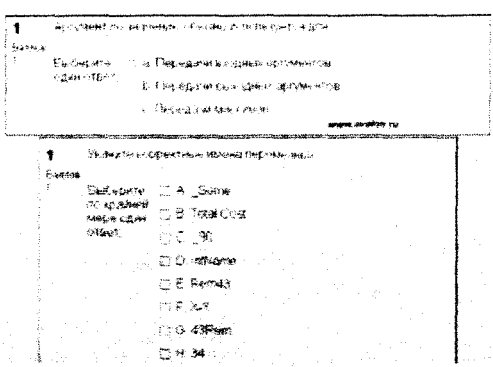


**Рис. 6. Типы вопросов: в закрытой форме (множественный выбор)**

**Вопрос на соответствие:** есть вопросы и ответы к ним, определить соответствие между вопросом и ответом, пример – на рис. 7.

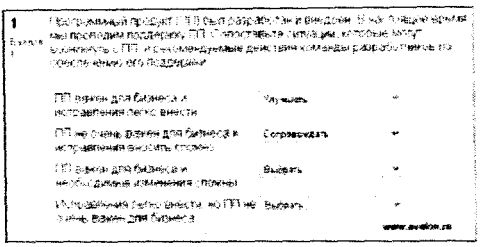


Рис. 7. Типы вопросов: на соответствие

**Вычисляемый вопрос:** похож на числовой, но ответ не в виде числа, а в виде формулы.

**Эссе:** письменный ответ, требующий ручного оценивания преподавателем.

**Случайный вопрос:** включение случайным образом в тест вопросов данной категории.

**Этап Добавление вопросов в тест**, представленный на рис. 8, состоит из трех операций.

1. Выбор теста.
2. Выбор категории.
3. Добавление вопросов в тест.

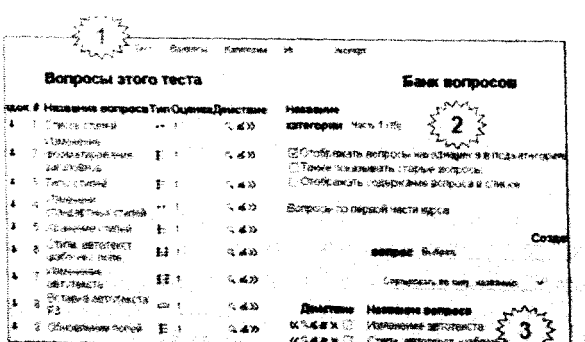



Рис. 8. Добавление вопросов в тест

Последовательность операций этого этапа приведена на примере рис. 9.

1. Перейти на вкладку «Редактирование».
2. Выбрать пункт «Тест».
3. Выбрать «Категорию».
4. Добавить либо вопросы по одному (4а),

либо выбрать несколько и добавить с помощью кнопки «Добавьте в тест» (4б),

либо выбрать все вопросы категории на данной странице (4в),

либо добавить случайные вопросы из текущей категории (4г).

**Добавление вопросов в тест**:

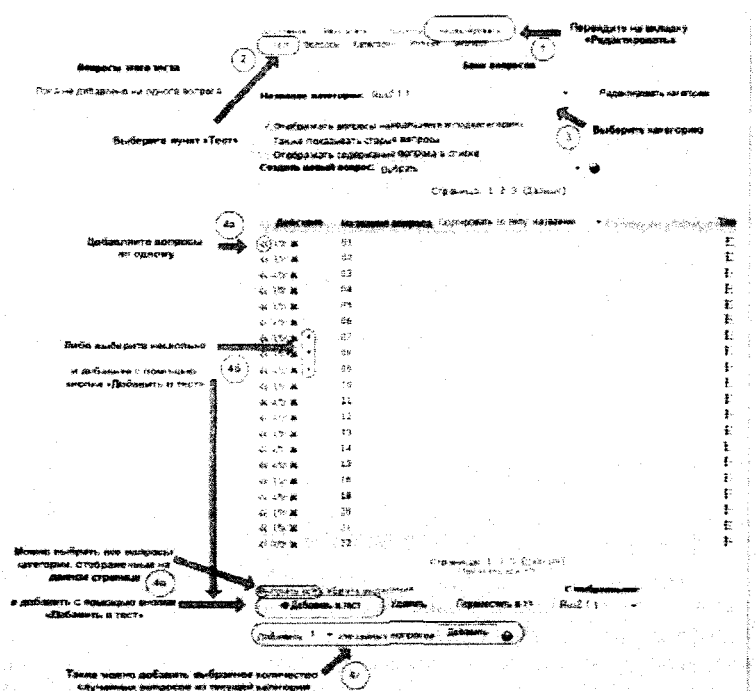



Рис. 9. Последовательность операций Добавление вопросов в тест

Последним этапом управления контентом «Тесты» является **просмотр результатов и анализ вопросов**.

Чтобы просмотреть результаты тестирования, необходимо щелкнуть на Названии теста и выбрать вкладку Результаты.

Появляются 4 ссылки.

- Просмотр: просмотр результатов тестирования.
- Переоценить: переоценка теста после его прохождения.
- Оценивание вручную: оценка преподавателем (например, Эссе).
- Анализ вопросов: анализ качества вопросов и процент слушателей, которые справились с ним.

Для каждого слушателя выводятся следующие данные.

- Фамилия и Имя.
- Дата и время начала попытки.
- Затраченное время.
- Набранное количество баллов.
- Оценки ответов на каждый вопрос теста.

Пример страниц просмотра результатов и анализа вопросов представлен на рис. 10.

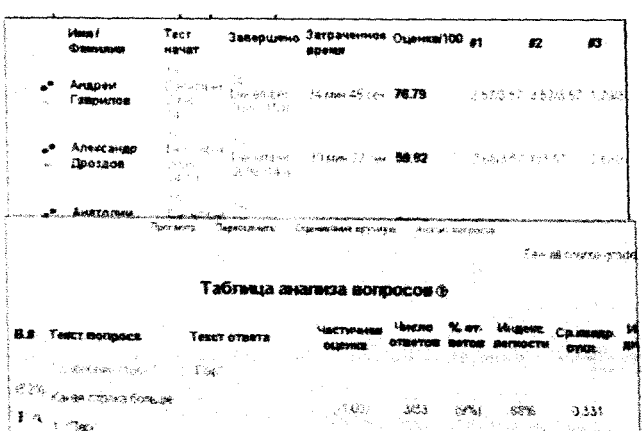



Рис. 10. Просмотр результатов и анализ вопросов

Анализ вопросов позволяет выяснить успеваемость соответствующей темы курса и качество вопросов.

Для каждого вопроса выводятся следующие данные:

- # (№ вопроса).
- Название и Текст вопроса.
- Текст ответа.
- Оценка ответа: определение преподавателем.
- Число ответов: в числителе – число попыток слушателей на заданный вариант ответа, в знаменателе – общее количество попыток ответов на данный вопрос.
- Процент ответов: процент попыток слушателей с данным вариантом ответа.
- Процент правильных ответов (индекс простоты вопроса): процентное отношение суммы баллов слушателей на этот вопрос к сумме баллов при правильном ответе.
- Стандартное отклонение: оценка различия между собой ответов разных слушателей.
- Индекс дискриминации: это качество вопроса, т. е. способность отличить сильных от слабых; индекс имеет значение от +1 до −1.
- Коэффициент дискриминации: это тоже качество вопроса, дает более точный результат; является коэффициентом корреляции между суммой баллов, набранных в данном вопросе, и в тесте в целом.

**Литература**

1. *Анисимов А. М.* Работа в системе дистанционного обучения Moodle: Учеб. пособие. – 2-е изд. – Харьков: ХНАГХ, 2009.

2. *Андреев А. В., Андреева С. В., Доценко И. Б.* Практика электронного обучения с использованием Moodle. – Таганрог: ТТИ ЮФУ, 2008.

3. *Щукин А. В.* Подготовка учебных курсов в системе дистанционного обучения [Электронный ресурс] / Факультет переподготовки специалистов, СПбГПУ // Портал дистанционного обучения. URL: http//www.dl.avalon.ru (дата обращения: 01.10.2012).

УДК 007

**Н. И. Сясин**

Санкт-Петербургский государственный
инженерно-экономический университет

# ИНФОРМАЦИОННЫЕ АСПЕКТЫ СВЯЗЕЙ С ОБЩЕСТВЕННОСТЬЮ

**Информация в PR-деятельности.**

Еще в трудах мыслителей Древней Греции и Рима можно найти достаточно свидетельств тому, что воздействию на общественное мнение уделялось большое внимание. В последние годы работа с общественностью приобрела качественно новый уровень, выделившись в самостоятельную сферу профессиональной деятельности.

Понятие «паблик рилейшнз» (Public relations (PR), ПР, «связи с общественностью») возникло в США в 1903 г. Сейчас эта отрасль знаний проникла практически во все сферы жизнедеятельности. Сегодня все общественные, политические, и коммерческие учреждения и организации имеют отделы «связей с общественностью».

Многие ученые под «связями с общественностью» подразумевают **управленческую деятельность**, направленную на установление и поддержание взаимовыгодных отношений между государственными или частными структурами и общественностью. В прагматическом же аспекте связи с общественностью рассматриваются как умение воздействовать на общественное мнение в интересах корпорации, фирмы таким образом, чтобы убедить потребителя, что корпоративная деятельность осуществляется, прежде всего, ради его благополучия.

Некоторые склонны сводить эти функции к **рекламной деятельности.** Однако, несмотря на то, что связи с общественностью и реклама имеют общую функцию воздействия на широкую аудиторию, каждая из коммуникативных сфер имеет свою цель. Реклама ставит основной

целью продать конкретный товар или услугу. Основной же целью связей с общественностью может являться создание и поддержание имиджа корпорации, фирмы, партии, политического лидера и пр.

Многие авторы рассматривают PR как составляющую часть рыночных механизмов. В то же время едва ли можно отрицать, что PR существует и в тоталитарных обществах, и в командно-административных системах. Связи с общественностью могут быть составной частью и политической деятельности.

**Любое явление должно иметь определение.**

Надо сказать, что, несмотря на многолетнюю (можно сказать, даже многовековую) историю развития этой сферы человеческой деятельности, у явления, именуемого «связи с общественностью», на данный момент нет четкого и однозначного определения, которое могло бы дать всеобъемлющую характеристику такого сложного и многогранного понятия, как ПР.

Закон Ома – это физический закон, определяющий соотношение между напряжением, силой тока и сопротивлением проводника в электрической цепи. (*Электрический ток похож на лентяя – он идет там, где легче.*)

Переменный ток – ток, изменяющийся по величине и направлению (*обходит пластины конденсатора по синусоиде*).

Закон Архимеда – закон статики жидкостей и газов, согласно которому на погруженное в жидкость (или газ) тело действует выталкивающая сила, равная весу жидкости в объеме тела. (*Тело, всунутое в воду, выпирает на свободу массой выпертой воды тела, впертого туды.*)

Число π. («Кто (3) и (1) шутя (4), и (1) скоро (5) пожелаетъ (9) пи (2) узнать (6), число (5) ужѣ (3) знаетъ (6). Получаем – 3,1415926536».)

Все вышеприведенные явления и законы имеют точные и строгие определения. Шуточные версии в скобках рассчитаны на мнемоническое запоминание – забытый, к сожалению, прием, облегчающий запоминание сложных, а

иногда и скучных определений. В Интернете, между прочим, есть несколько форумов, где «форумчане» вспоминают и приводят разные версии одного и того же мнемонического определения (пример: Шутливые формулировки и мнемонические правила. URL: http://www.baku.ru/frmpst-text.php?frm_id=22&frmpst_id=3050276 &cmm_id=136).

Что же касается предмета нашего разговора, то на сегодня проанализировано около 1000 определений, характеризующих связи с общественностью. Например, Сэм Блэк, генеральный секретарь Международной ассоциации паблик рилейшнз (IPRA), дает следующее очень известное определение PR: *«Public Relations – это искусство и наука достижения гармонии посредством взаимопонимания, основанного на правде и полной информированности»*. А вот еще одно: *«Связи с общественностью – наука и искусство, коммуникативная деятельность, направленные на формирование и поддержание гармоничных и доброжелательных отношений между субъектом (личность, организация, учреждение, партия, регион) и общественностью на основе информации»*. Это примеры наиболее всеобъемлющих (интегральных) определений.

Анализируя другие определения (порядка 150 выборочно), в конечном счете приходим к выводу, что во всех определениях PR присутствуют одни и те же смысловые блоки, описывающие цели, задачи, средства и результаты (содержание) PR-деятельности. И во всех этих смысловых блоках присутствует еще нечто приводящее все определения к чему-то общему. Это общее – информация. Если вдуматься, то информация (не зависимо от формы ее представления) составляет важнейшую часть нашей жизнедеятельности и часто бывает важнее, чем сам объект информации. А ситуацией всегда владеет тот, кто обладает большей информацией.

Поэтому возьмем на себя смелость сформулировать тысяча первое (почему бы и нет?) определение PR-деятельности. Оно может звучать так: **«Любую передачу и (или) получение каких либо сведений (информации)**

**предприятием, учреждением, корпорацией или фирмой можно назвать связями с общественностью».** Это определение можно определить как информационное.

Попытаемся проиллюстрировать это утверждение на примере. На рис. 1 изображена улица, на которой стоит дом с глухой стеной. Даже если за этой стеной расположена какая-то организация, мы, наблюдатели, не сможем этого даже заподозрить, так как присутствие этой организации в этом здании никоим образом не проявляется.

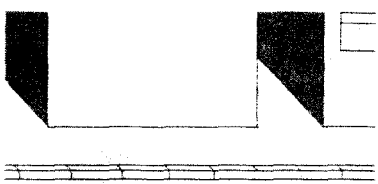


Рис. 1. Необнаружение

Надо сказать, что проблема необнаружения объекта глубоко исследуется применительно к военному делу. Это и режим радиомолчания при приближении к цели, и различные способы маскировки, в том числе отражение/поглощение радиоволн (технология «Стелс») и др. В общем, если объект не желает, чтобы его обнаружили, он или не передает никакой информации, или тщательно ее маскирует.

Если же на этой глухой стене вдруг появилась стальная дверь (рис. 2), то мы можем предположить, что в помещение, расположенное за этой дверью, приходят люди, но они решительно не желают ни с кем общаться, поэтому на двери нет никакой таблички. Наличие такой двери можно считать тем пороговым значением информации, которое позволяет нам утверждать, что в этом здании существует некая организация, все связи с общественностью которой ограничиваются этой дверью.

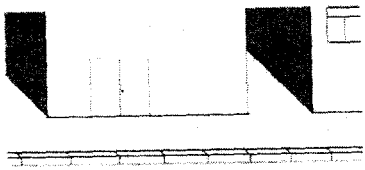


Рис. 2. Пороговая информация

Теперь внимательно рассмотрим рис. 3. Здесь на уже знакомой нам по предыдущему рисунку железной двери появилось переговорное устройство (домофон) с кодовым замком и кнопкой звонка.

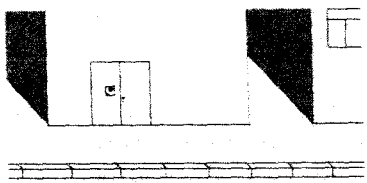


Рис. 3. Предположение

Значит, в этой организации существует охрана (или привратник) и есть возможность позвонить и спросить, что это за организация. Хотя, скорее всего, вам не ответят или ответят не очень вежливо, но по сравнению со вторым рисунком вы получаете об организации гораздо больше информации. Дополнительной информацией также является наличие кодового замка и звонка. Это позволяет предположить, что сюда приходят не только хорошо известные в этой организации люди, имеющие свой ключ, но и гости, которые нажимают кнопку звонка и проходят процедуру опознания сотрудником, осуществляющим аутентификацию и идентификацию пришедшего гостя, знающего кодовое слово (вы-то кодового слова не сказали и получили невежливый отказ). Вот сколько различной информации

можно узнать, если на двери присутствует обычный домофон. Заметьте, на двери так и нет никакой таблички.

Ну, а если к тому огромному объему информации, которым вы уже располагаете, изучив третий рисунок, добавится табличка, где написано название и род деятельности этой организации (рис. 4 и 5), то вам все станет понятно, и связи с общественностью будут осуществляться в полном (насколько организация считает нужным) объеме.

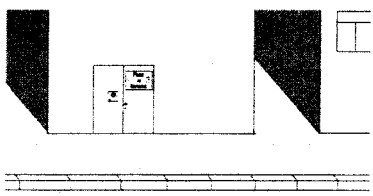


Рис. 4. Полный объем информации

РОГА И КОПЫТА

Поставка и установка рогов
и копыт для чертей всех мастей

Часы работы:
от полуночи до третьих петухов,
по пятницам – скидки,
в пятницу 13-го – бонус

Рис. 5. Пример информационной таблички

В вышеприведенном простейшем примере не учитывается множество нюансов. В нем ситуация упрощена до предела и доведена до абсурда. Но если вспомнить латинское выражение ad Absurdum (лат. «к абсурду»), то, используя этот философский прием, можно достаточно точно очертить границы, в которых идея работает.

Закончить свою краткую статью о значении информационных технологий и информации в связях с общест-

венностью хочется тем же, с чего она и начиналась: если нет достоверной информации, то ничего нельзя утверждать определенно. В качестве примера (многие сочтут его неудачным) можно привести организацию, носящую название «Масоны». Говорят и пишут о ней очень много, но...! Перефразировав известного сатирика, хочется спросить: «...они есть или их нет? Уже не важно, что они когда-то были. Пусть скажут: они есть или их нет!!!..». Не дают ответа! Энтропия не уменьшается. Результат – одни верят, что они есть, другие верят, что их нет. *И то и другое недоказуемо!*

УДК 004.77

**Ж. Г. Салимьянова**

Санкт-Петербургский государственный
инженерно-экономический университет

## ГРИД-ТЕХНОЛОГИИ КАК КАТАЛИЗАТОР НАУЧНО-ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ

Перспективным направлением развития современных информационных технологий являются грид-технологии, концепция которых предполагает создание глобального информационного пространства.

Развитие грид-технологий носит стратегический характер, потенциал их оценивается очень высоко мировым научным сообществом. Грид-технологии призваны обеспечить создание принципиально нового вычислительного инструмента для развития высоких технологий в различных сферах человеческой деятельности, позволяющего обрабатывать огромные объемы данных.

Как новая форма информационных технологий, грид предназначаются для решения сложных научных и инженерных задач, которые невозможно решить в разумные сроки на отдельных вычислительных установках.

Вопросы создания и эксплуатации грид-технологий нашли практическую реализацию во всех технологически развитых странах. Широкий интерес к ним, их развитие объясняются тем, что область применения грид с каждым годом расширяется и претендует на роль универсальной инфраструктуры для обработки данных.

Данные технологии способны решать не только конкретные прикладные задачи, но и объединять ресурсы путем создания компьютерной инфраструктуры нового типа, обеспечивающей глобальную интеграцию информационных и вычислительных ресурсов на основе сетевых технологий и специального программного обеспечения. А набор сервисных услуг, таких как поиск необходимых ресурсов, сбор информации о состоянии ресурсов, хранение и доставка данных, обеспечивает надежный совместный доступ к географически распределенным информационным и вычислительным ресурсам, отдельным компьютерам, кластерам, хранилищам информации и сетям.

Согласно классическому определению, грид (grid) [1] – согласованная, открытая и стандартизованная среда, обеспечивающая гибкое, безопасное, скоординированное разделение ресурсов в рамках виртуальной организации.

Грид – это виртуальное предприятие, в котором функционирует как потребители ресурсов, так и владельцы ресурсов. Это новый этап в цепочке Интернет, всемирной паутины www, где координируется режим коллективно разделяемого доступа к ресурсам в рамках виртуальных организаций. Все пользователи грида распределены по виртуальным организациям, под которыми подразумеваются группы пользователей, институтов и ресурсов, принадлежащих единой администрируемой области.

Интерес к грид-технологиям на первых стадиях был вызван реализацией сложных задач, которые невозможно было решить в разумные сроки на базе имеющих место информационных технологий. Сегодня грид-сети используются в самых разных областях науки, техники, промыш-

ленности, образовании, коммерческом сегменте, фундаментальных научных исследованиях и бизнес-проектах.

Современная вычислительная грид-технология позволяет:

• объединить компьютерные центры, расположенные в любых точках мира, и предоставить эти вычислительные ресурсы пользователям;

• охватить широкий класс задач, требующих на качественно новом уровне обработку огромных объемов экспериментальных данных;

• обеспечить моделирование сложнейших процессов;

• обеспечить визуализацию больших наборов данных, сложных бизнес-приложений в различных областях естественных наук, в промышленности, бизнесе с большими объемами вычислений;

• повысить эффективность вычислительной техники путем предоставления в грид временно простаивающих ресурсов;

• обеспечить возможность совместного использования данных и анализа результативной информации через установленные рубежи и географические границы.

Анализ мирового опыта разработок таких технологий позволил выделить три направления развития грид.

1. Вычислительные грид-технологии позволяют достичь высокопроизводительных вычислений за счет обеспечения глобального распределения их между компьютерами, серверами, суперкомпьютерами. Спецификация оборудования предполагает их деление на:

• настольные гриды. Основную часть ресурсов составляют многочисленные неиспользуемые ресурсы настольных компьютеров;

• серверные гриды. Характеризуются набором ресурсов серверов;

• инструментальные гриды. Определяющей их характеристикой является использование нестандартных элементов оборудования, например таких, как телескоп.

2. Грид-технологии интенсивной обработки данных. Обеспечивают доступ к данным, обработку значительных объемов данных, поступающих из различных систем и глобально распределенных источников информации, их хранение и синхронизацию.

3. Семантические грид-технологии. Это технологии высокоуровневого сервиса, они позволяют работать с семантической базой знаний и оперировать данными из разнотипных баз данных.

Важную роль в функционировании грид играют ресурсы [3]:

• **вычислительные ресурсы** – представляют собой кластеры, построенные на основе персональных компьютеров, соединенных локальной сетью. Множество установок объединяются таким образом, что каждую из них становится возможным использовать дистанционно для обработки приложений, оформляемых в виде заданий, где для каждого задания автоматически подбираются исполнительные ресурсы и создается соответствующая исполнительная среда;

• **ресурсы хранения данных** – диски и дисковые массивы, системы массового хранения данных. Ресурсы хранения данных – это не только запоминающие устройства, а также иерархические системы, в которых диски сочетаются с библиотеками со сменными носителями. Различные хранилища образуют общее пространство памяти, где и размещается глобальная файловая система;

• **сетевые ресурсы**. Ресурсы, присутствующие в сети, должны быть доступны для всех взаимодействующих служб. Это обеспечит не только интеграцию географически распределенных компьютерных ресурсов для крупномасштабных вычислений, но и создание пространственно распределенного компьютинга с различной предметной ориентацией;

• **программное обеспечение** – специализированное ПО, позволяющее использовать ресурсы (компьютеры, хранилища данных, сети) сообществам пользователей.

Программное обеспечение современных гридов имеет потенциал для эффективного применения в более широкой области, чем чисто счетные приложения и состоит из определенных подсистем. Число подсистем зависит от сложности грид и строится на базе существующих инструментальных средств, предоставляя высокоуровневые сервисы задачам и пользователям. Специальное программное обеспечение и простые удобные графические интерфейсы для управления данными позволяет обеспечивать оптимальное использование этих ресурсов.

Объединяя ресурсы разных типов, грид-технологии обеспечивают скоординированный доступ пользователей, независимо от места их нахождения ко всем ресурсам посредством пользовательского интерфейса.

Надо отметить, понятие ресурса в гриде является очень широким. Ресурсом, помимо перечисленных типов, может также являться, например, устройство, подключенное к сети, а также любое приложение, которое по каким-либо причинам не может быть установлено у всех, кто хочет обрабатывать с его помощью свои данные. Путем подключения к гриду владелец компьютера, на котором установлено такое приложение, может предоставить к нему доступ и определить круг лиц, которые могут им пользоваться.

Таким образом, учитывая вышесказанное, современные исследовательские направления в области грид, их можно охарактеризовать как пространственно-распределенную операционную среду с гибким, безопасным и скоординированным разделением ресурсов для выполнения приложений в динамически образующихся виртуальных организациях.

Являясь средой коллективного компьютинга, реализующей основную цель – создание условий для динамического распределения вычислительных ресурсов и ресурсов хранения, грид характеризуется следующими свойствами [4].

• Разнородность. Грид объединяют разнородные ресурсы, которые являются разнородными по происхождению, и обеспечивают коллективный доступ к этим ресурсам в глобальном пространстве.

• Масштабируемость. Спектр возможных ресурсов весьма широк и мог бы расти от нескольких ресурсов до тысяч. При этом ресурс может быть логической сущностью (например, распределенной файловой системой) или физической (например, кластером компьютеров). Коммуникационные и аутентификационные средства могут быть значительно улучшены за счет приложений, способных использовать имеющиеся ресурсы.

• Адаптивность. Менеджеры ресурса или приложения должны динамично адаптироваться таким образом, чтобы извлечь максимальную производительность из доступных ресурсов.

Ввиду открытости информационных ресурсов в грид-технологиях нельзя не затронуть тему информационной безопасности, приобретающую в этой среде особое значение. Анализ имеющихся разработок распределенных вычислительных систем показывает, что система безопасности «Грид» должна обладать следующими свойствами [5–7].

• Единый вход в грид-систему. Для получения доступа ко всем разрешенным ресурсам пользователь должен регистрироваться и аутентифицироваться только один раз в начале сеанса работы.

• Делегирование прав. Пользователь должен иметь возможность запуска программ от своего имени. В результате чего программы получают доступ ко всем ресурсам, на которых авторизован пользователь. Пользовательские программы могут, при необходимости, делегировать часть своих прав другим программам.

• Проверка целостности и конфиденциальности сообщений. Выбор уровня защиты может зависеть от различных факторов (типов передаваемых сообщений, инфра-

структуры, по которой осуществляется передача сообщения и т. д.).

• Безопасность совместного использования ресурсов.

• Поддержка различных протоколов связи, обеспечивающих доставку информационных пакетов. В основе грид лежат программные технологии, использующие новые стандарты и протоколы совместно с известными сетевыми и интернет-протоколами (TCP). Система безопасности «Грид» должна иметь возможность использования других протоколов, обладающих аналогичными свойствами.

• Наличие промежуточного программного обеспечения, состоящего из определенных подсистем. Число подсистем зависит от сложности системы «Грид».

Обеспечение безопасности современных грид, объединяющих различные организации и вычислительные ресурсы, имеющих разных владельцев, является актуальной задачей, имеющей широкое практическое применение.

**Литература**

1. The Grid 2: Blueprint for a New Computing Infrastructure / Foster and C. Kesselman (eds.). Morgan Kaufmann Publishers, 2009.

2. Overview of the Grid Security Infrastructure [Электронный ресурс]. URL: http://www.globus.org/security/overview.html (дата обращения: 10.10.2012).

3. DataGrid Project Documentation [Электронный ресурс]. URL: http://marianne.in2p3.fr/datagrid/documentation (дата обращения: 10.10.2012).

4. Портал семантического грида (Semantic Grid Community Portal) [Электронный ресурс]. URL: http://www.semanticgrid.org (дата обращения: 10.10.2012).

5. *Таковицкий О.* Технология Grid Computing [Электронный ресурс]. URL: http://www.bytemag.ru/?ID=601856 (дата обращения: 10.10.2012).

6. *Демичев А. П., Ильин В. А., Крюков А. П.* Введение в грид-технологии. Препринт НИИЯФ МГУ–2007–11/832.

7. *Ли М., Бейкер М.* Основные грид-технологии // John Wiley & Sons Ltd, 2008. – 423 с.

УДК 330.46

**С. А. Соколовская**

Санкт-Петербургский государственный
инженерно-экономический университет

# К ВОПРОСУ О МОДЕЛИ УПРАВЛЕНИЯ ВИРТУАЛЬНЫМ ПРЕДПРИЯТИЕМ

Виртуальные предприятия можно представить как группу агентов, которые совместно ведут бизнес, независимо от их физического местонахождения. Это позволяет им должным образом реагировать на изменения, происходящие на рынке при критически низких затратах с точки зрения традиционного бизнеса.

Виртуальное предприятие (ВП) обычно возникает, когда спрос рынка не может быть удовлетворен посредством модернизации существующих продуктов и технологий и требуется разработка новых, инновационных подходов, влекущая за собой существенные риски для производителей брендов. Развитие и широкие возможности телекоммуникационных инфраструктур позволяют исключить необходимость объединения агентов виртуального предприятия в одном месте, что способствует ужесточению требований к управлению и способам решения поставленных бизнес-задач.

Для эффективного управления ВП в быстро меняющихся условиях автор предлагает рассматривать корпоративные стратегии с позиций процессного подхода. В этом случае особенности моделирования бизнес-процессов ВП для задач стратегического управления заключаются в следующем:

- интегрирующая роль принадлежит «владельцу процесса»;
- необходим баланс интересов «владельцев процессов» и агентов, через которые проходит «сквозной межфункциональный процесс»;

• необходима оптимизация ресурсов и затрат;

• объектом моделирования является сбалансированная система показателей степени достижения целей управления ВП;

• поддержка создания, внедрения и сопровождения системы управления ВП инструментальными средствами.

С точки зрения процессного подхода роль ВП как «владельца интегрированных межфункциональных процессов», связанных с внешними выходами ВП, адекватна роли Руководителя проекта (Главного конструктора) в «проектных организациях» и при переходе компании к ориентации на процессы становится исключительно важной. То есть в результате на ВП вводится матричная структура управления в разрезе двух векторов – во-первых, это функциональные подразделения, которые выступают в качестве «центров управления ресурсами», а во-вторых, это реализуемые «сквозные» процессы, которые эти ресурсы используют.

Большинство ВП имеет несколько продуктовых линий (product lines) и, соответственно, несколько групп клиентов с отличающимися требованиями. Для их реализации используются общие специализированные ресурсы ВП (люди, оборудование), которые, как правило, сгруппированы по функциональным областям – подразделениям, имеющим свои интересы и критерии оценки эффективности их деятельности. Важно установить границы ответственности и формализовать отношения «владельца процесса» и агентов, через которые протекает процесс.

Эти отношения могут быть формализованы с помощью сбалансированной системы показателей (ССП), которыми оценивается деятельность каждого из них: «владелец процесса», главным образом, отвечает за показатели результативности процессов, а головной орган управления ВП – за эффективность использования ресурсов.

Выбор ключевых показателей результативности определяется необходимостью соблюдения баланса интересов агентов и клиентов в достижении поставленных целей, ис-

ходя из задач стратегического управления ВП. То есть можно говорить о достижении баланса интересов заказчиков продукта или услуг и ВП в лице владельцев-акционеров.

Таким образом, правильный подбор агентов и выбор ключевых показателей результативности ССП в рамках бизнес-процессов ВП, использующих единое информационное пространство и единую базу данных, поможет снизить степень неопределенности в процессе управления виртуальными организациями.

УДК 336

**В. А. Береговой, А. В. Перематка**

Санкт-Петербургский государственный инженерно-экономический университет

## МЕТОДЫ И МОДЕЛИ, ИСПОЛЬЗУЕМЫЕ В ПРАКТИКЕ ФИНАНСОВОГО МЕНЕДЖМЕНТА

Сейчас трудно указать область человеческой деятельности, где не применялись бы эвристические методы и модели. Особенно перспективными выглядят эти методы и модели при оценке таких интегральных экономических показателей, как «риск/доход», «цена/качество».

Сфера практического применения этих методов ограничивается возможностями и эффективностью формализации экономических проблем и ситуаций, а также состоянием информационного, математического, технического обеспечения используемых моделей.

Практическими задачами экономического моделирования являются анализ объектов и процессов; предвидение развития процессов; выработка управленческих решений на всех уровнях хозяйственной иерархии.

Результаты моделирования способствуют выбору наилучшего решения из всего набора предложенных моделей, но принятие решения остается за человеком.

В случае применения SWOT-анализа удается оценить рыночную ситуацию – опасности и возможности, которые ожидают коммерческую структуру, а также их слабые и сильные характеристики, основные направления факторов развития, т. е. определить базовые стратегии с учетом времени, ориентированные на возможную экспозицию факторов риска. Метод факторного SWOT-анализа позволяет систематизировать благоприятные и неблагоприятные факторы, потенциальные возможности, эндогенные и экзогенные угрозы.

SWOT-анализ факторов проводят с их объединением по шести условным группам: 1) рыночная конъюнктура; 2) институциональные рынки; 3) логистический фактор; 4) трудовые ресурсы; 5) рынок инвестиций; 6) организационные факторы.

Следует помнить, что при наличии большого количества факторов модель неустойчива, а при малом количестве – могут выявиться ошибки, отрицательно влияющие на принятие решений.

Отметим, что при составлении SWOT-матрицы и ее последующем анализе удается выявить множество парных комбинаций показателей.

Ключевой проблемой теории и практики финансового менеджмента является снижение затрат на производство продукции и услуг. Международная и отечественная практика рекомендует с этой целью использовать метод функционально-стоимостного анализа (ФСА). В его основе лежит понятие идеальности системы. Метод ФСА представляет собой программу действий, методические и технико-экономические приемы, нацеленные на обнаружение, предупреждение, снижение или ликвидацию излишних затрат. ФСА – это четкая последовательность его проведения, включающая в себя несколько взаимоувязанных этапов.

1. Подготовительный этап: выбор объекта анализа, определение сроков проведения и подготовка перечня необходимых материалов.

2. Информационный этап: сбор и систематизация оптимального количества информации о процессах объекта анализа и его аналогах; изучение затрат на их функционирование; составление структурной модели объекта анализа, определение затрат на стадиях разработки, производства и использования объекта ФСА.

3. Аналитический этап: формулирование всех возможных функций объекта анализа и его составных частей; построение функциональной модели объекта; оценка затрат, связанных с осуществлением выявленных функций.

4. Творческий этап: разработка вариантов упрощения и улучшения объекта ФСА, обсуждение различных предложений и отбор из них наиболее экономичных и реальных.

5. Исследовательский этап: отбор наиболее рациональных выдвинутых вариантов и их ранжирование.

6. Рекомендательный этап: оформление рекомендаций с соответствующими расчетами.

На основе ФСА в каждом конкретном случае выделяются лишние функции. Исключение из функциональной сферы объекта анализа избыточных и дублирующих функций приводит к уменьшению затрат.

ФСА как метод исследования систем направлен на оптимизацию соотношения «цена/качество» товаров и услуг при их проектировании, производстве, маркетинге, приобретении, доставке, применении, обслуживании клиентов.

Самостоятельным и весьма эффективным инструментом является математическое моделирование. Моделирование – это искусственное воспроизведение объекта исследования (процесса или состояния), точнее тех его сторон, закономерности которых интересуют исследователя. Подобные эксперименты способствуют выявлению интуиции – важного фактора любого творческого процесса.

К имитационному моделированию прибегают в случаях, когда дорого или невозможно экспериментировать на реальном объекте; невозможно построить аналитическую модель; в системе есть нелинейности, стохастические пе-

ременные; необходимо сымитировать поведение системы во времени.

При решении многих задач финансового менеджмента используются модели, содержащие случайные величины. Например, при оценке риска инвестиционных проектов, как правило, используют прогнозные данные об объемах продаж, затратах, ценах и т. д. В подобных случаях отсутствующие фактические данные заменяются величинами, полученными в процессе имитационного эксперимента.

Применение имитационных моделей дает множество преимуществ по сравнению с выполнением экспериментов над реальной системой и использованием других методов.

Социально-экономические системы относятся к сложным системам. Сложные системы обладают рядом свойств, которые необходимо учитывать при их моделировании.

Важнейшие из этих свойств:

- эмерджентность, т. е. наличие у экономической системы таких свойств, которые не присущи ни одному из составляющих систему элементов, взятому в отдельности, вне системы. Поэтому социально-экономические системы необходимо исследовать и моделировать в целом;
- массовый характер экономических явлений и процессов. Закономерности экономических процессов не обнаруживаются на основании ограниченного числа наблюдений. Поэтому моделирование должно опираться на масштабные наблюдения;
- динамичность экономических процессов, заключающаяся в изменении параметров и структуры экономических систем под влиянием среды (внешних факторов);
- случайность и неопределенность в развитии экономических явлений;
- невозможность изолировать протекающие в экономических системах явления и процессы от окружающей среды, чтобы наблюдать и исследовать их в чистом виде;
- активная реакция на появляющиеся новые факторы, способность социально-экономических систем к активным, не всегда предсказуемым действиям в зависимости от

отношения системы к этим факторам, способам и методам их воздействия.

Выделенные свойства экономических систем осложняют процесс их моделирования, начиная с выбора типа модели и кончая вопросами практического использования результатов моделирования. Поэтому целесообразно более детально проанализировать последовательность и содержание этапов моделирования, выделив следующие шесть этапов.

1. Постановка экономической проблемы и ее качественный анализ. На этом этапе требуется сформулировать сущность проблемы, принимаемые предпосылки и допущения. Необходимо выделить важнейшие черты и свойства моделируемого объекта, изучить его структуру и взаимосвязь его элементов, хотя бы предварительно сформулировать гипотезы, объясняющие поведение и развитие объекта.

2. Построение математической модели. Это этап формализации экономической проблемы, т. е. выражения ее в виде конкретных математических зависимостей (функций, уравнений, неравенств и др.). Для некоторых сложных объектов целесообразно строить несколько разноаспектных моделей. При этом каждая модель выделяет лишь некоторые стороны объекта, а другие стороны учитываются агрегированно и приближенно.

3. Математический анализ модели. На этом этапе чисто математическими приемами исследования выявляются общие свойства модели и ее решений. При аналитическом исследовании выясняется, единственно ли решение, какие переменные могут входить в решение, в каких пределах они изменяются, каковы тенденции их изменения и т. д.

4. Подготовка исходной информации. Математическое моделирование предъявляет жесткие требования к системе информации; при этом надо принимать во внимание не только принципиальную возможность подготовки информации требуемого качества, но и затраты на подготовку информационных массивов. В процессе подготовки информации используются методы теории вероятностей, тео-

ретической и математической статистики для организации выборочных обследований, оценки достоверности данных и т. д. При системном моделировании результаты функционирования одних моделей служат исходной информацией для других.

5. Численное решение. Этот этап включает разработку алгоритмов численного решения задачи, подготовку программ на ПК и непосредственное проведение расчетов; при этом значительные трудности вызываются большой размерностью экономических задач. Обычно расчеты на основе экономико-математической модели носят многовариантный характер.

6. Анализ численных результатов и их применение. На этом этапе решается важнейший вопрос о правильности и полноте результатов моделирования и применимости их как в практической деятельности, так и в целях усовершенствования модели.

Моделирование – это итеративный, циклический процесс. Недостатки, обнаруженные после первого цикла моделирования, можно исправить в последующих циклах.

В практике управления нужен такой метод построения модели, который позволяет строить модель на минимальном количестве исходных данных с опорой на эвристику.

Опыт показывает, что все рассмотренные выше методы эвристического моделирования успешно реализуются в среде Excel.

Большое развитие использования этих методов в финансовой деятельности уже достигнуто в США. Что касается стран Европы, Японии и России, то эти страны только приступают к их широкому применению.

Первостепенным моментом полномасштабного анализа является возможность использовать результаты SWOT-анализа и/или ФСА при последующем имитационном моделировании, что особенно актуально при принятии стратегических инновационных решений в корпоративном и банковском секторе экономики.

УДК 004.715; 519.876.5

**Тиамийу А. Осуолале**

Санкт-Петербургский государственный
университет телекоммуникаций

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕДСТВ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ТКС, ПОДДЕРЖИВАЮЩИХ ДОВЕРЕННУЮ МАРШРУТИЗАЦИЮ

В настоящее время значительная часть исследований телекоммуникационных сетей (ТКС) осуществляется с использованием программ имитационного моделирования – сетевых симуляторов, которые имитируют функционирование заданной топологии и конфигурации на ЭВМ. После чего результаты моделирования визуализируются и анализируются исследователем. Адекватность модели зависит от целей исследования, навыков моделирования и собственно характеристик программы имитационного моделирования.

Выбор подходящего сетевого симулятора для избранной предметной области исследования является непростой задачей вследствие наличия десятка достойных конкурентов (ns-2, OPNET, OMNeT++ и др.). Предлагается решение подобного рода задачи для целей исследования механизма доверенной маршрутизации (ДМ) в ТКС методом сравнительного анализа.

Дадим краткую характеристику сравниваемых программных продуктов.

**ns-2**. Является дискретным симулятором свободного распространения. Содержит модели наиболее распространенных сетевых технологий, и конкретное приложение создается за счет спецификации. Кроме того, предусмотрена большая библиотека записанных кодов. Инструментами анализа в ns-2 являются Сетевой Аниматор и файл трассировки.

**ns-3**. Является дальнейшим развитием ns-2 в части языка реализации: если в ns-2 в качестве языка програм-

мирования высокого уровня абстракции используется язык скриптов OTcl, то в ns-3 симулятор написан полностью в C++ с дополнительным построением на Python. Симулятор не имеет собственного графического интерфейса, однако для средств визуализации моделей используются проекты NetAnimator и PyViz.

**OPNET**. Симулятор имеет хороший графический интерфейс пользователя (GUI), что наряду со значительным количеством сопроводительной документации (включая результаты других исследований, которые поступают с лицензией) делает эту программу достаточно привлекательной. На OPNET могут быть настроены стандартные параметры пакетов и сетевых устройств, и это может сильно сказаться на требуемой точности результатов моделирования.

**NetSim**. Приложение Boson Netsim являет по сути своей эмулятором сетевых устройств компании Cisco. Программа позволяет работать с сетевыми устройствами, начиная от обычных управляемых свитчей и заканчивая роутерами 7-го поколения. В поставку включена утилита, в которой можно смоделировать любой тип сети или взять готовую из множества примеров.

**OMNeT++**. Многоцелевой дискретный инструмент моделирования событий. В OMNeT++ можно замедлить и ускорить моделирование, что может иметь важное значении при исследовании передачи пакетов различных категорий. Предоставляется возможность написания файлов трассировки.

**QualNet**. Продукт ориентирован на беспроводные сети, однако поддерживает и другие сетевые решения. Имеет очень современную библиотеку, что позволяет очень легко моделировать реальную сеть. Его GUI также очень современен: во время управляемого моделирования некоторые результаты могут быть активированы или дезактивированы, а скорость моделирования может быть замедлена или ускорена (однако анализ во время управляемого моделирования невозможен). Основной файл результатов содер-

жит статистическую информацию; возможна настройка собираемых параметров.

**AnyLogic**. Единственный симулятор, который поддерживает дискретный, длительный и гибридный методы моделирования. Его GUI имеет сложный дизайн для предоставления возможности получения быстрой сетевой модели, так как не «заточен» под ТКС. Доступен только для Windows.

При выборе средства имитационного моделирования механизма ДМ, под которым понимается возможность построения маршрута только через «доверенные» маршрутизаторы, следует учитывать целый ряд дополнительных характеристик. В частности, возможности работы с таблицей маршрутизации, поддержка протоколов сетевого и транспортного уровня, использование IP адресации и др.

В таблице приведены результаты сравнительного анализа рассмотренных средств имитационного моделирования на предмет исследования механизма ДМ.

**Средства имитационного моделирования**

| № п/п | Симуляторы / Характеристики | NS-2 | NS-3 | OPNET Modeler | Anylogic | OMNET+ | QualNet | NetSim |
|---|---|---|---|---|---|---|---|---|
| 1 | Операционная система и дружеские языки программирования | Unix, win. C++, OTcl | Unix, Socket programming, C++, Pythons | Unix, Win, MAC, C, C++ | Win, Java | Unix,Win CygWin, .Net, NED, C++, | Linux, Win, Java | Win, Linux, Java |
| 2 | Категория моделирования (дискретный или аналитический) | Dicrete | Dicrete | Dicrete, Hybrid & Analytical | Dicrete, Hybrid | Discrete | Dicrete | Discrete |
| 3 | GUI | – | – | + | + | + | + | + |
| 4 | Тип сети | Any | Any | Any | Any | Any | Mostly wireless | Any |
| 5 | Лицензия | ops | ops | ops/xops | xops | ops/xops | xops | xops |
| 6 | Простота использования | +/– | +/– | + | + | + | + | + |

Окончание

| № п/п | Симуляторы / Характеристики | NS-2 | NS-3 | OPNET Modeler | Anylogic | OMNET+ | QualNet | NetSim |
|---|---|---|---|---|---|---|---|---|
| 7 | TCP | + | + | + | + | + | + | + |
| 8 | MPLS | +/– | + | + | ? | + | + | + |
| 9 | BGP and IS-IS | + | + | + | + | + | + | + |
| 10 | Конфигурация QoS | + | + | + | + | + | + | + |
| 11 | IPSec | + | + | + | + | + | + | + |
| 12 | EIGRP | – | – | + | + | + | + | + |
| 13 | IGRP | + | + | + | + | + | + | + |
| 14 | IPv6 Addressing | + | + | + | + | + | + | + |
| 15 | OSPF | + | + | + | + | + | + | + |
| 16 | OSPF Аутентификация | + | + | + | + | + | + | + |
| 17 | Point-to-Point/Point-to-Multipoint Serial | + | + | + | + | ? | + | + |
| 18 | Политика маршрутизации | + | + | + | + | + | + | + |
| 19 | PPP and CHAP | + | + | + | + | + | + | + |
| 20 | Перераспределение маршрута | + | + | + | + | ? | + | + |

Сравнительный анализ показал, что большинство сетевых симуляторов подходит для исследования механизма ДМ в ТКС. Есть, правда, и некоторые нюансы, например:

• модели QualNet позиционируются как более сложные, поэтому обеспечивают более подробное моделирование и более глубокий анализ исследуемых процессов и явлений;

• наиболее неудобными с позиций GUI являются ns-2, 3, однако именно они наиболее отработаны и наименее затратны, etc.

С учетом вышеизложенного можно сделать вывод, что выбор «сбалансированного» сетевого симулятора для исследования механизма ДМ в ТКС будет в большей степени определяться сценарием модельного эксперимента и опытом работы исследователя с тем или иным продуктом.

**Литература**

1. *Svilen Ivanov.* Experimental validation of the ns-2 wireless model using simulation, emulation, and real network, WMAN 2007.

2. Scalable Network Technologies Inc. Qualnet 5.1 user's guide, June 2011.

3. *Pedro Velho and Arnaud Legrand.* Accuracy Study and Improvement of Network Simulation in the SimGrid Framework. SIMUTools 2009.

УДК 004.051

**Ю. В. Скворцов**

Санкт-Петербургский государственный
университет телекоммуникаций

# АНАЛИЗ ЭФФЕКТИВНОСТИ ПРИЛОЖЕНИЯ ДЛЯ ЧТЕНИЯ RRS НА ПЛАТФОРМЕ WINDOWS PHONE 7 С ЕДИНЫМ СЕРВЕРОМ-АГРЕГАТОРОМ

Для своевременного получения информации пользователям приходится часто проверять множество сайтов на наличие обновлений, и по мере роста количества источников это начинает занимать все больше и больше времени. Поэтому многие сайты стали использовать новостные ленты в форматах RSS/RDF/ATOM, которые обрабатываются так называемыми программами-агрегаторами. Они автоматизированно проверяют сайты и уведомляют пользователя, если те обновились. На сегодняшний день практически все известные сайты и платформы для ведения блогов имеют поддержку новостных лент в одном или нескольких указанных форматах.

Однако если обычные сайты разделяют новости на категории, то большинство популярных агрегаторов этого не делает, в результате новостной сайт может в день добавлять около 200 записей, большая часть которых пользователя не интересует. То есть налицо перекос между ак-

туальными информационными потребностями пользователя и предоставляемыми информационными возможностями сайта (в пользу последнего).

Было решено написать новый агрегатор, в котором можно было бы разделять данные на категории и в результате уменьшить «информационный шум». К сожалению, ни GoogleReader, ни Яндекс.Ленты не имели такой функциональности, поэтому пришлось делать серверную часть, так как для пользователя клиент-серверная система обладает неоспоримыми преимуществами в виде уменьшения трафика, фильтрования, скорости проверки новых данных и др. В качестве платформы была выбрана Windows Phone 7, так как на момент написания она только появилось, и поэтому большинство пользователей еще не успело установить какой-нибудь традиционный RSS-reader, а переход с привычной программы на новую без массивной рекламной компании представлялся слишком маловероятным.

В процессе работы над программой и сбора данных об информационных потребностях выяснилось, что большинство пользователей не удовлетворено текущими программами и хотело бы иметь бóльшую функциональность, чем предоставляли изданные на тот момент приложения. Эта функциональность была реализована в программе Iria.

Целью аналитического отчета, представленного в настоящей статье, является оценка эффективности особенностей приложения Iria, отсутствующих на аналогичных сервисах.

**О программе**

Клиентское приложение написано на языке C# с использованием .NET Framework 4.5, и использует следующий набор технологий: Silverlight – для графического интерфейса пользователя; HTML – для просмотра содержимого лент; SQL Server Compact Edition – как БД для локального кэша; Windows Communication Foundation.

Приложение работает в операционных системах Windows Phone 7.5 (Mango) и Windows Phone 8 и распростра-

няется через систему Windows Phone Marketplace в России, Казахстане и на Украине.

Серверная часть написана на языке C# с использованием .NET Framework 4.5, и включает следующие приложения и службы:

• Crawler – программа, скачивающая RSS-ленты и обновляющая БД сервера (запускается планировщиком задач ОС);

• Ageru – программа, отмечающая старые записи как прочтенные;

• WebService – служба, работающая с клиентом;

• Web – веб-сервер, обеспечивающий дополнительную функциональность, которую нельзя реализовать средствами службы, и предоставляющий доступ к администрированию и мониторингу статистики.

Сервер работает на ОС Windows Server 2008 R2 и использует следующий набор программ и технологий: SQL Server 2008 – СУБД; IIS 6 – служба, обеспечивающая работу WCF-службы и веб-сервера; Windows Scheduler – планировщик задач; LINQ; WCF.

Для взаимодействия клиента и сервера используется протокол SOAP.

**Категории**

На многих веб-сайтах поступающая информация разделяется по категории (которые могут именоваться иначе – теги, ключевые слова, или аналогичным образом), при этом на сайте есть только одна RSS-лента, в которую попадают все категории, а пользователю интересна лишь часть. Как правило, подобные ленты имеют один или несколько узлов <category>, которые можно использовать в качестве фильтра.

В настройках фильтров к ленте пользователю отображаются категории, когда-либо приходившие с этой лентой, и существует возможность указать, какие категории он хотел бы получать. В анализируемой программе можно выбрать все сообщения, попадающие в определенные категории. Можно убирать не интересующие категории и пока-

зывать все остальное. Третий режим является комбинацией первого и второго вариантов, при этом запрет имеет приоритет над показом. Например, выбрав разрешение на показ новостей из России и запретив показ категории «оружие», не будет показываться даже оружие, изготовленное в России.

Согласно статистике, 70% активных пользователей имеют хотя бы один установленный фильтр по категориям, при этом запрещающие фильтры использует 5%, а третий режим не используется вовсе.

Использование категорий на некоторых сайтах может быть затруднено тем, что количество категорий на них так велико, что пользователи зачастую закрывают список сразу после его получения. Тем не менее статистика использования показывает, что эта одна из наиболее популярных возможностей программы, так как позволяет получать более актуальную и нужную информацию, которую легко можно настроить «под себя».

**Группировка**

Некоторые сайты имеют схожую тематику, и поэтому некоторым пользователям хотелось иметь возможность читать RSS про автомобили Ferrari и BMW с одной страницы; при этом реально информация бралась бы со многих сайтов. Пользователь сам определяет для себя группы и добавляет в них элементы через контекстное меню.

Согласно статистике использования, количество пользователей этой функциональности уменьшилось с 5% в первые месяцы работы программы до нуля в настоящий момент. Поэтому в последующих версиях программы группировка, вероятно, будет убрана, так как она оказалась нужной слишком малому количеству людей и в то же время достаточно сложной для поддержания этой функции.

**Удаление рекламы**

Некоторые сайты добавляют рекламу в свои RSS-потоки. В отличие от страниц в Интернете, RSS-сообщения, как правило, имеют небольшой объем, поэтому добавление рекламы в конец маленьких блоков сильно снижает удов-

летворенность пользователей от просмотра содержимого, так как на каждые 4–5 строк текста приходится примерно равный или больший по высоте рекламный блок. Программа Igia имеет антирекламный фильтр, который позволяет вырезать рекламную часть.

В первых версиях программы существовала «волшебная кнопка», позволяющая пожаловаться администратору, после чего администратор должен был сформировать и добавить новое правило для ленты. В большинстве случаев эта кнопка нажималась даже тогда, когда лента не содержала рекламы, и при этом требовалось следить за этими сообщениями, что являлось значительным неудобством для поддержания программы. Поэтому в следующей версии серверной части была реализована полностью автоматическая проверка на основе анализа последних сообщений.

Это достаточно сложная для оценки эффективности функциональность, так как сервер не содержит статистику использования этой функциональности и единственными данными по ней являются отзывы пользователей. Согласно отзывам по электронной почте, никто с рекламой не сталкивался – бóльшая часть пользователей считала, что в RSS реклама всегда отсутствует.

**Устаревание**

Существуют категории сайтов, информация на которых актуальна только ограниченное количество времени. На таких сайтах может быть размещена информация о концертах, скидках, и, если не прочитать ее вовремя, она становится бесполезной. В программе присутствует возможность отмечать записи, непрочитанные за указанный временной промежуток, как прочитанные. Можно указать число дней от одних суток до 20 дней.

Подобной функциональностью пользуется 30% активных пользователей, при этом одни сутки установлены в 35% случаев, а 2 дня установлено в 25%. Ленты, для которых установлена эта возможность, имеют более 30 сообщений в день.

**Фоновая программа**

Фоновая программа обеспечивает вывод на рабочий стол пользователя количества обновленных лент, используя «живые иконки» (live tiles, обновляющаяся пиктограмма, отображающая пользователю состояние программы), и «тосты» (Toast notifications, маленькое информационное окно). Есть возможность получения как просто уведомлений, так и полной загрузки новых записей.

50% активных пользователей используют эту функциональность, из них 30% закачивают новые записи, 85% используют «тосты» (а «живая иконка» обновляется всегда). Многие пользователи жаловались, что при использовании данной функциональности программа будит их информационным уведомлением, даже несмотря на то, что в ночное время сообщения отключены, поэтому в следующей версии была добавлена возможность отключать их и в дневное время, которой воспользовались 15% людей.

**Сообщения за определенную дату**

Еще одной уникальной возможностью программы является получение и просмотр сообщений за определенную дату для ленты или группы лент.

Сервер не отслеживает количество уникальных пользователей этой функциональности, а только число обращений к данной функции. Данной возможностью пользуются в среднем 34 раза за сутки (при 700 запросах лишь последних сообщений).

**Быстрый старт**

Для быстрого начала работы с программой пользователю предлагается список подготовленных администратором разделов, в котором пользователь может быстро подписаться на ленты. В настоящий момент в список разделов входят: информационные технологии, включающие ленты о программном и аппаратном обеспечении, телефонах, некоторых фирмах; новости; юмор; блоги; спорт. Количество лент, входящих в каждый раздел, варьируется от 4 до 11.

90% всех подписок на ленты осуществляются в пределах этого списка, что можно объяснить его достаточно

полным охватом наиболее популярных ресурсов. Либо пользователи просто хотят получить ту или иную информацию наиболее простым способом, просто выбирая из предложенного списка.

**Добавление лент**

Первоначально ленты можно было добавлять, лишь вводя URL RSS-ленты. Однако оказалось, что большинство пользователей вводит лишь адрес сайта, его части, или просто поисковые запросы. В настоящий момент программа поддерживает все типы ввода; при вводе адреса сайта сервер загружает страницу и пытается найти на ней отсылки на RSS/ATOM ленты, после чего возвращает полученный список клиенту.

**Социальные сети – поделиться**

Данная возможность появилась благодаря настойчивым просьбам некоторых пользователей. Самой важной частью социального взаимодействия является возможность поделиться RSS-сообщением через ВКонтакте и Твиттер.

К сожалению, в Твиттере не публикуется информация об использовании приложения, зато ВКонтакте предоставляет достаточно полную информацию об использовании социального компонента программы. В среднем, каждый день пользователи публикуют 15 ссылок, 99,54% – это мужчины, 70% имеют возраст от 27 до 35; 91% из России, и по городам Москва, Санкт-Петербург, Воронеж имеют 34, 19 и 15% соответственно. Скорее всего, половой и возрастной перекос связан с не очень удачным текстом, описывающим программу, поэтому он охватывает в основном только мужчин от 27 до 35 лет.

Проведенный анализ эффективности приложения Iria в контексте его функциональных особенностей дает разработчикам необходимую информацию по их использованию, рациональности их применения в программах-аналогах на других платформах.

## *Раздел 2*

# ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056

**В. Г. Петров, Д. М. Шакин**
ФСТЭК России
по Северо-Западному федеральному округу

## ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

*Информация пронизывает все поры жизни людей и общества.*
Академик, инженер-адмирал А. И. Берг [1]

Современное общество вступило в постиндустриальный период своего развития, который по сути своей назван информационным.

По мнению авторов концепции «информационного общества», этот период добавил к трем известным человечеству способам накопления национального богатства путем накопления капитала, военных захватов и территориальных приращений – четвертый способ, заключающийся в *«использовании технологий, позволяющих переводить нематериальные ресурсы* (прежде всего информацию. – *примеч. авт.) в материальные ресурсы»* [2].

При этом в странах с инновационным развитием экономики перевод нематериальных ресурсов (так называемых «нересурсов») в материальные ресурсы стал основным способом создания богатства. Этот значимый фактор развития общества не умаляет значения материальных ресурсов, а свидетельствует об усилении взаимного влияния состояния пары «материальные – нематериальные ресурсы» друг на друга и на безопасность социума в целом. Осозна-

ние этой закономерности позволило в 1976 г. американскому исследователю Т. Рона в отчете, подготовленном им для корпорации «Боинг», впервые сформулировать вывод о том, что *«информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время она* (информационная инфраструктура экономики. – *примеч. авт.*) *становится уязвимой целью, как в военное, так и в мирное время»* [3].

Информация стала стратегическим национальным ресурсом, «мишенью» и эффективным оружием развитых стран мира в геополитической конкуренции.

Следуя логике современной политической социологии, созданные в целях прогресса технические средства и информационные технологии не только привели к информатизации общества, но и породили современные информационные опасности. Стремление преодолеть информационные опасности порождает необходимость дальнейшего развития технических средств и технологий защиты и далее, по принципу обратной связи, приводит к возникновению новых информационных опасностей на более высоком уровне их развития [4].

Так, в 60-х гг. прошлого века, начиная с Соединенных Штатов Америки, в мире закономерно возникло новое социальное явление – «преступность в информационной сфере» или «киберпреступность», и появились новые социальные группы профессиональных преступников – «хакеры», а само общество приобрело черты «глобального информационного общества».

По мнению ведущего специалиста Европейской рабочей группы по оружию нелетального действия (*EWG-NLW*) доктора Джорджа Б. Александера, именно *страны с наиболее информатизированным обществом в мире являются ранимыми от информационных атак, от которых застрахованы страны с аграрной экономикой.*

*«В развитии информационных технологий заложен парадокс: распространение информации – это сила, в то время как открытость информационных систем является*

*их слабостью. Поэтому демократии, с присущей им открытостью, уязвимы для информационного оружия»* [5].

*«Арабская весна»*, по словам Президента Российской Федерации В. В. Путина, *ярко продемонстрировала, что Интернет и социальные сети превратились в эффективный инструмент политики, требующий осмысления для того, чтобы уменьшить риск использования* (информационных средств, систем и технологий. – *примеч. авт.) террористами и преступниками»* [6].

«Информационный терроризм» стал неотъемлемым атрибутом глобального информационного общества.

Любой терроризм, в том числе и информационный, представляет собой способ управления обществом посредством превентивного устрашения [7].

При этом любое проявление терроризма по сути своей носит именно информационный характер. Это утверждение авторов основывается на том, что обязательным условием терроризма является резонанс террористической акции в обществе.

Терроризм принципиально декларативен.

*Широкое распространение информации о теракте, превращение его в наиболее обсуждаемое событие представляет собой ключевой элемент тактики терроризма.*

Оставшийся незамеченным или засекреченный теракт утрачивает всякий смысл.

Авторы считают информационный терроризм *проявлением крайнего экстремизма в информационной сфере*, направленным на достижение *политических целей* через выдвижение отдельными лицами или организованной группой лиц, требований к властным структурам, которые не могут быть удовлетворены в рамках существующего правового поля.

Цели информационного терроризма реализуются с использованием *информационных средств* и *информационных технологий*, применение которых непосредственно влечет или потенциально может повлечь за собой угрозу жизни или здоровью людей, значительный по масштабу и

уровню ущерб материальным объектам, а также другие последствия, которые создадут в обществе атмосферу страха и напряженности.

Авария на Саяно-Шушенской ГЭС в августе 2009 г. и взрыв на Баксанской ГЭС в июле 2010 г. не оставили сомнений в том, что деструктивное воздействие на элементы национального хозяйственного комплекса способно привести к дезорганизации управления экономикой, угрозе безопасности жизнедеятельности населения и снижению уровня национальной безопасности. При этом подобные катастрофические последствия могут быть вызваны не только прямым физическим воздействием на критически важные объекты топливно-энергетического комплекса, но и организацией удаленного деструктивного информационного воздействия[1] на автоматизированные системы управления производственными и технологическими процессами критически важных объектов национального хозяйственного комплекса.

Известно, что компьютерный вирус Stuxnet нанес ущерб ядерным объектам Ирана, сопоставимый с ущербом от атаки израильских Военно-воздушных сил.

В отличие от обычного терроризма, информационный терроризм использует более совершенные – инновационные инструменты скрытого и удаленного деструктивного информационно-технического воздействия. По мнению ряда специалистов, эволюционирование вредоносных компьютерных программ – компьютерных вирусов (Stuxnet – Dugu – Wiper – Flame – Gauss –...?), происходит по пути

---

[1] Под деструктивным информационным воздействием на автоматизированные системы управления производственными и технологическими процессами авторы предлагают понимать несанкционированное информационное воздействие на элементы критической информационной инфраструктуры ТЭК и обеспечивающие их взаимодействие информационно-телекоммуникационные сети. Результатом подобного воздействия могут стать возникновение аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизация работы органов власти, предприятий, организаций, нанесение материального ущерба в крупном размере, смерть или нанесение тяжкого вреда здоровью хотя бы одного человека и (или) иные тяжелые последствия.

расширения их функциональных возможностей и перечня объектов деструктивного воздействия.

Анализ угроз деструктивных информационных воздействий с террористическими целями на автоматизированные системы управления производственными и технологическими процессами критически важных объектов национального хозяйственного комплекса позволяет сделать следующие выводы.

1. К числу вероятных сценариев кибертеррористической атаки на критически важные объекты национального хозяйственного комплекса следует отнести те, которые обеспечивают не только временную или полную потерю их функциональности, но и, как следствие (вторичный эффект), создают широкомасштабную чрезвычайную ситуацию с высоким уровнем материальных, человеческих и др.

2. Реализация таких сценариев с высокой вероятностью будет осуществляться группой координирующих свои действия агентов из разных точек сетевой среды, которые обеспечивают доступ к ресурсам объекта атаки, в том числе, из точек, расположенных вне страны, объекты которой подвергаются атаке.

3. Наиболее значимыми с позиции величины потенциального ущерба (социального, материального, политического) являются:

а) сложно предотвращаемые в оперативном порядке распределенные атаки на отказ в обслуживании (*DDoS – Distributed Denial of Service*);

б) комплексные атаки, результатом которых является получение контроля над управляемым производственным объектом или важными технологическими процессами, обеспечивающими его функционирование по назначению.

Отличительной особенностью каждой из представленных выше атак является тот факт, что сценарии их реализации предполагают многоэтапную подготовку и скоординированный характер действий группы террористов, распределенных по сетевой среде.

Это обстоятельство указывает на необходимость детального изучения подобных сценариев, требует разра-

ботки средств противодействия им на всех уровнях обеспечения информационной безопасности критически важных объектов. Эффективное использование таких знаний и средств противодействия возможно только на основе скоординированных действий всех организаций, задействованных на обслуживании информационных систем и средств телекоммуникаций, которые могут быть использованы для проведения кибертеррористических атак. Такая консолидация необходима на всех этапах – от анализа возможности организации тех или иных атак, сценариев их реализации, мониторинга состояния инфокоммуникационной инфраструктуры на предмет наличия деструктивных воздействий до совместных действий на этапе выработки мер оперативного реагирования и средств противодействия.

Принимая во внимание транснациональный характер сетевой среды и энергетической инфраструктуры, который эта среда поддерживает, большую роль в создании эффективной системы противодействия кибертеррористической угрозе призвана сыграть консолидация сил на международном уровне.

Усиление угрозы кибертерроризма, рост числа противоправных деяний с использованием информационных и коммуникационных технологий (кибератак) определили необходимость системного решения проблемы *обеспечения антитеррористической защищенности* критически важных объектов национального хозяйственного комплекса в информационной сфере.

Логично предположить, что поэтапно создаваемая «Национальная система антитеррористической защищенности критически важных объектов инфраструктуры Российской Федерации», по мнению авторов, должна содержать ряд важнейших взаимосвязанных элементов, реализуемых в строго очерченном нормативном правовом поле и при обязательном государственном регулировании.

К числу основных элементов такой системы целесообразно отнести [8]:

1) *единую государственную систему обнаружения и предупреждения компьютерных атак*[1] на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов;

2) *силы обнаружения и предупреждения компьютерных атак.*

К ним относятся уполномоченные подразделения федерального органа исполнительной власти, а также физические лица, осуществляющие эксплуатацию автоматизированных систем управления КВО и принимающие участие в обнаружении и предупреждении компьютерных атак на критическую информационную инфраструктуру, мониторинге уровня ее реальной защищенности и ликвидации последствий компьютерных инцидентов[2];

3) *средства обнаружения и предупреждения компьютерных атак.* К ним относятся технические, программные, лингвистические, правовые, организационные средства и информационные технологии, предназначенные для обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру, мониторинга уровня ее реальной защищенности и ликвидации последствий компьютерных инцидентов;

4) *силы ликвидации последствий компьютерных инцидентов* в критической информационной инфраструктуре. В состав указанных сил входят уполномоченные подразделения федерального органа исполнительной власти и физические лица, осуществляющие эксплуатацию автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры, включая разработчиков аппаратных средств и программного обеспечения, используемых в автоматизированных системах управ-

---

[1] Компьютерная атака – целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети специальными программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях.

[2] Компьютерный инцидент – факт нарушения штатного режима функционирования элемента критической информационной инфраструктуры или критической информационной инфраструктуры в целом.

ления ТП, принимающие участие в восстановлении штатного режима функционирования после компьютерных инцидентов;

5) *средства ликвидации последствий компьютерных инцидентов* в критической информационной инфраструктуре – информационные технологии, а также технические, программные, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, предназначенные для восстановления штатного режима функционирования элементов критической информационной инфраструктуры после компьютерных инцидентов.

Авторы не без основания полагают, что решая проблему обеспечения антитеррористической защищенности критически важных объектов национального хозяйственного комплекса в информационной сфере, необходимо использовать опыт ФСТЭК России по обеспечению безопасности ключевых систем информационной инфраструктуры.

Методическими документами ФСТЭК России регламентированы технические требования не только к средствам защиты информации, но и к организации процессов управления информационной безопасностью ключевых систем информационной инфраструктуры. Реализация подобного комплекса технических мер и организационных мероприятий на критически важных объектах национального хозяйственного комплекса страны позволит обеспечить их антитеррористическую защищенность в информационном пространстве.

По мнению авторов, основными направлениями деятельности по решению проблем информационной безопасности в современном российском обществе являются следующие.

1. Теоретическое обоснование (уточнение) периодизации, особенностей и противоречий становления информационного общества в Российской Федерации, формирование (уточнение) системы терминов и категорий предметной области.

2. Формирование нормативного правового и методического обеспечения противодействия угрозам использования информационных технологий в преступных целях, в том числе террористического характера.

3. Обеспечение суверенности права в информационном обществе, развитие технологий защиты информации в целях обеспечения неприкосновенности частной жизни, формирование информационной культуры.

4. Обеспечение технологической независимости, разработка, организация выпуска отечественной компонентной электронной базы (ЭКБ), приоритетное развитие рынка российских программных продуктов и высокотехнологичного производства.

Обеспечение информационного суверенитета Российской Федерации.

Проблема обеспечения информационной безопасности в современном обществе является приоритетной среди других проблем национальной безопасности. Важно отметить, что эта проблема касается всех: человека, общества, государства. Включает в себя не только организационно-технические вопросы, но и втягивает в свою орбиту правовые и социальные аспекты, а также задачи обеспечения информационно-психологической безопасности [9].

**Литература**

1. *Берг А. И.* Кибернетика – наука об оптимальном управлении. – М.: Энергия, 1964.

2. *Тоффлер О.* Смещение власти: знание, богатство и принуждение на пороге XXI века. – М.: Изд-во АН СССР, 1991.

3. *Thomas P. Rona.* Weapon Systems and Information War. Boeing Aerospace Co., Seattle, WA, 1976.

4. *Шакин Д. Н.* и др. Информационная безопасность: Коллективная монография. – М.: Оружие и технологии, 2009.

5. *Пирумов В. С.* Информационное противоборство. Четвертое измерение противостояния. – М.: Оружие и технологии, 2010.

6. *Путин В. В.* Россия и меняющийся мир // Московские новости. 2012. № 221. 28 февр.

7. International Crime Treat Assessment, 2000 [Электронный ресурс]. URL: http://clinton4.nara.gov/WH/EOP/NSC/html/documents/pub45270/pub45270index.html (дата обращения: 01.10.2012).

8. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, 04.07.2012 [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/6/113.html (дата обращения: 01.10.2012).

9. *Азамов О. В.* и др. Информационная безопасность [Электронный ресурс]. URL: http://naukaxxi.ru/materials/41 (дата обращения: 01.10.2012).

УДК 004.056

**А. А. Марков, Ю. Р. Акчурина**

Санкт-Петербургский государственный инженерно-экономический университет

# СОВРЕМЕННЫЕ ГЛОБАЛЬНЫЕ ИНФОРМАЦИОННЫЕ УГРОЗЫ И ИХ ИСТОЧНИКИ

Глобальный характер информационных угроз и их источников в настоящее время недостаточно изучен и учитываем разве что при исследовании национальных информационных угроз. Причина этому, на наш взгляд, находится в наднациональном и надгосударственном понимании глобальности информационных угроз. Иными словами, глобальная угроза (и не только информационного характера) не направлена конкретно против какого-то государства или его социума. Это, естественно, не предполагает обязательности управленческих, правовых и организационных решений для реализации должного противодействия такой угрозе со стороны отдельного государства или нации.

Чаще всего реакция на подобные угрозы заключается в некоем коллективном документе (декларации, коммюнике, обращении и др.), принимаемом руководством ряда/многих государств на всемирном или континентальном уровне. Такой документ, по сути, содержит общее признание существования глобальной проблемы или угрозы и декларативные призывы к решению данной проблемы или

угрозы, которые рассчитаны только на добрую волю государств и их наций к взаимному сотрудничеству по решению или предотвращению проблемы/угрозы, но не являются предписывающими и требующими немедленной реакции. Примером тому является проблема (угроза) глобального потепления, о которой с достаточным беспокойством сообщается на самых серьезных международных форумах и саммитах, предлагаются различные решения. Но по большому счету до сих пор нет выработанного единого мирового подхода к решению данной проблемы, потому что данная проблема не является национальной или государственной. Например, Киотский протокол для ряда ведущих государств мира представляет большую проблему в плане подписания, ибо он не соответствует национальным интересам больше, нежели глобальное потепление.

Несмотря на то, что мировое сообщество признало существование глобального информационного пространства и эволюцию развития цивилизации в постиндустриальной эре на основе информационного общества, проблемы и угрозы обеспечения глобальной информационной безопасности конкретные социумы не интересуют, ибо не затрагивают их интересы. Все может измениться только в том случае (как с той же проблемой глобального потепления), если какая-либо глобальная угроза превратится в национальные угрозы, т. е. будет спроецирована на жизненно важные интересы конкретного общества и государства, т. е. приобретет естественный социально выраженный характер.

На наш взгляд, можно выделить следующий ряд источников глобальных информационных угроз, которые на данное время являются наиболее актуальными.

*В технических процессах формирования информационной безопасности:*

1) глобальная компьютеризация, активно внедряющаяся в различные системы управления, в том числе государственные и военные различных стран, даже при наличии сложных схем дублирования и защиты, остается уязвимой не только по причине возможных технических сбоев, но и под влиянием неодолимой силы, т. е. внешних об-

стоятельств (землетрясение, наводнение, энергетическая авария и др.), которые могут вызвать неконтролируемую искаженную работу компьютерных программ, результатом чего может быть локальная или всемирная техногенная катастрофа, непредвиденный военный конфликт, навигационные проблемы и т. д.;

2) хакерство. Сегодня хакеры представляют собой интернациональное виртуальное сообщество, располагающее в сети значительными информационными и интеллектуальными ресурсами и механизмами самоорганизации своей деятельности. В зависимости от мотивов деятельности субкультуры хакеров С. В. Масленченко делит их на следующие группы. *«Белые» хакеры* – малочисленная группа, оказывающая помощь программистам и пользователям в совершенствовании управления компьютером и виртуальными сетями, модернизации и создании новых программ, борьбе с «черными» хакерами. *«Черные» хакеры*, или *кракеры*, занимаются несанкционированным доступом к сетям и информации. В зависимости от целей деятельности в кракерской среде можно выделить следующие группы: *вандалы*, главная цель которых – взломать систему для ее дальнейшего разрушения; *шутники* действуют для достижения известности путем взлома компьютерных систем и внесения туда различных юмористических (с их точки зрения) эффектов; *взломщики* – профессиональные кракеры, действующие с преступной целью кражи или подмены хранящейся информации; *пираты* воруют свежие программы с помощью средств, самостоятельно разработанных или заимствованных у взломщиков, и обладают определенной специализацией: *пираты-взломщики* взламывают компьютерную защиту, *пираты-курьеры* копируют ворованное программное обеспечение на свой компьютер, *пираты-дистрибьюторы* занимаются распространением ворованного ПО; *шпионы* охотятся за секретной информацией; *кардеры* используют чужие (ворованные) кредитные карты для электронной оплаты товаров или услуг; *фишеры* – интернет-мошенники, выдающие свои страницы за

сайты других; *фрикеры* осуществляют взлом телефонных автоматов и сетей, обычно с целью получения бесплатных звонков или связи с Интернетом; *спамеры* занимаются формированием и рассылкой непрошеной корреспонденции рекламного характера и обладают внутренней специализацией: *спамеры-кракеры* создают программы для сбора адресов компьютеров пользователей с сайтов и форумов и превращения их в машины для рассылки спама, *спамеры – собиратели баз данных* обслуживают нужды рассыльщиков и собирают для них почтовые адреса, которые объединяют в базы адресов, *спамеры службы рассылок* рассылают спам. В качестве социальной базы индустрии, обслуживающей кракеров, традиционно выступают *клаберы* (постоянные посетители компьютерных клубов) и *геймеры* (любители компьютерных игр) как агенты, разносящие вирусосодержащее программное обеспечение и спам[1].

Мы намеренно дали расширенную характеристику хакерской субкультуры, чтобы продемонстрировать социальную масштабность и разносторонность хакерских «притязаний» на виртуальное пространство. Знание ими этого пространства и эксплуатация в своих интересах способны дестабилизировать мировое информационное сообщество, потому что данные интересы могут быть сопряжены с корыстными, агрессивными, амбициозными, разрушительными и другими осознанными или спонтанными целями (например, от несанкционированного доступа в банковскую сеть для незаконного обогащения и взлома секретных и военных компьютерных баз ради шутки до «запуска» в сеть Интернет эффективных вирусов, способных уничтожить как локальные, так и глобальные форматы данной сети). Такие хакерские действия могут привести к нарушению правильной работы информатизационных и информационно-коммуникационных систем и технологий, чем вызвать существенные сбои в национальных и глобальных системах управления важнейших отраслей обес-

---

[1] См.: *Масленченко С. В.* Субкультура хакеров как порождение информатизации общества: Автореф. дис. ... канд. культ. наук. – СПб.: СПбГУ, 2008.

печения жизнедеятельности национальных и мировых социумов;

3) совершенствование технического прогресса. Как ни парадоксальна на первый взгляд данная угроза в плане эволюции мирового сообщества, на наш взгляд, она имеет обоснование. Современные информатизационные системы и информационно-телекоммуникационные технологии (ИКТ) развиваются быстрыми темпами, и все чаще работу таких систем контролирует не человек, а аналогичные защитные или дублирующие электронные системы. Участие в данных процессах человека становится все более опосредованным, а не управляющим действием. Автоматизированные компьютерные системы управления и контроля за управлением (АКСУ) уже являются саморегулируемыми в организации, ведении и коррекции любых информатизационных процессов. В перспективе участие человека в этом плане может быть сведено к предельному минимуму либо к созданию элитных специальных коллективов (подразделений), которым будет предоставлено право контроля подобных процессов, что даст им преимущественную возможность воздействия на различные глобальные и национальные эксцессы и события, сопряженные с информационной средой, и управления ими. Это приведет к узурпации властных полномочий, доминированию своего положения отдельными национальными и наднациональными группами, соответственно – к конфликтным ситуациям и негативным последствиям для цивилизации.

*В психофизических процессах формирования информационной безопасности:*

1) нерегулируемый рост информационных потоков в ИКТ. На сегодняшний день глобальное информационное пространство предельно насыщено не только полезной, но и вредной информацией, распространяющей асоциальные, агрессивные, человеконенавистнические, террористические, экстремистские, порнографические, аморальные и т. п. сведения, установки, инструкции, демонстрации, направленные на негативное восприятие действительности, на мани-

пулирование и коррекцию общественным и индивидуальным сознанием, на пропаганду и воспитание в индивидууме и обществе фобий, радикальных, экстремистских, мизантропических идей и воззрений. Любая поисковая система в сети Интернет способна оперативно предоставить такую информацию для глобального пользователя. Тем самым возникает опасность формирования интеллектуального зомбирования личности, в потенциале – социальных групп, в перспективе – социума, безотносительно национальной принадлежности и ментальных качеств;

2) усиление воздействия на сознание и психику человека. Глобальный характер ИКТ оказывает возрастающее давление на поведенческие парадигмы личности. Рекреативные и иные функции и возможности современных ИКТ (от персональных компьютерных игр до массовых коммуникационных развлечений (например, ТВ-шоу)) привлекают огромное количество людей, которые основное времяпрепровождение отдают электронным формам досуга, подпадая под информационную зависимость от данных технологий. Это приводит к изменению, поражению и трансформации психики и сознания человека, а также асоциальности и девиантности поведения социально-неустойчивых групп. Уже нередки случаи, когда человек теряет способность реального и виртуального восприятия действительности, что приводит его к инфантильному или криминальному реагированию на эту действительность. Совершенствование ИКТ будет способствовать прогрессу таких явлений;

3) информационно-коммуникационные технологии все чаще заменяют собой иные возможности познания мира. ИКТ превратились в самую мобильную и эффективную силу, обучающую, воспитывающую, диктующую определенную систему современных норм поведения и духовных ценностей, тем самым оставляя вторичными традиционные схемы воспитания и развития личности. Заданная техногенность подобного воздействия на воспитательные и развивающие параметры личности ограничивают процессы

познания ею действительности, сводя их к жестким информационным форматам. Таким образом, индивид или социальная группа сегодня и в дальнейшем все чаще и легче будет воспринимать организационно-коммуникационные механизмы собственного формирования, являющиеся искусственными и навязываемыми, нежели будет формироваться как личность на основе спонтанного, эмпирического познания действительности.

УДК 004.056

**Т. Н. Нестерук**

Санкт-Петербургский государственный инженерно-экономический университет

**Ф. Г. Нестерук**

НИЛ ПКБ СПИИРАН

## ВЛИЯНИЕ УЯЗВИМОСТЕЙ В WEB-ТЕХНОЛОГИЯХ НА УПРАВЛЕНИЕ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

Угроза безопасности как со стороны стороннего злоумышленника, так и изнутри компании может отрицательно повлиять на репутацию бренда, акционерную стоимость компании, повлечь за собой утечку конфиденциальной бизнес-информации и, как результат, серьезные финансовые потери.

Знания и умения использовать на практике стандарты и практики управления непрерывностью бизнеса – BCM (Business Continuity Management) необходимы сегодня любым предприятиям – убытки, вызванные нарушением нормального функционирования бизнес-процессов, постоянно растут.

Эксперты системных администраторов и администраторов безопасности различают план непрерывности бизнеса (BCP) и план аварийного восстановления (DRP). При

этом BCP в отличие от DRP играет основную роль в программе управления непрерывностью бизнеса организации. Основные этапы жизненного цикла разработки BCP:

- этап программы управления непрерывностью бизнеса, где рассматриваются вопросы политики, актуальности, области действия BCM, основных целей и задач программы, управления затратами на программу и т. д.;
- анализ требований к программе BCM, дается краткая характеристика деятельности организации, проводится оценка воздействия на бизнес, оценка существующих угроз, таких как воздействие на инфраструктуру, нарушение финансовой устойчивости и пр., а также проводится всесторонняя оценка рисков;
- определение стратегии BCM. Стратегия детально рассматривает действия в отношении технологий, информационных активов (защита электронных данных, безопасность отчуждаемых носителей информации, доступность аппаратно-программных активов) и др.;
- формирование планов реагирования на инциденты (Incident Management Plan, IMP) и непрерывности бизнеса (Business Continuity Plan, BCP);
- поддержка и сопровождение программы BCM в соответствии с потребностями бизнеса для обеспечения его непрерывности;
- формирование культуры BCM в организации.

Параллельно с анализом критичности бизнес-процессов и зависимости масштабов потерь от нарушений функционирования бизнес-процессов рекомендуется проводить анализ информационных сервисов с привязкой к бизнес-процессам и информационным потокам, например, на основе хранилища данных, информационного портала, корпоративной электронной почты – любого web-сервиса, различным образом задействованного в бизнес- процессах компании. При выборе информационных сервисов производятся анализ возможных нарушений в их функционировании и предварительная оценка значимости сервисов с точки зрения бизнеса.

Безопасность процессов и систем требует анализа уязвимостей и выявления «узких мест» и точек возникновения риска в технологиях и бизнес-процессах.

Одним из наиболее распространенных путей проникновения в корпоративные информационные системы являются уязвимости web-сайтов и web-приложений. Недооценка риска, который могут представлять уязвимости в web-ресурсах, доступные из сети Интернет, является, возможно, основной причиной низкого уровня защищенности большинства из них. Большинство web-приложений содержит уязвимости различной степени критичности в результате недостаточного внимания к вопросам безопасности и качества программного кода.

Самым популярным языком программирования web-приложений по результатам анализа уязвимостей, проведенного специалистами по информационной безопасности, оказался PHP – на нем написано 63%, ASP.NET (19%), Java (14%). Остальные языки программирования встречаются гораздо реже. Проведенное сравнение защищенности сайтов на языках PHP, ASP.NET и Java по уязвимостям, обусловленным ошибками в программной реализации, составило, соответственно, 81, 26 и 59%. PHP оказался самым незащищенным, соответственно, наименее подвержены уязвимостям – сайты на ASP.NET.

Две наиболее распространенные угрозы, связанные с передачей входных данных web-приложению, – атаки с применением кросс-сайтовых сценариев и с внедрением злонамеренного SQL-кода (SQL-инъекция).

При атаке с применением кросс-сайтовых сценариев (межсайтовый скриптинг или XSS) в параметр, определяющий выводимые пользователю данные, передается сторонний программный код. Иначе говоря, это уязвимость, при которой атакующий посылает злонамеренные данные (обычно это HTML, содержащий код JavaScript), которые возвращаются приложением, что вызывает исполнение JavaScript кода. Является критичной уязвимостью, так как взломщик может получить конфиденциальные данные,

хранимые в браузере клиента. Для борьбы с XSS-атаками можно сделать одним из элементов своей стратегии проверки ввода отклонение любых входных данных, которые могут содержать XSS-сценарии, и использовать HTML-кодирование любых входных данных, эхо которых возвращается клиенту, это делает XSS-сценарии абсолютно безвредными.

При атаке с внедрением злонамеренного SQL-кода фрагменты SQL-запросов, сформированные специальным образом, встраиваются во входные данные, используемые при динамическом конструировании SQL-запросов. Также является критичной уязвимостью, так как взломщик может получить конфиденциальные данные, хранимые в базе данных. Для изменения запроса взломщик может использовать следующие конструкции: SELECT, UNION, UPDATE, INSERT, OR, AND. Для защиты от атак с внедрением SQL-кода требуется строгая проверка входных данных на допустимость и отказ от динамического построения SQL-запросов на основе данных, вводимых клиентом. Вместо этого можно использовать фиксированные запросы или хранимые процедуры со строго типизированными параметрами, которые инициализируются данными, вводимыми клиентом.

Для того чтобы в web-приложении не возникло потенциальных уязвимостей, нужно использовать передовые методики защиты, следовать этим методикам на этапах проектирования, разработки и развертывания. Поскольку постоянно изобретаются новые классы атак и новые способы эксплуатации уязвимостей ПО, нужно сокращать области, доступные для атак, и поддерживать многоуровневую защиту в течение всего жизненного цикла приложения, в будущем это поможет защититься от атак, которые не всегда можно предвидеть. Для защиты от этого класса угроз существуют специализированные средства защиты, которые называются Web Application Firewall (WAF). Помимо защиты самих web-приложений насущно необходимо обеспечить защиту и разграничение доступа к СУБД, к

которой обращается приложение, соответствующие решения могут предложить компании Imperva и Fortinet. Эти решения легко интегрируются в существующую инфраструктуру, не требуют перезагрузки или внесения изменений на защищаемых ресурсах и обладают богатым функционалом:

- анализ структуры web-приложений и поведения пользователей в автоматическом режиме;
- поиск и классификация информации в СУБД и на файловых серверах;
- оценка уязвимости СУБД;
- интеллектуальные механизмы защиты приложений и СУБД;
- репутационный анализ внешних пользователей;
- аудит доступа к СУБД и файловым серверам;
- контроль прав доступа к СУБД и файловым серверам;
- оповещение в режиме реального времени;
- интеграция со службами каталогов;
- возможность работы как в режиме мониторинга, так и в режиме активной блокировки.

При сравнении уязвимостей в зависимости от использованных web-серверов (наиболее часто используемые – Microsoft IIS, Apache, nginx) можно отметить минимальное количество уязвимостей, связаннных с web-сервером Microsoft IIS, а nginx-сервер превосходит все остальные web-серверы по количеству уязвимых сайтов для всех типов уязвимостей, связанных с ошибками администрирования.

Анализ защищенности web-ресурсов, принадлежащих к различным отраслям экономики, показал, что лидером по количеству уязвимых сайтов оказался телекоммуникационный сектор, это обусловлено пестрым разнообразием типов систем, которое зачастую становится следствием роста компаний, а также сделок по слиянию и поглощению.

Относительно низкая доля сайтов, содержащих критические уязвимости, была выявлена в финансовом секторе (43%), а в системах дистанционного банковского обслуживания, ДБО, критичные бреши практически истреб-

лены. Однако в этой сфере присутствуют специфические уязвимости – CSRF (Cross-Site Request Forgery, найдена в 6% систем ДБО), XSS (Cross-Site Scripting, 18%), которые не представляют большой опасности, но способны облегчить задачу фишерам и банковским грабителям.

Анализ воздействия на бизнес рекомендуется завершать построением модели причинно-следственных взаимосвязей между функционированием бизнес-процессов, информационных сервисов и информационных потоков. Данная модель позволяет на основании информации о критичности бизнес-процессов и информационных потоков, а также о масштабах возможных потерь получить для каждого класса сервисов оценку критичности сервиса с точки зрения бизнеса компании и возможных потерь для бизнеса компании в зависимости от нарушения в функционировании сервиса и времени восстановления, экономически оправданных затрат на повышение уровня доступности сервиса.

**Литература**

1. *Козлов Д. Д., Петухов А. А.* Методы обнаружения уязвимостей в web-приложениях [Электронный ресурс]. URL: http://lvk.cs.msu.su/~ddk/pubs/methods_for_webapp_vuln_scanning.pdf (дата обращения: 01.11.2012).

2. *Евтеев Д.* Анализ защищенности Web-приложений [Электронный ресурс] // Открытые системы. 2009. № 02. URL: http://www.osp.ru/os/2009/02/7322807 (дата обращения: 01.11.2012).

3. *Йоханссон Д.* Как злоумышленник может проникнуть в вашу сеть [Электронный ресурс] // Журнал TechNet. URL: http://technet.microsoft.com/ru-ru/library/dd451059.aspx (дата обращения: 01.11.2012).

4. Википедия, свободная энциклопедия [Электронный ресурс]. URL: http://ru.wikipedia.org (дата обращения: 01.11.2012).

5. *Евтеев Д.* Такой (не)безопасный веб [Электронный ресурс] URL: http://www.slideshare.net/devteev/ss-13377233 (дата обращения: 01.11.2012).

УДК 004.056

**И. Г. Гниденко, О. Д. Мердина**

Санкт-Петербургский государственный
инженерно-экономический университет

# ПРИНЦИПЫ ОРГАНИЗАЦИИ И ОСНОВНЫЕ ПРОБЛЕМЫ ПРОГРАММНОЙ АРХИТЕКТУРЫ КЛИЕНТ-СЕРВЕР

Современный бизнес немыслим без эффективного управления. Во многом эффективность работы любого предприятия зависит от того, как организованы системы обработки и хранения информации. Основой информационного обеспечения в таких системах являются базы данных. Именно поэтому базы данных по-прежнему остаются динамически развивающимся теоретико-прикладным направлением. Развитие прикладной составляющей идет по нескольким направлениям, например таким, как переход к объектно-реляционным базам данных, определение моделей данных для новых типов (пространственные данные), масштабирование баз данных и т. д. Актуальным остается и направление совершенствования программной архитектуры клиент-сервер.

В основе программной архитектуры клиент-сервер лежит разбиение программного комплекса на несколько независимых компонентов и наделение их ролями поставщиков и заказчиков определенных услуг. Такое разбиение позволяет преодолеть хаос, нарастающий по мере увеличения сложности и расширения функциональности программного продукта, кроме того, открывает возможности интегрирования сторонних компонентов либо разработки компонентов для интеграции в другие продукты. Клиент-серверный подход, использующий концепцию модульного программирования, отвечает требованиям современного программирования, хорошо применим для длительной разработки больших продуктов, особенно когда в процесс вовлечено несколько команд разработчиков.

Центральным, ключевым понятием клиент-серверного взаимодействия является интерфейс. Интерфейс в широком смысле слова обозначает совокупность средств, методов и правил взаимодействия между какими-либо объектами или функциональными элементами, специфицирующими обращение одного из компонентов к другому. В узком смысле слова, применительно к теме статьи, следует рассматривать интерфейс как семантическую конструкцию программы, определяющую множество услуг, предоставляемых каким-либо компонентом, его функциональность с точки зрения внешнего клиента. Такой интерфейс называется программным, он специфицирует взаимодействие виртуальных объектов, существующих на уровне программиста. В качестве программного интерфейса может выступать прототип отдельной функции, интерфейс динамической библиотеки, комплекта средств разработки, а также API операционной системы, т. е. интерфейсы существуют как на микро-, так и на макроуровне.

Одной из важных черт любого интерфейса является абстрагирование, способность ограничить связь клиента и сервера необходимым минимумом. Все, что клиенту известно про сервер, это сам факт, что сервер поддерживает, реализует функциональность, определенную данным интерфейсом. Клиент не должен знать о механизмах работы сервера, в то время как сервер не должен знать, с какой целью клиент обратился по тому или иному методу интерфейса. Такая слабая связь между клиентом и сервером обеспечивает универсальность, переносимость, заменимость компонентов.

Если же обозначенные принципы нарушаются, это приводит к появлению «сильной связи» между клиентом и сервером. Теряется смысл разбиения программного комплекса на функциональные элементы.

Избыточность интерфейса, т. е. возможность клиента запросить одну и ту же услугу несколькими способами, плоха потому, что обусловливает увеличение нагрузки на сервер и ухудшает расширяемость. Однако на макроуров-

не, в случае комплектов средств разработки (SDK) или программных интерфейсов ОС, избыточность встречается достаточно часто и вполне допустима.

В языках объектно-ориентированного программирования (ООП) любой класс порождает определенный интерфейс, в состав которого входит его открытая (public) секция. Только эта часть класса доступна извне, для владельца экземпляра данного класса, и только к этим методам он может обращаться. Внутренняя реализация класса, а также его состояние, описываемое переменными-членами, неизвестно для клиента и не является частью интерфейса. В то же время вся семантическая нагрузка класса состоит именно в реализации интерфейса. В случае функции интерфейсом является список ее параметров, а также тип возвращаемого ей значения, интерфейс библиотеки включает прототипы экспортируемых ей функций.

Помимо описанных интерфейсов в ООП появилась необходимость описать интерфейс явным образом, сгруппировав семантически связанные виртуальные методы, выделить для этого самостоятельную семантическую конструкцию.

Скелет объявления интерфейса в языке C++ выглядит следующим образом:

```
class ISmth
{
public:
 virtual ~ISmth () {}
 virtual type1 Method1 (...) = 0;
 virtual type2 Method2 (...) = 0;
 virtual type3 Method3 (...) = 0;
 ...
};
```

Класс, представляющий собой интерфейс, включает в себя виртуальный деструктор и несколько чисто виртуальных методов без реализации. Класс является абстрактным, его невозможно инстанцировать. При вызове метода че-

рез указатель на ISmth происходит выборка из таблицы виртуальных функций, и метод будет адресован конкретному классу, реализующему ISmth.

Механизм виртуальных функций позволяет клиенту абстрагироваться не только от реализации метода, но и от того, какой класс предоставляет реализацию интерфейса. Все знание клиента о сервере ограничивается процедурой инстанциирования указателя на интерфейс. Таким образом, интерфейс как элемент ООП отвечает принципам инкапсуляции и полиморфизма, так как ограждает, специфицирует доступ клиента к некоторому объекту, реализующему этот интерфейс, а также поддерживает множественность реализаций.

Реализация методов интерфейса классом в разных языках объявляется либо напрямую через наследование, либо посредством ключевого слова implements:

```
public class CSmthImpl implements ISmth
{
  ...
}
```

В языках ООП один и тот же класс может реализовывать неограниченно много интерфейсов. Указатели (ссылки) на все интерфейсы, которые реализует класс, экземпляром которого является их объект, совместимы между собой, допустимо их приведение друг к другу. Если класс C1 реализует интерфейсы I1 и I2 и имеется указатель (ссылка) на I1, под которым лежит C1, то ее приведение к типу I2 – вполне допустимая операция, а попытка привести указатель к некоторому интерфейсу I3 завершится с ошибкой.

Такое приведение, называемое запросом интерфейса, удобно в тех случаях, когда сервер поддерживает сразу несколько интерфейсов; клиенту необязательно хранить указатели на каждый из них, достаточно хранить один на любой из них и при необходимости запрашивать нужный интерфейс.

В ряде случаев сервер инкапсулирует не только реализацию своих объектов, но и механизм инстанциирования. Для этого сервер предоставляет клиенту доступ к фабрике классов (шаблон проектирования «абстрактная фабрика»), реализующей инстанциирование, в частности определяющей, в каких случаях необходимо создание нового объекта, а в каких – достаточно вернуть ссылку на уже имеющийся.

Достаточно распространенной является ситуация, при которой множество клиентов в программе обращаются к одному экземпляру сервера через методы интерфейса. При такой архитектуре каждый клиент владеет одной ссылкой на сервер и ничего не знает о других клиентах, использующих тот же сервер. В этой ситуации существует неопределенность с временем жизни сервера: непонятно, в какой момент следует разрушать объект, реализующий функциональность сервера. Если разрушить объект до того, как последний клиент завершит работу с ним, это в лучшем случае приведет к потере данных, в худшем – к крашу. Если же вовремя не сделать этого, появятся неосвобожденные ресурсы и утечки памяти, что в большинстве случаев недопустимо.

Стандартным способом решения этой проблемы является механизм подсчета ссылок. Каждый серверный объект хранит свой внутренний счетчик ссылок, который увеличивается каждый раз, как новый клиент подключается к нему, и уменьшается, когда клиент завершает работу с сервером. Когда значение внутреннего счетчика доходит до нуля, это означает, что сервер больше никому не нужен, память и ресурсы можно освобождать. Для сервера, рассчитанного на работу с несколькими клиентами, необходимость подсчета ссылок возникает практически всегда.

Как уже было отмечено, знание клиента об объекте, реализующем интерфейс, ограничивается процедурой инстанциирования. Сама реализация может находиться как «рядом», так и в другом бинарном модуле и, возможно, на другой машине – для клиента это безразлично. Для серве-

ров, находящихся вне клиентского модуля, существует разбиение на внутрипроцессные (inproc server) и внепроцессные (out of proc server).

Внутрипроцессный сервер реализуется в виде динамической библиотеки и загружается в адресное пространство клиента. Когда число ссылок на серверный объект достигает нуля, клиентский процесс инициирует выгрузку динамической библиотеки, на этом работа внутрипроцессного сервера завершается. Достоинством такого подхода является простота, возможность четко определить время жизни сервера. Например, если при выполнении серверного кода происходит фатальная ошибка, то она влечет за собой краш клиентского процесса. Одновременно с этим завершение клиентского процесса автоматически влечет за собой уничтожение всех объектов в его адресном пространстве, в том числе и сервера. Если в момент завершения другие клиенты продолжали работать с сервером, их ссылки станут указывать на уничтоженный объект. Поэтому совместное использование внутрипроцессного сервера несколькими клиентами становится затруднительным.

Альтернативой этому подходу является реализация внепроцессного сервера, существующего в виде отдельного приложения. Этот вариант является более сложным, так как вопрос времени жизни сервера уже не имеет однозначного ответа. Как правило, серверный процесс запускается в момент обращения к нему первого клиента и завершается, когда последний клиент завершает работу с ним. При этом функциональность, связанная с подсчетом ссылок и завершением процесса, реализуется сервером, и он должен самостоятельно отслеживать наличие открытых ссылок со стороны клиентов. Внепроцессный сервер автоматически обеспечивает распределенность, параллельность вычислений, клиентский процесс может продолжать работу, а не останавливаться в ожидании ответа от сервера. С другой стороны, это приводит к необходимости синхронизации работы процессов. Синхронизация сервера при работе с несколькими клиентами в ряде случаев может быть достаточно сложной.

Многим из обозначенных ранее требований к архитектуре клиент-серверного взаимодействия отвечает технология COM (Component Object Model – компонентная объектная модель) компании Microsoft. Для инстанциирования интерфейса клиенту достаточно указать глобальный идентификатор COM-класса (CLSID), прописанного в реестре. Запись в реестре создается посредством регистрации COM-объекта и включает полный путь к серверному бинарному модулю. Фабрика классов COM (интерфейс IClassFactory) унифицирует этот процесс. Каждый COM-объект поддерживает базовый интерфейс IUnknown, методы которого позволяют управлять счетчиком ссылок объекта, а также осуществлять запрос интерфейса. Технология COM включает собственный язык описания интерфейсов (MIDL), а также поддерживает работу как с внутрипроцессным, так и с внепроцессным сервером.

Технология COM, несмотря на свою широкую распространенность, не лишена недостатков. Одной из классических проблем является явление циклических ссылок. Если какой-либо клиент владеет двумя COM-объектами, хранящими ссылки друг на друга и захочет уничтожить их, он вызовет для каждого из них метод IUnknown :: Release. Однако ни один из объектов в действительности не будет уничтожен, так как счетчик ссылок каждого из них будет равен 1, благодаря ссылке другого объекта на него. Трудности, связанные с решением подобного рода коллизии, ложатся на плечи клиента. Еще одним серьезным недостатком является порождение известного явления DLL Hell («ад динамических библиотек»). Поскольку CLSID COM-объекта, прописанный в реестре, однозначно определяет серверную динамическую библиотеку, все клиенты, инстанциируя интерфейс данным CLSID, будут обращаться к ней. В ряде случаев такой эффект является нежелательным и влечет за собой конфликты разных программных продуктов, установленных на одной машине. Однако главным недостатком COM все-таки является неоправданная сложность. Это привело к появлению ряда оберток над COM, таких как ATL.

В качестве альтернативы COM выступает технология CORBA (Common Object Request Broker Architecture), продвигаемая консорциумом OMG. CORBA, как и COM, имеет собственный язык описания интерфейсов. Функциональность CORBA-объекта становится доступной для клиента благодаря созданию серванта, отвечающего за реализацию интерфейса и имеющего свой счетчик ссылок. Функции создания CORBA-объекта и доставки запроса клиента нужному серванту возложены на объектный адаптер POA (Portable object adapter). Объектные адаптеры в приложении образуют древовидную структуру.

Важным достоинством CORBA является поддержка распределенных вычислений: клиент и сервер могут находиться на разных машинах и взаимодействовать через TCP/IP. Аналогичная технология от Microsoft носит название DCOM (Distributed COM).

В последнее время платформа .NET и управляемые языки программирования все чаще используются при разработке крупных проектов.

Клиент-серверное взаимодействие в рамках управляемой среды реализуется достаточно просто – большую часть проблем связи клиента и сервера .NET берет на себя. Однако при разработке .NET-приложений остро встает вопрос связи с неуправляемыми библиотеками либо интеграции разрабатываемого компонента в существующую систему. Серьезной проблемой становится сложность маршалинга – обращения из неуправляемого кода к управляемому, или наоборот.

Существуют три основных метода работы с неуправляемым кодом из среды .NET Framework. К ним относятся Platform Invoke – обращение к функциям, экспортируемым динамическими библиотеками, COM Interop – обращение к COM-компонентам из managed-кода, а также механизм unsafe (небезопасных) вызовов. Как правило, для организации взаимодействия .NET-приложение регистрирует сборку в реестре и генерирует библиотеку типов (.tlb). Неуправляемый COM-клиент импортирует библио-

теку типов и получает доступ к фабрике классов управляемого сервера так, как будто работает с обычным COM-сервером.

Еще одной существенной проблемой в организации клиент-серверного взаимодействия является поддержка обратной совместимости. Обратная совместимость какого-либо компонента программного комплекса предполагает поддержку интерфейсов, присутствующих в своей более старой версии, что гарантирует сохранение целостности системы при переходе к более новой версии компонента. Поддержка обратной совместимости увеличивает время и стоимость разработки, приводит к дублированию функциональности, увеличивает затраты на тестирование. В то же время отсутствие обратной совместимости приводит к тому, что изменение архитектуры или базовой технологии какого-либо из компонентов требует немедленного обновления.

Сложность разработки сервера, обслуживающего множество клиентов, заключается, прежде всего, в том, что он ориентирован на длительную бесперебойную работу. Диагностика и устранение ошибок, приводящих к краху системы с периодичностью раз в месяц, являются сложной и затратной работой, в ряде случаев именно ее длительность приводит к переносу сроков выпуска продукта. Обеспечение стабильности при длительной работе компонента ужесточает требования к программистам, заставляет четко отслеживать безопасность кода, наличие необходимых проверок и корректной обработки ошибок. Большую роль в данном случае играет выбор языка программирования, используемых API и SDK, а также целевая платформа.

Эти рассуждения приводят к выводу, что грамотная организация клиент-серверного взаимодействия является сложной задачей, имеющей множество подводных камней. Развитие архитектуры, а значит, и всего программного продукта в целом во многом определяется успешностью первоначального проектирования, если в начале разработки продукта удается правильно предсказать направление

развития, возможные проблемы и разработать интерфейс, максимально гибкий и универсальный, обладающий способностью к саморасширению. Конкретная предметная область и конкретная задача во многом определяют выбор того или иного архитектурного решения.

УДК 004.056

**Г. А. Мамаева**

Санкт-Петербургский государственный
инженерно-экономический университет

## ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ СИСТЕМ

Виртуализация – сегодня одна из самых востребованных информационных технологий. На данный момент виртуализация применяется на самых различных уровнях абстракции программных и аппаратных систем, начиная от виртуализации приложений и заканчивая виртуализацией систем хранения данных (СХД).

Решения для виртуализации IT-инфраструктуры позволяют компаниям эффективнее использовать свои IT-ресурсы, быть более гибкими, динамичными, а значит, и конкурентоспособными.

Бурное развитие рынка технологий виртуализации за последние несколько лет произошло во многом благодаря увеличению мощностей аппаратного обеспечения, позволившего создавать по-настоящему эффективные платформы виртуализации как для серверных систем, так и для настольных компьютеров. Технологии виртуализации позволяют запускать на одном физическом компьютере (хосте) несколько виртуальных экземпляров операционных систем (гостевых ОС) для обеспечения их независимости от аппаратной платформы и сосредоточения нескольких виртуальных машин на одной физической.

Виртуализация предоставляет множество преимуществ как для инфраструктуры предприятий, так и для конечных пользователей. За счет виртуализации обеспечивается существенная экономия на аппаратном обеспечении, облуживании, повышается гибкость IT-инфраструктуры, упрощается процедура резервного копирования и восстановления после сбоев. Виртуальные машины, являясь независимыми от конкретного оборудования единицами, могут распространяться в качестве предустановленных шаблонов, которые могут быть запущены на любой аппаратной платформе поддерживаемой архитектуры.

С помощью технологии виртуализации рабочих мест (Virtual Desktop Infrastructure – VDI) сотрудник, имея любое устройство с доступом в Интернет – смартфон, планшетный компьютер, может получить доступ к персональному рабочему столу и корпоративным информационным ресурсам. Внедрение VDI позволяет компании упростить создание и администрирование рабочих мест пользователей, обеспечить гибкость своей IT-инфраструктуры.

К очевидным плюсам виртуализации можно также отнести:

- повышение изоляции одной виртуальной системы от другой, что позволяет увеличить стабильность работы информационной системы предприятия в целом – если какой-то сервис выходит из строя вместе с одним из виртуальных серверов, то остальные виртуальные серверы продолжают работать;
- распределение задач администрирования – возможность соответствующим образом ограничить права каждого администратора, что позволит ему управлять без проблем объектами, с которыми связана непосредственно его работа. Но при этом объекты, не связанные с работой, будут недоступны;
- распределение аппаратных ресурсов – каждой виртуальной машине выделяется ровно то количество ресурсов, которое необходимо для осуществления возложенных на нее задач;
- повышение качества администрирования – более легкое в исполнении проведение различных тестов и ис-

следований, связанных с изучением эффективности и корректности работы информационной системы предприятия;

• постоянная доступность – если с одним из хостинг-серверов виртуальных машин возникают проблемы, можно достаточно просто провести их временную миграцию на другой хостинг-сервер без перерыва в обслуживании клиентов; также благодаря этому преимуществу можно производить плавное обновление всего парка программного обеспечения, в том числе – обслуживающего виртуальную инфраструктуру.

Использование технологий виртуализации на предприятиях постоянно возрастает. Согласно статистике «Лаборатории Касперского»: 59% опрошенных российских компаний с локальными сетями от 100 компьютеров и выше уже внедрили или планируют внедрить виртуализацию серверов. При этом почти на всех предприятиях, где используется виртуализация серверов, они используются для обеспечения функционирования баз данных (80%). Далее по популярности идет электронная почта (64%), ERP-системы (50%), CRM-системы (41%) и приложения для финансового менеджмента (34%) [1].

Среди наиболее важных преимуществ виртуализации отечественные специалисты отмечают надежность (89%), простоту резервного копирования и восстановления данных (86%), операционную эффективность (85%) и консолидацию серверов с эффективным использованием аппаратных ресурсов (84%) [2].

Но, к сожалению, большинство этих, безусловно, положительных особенностей виртуализации вносят дополнительные проблемы безопасности. Это обусловлено тем, что обработка информации в виртуальной среде имеет свои специфические особенности, отсутствующие в физической среде [3]:

• информация обрабатывается в гостевых машинах, которые находятся под полным контролем гипервизора[1],

[1] Гипервизор – среда, обеспечивающая параллельное выполнение многих операционных систем на одном хост-компьютере.

способного абсолютно незаметно для традиционных средств защиты информации перехватывать все данные, идущие через устройства;

• администратор виртуальной инфраструктуры, имеющий права доступа к гипервизору, становится очень важным субъектом безопасности информационной системы – фактически он может получить доступ к информационным ресурсам в обход существующей политики информационной безопасности компании;

• средства управления виртуальной инфраструктурой представляют собой самостоятельный объект атаки, проникновение к ним дает возможность нарушителю получить доступ к гипервизорам серверов виртуализации, а затем к конфиденциальным данным, обрабатываемым на гостевых машинах;

• традиционные средства защиты информации, разработанные для защиты физической инфраструктуры, могут не учитывать существование гипервизора, являющегося фактически нарушителем, реализующим атаку «человек в середине» (Man in the Middle, MITM) при взаимодействии гостевой машины со всеми устройствами;

• диски гостевых машин обычно размещаются в сетевых хранилищах, которые должны физически защищаться как самостоятельные устройства;

• традиционные межсетевые экраны не контролируют трафик внутри сервера виртуализации, где могут находиться десятки гостевых машин, взаимодействующих между собой по сети, однако этот сетевой трафик не покидает сервера виртуализации и не проходит через физические межсетевые экраны и другое физическое сетевое оборудование;

• каналы передачи служебных данных серверов виртуализации обычно не защищены, хотя по этим каналам среди прочих данных передаются фрагменты оперативной памяти гостевых машин, которые, разумеется, могут содержать конфиденциальные данные.

Стандартный набор средств защиты без учета особенностей виртуализации включает средства аутентификации и управления доступом, межсетевые экраны, криптографические средства для шифрования или электронно-цифровой подписи, антивирусы, средства обнаружения вторжений и т. п. Кроме того, аппаратными средствами защиты могут быть, например, платы контроля целостности и доверенной загрузки компьютера (устройства PCI/PCI Express), аппаратные межсетевые экраны и отчуждаемые устройства для аутентификации или криптографии (смарт-карты, токены или «таблетки» Touch Memory).

Рассмотрим ситуацию, когда защищенная стандартными средствами инфраструктура погружена в самую популярную виртуальную среду – VMware vSphere. Что изменится?

Первое, что можно заметить, – это то, что аппаратные межсетевые экраны становятся не везде применимы. Трафик между двумя виртуальными машинами, находящимися на одном хосте, уже не покинет его, а следовательно, не будет проходить через межсетевой экран.

Таким образом, чтобы защититься от атаки одной скомпрометированной виртуальной машины на другую виртуальную машину, необходимо применять иные решения. Следует заметить, что подобная угроза актуальна не только в пределах одного хоста. Вполне можно представить ситуацию, когда на первом этапе скомпрометированная виртуальная машина получит контроль над виртуальными машинами на данном хосте, а на втором этапе, при vMotion[1] одной из виртуальных машин на другой хост, компрометация распространится далее.

Второй важной сетевой особенностью виртуальных инфраструктур является то, что мы не можем больше рассчитывать исключительно на статические сетевые правила

---

[1] VMotion – это технология, которая позволяет переместить виртуальную машину с одного физического сервера на другой, не прерывая ее работы.

на коммутаторах. В физическом мире мы не привыкли (за исключением кластерных решений), что серверы могут постоянно перескакивать между физических портами, в то время как в виртуальной инфраструктуре в процессе vMotion это является порядком вещей.

По информации специалистов компании «Код безопасности», угрозы, направленные на виртуализацию, можно разделить на следующие типы [4]:

- атака на гипервизор с виртуальной машины;
- атака на гипервизор из физической сети;
- атака на диск виртуальной машины;
- атака на средства администрирования виртуальной инфраструктуры;
- атака на виртуальную машину с другой виртуальной машины;
- атака на сеть репликации виртуальных машин;
- неконтролируемый рост числа виртуальных машин.

Реализуются же эти атаки на элементы инфраструктуры самыми различными образами. Например, существует возможность кражи файла, относящегося к виртуальной машине, простым копированием на флешку. Содержимое виртуальных машин при некоторых условиях можно перехватить посредством атаки «Man in the Middle» во время ее миграции с одного хост-сервера на другой. Можно получить доступ непосредственно к хранилищу виртуальных машин на ESXi-сервере и за считанные секунды уничтожить всю виртуальную инфраструктуру предприятия, которая может составлять основную часть информационной системы.

Как видно, количество информационных угроз при использовании виртуальных инфраструктур, существенно возрастает. Поэтому очень важно правильно организовать их полноценную защиту. Поскольку полноценно защитить виртуальную инфраструктуру предприятия с помощью единственного защитного решения на данный момент невозможно, рекомендуется сочетать как продукты, предла-

гаемые компанией VMware, так и продукты сторонних разработчиков, несмотря на то, что это значительно повышает стоимость внедрения виртуализации.

В настоящее время в состав программного обеспечения для виртуализации VMware vSphere входит множество компонентов под названием VMware vShield. Данная технология пришла на смену технологии VMware vSafe, которую раньше могли использовать лишь некоторые сторонние производители защитного программного обеспечения. VMware vShield призван упорядочить подход к безопасности виртуальных инфраструктур и открывает больше возможностей сторонним производителям для интеграции с системой безопасности, созданной VMware для организации защиты виртуальных инфраструктур VMware vSphere.

На базе технологии VMware vShield компания VMware создала несколько собственных защитных продуктов, среди которых:

- VMware vShield App – для защиты приложений от сетевых угроз;
- VMware vShield Edge – обеспечение безопасности периметра сети;
- VMware vShield Zones – базовая защита от сетевых угроз;
- VMware vShield Manager – полноценное управление системой безопасности;
- VMware vShield Endpoint – перенос средств защиты с клиентских систем на уровень гипервизора.

При этом VMware vShield Endpoint как раз позволяет сторонним антивирусным продуктам устанавливаться на хост-сервере в качестве одной из виртуальных систем, обеспечивая возможность осуществлять защиту извне защищаемых виртуальных систем без необходимости установки антивирусного агента на каждую защищаемую систему.

Таким образом, можно сделать следующие выводы.

1. В виртуальной среде следует применять новые средства защиты, учитывающие аспекты обеспечения информационной безопасности виртуализации.

2. Далеко не все аппаратные средства защиты будут работать в виртуальной среде.

3. Новые компоненты (гипервизор, средства управления виртуальной инфраструктурой и т. п.) тоже нужно защищать. Причем комплексную и многоуровневую защиту могут обеспечить только специализированные средства.

**Литература**

1. SECURELIST. Аналитика [Электронный ресурс]. URL: http://www.securelist.com/ru/analysis (дата обращения: 10.11.2012).

2. *Ледовской В.* Виртуальным инфраструктурам – прогрессивная защита [Электронный ресурс]. URL: http://www.anti-malware.ru/analytics/Progressive_Defense_for_Virtual_Infrastructures (дата обращения: 10.11.2012).

3. *Пичугов К.* Безопасность виртуальной инфраструктуры: новые вызовы, новые решения // Information Security = Информационная безопасность. 2009. № 5.

4. Безопасность виртуальной инфраструктуры [Электронный ресурс]. URL: http://www.securitycode.ru/solutions/virtual/security (дата обращения: 10.11.2012).

УДК 004.056

**Д. Д. Николаев**
ЗАО «АКУТА»

## АДАПТИВНОЕ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

По данным исследования, проведенного в июле 2012 г. по заказу компании Cisco, 90% руководителей отделов информационных технологий признают актуальность облачных технологий, при этом годом раньше показатель был на уровне лишь 52%. Треть из опрошенных признают, что

функционирование используемых облачных вычислений является критически важным для поддержания деятельности предприятия. Помимо явно положительных моментов с точки зрения экономии для предприятия, благодаря снижению количества используемых технических средств, площади требуемых помещений для их размещения, снижению потребляемой энергии, существует проблема обеспечения безопасности информационных процессов, происходящих при использовании технологии облачных вычислений.

В настоящий момент при использовании облачных сервисов, особенно предоставляемых сторонними организациями, нет четкого понимания рисков, а иногда и применяемых механизмов защиты обрабатываемых и хранящихся данных.

Использование технологии облачных вычислений осуществляется на основе виртуализации программных и технических ресурсов, что, безусловно, добавляет новые слои технологий и приводит к возрастанию затрат на обеспечение безопасности и требует привлечения дополнительных специализированных мер и средств защиты информации. Появление новых угроз обусловлено следующими причинами:

- техническая сложность (по сравнению с традиционными средствами вычислительной техники);
- совместное использование информационных ресурсов;
- расширение возможностей администраторов и обслуживающего персонала по доступу к информационным ресурсам.

Для защиты информации на уровне программного обеспечения в отдельной виртуальной машине применимы те же самые средства защиты, что и для обычных автоматизированных рабочих мест с ограничениями, накладываемыми аппаратным обеспечением (совместимостью). При защите каждой операционной системы в отдельности остаются незащищенными средства виртуализации. При этом

требуется учитывать, что виртуальные операционные системы. Формальная сторона вопроса в случае необходимости приведения системы в соответствие требованиям регулятора (руководящим документам ФСТЭК) будет выполнена. При этом законодательство России не делает различий между физическими и виртуальными системами, предназначенными для обработки информации ограниченного доступа.

Для оптимизации процесса обеспечения безопасности наиболее выигрышным выглядит вариант доступа к виртуальным машинам через единую точку доступа – единый сервер авторизации (аутентификации), регистрации событий безопасности, обеспечивающий реализацию механизмов мандатного и дискреционного доступа, контроль целостности средств виртуализации. Непосредственно на платформе виртуализации необходимо производить контроль целостности аппаратных ресурсов, а также обеспечивать доверенную загрузку.

Единая точка доступа и авторизации должна получать сведения от средств защиты, установленных непосредственно на виртуальных машинах (в частности, сведения о вирусных заражениях, попытках НСД) для возможности еще на этапе авторизации на сервере заблокировать или ограничить доступ пользователя.

Необходимо строгое разграничение пользователей по возможности создавать резервные копии ВМ (в том числе для резервного копирования).

Необходима оценка рисков до внедрения системы единой точки доступа и после нее, поскольку, исходя из условий функционирования, возможна защита существующими средствами для формальной стороны вопроса.

Необходима тщательно составленная модель угроз. Сравнение расчетов рисков при использовании средств защиты только ПО и ОС и при использовании средств защиты гипервизора.

УДК 004.451.2

**Ю. Е. Евелев, Г. М. Чернокнижный**

Санкт-Петербургский государственный
инженерно-экономический университет

# ЗАЩИТА ВИРТУАЛИЗИРОВАННЫХ ЦОД С ИСПОЛЬЗОВАНИЕМ СЗИ НСД VGATE R2

В настоящее время владение традиционной IT-инфраструктурой становится все более и более неоправданным. Во многих компаниях серверные комнаты зачастую наполнялись совершенно разным оборудованием, зачастую несовместимым. Кроме того, данное оборудование за многие годы устарело морально и физически. Стоимость владения и поддержания работоспособности систем, основанных на таком подходе к приобретению «железа», весьма высока, а его использование – не оправданно. Решить эту проблему и призвана виртуализация и, как следствие, консолидация серверного пула. Именно абстрагирование аппаратных средств и позволяет добиваться таких результатов. Для того чтобы снизить расходы, необходимо пересмотреть многие прикладные задачи, такие как обновление программного обеспечения, резервное копирование, аварийное восстановление системы и пр.

Современные технологии виртуализации помогают получать максимальную отдачу от предоставленных ей вычислительных ресурсов, сокращают издержки на содержание парка программного и аппаратного обеспечения за счет переноса его в виртуальное пространство. На сегодняшний день практически все компании, представляющие крупный или средний бизнес, стараются повысить управляемость информационных систем, сократив при этом расходы на эксплуатацию. Именно такие возможности и дает ЦОД – центр обработки данных. Центр обработки данных позволяет консолидировать все вычислительные ресурсы компании, а виртуализация освобождает ресурсы, повыша-

ет эффективность, придает динамичность и гибкость, позволяет снижать затраты на аппаратное обеспечение и электроэнергию. Она дает возможность, в случае необходимости, за максимально короткое время переместить сервер из более загруженного сегмента сети в менее загруженный, возможность быстро развернуть дублирующую машину для балансировки нагрузки.

Виртуализация серверов и рабочих станций позволяет программно или аппаратно эмулировать виртуальный сервер/компьютер, имеющий, как и все компьютеры, процессор, память, жесткий диск и т. д. Данная эмуляция происходит благодаря монитору виртуальных машин (или гипервизору).

Но зачастую заказчики отождествляют слова «виртуализация» и «безопасность», считая, что если все ресурсы ЦОД перенесены в виртуальное пространство, то они априори безопасны. Но сложность процессов обслуживания всего пула ресурсов – неотъемлемая плата за удобство использования виртуализации.

Основная проблема обеспечения безопасности виртуализированной среды ЦОД связана с тем, что традиционные средства защиты информации не способны обеспечить защиту от новых угроз безопасности информации, специфичных именно для виртуальной инфраструктуры. Привычные решения зачастую несовместимы со средой виртуализации, так как изначально разрабатывались для использования в физической среде. Если нарушитель получает доступ к средствам управления виртуальной инфраструктурой, операционная среда традиционных средств защиты информации оказывается полностью скомпрометированной. Например, через гипервизор нарушитель может незаметно для традиционных средств защиты информации, работающих в виртуальных машинах, совершать следующие злоумышленные действия:

- копировать и блокировать поток данных, идущий на все устройства (HDD, принтер, USB, сеть, дискеты);

• читать и изменять данные на дисках виртуальных машин, даже когда они выключены или не работают, без участия программного обеспечения этих виртуальных машин.

Поэтому и выполнить требования по нормативному соответствию (например, требования отраслевого стандарта PCI DSS или ФЗ № 152 «О персональных данных») в условиях виртуальной среды с помощью традиционных средств защиты информации довольно затруднительно.

При определенных обстоятельствах на территорию ЦОД могут получить физический доступ различные группы лиц. Это и персонал ЦОД, не имеющий непосредственного доступа к среде, и представители других организаций, арендующие стойки или серверы, представители третьих организаций и т. д. Как правило, в большинстве ЦОД эта проблема решается с помощью комплекса организационных мер.

При переносе данных клиентов в виртуальную среду появляются новые каналы утечки информации, специфичные для виртуальной среды. Поэтому стандартных организационных мер для решения этой проблемы может быть уже недостаточно [1].

Инфраструктура центра обработки данных включает в себя не только серверы, сетевые компоненты, системы хранения данных, программное обеспечение и агенты виртуализации. Необходимо рассматривать всю структуру функционирования ЦОД как единое целое: не стоит забывать про энергоснабжение, кондиционирование и охлаждение серверов, системы контроля и учета доступа, системы видеонаблюдения. Многие вендоры стараются не объединять все вышеупомянутое оборудование в одну систему в связи с тем, что есть определенный риск бизнесу. Величина риска зависит от того, насколько хорошо тот или иной вендор «знает предмет».

В последние годы при подходе к проектированию систем управления ЦОД наблюдается переход от декомпози-

ции всей инфраструктуры ЦОД на отдельные участки (сетевая инфраструктура, вычислительные мощности, системы хранения данных, инженерные структуры) к интеграции. Наблюдать это можно уже на стадии интеграции систем управления аппаратными платформами в среду управления виртуальными серверами (плагины к VMware vCenter для управления всей инфраструктурой и ее аудита).

Аналитики предрекают унификацию управления всем ЦОД: сведение всех систем управления в единый пользовательский интерфейс. Кроме того, такие средства должны снижать до минимума человеческий фактор. Именно унификация позволяет сделать виртуализацию по-настоящему прозрачной: системным администраторам не нужно предварительно выяснять, с какими типом сервера они работают (с виртуальным или физическим), и использовать отдельное ПО для доступа к каждому типу систем. Помимо этого для отслеживания событий управления на ресурсах обоих типов используется консолидация событий и предупреждений, поступающих от физических и виртуальных серверов.

Известен ряд подходов к защите виртуализированных сред (например, компании Cisco [2]). По мнению авторов, решение задачи безопасной эксплуатации виртуализированного ЦОД с помощью средства защиты информации от несанкционированного доступа (СЗИ от НСД) vGate R2 компании «Код безопасности» является одним из лучших решений. СЗИ от НСД vGate R2 обеспечивает безопасность ***виртуальной инфраструктуре*** ЦОД, реализованной на VMware vSphere (vGate for VMware), и при этом сертифицировано ФСТЭК России. Сертификат подтверждает соответствие требованиям руководящих документов:

- в части защиты от несанкционированного доступа по 5-му классу защищенности (СВТ5);
- для контроля отсутствия недекларированных возможностей по 4-му уровню контроля (НДВ4);

• по классу защищенности в автоматизированных системах (АС) до 1Г включительно;

• для защиты информации в информационных системах персональных данных (ИСПДн) до 1-го класса включительно.

Основные возможности СЗИ НСД vGate R2[3]:

• позволяет автоматизировать работу администраторов по конфигурированию и эксплуатации системы безопасности;

• способствует противодействию ошибкам и злоупотреблениям при управлении виртуальной инфраструктурой;

• позволяет привести виртуальную инфраструктуру в соответствие с законодательством, отраслевыми стандартами и лучшими мировыми практиками;

• усиленная аутентификация администраторов виртуальной инфраструктуры и администраторов информационной безопасности;

• защита средств управления виртуальной инфраструктурой от НСД;

• защита ESX-серверов от НСД;

• мандатное управление доступом;

• контроль целостности конфигурации виртуальных машин и доверенная загрузка;

• контроль доступа администраторов ВИ к данным виртуальных машин;

• регистрация событий, связанных с информационной безопасностью;

• контроль целостности и доверенная загрузка ESX-серверов;

• контроль целостности и защита от НСД, компонентов СЗИ;

• централизованное управление и мониторинг.

Очевидно, что приведенный выше перечень возможностей vGate R2 является одновременно списком достоинств перед многими известными СЗИ.

К средствам управления виртуальной инфраструктурой относятся:

- ESX-хосты, предназначенные для запуска виртуальных машин;
- серверы vCenter, предназначенные для централизованного управления виртуальной инфраструктурой;
- средства, предназначенные для обслуживания инфраструктуры, например, VMware Consolidated Backup, VMware Update Manager;

В настоящее время системными требованиями продукта vGate R2 к компьютерам являются:

- к серверу авторизации и к резервному серверу авторизации: Windows Server 2008 x86/x64 SP2;
- к модулям защиты ESX:
  VMware vSphere 4 (VMware ESX Server 4.0, Update 2);
  VMware vSphere 4.1 (VMware ESX Server 4.1, VMware ESX;
  Server 4.1 Update 1, VMware ESXi Server 4.1);
  VMware vSphere 5 (VMware ESXi Server 5.0);
- к компоненту защиты vCenter:
  Windows Server 2008 SP2;
  Windows Server 2003 R2/SP2;
  VMware vSphere 4 (VMware vCenter 4.0, Update 2);
  VMware vSphere 4.1 (VMware vCenter 4.1);
  VMware vSphere 5 (VMware vCenter 5.0).

Требования к конфигурации компьютера, на который устанавливаются компоненты vGate R2, совпадают с требованиями к операционной системе, установленной на нем. Сам сервер авторизации рекомендуется устанавливать на выделенный физический сервер, однако в случае его отсутствия решение можно развернуть в виртуальной машине – это полностью поддерживаемая конфигурация. На компьютере, предназначенном для сервера авторизации, должно быть не менее двух Ethernet-интерфейсов, один из которых будет подключен к сети администрирования виртуальной инфраструктуры, а другой – к внешнему пери-

метру сети администрирования, в котором находятся рабочие места администраторов vSphere и администратора vGate, а также сетевые службы (например, DNS, AD).

С целью более эффективной защиты сервера виртуализации помимо vGate R2, необходимо применить программно-аппаратный комплекс (ПАК) «Соболь» версии 3.0 для реализации следующих защитных механизмов:

- идентификация и аутентификация пользователей на входе в систему (непосредственно при запуске сервера);
- ведение журнала безопасности;
- сигнализация попыток нарушения защиты;
- запрет загрузки с внешних носителей.

Перечисленный комплекс возможностей не позволит злоумышленнику (в случае если он получил физический доступ к серверу виртуализации) реализовать одну из наиболее распространенных угроз – перезагрузку сервера и загрузку с внешнего носителя для получения доступа ко всей информации, хранящейся на сервере, и, таким образом, эффективно защитить серверы, входящие в ЦОД.

Наличие у продуктов сертификатов ФСТЭК России позволяет использовать vGate R2 и ПАК «Соболь» версии 3.0 для защиты информации, составляющей коммерческую или государственную тайну в автоматизированных системах с классом защищенности до 1Б включительно.

**Литература**

1. *Орлов С.* Управление виртуализированным ЦОД [Электронный ресурс]. URL: http://www.osp.ru/dcworld/2011/03/13015004.html (дата обращения: 12.10.2012).

2. Cisco предлагает новые решения для информационной безопасности быстро развивающихся центров обработки данных [Электронный ресурс]. URL: http://www.cisco.com/web/RU/news/releases/txt/2012/091712d.html (дата обращения: 15.11.2012).

3. *Самойленко А.* Принципы разграничения доступа к конфиденциальным ресурсам VMware vSphere в vGate R2 [Электронный ресурс]. URL: http://www.vmgu.ru/articles/vgate-r2-vmware-securing-virtual-env (дата обращения: 15.11.2012).

УДК 004.056

**М. А. Шапченко**

Санкт-Петербургский государственный
инженерно-экономический университет

# INTEL И MCAFEE ПОВЫШАЮТ БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Облачные технологии становятся все более популярными по мере того, как компании стремятся к тому, чтобы повысить оперативность своих бизнес-процессов и эффективнее управлять все возрастающим количеством пользователей, устройств и постоянно растущим объемом данных. По прогнозам Intel, к 2015 г. во всем мире 3 млрд пользователей и 15 млрд устройств будут обладать доступом к Интернету, а это увеличит трафик до 1500 экзабайт. IDC предполагает, что около 20% трафика будет обрабатываться с помощью «облака». Надо понимать, что, несмотря на стремительный рост темпов внедрения облачных технологий, а соответственно, и темпов роста объема данных, вопросы безопасности сохраняют свою актуальность, и компании ищут способы защиты своих корпоративных данных и стремятся соответствовать требованиям регулирующих органов.

4 мая 2012 г. Intel и McAfee рассказали о вопросах защиты данных, которые появляются при рассмотрении возможности внедрения облачных технологий, и о том, как они помогают компаниям создавать инновационные решения для защиты путем внедрения совместных и доступных на рынке решений. Компании также представили ключевые вопросы, которые необходимо будет решить в будущем для повышения безопасности облачных вычислений.

Для более глубокого понимания проблем, которые возникают в сфере ИТ, и определения, каким образом можно повысить уверенность компаний при внедрении облачных технологий, Intel недавно провела опрос. Согласно его результатам, 61% специалистов обеспокоен потерей

контроля над частными средами, 55% обеспокоены недостаточной защитой данных в публичных инфраструктурах, а 57% опрошенных отказались размещать данные, для которых необходимо соблюдение требований регулирующих органов, в облачные центры обработки данных (ЦОД). Респонденты отметили, что решение этих проблем положительно скажется на их уверенности в надежности защиты данных и будет способствовать внедрению облачных технологий в их корпоративных средах.

Intel и McAfee используют комплексный подход для обеспечения безопасности облачных сред и повышения доверия к частным, публичным и гибридным облачным инфраструктурам. Общая цель этих компаний – создать модель облачных вычислений, которые будут также или даже более безопасны, чем традиционные, лучшие в своем классе методики защиты, используемые в корпоративных средах. Компании объединяют свои усилия по четырем основным направлениям для обеспечения защиты и для создания различных открытых решений для безопасности, реализуемых в рамках всей отрасли. Эти направления состоят из обеспечения защиты ЦОДов, сетевых подключений, устройств, подключаемых к облачным сервисам, и ускорения разработки унифицированных стандартов в области защиты облачных данных.

Современные ИТ-департаменты контролируют достаточно надежно свои корпоративные ЦОД за счет использования проверенных временем инструментов и методик для мониторинга систем и выполнения проверок на соответствие требованиям регулирующих органов. С использованием облачных инфраструктур ИТ-оборудование становится виртуализированным и распределяется между различными подразделениями или даже организациями, а это приводит к снижению уровня контроля в сравнении с традиционными методиками организации работы. Ситуация с безопасностью становится еще более проблематичной при использовании публичных облачных инфраструктур, которые управляются сторонними организациями. Кроме того, проведение проверок на предмет соответствия норматив-

ным требованиям в частных и публичных ЦОД становится еще более сложной задачей.

Для того чтобы решить эту задачу, Intel и McAfee акцентировали свое внимание на вопросах повышения целостности инфраструктуры, защиты данных и предоставления возможностей для упрощения контроля соответствия облачных сред нормативным требованиям. Так, например, программный комплекс McAfee ePolicy Orchestrator (McAfee ePO) обеспечивает согласованное управление на базе политик всеми физическими, виртуальными и облачными средами. Будущие разработки Intel и McAfee позволяют расширить и усилить защиту данных и реализовать возможность для проведения проверок соответствия нормативным требованиям.

Существуют две основные проблемы, с которыми приходится сталкиваться компаниям при рассмотрении возможности внедрения облачных технологий. Это возможность потери данных и вероятность ограничения доступа к информации. Пользователи с ненадежными паролями представляют собой основную угрозу безопасности. А, кроме того, интернет-трафик (веб-ресурсы и электронная почта), передаваемый между удаленными офисами и мобильными устройствами сотрудников компаний, также может стать источником утечки данных.

Решением стала платформа McAfee Cloud Security Platform, которая повышает безопасность данных за счет обеспечения защиты данных, интернет-трафика, электронной почты и персональных данных, передаваемых между устройствами и ЦОД.

С помощью платформы McAfee Cloud Security Platform ИТ-подразделения могут ограничить доступ к информации за счет внедрения политик безопасности и доступа в облачные среды. Новая разработка использует преимущества уникальной технологии McAfee Global Threat Intelligence (McAfee GTI), которая, в свою очередь, обеспечивает в реальном времени защиту от существующих и новых угроз. За счет сохранения контроля над всеми потенциальными источниками угроз – сетью Интернет,

файлами, электронной почтой и корпоративной сетью – и оперативного получения информации обо всех последних уязвимостях McAfee сопоставляет данные, полученные от многочисленных физических источников, с целью обеспечения комплексной защиты облачных соединений.

Увеличивается количество различных устройств, растут тенденции к использованию личных устройств для работы. Все это создает новые проблемы для обеспечения безопасности в облачных средах. Эти проблемы включают в себя комплексное управление идентификаторами пользователей (в среднем, 12 комбинаций имени и пароля пользователя), новые виды вредоносного ПО и постоянно увеличивающееся количество онлайн-атак. Чтобы бороться с этим, нужны новые уровни обеспечения безопасности для устройств, подключаемых к облачным сервисам.

Для того чтобы минимизировать подобного рода риски, Intel и McAfee приняли решение о повышении защиты устройств, включая настольные и мобильные ПК, путем защиты данных и ограничения доступа к информации и приложениям. Решение McAfee Deep Defender, совместно разработанное McAfee и Intel, представляет собой новое поколение аппаратных решений для защиты клиентских устройств. Для более эффективного управления идентификаторами пользователей ПО McAfee Cloud Identity Manager, предлагаемое в рамках McAfee Cloud Security Platform, обеспечивает комплексный контроль доступа для облачных приложений, использующих корпоративные идентификаторы. Также для этих целей может использоваться инструмент Intel Cloud SSO (single-sign on), который создает в облачных средах решение «идентификатор-как-услуга». Технология Intel Identity Protection обеспечивает дополнительную аппаратную защиту, которая использует вспомогательные данные для идентификации.

В дальнейшем разработки будут направлены на оптимизацию защиты данных и идентификаторов устройств, использующих облачные сервисы.

В перспективе Intel и McAfee планируют реализовать общую стратегическую задачу для создания в будущем за-

щищенных облачных решений для того, чтобы ИТ-департаменты могли получить 100%-ю уверенность в том, что:

• приложения, данные и инфраструктура надежно защищены;

• требования регулирующих органов соблюдаются в автоматическом режиме;

• корпоративные политики безопасности автоматически применяются при обработке всех задач;

• решения предоставляют отчеты в режиме 24/7 и отличаются простотой реализации.

С помощью аппаратных технологий защиты, программных решений и сервисов, предлагаемых Intel и McAfee, обе компании могут начать строительство надежной основы сегодня для создания защищенных облачных решений для будущего.

**Литература**

1. Intel. Making the Cloud Work for You [Электронный ресурс]. URL: www.intel.com/cloud (дата обращения: 10.11.2012).

2. Intel. Семейство процессоров Intel® Xeon® E5 [Электронный ресурс]. URL: www.intel.ru/xeon (дата обращения: 10.11.2012).

3. *Шатченко М. А., Ильин Б. В.* Виртуализация и облачные вычисления // Информационные аспекты экономики: Материалы науч.-практ. конф. 2 дек. 2011 г. – СПб.: СПбГИЭУ, 2012. – С. 166–168.

УДК 004.056

**Р. Г. Хуснулин**

Независимый эксперт, Москва

# К ВОПРОСУ ОБ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ В АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСАХ

В рамках работ по созданию произвольного аппаратно-программного комплекса (АПК) организация защиты информации (ЗИ) является важнейшей частью. Под орга-

низацией ЗИ понимается содержание и порядок действий по ее обеспечению. Уточнение отдельных аспектов организации ЗИ проводится при необходимости на основании методических материалов специализированной организации, выполняющей работы по обеспечению информационной безопасности АПК в целом.

Организация ЗИ в АПК заключается, в том числе, в создании подсистемы защиты и обеспечении ее эксплуатации в соответствии с нормативными документами и требованиями политики безопасности предприятия, осуществляющего эксплуатацию АПК. Под политикой безопасности понимается совокупность правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

Работы по созданию подсистемы защиты проводятся совместно с работами по созданию АПК в целом. С целью обеспечения соответствующего уровня ЗИ разработчику предоставляются необходимые исходные данные, содержащие следующие сведения:

- назначение создаваемой (или модернизируемой) автоматизируемой системы в защищенном исполнении (АСЗИ) в виде перечня реализуемых в АСЗИ информационных технологий и выполнения установленных функций;
- комплекс основных технических и программных средств, предполагаемых к использованию в АПК, и принципы взаимодействия этих средств;
- перечень защищаемой в АПК информации, максимальный уровень ее конфиденциальности, класс защищенности;
- основные характеристики безопасности защищаемой информации;
- положения политики безопасности эксплуатирующей организации.

Анализ на защищенность АПК проводится при разработке модели нарушителя. Под моделью нарушителя по-

нимаются предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях этих возможностей.

Содержание модели нарушителя определяется путем:

• исключения тех предположений по возможностям нарушителя, которые не имеют места для АПК в силу его специфики;

• конкретизации и детализации предположений модели нарушителя;

• описания возможностей нарушителя.

Модель нарушителя содержит описание возможных нарушителей АПК и их действия, а также меры противодействия.

Средства защиты информации (СрЗИ) вытекают из модели нарушителя и учитывают определенные в ней способы нейтрализации атак, а также требования по защите от несанкционированного доступа (НСД) к информации.

В настоящее время создание автоматизированных систем (или АПК) в защищенном исполнении регулируется ГОСТ Р51583–2000 «Порядок создания автоматизированных систем в защищенном исполнении». С учетом этого, в процессе создания подсистемы защиты является целесообразным:

1) обеспечить гарантии проектирования, предусматривающие:

• уточнение, при необходимости, модели нарушителя;

• разработку и обоснование модели защиты от НСД к информации, содержащей непротиворечивые правила разграничения доступа (ПРД) и изменения ПРД;

• разработку и обоснование модели механизма управления доступом и высокоуровневой спецификации системы защиты;

2) определить технические и программные АПК, взаимодействующие с подсистемой и средствами защиты;

3) определить порядок конфигурирования, настройки и эксплуатации СрЗИ в составе подсистемы защиты.

На этапе эксплуатации подсистемы защиты необходимо предусмотреть и учитывать следующее:

• изменения технических, программных и программно-технических средств АПК допускаются либо в рамках, определенных положительным заключением экспертной организации на соответствие системы защиты требуемому уровню защиты от НСД к информации, либо после проведения необходимых исследований и получения положительного заключения экспертной организации на соответствие модифицированной АПК требованиям безопасности;

• ответственность за обеспечение защиты возлагается на руководителя (начальника) эксплуатирующего подразделения;

• назначение администраторов безопасности (привилегированных пользователей, обеспечивающих штатное функционирование СрЗИ и системы защиты от НСД к информации на основе реализации положений политики безопасности) для эксплуатации подсистемы защиты в соответствии с указанием руководителя (начальника) эксплуатирующего подразделения;

• порядок проведения эксплуатация подсистемы защиты (возможно только в соответствии с требованиями разработанных на этапе создания АПК документов).

Администраторы безопасности при использовании криптографических средств назначаются из числа сотрудников шифровальной службы эксплуатирующего подразделения.

Администраторы безопасности осуществляют:

• сопровождение средств и системы защиты, включая вопросы организации работы и контроля использования средств защиты в АПК;

• оперативный контроль функционирования СрЗИ в АПК;

• выявление отклонений фактических эксплуатационных характеристик СрЗИ от проектных значений и устранение этих причин;

• контроль соответствия технических, программных и программно-технических средств АПК требованиям, предъявляемым к ним средствами и подсистемой защиты;

• разработку инструкций, регламентирующих обязанности и права пользователей при обработке защищаемой информации;

• обеспечение ЗИ при проведении ремонтных (регламентных) работ и при выводе из эксплуатации компонентов АПК.

Контроль эффективности ЗИ следует проводить в строгом соответствии с требованиями нормативных документов.

Контроль при этом может быть периодическим (осуществляется администраторами безопасности) и инициированным (по мере необходимости) контролирующими органами.

Инициатива проведения проверок принадлежит организациям, информация которых обрабатывается в АПК, или ведомственным подразделениям контроля, создающим с этой целью соответствующие комиссии из своих представителей. В указанные комиссии могут включаться (по согласованию) представители подразделения службы безопасности и экспертной организации.

Проверку функционирования средств защиты в основном предлагается осуществлять с применением технических, программных и (или) программно-технических средств, тестовых и контрольных примеров, достаточных для проверки соответствия средств защиты информации специальным требованиям, изложенным в специальном техническом задании.

По результатам проверки оформляется акт (заключение), который доводится до сведения руководителей (начальников) эксплуатирующего подразделения, организации, информация которого обрабатывается в АПК, и других должностных лиц в соответствии с уровнем контроля.

В зависимости от характера нарушений, связанных с функционированием СрЗИ в АПК, соответствующими должностными лицами принимаются меры по устранению нарушений, вплоть до приостановки обработки информации.

УДК 004.056

**Е. В. Черток**

Санкт-Петербургский государственный
инженерно-экономический университет

# ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СЕТЯХ НА ЭТАПАХ ВВОДА И ВЫВОДА

В настоящее время осуществляется активный переход к сетевой экономике. Внутренняя корпоративная сеть – объективная необходимость современного офиса, и виртуальные частные сети (VPN) уже становятся типовым решением, в том числе и для государственных организаций. Вместе с тем гриф конфиденциальности существенно ограничивает распространение по сети такой информации: чем больше количество конфиденциальной информации, тем в меньшей степени могут быть использованы возможности VPN. При этом основным каналом утечки информации является персонал. В случае же реализации мер защиты от потенциальных внутренних нарушителей эффективную помощь могут оказать специальные технические устройства, которые эффективно дополняют основные меры защиты от несанкционированного доступа (НСД).

**Угрозы документу.**

Угрозы документу при его обработке в сети представляют «атаки» на обрабатываемую информацию и на офисные устройства со стороны внутренних и внешних нарушителей, результатом которых может стать получение несанкционированного доступа к обрабатываемой информации, нарушение ее свойств (целостности, достоверности и т. д.), а также работоспособности программно-аппаратных средств.

Основным каналом утечки информации являются внутренние нарушители. Подтверждением этому служат данные ежегодных исследований Института компьютерной

безопасности США [1], согласно которым количество успешных вторжений в информационные системы увеличивается каждый год и более половины всех нарушений совершают сотрудники компаний.

В последнее время установка систем обеспечения безопасности документооборота считается приоритетной задачей для современных офисов [2]. Среди основных мер защиты от несанкционированного доступа можно выделить:

1) организационные меры;
2) мандатное управление доступом;
3) многопользовательскую операционную систему.

**Меры защиты от НСД.**

1. Организационные меры защиты.

Одной из задач в сфере защиты от НСД является комплексное обеспечение конфиденциальности информации, в том числе при работе с бумажными копиями документов. Основное назначение предлагаемых в этой сфере средств – исключить НСД посторонних лиц к информации, хранящейся в самом компьютере, но определенное внимание уделяется и завершающим этапам обработки информации: печати, сканированию, копированию и т. д. При этом традиционно используются организационные меры:

1) установка соответствующей офисной техники в закрытых помещениях, доступ в которые ограничен и контролируется;

2) реализация правил разграничения доступа к устройствам создания твердых копий;

3) закрытие доступа к портам печати – для вывода конфиденциальной информации на «твердую» копию необходимо вызвать администратора, который разрешит печать конфиденциальной информации;

4) наличие и поддержание в актуальном состоянии различных списков контроля доступа;

5) развитые средства протоколирования событий, происходящих в системе при обработке документа;

6) использование для печати конфиденциальных документов персональных принтеров, подключенных непо-

средственно к компьютерам сотрудников, допущенных к работе с такой информацией, и др.

2. Мандатное управление доступом.

К наиболее существенным элементам программного обеспечения безопасности в государственных и коммерческих структурах относится мандатное управление доступом, суть которого заключается в том, что для каждого пользователя устанавливается определенный уровень доступа к конфиденциальной информации, при этом каталогам и файлам назначается определенная категория конфиденциальности. Доступ к файлу пользователь получит только в том случае, если его уровень допуска не ниже уровня конфиденциальности файла.

При работе системы в режиме полномочного управления доступом для контроля перемещения документа:

1) используется контроль потоков, при котором, например, «конфиденциальный» документ нельзя переместить в «неконфиденциальную» директорию;

2) контролируется буфер обмена операционной системы, чтобы исключить возможность печати всего документа или его части с помощью буфера, и другие возможности;

3) при печати конфиденциальной информации ведется автоматическая маркировка каждой страницы грифом конфиденциальности, порядковым номером, а также указывается имя пользователя, производившего печать;

4) факт печати вносится в журнал регистрации, указывается дата и время печати, имя распечатанного файла и гриф конфиденциальности, имя пользователя, распечатывавшего документ, количество распечатанных копий.

3. Многопользовательская операционная система (МОС).

Одним из эффективных решений является многопользовательская операционная система, в состав которой входит специальная система, позволяющая осуществлять печать документов в соответствии с требованиями, предъявляемыми к защищенным системам. С помощью средств МОС происходит анализ уровня конфиденциальности документа. Если документ является конфиденциальным, за-

дание перенаправляется на сервер печати, если нет – документ печатается локально.

На этапе формирования задания на печать определяется уровень конфиденциальности документа, и задание автоматически направляется на принтер в соответствии с правилами печати, принятыми в данной организации. Каждый напечатанный лист автоматически маркируется учетными атрибутами документа, включающими фамилию пользователя, распечатавшего документ, и имя компьютера, с которого было отправлено задание на печать. Приложения, выводящие на печать, учитывают маркировку листов. Факт печати регистрируется в специальном журнале учета размножения печатных документов. Для работы с этим журналом используется специальная программа, позволяющая просматривать, редактировать некоторые поля записей и распечатывать их.

Анализ рассмотренных мер защиты от НСД показывает, что большинство мер направлено на защиту от внешних, а не внутренних нарушителей. Например, сотрудник, имеющий доступ к жесткому диску, потенциально может извлечь конфиденциальную информацию, уже подготовленную для печати или иной обработки. Пользуясь возможностями внутренней электронной почты, внутренний нарушитель может перенаправить документ или его обезличенную часть по не установленному адресу и т. д.

В случае же реализации мер защиты от потенциальных внутренних нарушителей эффективную помощь могут оказать специальные технические устройства. В настоящее время разрабатываются и используются решения, удовлетворяющие требованиям как по оперативной и качественной обработке документов, так и по безопасности их обработки и представления.

**Способы защиты конфиденциальной информации на этапах ввода и вывода информации из корпоративных сетей.**

К наиболее распространенным способам защиты конфиденциальной информации на этапах ввода и вывода

информации из корпоративных сетей относятся следующие [3].

1. Материалы, отправленные на печать, защищаются паролем и не распечатываются до тех пор, пока исполнитель не введет пароль либо с дисплея печатающего устройства, либо удаленно со своего терминала.

Защита документов обеспечивается за счет применения специального модуля, который задерживает передачу задания на печать до тех пор, пока пользователь не идентифицирует себя с помощью пароля на каком-либо из сетевых принтеров. Сервер печати сверяет IP-адрес компьютера пользователя со списком «авторизованных». Все обращения к устройствам допустимы только с тех компьютеров, чьи IP-адреса зарегистрированы на сетевой плате, остальные запросы игнорируются, неавторизированные – блокируются. Конфиденциальные документы распечатываются только после введения пароля на панели управления аппарата в присутствии пользователя.

2. Временные данные, которые сохраняются после выполнения любой операции на аппарате в памяти, стираются способом, не допускающим восстановления, например многократной перезаписью кода случайными последовательностями чисел [4].

3. Задания при отправке на печать зашифровываются и расшифровываются непосредственно перед печатью.

Применяются наборы защиты данных – специальное программное обеспечение устройств ввода/вывода и компьютеров, защищающие информацию комплексно. Такие наборы обеспечивают безопасность электронных данных, находящихся во внутренней памяти копира/принтера, шифруют все данные, сохраняемые в оперативной памяти принтера и на жестком диске, защищают данные от доступа, использующего сеть, интерфейсы принтера, линии связи и др.

4. Обращения к печати разрешаются только с тех компьютеров, адресам которых присвоены соответствующие полномочия.

5. Предусматривается автоматическая сортировка выводимых документов по персональным ячейкам сотрудников, физически закрываемых на ключ. Решение интересно удачным сочетанием организационных и технических мер защиты информации.

6. Используется функция сканирования на сервер электронной почты (scan-to-e-mail) с дальнейшим направлением отсканированных документов с панели управления аппарата на компьютер конкретного пользователя в заданную папку (scan-to-folder).

7. Для обеспечения безопасности предусматриваются и специальные меры: наличие малозаметных точек при печати, печать на фоне логотипа предприятия, с учетом места расположения и др. На оригинале может присутствовать скрытый упорядоченный набор точек, который и сигнализирует устройству о необходимости проигнорировать задание, например, создания копии.

8. Специальное клиентское ПО позволяет производить печать конфиденциальных документов при условии идентификации пользователя, а также имеет гибкие возможности по разграничению прав сотрудников на использование печатающих устройств посредством подключения специальных идентификационных устройств напрямую в локальную сеть в непосредственной близости от сетевых принтеров.

В качестве идентификационных устройств могут использоваться клавиатуры ввода PIN-кода, системы идентификации на основе магнитных или бесконтактных карт, системы ввода отпечатков пальцев и др. В комплекте с продуктом поставляются специальные утилиты, позволяющие эти данные получать с принтера, а также администрировать работу продукта. Каждому пользователю, который будет применять систему безопасности, на компьютер ставится небольшой драйвер, выдается смарт-карта и/или сообщается собственный PIN-код. При отправке документа на печать программа запрашивает необходимость его шифрования и использования функции безопасности. Задания

на жестком диске принтера хранятся в зашифрованном виде, они не дешифруются и не печатаются до тех пор, пока адресат не подойдет к принтеру и не авторизуется карточкой и/или PIN-кодом.

Такое программное обеспечение сертифицируется на соответствующие уровни безопасности международных стандартов, в частности стандарта ISO/IEC 15408.

Таким образом, можно сделать следующие выводы. Учет разнообразных условий обеспечения и выполнения требований по безопасности теперь стал отдельной и непростой задачей. В последних решениях ведущих производителей реализуются дополнительные функции, направленные на обеспечение удобства работы системных администраторов и пользователей; не только на составление, но и на кодирование списков персонала, допущенного к конфиденциальной информации, и др.

В устройствах последнего поколения не требуется запоминания дополнительных паспортов, идентификаторов для пользователей, традиционных кодов доступа к сетевому оборудованию. Имена пользователей и пароли, вводимые при стандартной авторизации Windows, используются и для «входа» на многофункциональное устройство, что особенно удобно для организаций с распределенной структурой управления.

Использование электронного документооборота в организациях, обрабатывающих конфиденциальную информацию, существенно сдерживается сложностью контроля ее обработки и пересылки по каналам электронной почты. В частности, практика работы с конфиденциальной информацией потребовала исключить возможность подделки поля «от кого» в шаблоне письма электронной почты при реализации функции «сканирование с последующей отправкой по каналам электронной почты» (scan-to-e-mail). Теперь авторизованное имя пользователя автоматически поступает в поле «имя отправителя» и изменить его нельзя, а отсканированный материал отправляется только по заданному адресу и недоступен другим пользователям.

Причем только пользователи, которым даются соответствующие полномочия, могут переправить файл в иное место после сканирования. Для затруднения доступа внутренних нарушителей к обрабатываемой информации реализована также функция «сканирование в папку» (scan-to-folder) заданного пользователя на его рабочей станции минуя каналы электронной почты, что еще более существенно сужает круг лиц, работающих с конфиденциальной информацией.

Существующие функции политики управления файлами и доступа к приложениям обеспечивают такую высокую степень гибкости администрирования процессов обработки документов, что обычный администратор компьютерной сети может поддерживать и функции администрирования многофункционального устройства. При этом пользователи могут быть объединены в группы, для которых задаются различные разрешенные функции печати и копирования.

Ограничению доступа к информации, которая может быть значимой для внутреннего нарушителя, способствует решение о кодировании адресной книги, в которой аккумулируются сведения обо всех зарегистрированных лицах, допущенных к работе на данном аппарате.

В качестве основного критерия выбора многофункциональных офисных устройств целесообразно использовать «цену отпечатка». В этом критерии в консолидированном виде отражаются все основные характеристики многофункциональных устройств, в том числе одна из ключевых составляющих совокупной стоимости владения – стоимость расходных материалов.

**Литература**

1. Computer Security Institute [Электронный ресурс]. URL: http://gocsi.com (дата обращения: 01.11.2012).

2. Computer Crime Research Center. Угрозы безопасности АС [Электронный ресурс]. URL: http://www.crime-research.ru/library/security7.htm (дата обращения: 03.11.2012).

3. *Абросимов В.* Как сохранить конфиденциальность в офисе // Директор информационной службы. 2007. № 03. – С. 11–16.
4. *Цапко И. В.* Структуры и алгоритмы обработки данных: Учеб. пособие. – Томск: Изд-во Томского политехнического университета, 2007. – 184 с.

УДК 004.056

**Е. И. Неёлов, А. М. Поляков, А. Н. Тюрин, Д. В. Частухин, Д. С. Евдокимов, А. А. Оприско**
ООО «Диджитал Секьюрити»

## БЕЗОПАСНОСТЬ SAP

Ядро каждой крупной компании – это ERP-система; в ней проходят все критичные для бизнеса процессы, начиная от закупки, оплаты и доставки и заканчивая управлением человеческими ресурсами, продуктами и финансовым планированием. Вся информация, хранящаяся в ERP-системах, имеет огромное значение, и любой неправомерный доступ к ней может понести за собой громадные потери вплоть до остановки бизнеса. Согласно отчету Ассоциации специалистов по расследованию хищений и мошенничества (ACFE), в период с 2006 по 2010 г. потери организаций от внутреннего фрода составили порядка 7% от ежегодной выручки [1].

Распространенный миф о том, что безопасность ERP – это только матрица SOD, в последнее время исчерпал себя и уже кажется многим историей давно минувших дней. В течение последних 5 лет специалистами в области безопасности SAP было представлено множество докладов, рассказывающих в подробностях о различных атаках на внутренние подсистемы SAP, как то: протокол обмена данными RFC, систему разграничения доступа – SAP ROUTER, на веб-приложения SAP и на клиентские рабо-

чие станции под управлением SAP GUI [2]. Каждый год интерес к теме возрастает в геометрической прогрессии: если в 2007 г. на специализированных технических конференциях по взлому и защите был всего 1 доклад про SAP [3], то в 2011 г. их было более 20. За последнее время был выпущен ряд утилит для взлома, подтверждающих возможность осуществления атак на SAP [4–6].

Согласно статистике уязвимостей в бизнес-приложениях, за 2009 г. было устранено более 100 уязвимостей в продуктах SAP, тогда как за 2010 г. их было уже более 500. А всего на март 2012 г. насчитывается более 2000 SAP security notes – уведомлений об уязвимостях в тех или иных компонентах SAP.

Большинство из этих уязвимостей позволяет неавторизированному пользователю получить доступ ко всем критичным для бизнеса компании данным, что вынуждает задуматься о применении тех или иных решений, направленных на защиту SAP-систем.

Недостаточная забота о безопасности SAP может привести к экономическим и репутационным рискам, а также к остановке бизнес-процессов. Последствиями могут быть:

- шпионаж (кража финансовой информации, кража персональных секретов, списки поставщиков и контрагентов);
- саботаж (отказ в обслуживании, модификация финансовой отчетности, нарушение работоспособности доверенных систем);
- мошенничество (подмена данных о платежах, ложные транзакции).

Тенденции развития инфраструктуры компаний в последнее время движутся от децентрализованной модели к интеграции всех бизнес-процессов в единые системы. Если раньше в компании было множество серверов, таких как почтовый, файловый, контроллер домена и пр., то сейчас все эти функции интегрируются в единое бизнес-приложение, чем обеспечивают, с одной стороны, удобство доступа, а с другой – единую точку отказа. В бизнес-

приложениях и в ERP-системах хранятся все критичные данные компании, начиная от финансовой отчетности и персональных данных и заканчивая списками контрагентов и объектами корпоративной тайны. Для внешнего злоумышленника или инсайдера такая система представляет собой основную мишень, и его конечная цель – это отнюдь не права администратора на контроллере домена.

Тем не менее сейчас многие специалисты по безопасности, к сожалению, крайне поверхностно осведомлены о защите таких бизнес-приложений, как SAP. Проблема также состоит в том, что функции обеспечения безопасности лежат не на CISO, а на владельцах системы, которые фактически контролируют сами себя. В итоге за безопасность наиболее критичных элементов системы никто не отвечает.

Из менее глобальных проблем также стоит отметить следующие.

• Отсутствие квалифицированных специалистов. В большинстве компаний безопасность SAP со стороны SAP-специалистов воспринимается только как проблема SOD, со стороны же службы безопасности понимание угроз SAP в лучшем случае поверхностно, не говоря уже о тонких настройках.

• Огромное количество тонких настроек. В стандартных настройках системы существует более 1000 параметров, а также огромная масса тонких настроек, не говоря уже о разграничении прав к различным объектам, таким как транзакции, таблицы, RFC-процедуры и прочие – к примеру, одних только веб-интерфейсов для доступа к системе может быть несколько тысяч. Во всей этой массе настроек задача по обеспечению безопасности даже одной системы может быть непростой задачей.

• Кастомизируемые настройки. Вряд ли найдутся две одинаковые SAP-системы, поскольку большая часть настроек так или иначе «затачивается» под заказчика, и, кроме того, разрабатываются свои программы, безопасность которых также следует учитывать при комплексной оценке.

• Автоматизация. Наличие большого количества систем с постоянно изменяемыми конфигурациями также вносит дополнительные проблемы.

Кроме всего, необходимо понимание того, что безопасность требуется обеспечивать на всех возможных уровнях: сервера приложений, сервера баз данных, операционной системы сервера, сетевой инфраструктуры, анализа безопасности кода и клиентских систем.

Периодически компания SAP выпускает внутренний документ, который называется «уведомление о безопасности» (SAP Security note). В нем, как правило, хранится информация об одной или более уязвимостях в продуктах SAP или ошибках конфигурации, которые представляют риск для систем SAP. Первое такое уведомление было опубликовано в 2001 г. Начиная с 2007 г. их количество растет в геометрической прогрессии (рис. 1).

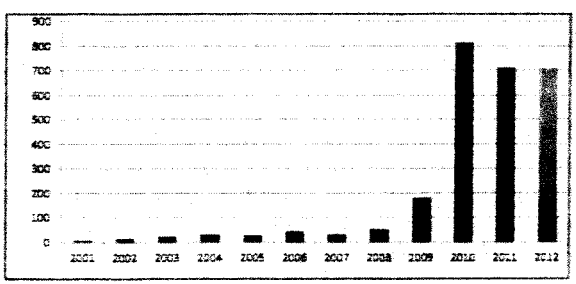



Рис. 1. Количество уведомлений о безопасности

В течение 2011 г. в День критических патчей (каждый второй вторник) обычно публиковалось примерно 65 уведомлений о безопасности SAP. Если сравнивать с другими производителями, то это больше, чем у Microsoft, Oracle и Cisco. Стоит отметить, что всего 3 года назад их было намного меньше.

По данным на 26 апреля 2012 г., опубликовано более 2000 уведомлений о безопасности SAP.

SAP использует 5 уровней критичности для своих уведомлений (рис. 2).

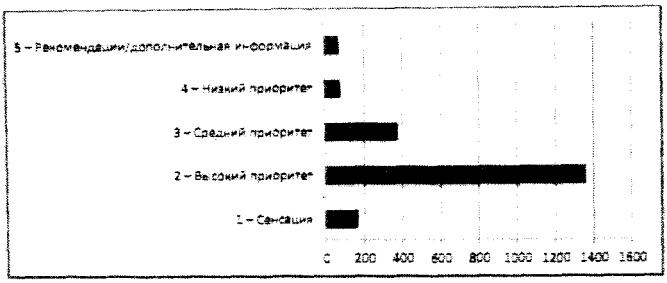



Рис. 2. Уровни критичности уведомлений

Большинство проблем (69%) имеют высокий приоритет, а это означает, что около 2/3 публикуемых уязвимостей необходимо исправлять быстро.

В 2010 г. SAP приняла решение благодарить сторонних исследователей безопасности за уязвимости, найденные в их продуктах (рис. 3). На диаграмме можно увидеть количество уязвимостей, обнаруженных сторонними исследователями с 2010 г. Половина уязвимостей была найдена и успешно исправлена компанией SAP с помощью Digital Security (50 уязвимостей и 26% от общего количества) и VirtualForge (44 уязвимостей, т. е. 23%). Вторая половина была обнаружена двумя десятками других компаний, и их количество растет, что доказывает рост популярности данной области [7].

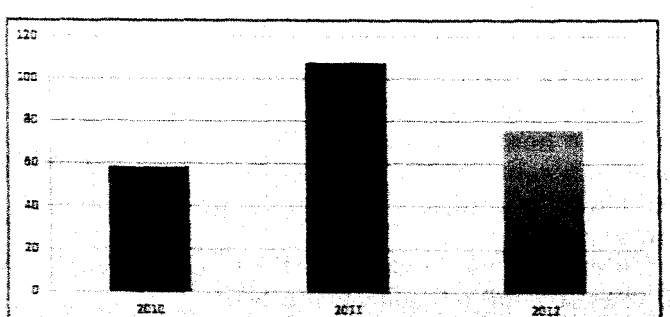



Рис. 3. Количество благодарностей исследователям безопасности

Наибольшую опасность представляют уязвимости, информация об эксплуатировании которых (подробное описание уязвимости, PoC-эксплойты или полноценные эксплойты) доступна онлайн (рис. 4).

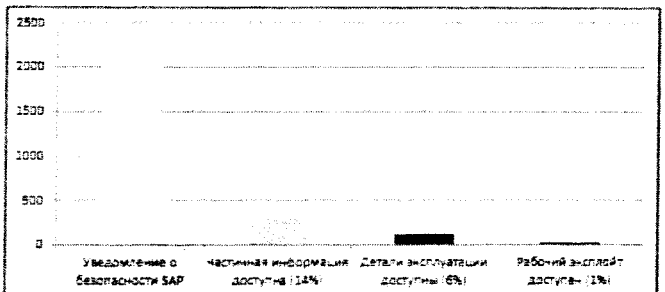



Рис. 4. Доступность информации об уязвимостях

На графике уязвимости отсортированы по вероятности и простоте эксплуатации, согласно количеству информации, которая доступна хакерам в публичных источниках, а не в закрытых уведомлениях о безопасности SAP.

Существуют ресурсы, которые собирают и классифицируют информацию об уязвимостях и экслойтах:

- SecurityFocus [8] – здесь можно найти детальное описание, иногда PoC-эксплойт. Все уязвимости в этой базе имеют высокую вероятность эксплуатации. Здесь были найдены подробности о 123 уязвимостях (6% от общего количества);
- Exploit-DB [9] – здесь расположены готовые эксплойты, которыми можно пользоваться, не внося изменений и не имея никаких знаний об эксплуатировании соответствующей системы. Все уязвимости в этой базе имеют критичную вероятность эксплуатации. Здесь были найдены 24 эксплойта (1% от общего количества уязвимостей).

Компания Digital Security, поставщик лидирующего в области безопасности SAP решения ERPScan – системы мониторинга защищенности SAP-систем, провела глобаль-

ное исследование безопасности SAP. Из опубликованного доклада [10] очевидно, что интерес к безопасности SAP растет в геометрической прогрессии.

Учитывая растущее количество уязвимостей (рис. 5) и огромное количество систем SAP, доступных через Интернет, системы SAP могут стать мишенью не только для прямых направленных атак (так называемых APT), но и для массовой эксплуатации посредством «червей», в том числе использующих множество уязвимостей одновременно.

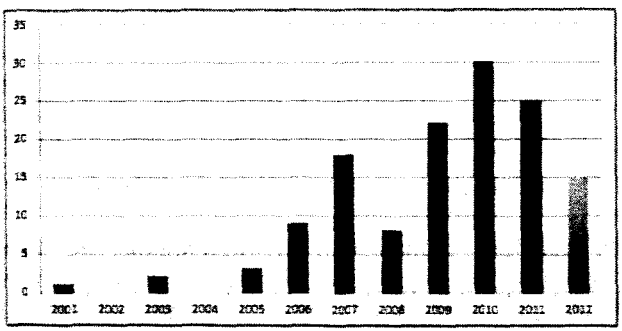



Рис. 5. Количество уязвимостей и эксплойтов

Компания SAP регулярно публикует новые документы по безопасной конфигурации SAP-систем, тем самым обучая администраторов методам защиты от новых угроз. На данный момент основная миссия по защите SAP-систем возложена на службу безопасности и администраторов, которым необходимо защищать свои системы, изучая руководства, настраивая безопасные конфигурации, устанавливая последние обновления и проводя аудит кода ABAP программ на постоянной основе.

## Литература

1. *Goldman A.* As economy falters, employee theft on the rise [Электронный ресурс]. 06.11.2009. URL: http://www.lasvegassun.com/news/2009/nov/06/managing-fraud-lesson-recession (дата обращения: 10.11.2012).

2. *Polyakov A.* SAP Security: attacking SAP clients [Электронный ресурс]. 03.09.2009. URL: http://erpscan.com/publications/sap-security-attacking-sap-clients (дата обращения: 10.11.2012).

3. *Lord S.* Mo' Budget, Mo' Problems [Электронный ресурс]. URL: http://cansecwest.com/slides06/csw06-lord.ppt (дата обращения: 10.11.2012).

4. ERPScan's SAP Pentesting Tool [Электронный ресурс]. URL: http://erpscan.com/products/erpscan-pentesting-tool (дата обращения: 10.11.2012).

5. ERPScan WEBXML Checker [Электронный ресурс]. URL: http://erpscan.com/products/erpscan-webxml-checker (дата обращения: 10.11.2012).

6. Sapyto – SAP Penetration Testing Framework [Электронный ресурс]. URL: http://www.cybsec.com/EN/research/sapyto.php (дата обращения: 10.11.2012).

7. Acknowledgments to Security Researchers [Электронный ресурс]. 14.11.2012. URL: http://scn.sap.com/docs/DOC-8218 (дата обращения: 15.11.2012).

8. SecurityFocus. Vulnerabilities [Электронный ресурс]. URL: http://securityfocus.com (дата обращения: 15.11.2012).

9. The Exploit Database. [Электронный ресурс]. URL: http://exploit-db.com (дата обращения: 15.11.2012).

10. *Поляков А.* и др. Безопасность SAP в цифрах. Результаты глобального исследования за период 2007–2011 [Электронный ресурс]. URL: http://erpscan.ru/wp-content/uploads/2012/06/Безопасность-SAP-в-цифрах-результаты-глобального-исследования-2007–2011.pdf (дата обращения: 15.11.2012).

УДК 004.056

**Т. Г. Семёнова**

Санкт-Петербургский государственный
инженерно-экономический университет

# ЛИЦЕНЗИОННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КАК ФАКТОР БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

При оценке общей стоимости активов современных компаний наблюдается увеличение доли нематериальных

активов, в частности, доля программного обеспечения в общей стоимости электронных систем предприятия достигла 25%. Не материальные ценности, а изобретения, открытия, ноу-хау и компьютерные программы становятся одной из важнейших составляющих информационных систем предприятий. Чем крупнее предприятие, тем выше требования по безопасности предъявляются к ИТ-системе для надежной работы всех его подразделений. С внедрением и применением информационных технологий значительно повышаются производительность труда сотрудников, эффективность и конкурентоспособность компании в целом. Однако частичная или полная неработоспособность ИТ-системы в случае отказа, сбоя или несовместимости аппаратного или программного обеспечения может привести к серьезным последствиям. Не последнюю роль в этом играет лицензионная чистота программного обеспечения организации.

По статистике НППП (Некоммерческого партнерства поставщиков программных продуктов)[1], за 2011 г. только на территории России было возбуждено более 5890 уголовных дел, связанных с незаконной деятельностью в сфере информационных технологий. По сведениям информационного агентства БалтИнфо[2], в период с 9 по 19 октября 2012 г. в Санкт-Петербурге сотрудниками УЭБ и ПК ГУ МВД России проводилось оперативно-профилактическое мероприятие «Контрафакт». По итогам мероприятия за 10 дней проверено 1035 предприятий, выявлено 89 правонарушений. Всего изъято более 22 тыс. ед. носителей информации на сумму свыше 600 тыс. руб. Из них 1501 ед. программного обеспечения для ЭВМ.

При таких обстоятельствах перед руководителями организаций и ИТ отделов все чаще встает вопрос о прекра-

---

[1] Некоммерческое партнерство поставщиков программных продуктов: Официальный сайт [Москва] [Электронный ресурс]. 2001–2010. URL: http://www.appp.ru/index.php (дата обращения: 15.11.2012).

[2] Балтийское информационное агентство БалтИнфо: Официальный сайт «Балтийская Медиа Группа» [СПб.] [Электронный ресурс]. 2009–2012. URL: http://www.baltinfo.ru/2012/10/30/V-Peterburge-podvedeny-itogi-operatcii-Kontrafakt (дата обращения: 15.11.2012).

щении использования контрафактного и переходе на лицензионное ПО. Причин, по которым необходимо отказаться от использования нелицензионного программного обеспечения на предприятии, может быть несколько.

*Нелицензионное ПО. Риски использования.*

1. Правовая ответственность. Работа с нелицензионным программным обеспечением противоречит требованиям законодательства о соблюдении прав интеллектуальной собственности и может привести к уголовной, административной, гражданско-правовой ответственности.

2. Финансовые потери в случае длительных простоев в деятельности организации при проведении проверки правоохранительными органами и изъятии компьютеров и серверов.

3. Налоговые претензии. С точки зрения налогового законодательства факт установки и использования ПО, стоимость которого не имеет соответствующего отражения в балансе, может быть истолкован как нарушение правил учета объектов налогообложения и неуплата соответствующих сумм налогов, влекущие ответственность в соответствии с Налоговым кодексом.

4. Риски потери клиентов, связанные с неисполнением договорных обязательств из-за изъятия компьютеров и серверов.

5. Риски потери репутации, связанные с ухудшением имиджа организации и уровня доверия к ней в случае привлечения генерального директора или сотрудников к уголовной ответственности, как следствие, падение доверия партнеров и инвесторов.

6. Технологические риски, связанные с нестабильностью работы контрафактных программ, отсутствием обновлений, отсутствие сервиса технической поддержки. Потеря данных и невозможность обеспечения бизнес-процессов вследствие возникновения критических сбоев системы, ведущих не только к простою предприятия, но и к прямым финансовым потерям. При этом, как правило, такие сбои начинают происходить именно тогда, когда используемое

ПО работает с максимальной нагрузкой, а его бесперебойное функционирование критически важно.

7. Проблемы глобального развития компании и выхода на мировой рынок. Выпуск акций возможен только при условии использования лицензионного ПО. Кроме этого, не представляется возможным пройти сертификацию по стандартам ISO без лицензирования ПО, используемого для поддержки сертифицируемых бизнес-процессов.

8. Утечка коммерческой и прочей информации вследствие отсутствия обновлений безопасности, выпускаемых производителем.

9. Возникновение мелких сбоев пользовательских систем, приводящих к постоянным простоям сотрудников и снижению производительности труда, к увеличению затрат.

Независимо от того, по какой причине руководство предприятия задумалось о прекращении использования контрафактного программного обеспечения, решать этот вопрос необходимо как можно раньше, поскольку нарушение закона влечет привлечение к ответственности.

Виды ответственности за использование нелицензионного программного обеспечения:

- административная;
- уголовная;
- гражданско-правовая.

Административная ответственность за нарушение авторских прав наступает в случае, если стоимость контрафактных экземпляров программ для ЭВМ составит менее 50 000 руб. При этом необходимо учитывать, что стоимость конкретных экземпляров будет рассчитываться исходя из стоимости лицензий, реализуемых в рознице.

Уголовная ответственность наступает в случае, если стоимость контрафактных экземпляров произведений составляет более 50 000 руб., при этом преступление считается совершенным в крупном размере, если стоимость контрафактных произведений составляет не более 250 000 руб., в противном же случае преступление считается совершенным в особо крупном размере. Также уголовная от-

ветственность может наступать, если преступление совершено хотя и в крупном размере (стоимость контрафактных экземпляров составляет до 250 000 руб.), но группой лиц по предварительному сговору или лицом с использованием своего служебного положения.

Необходимо отметить, что за нарушение авторских прав наступает или административная, или уголовная ответственность в зависимости от суммарной стоимости экземпляров произведений. При этом к административной ответственности может быть привлечен как гражданин, так и должностное лицо (например, руководитель), и сама организация. К уголовной ответственности привлекается физическое лицо – как правило, или генеральный директор, или системный администратор (IT-руководитель). Юридическое лицо не может быть привлечено к уголовной ответственности.

Вместе с тем вне зависимости от наступления уголовной или административной ответственности правообладатель может привлечь нарушителя (юридическое лицо) к гражданско-правовой ответственности.

Гражданско-правовая ответственность наступает, как правило, в виде обязанности по выплате компенсации за нарушение авторских прав или убытков[1].

Если по общему правилу взысканию подлежат убытки (которые трудно доказать), закон существенно упростил положение правообладателя и предоставил ему возможность взыскать или убытки или компенсацию, причем последняя взыскивается в размере от 10 000 до 5 000 000 руб. по усмотрению суда или в двукратном размере стоимости контрафактных экземпляров произведений при доказанности только факта нарушения авторских прав. Иными словами, для получения компенсации правообладателю достаточно доказать только факт нарушения своих прав, а размер компенсации доказывать не нужно.

---

[1] Гражданский кодекс РФ от 18.12.06 № 230-ФЗ. Ч. IV: Принят Гос. думой 24 ноября 2006 г.; одобрен Советом Федерации 8 декабря 2006 г. Федеральный закон № 323423-4 (ред. от 04.10.10 № 259-ФЗ). Ст. 1261, 1228, 1229,1270, 1285, 1286.

Кроме выплаты компенсации нарушитель также может быть привлечен к еще одному виду гражданско-правовой ответственности: юридическое лицо может быть ликвидировано принудительно. Если юридическое лицо неоднократно или грубо нарушает исключительные права на результаты интеллектуальной деятельности, суд может принять решение о ликвидации такого юридического лица по требованию прокурора.

В подавляющем большинстве случаев проверки проводятся сотрудниками подразделений по борьбе с экономическими преступлениями или подразделениями по борьбе с преступлениями в сфере высоких технологий (отделы или управления «К») на основании Закона «Об оперативно-розыскной деятельности».

Указанный закон делит основания для проведения оперативно-розыскного мероприятия на 2 категории: когда уголовное дело возбуждено или нет.

В первом случае основанием для проведения проверки будет служить отдельное поручение следователя, причем оперативный уполномоченный по такому поручению может производить как оперативно-розыскные мероприятия, так и следственные действия.

Во втором случае, когда уголовное дело еще не возбуждено и проводимые оперативно-розыскные мероприятия осуществляются лишь с целью возбуждения уголовного дела, оперативный уполномоченный действует на основании постановления о производстве оперативно-розыскного мероприятия. Данное постановление должно содержать наименование оперативно-розыскного мероприятия (или мероприятий); перечень лиц, которые проводят такое мероприятие, и постановление в обязательном порядке должны быть утверждены начальником криминальной милиции или подразделения, которое производит проверку.

Следует сказать о том, что в настоящее время встречаются случаи, когда проверка проводится в организациях, которые уже используют лицензионное программное обеспечение. Для таких организаций, к сожалению, также оста-

ется угроза изъятия компьютеров и серверов, однако грамотное доказывание проверяющим законности использования программного обеспечения и предъявление всех необходимых документов в большинстве случаев позволяют решить вопрос без изъятия. К сожалению, в случае изъятия исследование на предмет признаков нелегальности, конечно, установит, что программы для ЭВМ используются законно, но на это уйдет определенное количество времени, а компьютеры все это время будут находиться у правоохранителей.

В случае использования лицензионных программ и проведения проверки можно рекомендовать предоставить максимально возможный комплект документов на используемый софт. При наличии документов и грамотного поведения проверяемых (когда сотрудники правоохранительных органов понимают, что их действия по изъятию являются незаконными и обязательно будут обжалованы) изъятия компьютеров, как правило, не происходит.

Термин и понятие Software Asset Management не часто встречается в прессе, зачастую вопросы лицензирования ПО и управления программными активами рассматривают разве что на специализированных сайтах. Однако эти вопросы напрямую связаны с правовыми рисками компаний и вопросами безопасности информационных систем компаний.

Управление лицензиями – SAM (Software Assets Management) – набор процедур, позволяющих манипулировать лицензиями на ПО как особым активом: минимизировать затраты, увеличивать отдачу от использования, снижать риски.

Внедрение технологии управления лицензиями позволяет в любой момент времени иметь полную информацию о том, какие программы и лицензии на ПО используются в организации. Управление лицензиями включает в себя регулярную инвентаризацию лицензий и используемых программ, введение стандартов использования ПО, централизованные закупки и многое другое. Использование этой технологии способствует оптимальному выбору

подходящего варианта лицензирования, оптимизации и эффективному планированию расходов на развитие информационной системы, а также грамотному обоснованию необходимости инвестиций в корпоративное ПО.

Результатом внедрения технологии является проработанный стратегический план управления активами, который позволяет контролировать приобретение программных продуктов, а также благодаря гибкой системе скидок экономить денежные ресурсы и повышать эффективность работы как ИТ-службы, так и всей организации в целом. Компания в итоге получает оптимизированную информационную инфраструктуру, которой можно легко управлять и масштабировать.

Практически не предлагают внедрения технологий управления программными активами продавцы ПО, им это не выгодно с точки зрения падения объемов продаж. Существуют ситуации, когда в компаниях присутствует «перелицензирование», т. е. ПО приобретается организацией неоднократно. Подобную ситуацию необходимо исправлять, информируя пользователей и прививая культуру уважения к авторским правам у будущих инженеров по информационной безопасности.

Российские компании еще не приняли идею управления ПО в полном масштабе. Бизнес не понимает всей важности и сложности лицензионных соглашений, проблем с бесплатным и свободным ПО. Бизнес чувствует риски от отсутствия SAM только тогда, когда уже пришли с судебным иском или сеть компании упала, данные потеряны.

На очередной ежегодной конференции SAM, проходившей под флагом SiRB (Software Industry Research Board) – дочерней организации FAST (Federation Against Software Theft)[1], в очередной раз в нескольких докладах была представлена статистика главных движущих факто-

---

[1] FAST (Federation Against Software Theft) – Федерация против компьютерного пиратства: Официальный сайт: [UK, York House] [Электронный ресурс]. 2012. URL: http://www.fastiis.org (FAST – британский аналог американской BSA (Business Software Alliance) и российской НППП (Некоммерческого партнерства поставщиков программных продуктов)).

ров SAM. Анализировались факторы, которые побуждают организации заняться учетом ПО. Лидирующие мотивы связаны с соблюдением лицензий (License Compliance) и рисками нарушения закона (Legal Risks). Именно юридические риски заставляют в первую очередь задуматься о точном учете и контроле. И уже потом, когда в юридической части наведен хотя бы частичный порядок, на сцену выходят технические факторы. И только в последний момент, когда база готова, организация готова рассматривать программное обеспечение как неотъемлемый и ощутимый актив и «рулить» им как частью общего финансово-корпоративно-управленческого механизма.

На конференции также были представлены инструменты учета и контроля ПО[1]. Производители давно осознали, что недостаточно сканировать реестр компьютера, и уже умеют определять программное обеспечение по файлам и другим косвенным признакам, широкое применение получает технология мониторинга работы пользователей. Мониторинг позволяет выявить программные продукты, которые никаким другим образом не находятся, например запускаемые из сети или с подключаемых носителей. Кроме того, мониторинг незаменим для определения, какими программными средствами сотрудники организации пользуются чаще всего. А это данные для уточнения состава ПО и в дальнейшем повышения эффективности вложений.

В качестве основных проблем развития инструментов учета и контроля за ПО ведущие эксперты в области SAM[2] называют виртуализацию, как серверную, так и приложений, и связанную с этим тему терминальных клиентов. К сожалению, все еще мало внимания уделяется учету и контролю параметров, отличных от количества инсталляций: количеству сессий, почтовых ящиков и т. п. Каждый производитель ПО накладывает свои ограничения, в

---

[1] Software Licence Management Product Reviews: Инструменты учета программных продуктов [Электронный ресурс]. URL: http://www.fastiis.org/evaluation.

[2] Сайт об управлении программным обеспечением [Москва] [Электронный ресурс]. 2012. URL: http://samexpert.ru (дата обращения: 15.11.2012).

зависимости от модели бизнеса, а интерфейсы для контроля этих параметров не стандартизованы. Остается надеяться на скорейшее принятие новых стандартов семейства ISO/IEC 19770[1], о чем также говорили многие на конференции. А также на государственную поддержку и адаптацию ISO/IEC 19770 в виде ГОСТов.

**Литература**

1. Гражданский кодекс Российской Федерации. Ч. IV (ГК РФ) [Электронный ресурс]. URL: http://www.consultant.ru/ popular/gkrf4 (дата обращения: 16.11.2012).

2. Государственная система правовой информации: Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://www.pravo.gov.ru (дата обращения: 16.11.2012).

3. *Семенова Т. Г.* Проблемы моделирования управления программными активами // Вестник ИНЖЭКОНа. – 2012. № 2(53). – С. 296.

УДК 004.056

**Р. А. Васильев**

Нижегородский научно-технический центр
ФГУП «НПП "Гамма"»,
НГЛУ им. Н. А. Добролюбова

# ИССЛЕДОВАНИЕ ОСОБЕННОСТЕЙ ФОНЕТИЧЕСКОГО СТРОЯ РЕЧИ И ИДЕНТИФИКАЦИЯ ДИКТОРОВ ПО ГОЛОСУ

В связи с возросшей информатизацией современного общества, увеличением числа объектов и потоков информации, которые необходимо защищать от несанкционированного доступа, а также необходимостью интеллектуализации всех форм взаимодействия пользователей автоматизированных систем управления с техническими средствами

[1] Международный стандарт ISO/IEC 19770-2:2009: Information technology – Software asset management [Электронный ресурс]- URL: http://www.iso.org/iso (дата обращения: 15.11.2012).

все более актуальными становятся проблемы использования механизмов речевых технологий для разграничения доступа к информационно-вычислительным системам, в частности метод идентификации пользователей системы по голосу. Привлекательность данного метода – удобство в применении. Продукты с проверкой голоса сейчас предлагают более 20 компаний.

Из экспериментальной фонетики хорошо известно, что у дикторов разного возраста и пола как состав, так и свойства элементов списка фонем сильно варьируются. Поэтому, сопоставляя фонетические базы данных (ФБД) разных дикторов, мы по их рассогласованию можем с высокой точностью и чувствительностью оценить его принадлежность произнесенных фонем тому или иному диктору, причем благодаря информационной теории восприятия речи (ИТВР) – с количественной характеристикой его отклонения от нормы. Этим дается одновременно наиболее информативное и компактное описание каждой отдельной фонемы. В таком случае множество всех выделенных из речевого потока речевых единиц и определяет в конечном итоге фонетический строй речи данного диктора на роль высокоинформативной базы данных для идентификационных обследований.

Задача распознавания диктора по голосу может быть разделена на две подзадачи: идентификация и верификация. Распознаваемый голос сравнивается с эталонными голосами, и из набора выбирается тот диктор, голос которого в наибольшей степени соответствует данному. В случае верификации говорящий вначале предъявляет свой идентификатор (объявляет, кто он такой), а затем система определяет, принадлежит ли распознаваемый голос диктору с указанным идентификатором или нет. В задаче верификации при росте числа пользователей время принятия решения не увеличивается и является постоянным для различного числа пользователей. Это определяет возможность более широкого применения систем верификации, чем систем идентификации.

К настоящему моменту у нас и за рубежом реализованы системы автоматической идентификации по голосу, большинство из которых строятся по единой концептуальной схеме:

- производится регистрация пользователя и вычисляется шаблон;
- выбираются участки речевого потока для дальнейшего анализа;
- осуществляется первичная обработка сигнала;
- вычисляются первичные параметры;
- строится «отпечаток» (шаблон) голоса;
- производится сравнение «отпечатков» голосов и формируется решение по идентичности голосов или «близости» голоса к группе голосов.

В поисках путей решения проблемы *адекватной системы описания отдельных фонем* в работах [3, с. 24–33], [4, с. 26–31] само понятие «фонема» впервые было строго определено в теоретико-информационном смысле как *«множество однородных минимальных звуковых единиц (МЗЕ), объединенных в кластер по критерию минимального информационного рассогласования (МИР) в метрике Кульбака-Лейблера»*. Условно говоря, человеческий мозг объединяет и запоминает в себе как нечто целое (в виде абстрактного образа) разные образцы (произношения) каждой отдельной фонемы в соответствующей «сфере» своей памяти вокруг абстрактного «центра» с заданным «радиусом» (рис. 1) [1, с. 3–9].

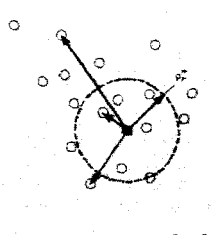


**Рис. 1. Образцы произношения каждой отдельной фонемы в соответствующей «сфере»**

Несмотря на существующие различия в реализациях фонем одного диктора, все они воспринимаются человеком как нечто общее, иначе речь утратила бы свою информативность. Можно поэтому утверждать, что одноименные реализации $x_{r,j}$, $j=\overline{1,J_r}$, $J_r \gg 1$ в сознании человека группируются в соответствующие классы или речевые образы фонем $X_r=\{x_{r,j}\}, r=\overline{1,R}$, вокруг некоторого центра – эталонной метки данного образа. В информационной теории восприятия речи указанные эталоны определяются в строгом, теоретико-информационном смысле [3, с. 24–33]: речевая метка $x_r^* \subset X_r$ образует *информационный центр-эталон* $r$-го речевого образа, если в пределах множества $X_r$ она характеризуется минимальной суммой информационных рассогласований (ИР) по Кульбаку-Лейблеру относительно всех других его меток-реализаций $x_{r,j}$, $j=\overline{1,J_r}$.

Нетрудно увидеть, что именно в понятии информационного центра (ИЦ) $r$-го множества реализаций $X_r$ дается наиболее информативное описание свойств соответствующей фонемы. Одновременно становится очевидным и механизм формирования самого этого множества. Анализируемый (входной) речевой сигнал $X(t)$ в дискретном времени $t$ = 0, 1, ... сначала разбивается на ряд последовательных сегментов данных $x(t)$ длиной в одну МЗЕ: примерно 10–15 мс. После этого каждый такой парциальный сигнал рассматривается в пределах конечного списка фонем $\{X_r\}$ и отождествляется с той $X_\nu$ из них, которой отвечает минимум информационного рассогласования (МИР) между вектором $x(t)$ и соответствующим эталоном $x_\nu^*, \nu \le R$. Это известная [4, с. 26–31] формулировка критерия МИР в задачах автоматического распознавания речи. Задача существенно упрощается, если воспользоваться гауссовой (нормальной) аппроксимацией закона распределения каждой фонемы вида $P_r = N(K_r)$, где $K_r$ – автокорреляционная матрица (АКМ) размера $n \times n$, $n \ge 1$.

Голос формируется из комбинации физиологических и поведенческих факторов. В настоящее время идентификация по голосу используется для управления доступом в помещение средней степени безопасности, например лаборатории и компьютерные классы. Идентификация по голосу удобный, но в то же время не такой надежный, как другие биометрические методы. Например, человек с простудой или ларингитом может испытывать трудности при использовании данных систем. Существует также возможность воспроизведения звукозаписи с магнитофона.

**Особенности фонетического строя речи.**

В связи с тем, что голосовая автоматическая идентификация дикторов бесконтактна и не требует от человека особых усилий, в России и за рубежом активно ведутся работы по созданию голосовых замков и систем ограничения доступа к информации. Интерес к этой тематике активно подогревается тем, что, по прогнозам, наличие голосовых интерфейсов обмена информацией должно стать стандартом для карманных компьютеров и сотовых телефонов. Автоматическое распознавание дикторов – это один из важных фрагментов будущих голосовых интерфейсов. На сегодняшний день существуют два различных подхода к решению задачи биометрической идентификации человека по голосу. Оба этих подхода построены на учете структуры речевого сигнала. В свою очередь, структура речевого сигнала образуется последовательностью всплесков колебаний и пауз между ними (рис. 2).

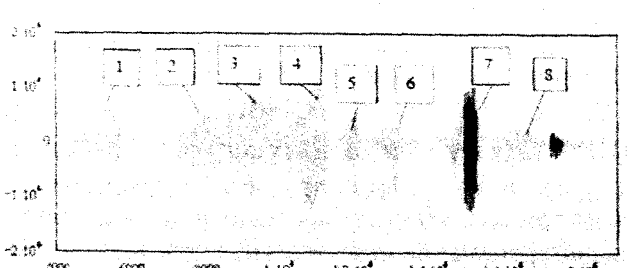



Рис. 2. Пример голосовой фразы и выделения из нее 8 фрагментов

Всего в русской речи выделяют 42 фонемы, но далеко не все фонемы пригодны для идентификации человека [3, с. 24–33]. Часть фонем хорошо согласованы, и именно они носят ярко выраженный индивидуальный характер. К хорошо согласованным (колебательным) фонемам относятся звуки «э», «о», «л», «а», «и», ... . Другая часть фонем шипящие (шумоподобные), к ним относятся звуки «ц», «ч», «ш», «щ», ... . Эти звуки не носят индивидуального характера и использовать их при идентификации диктора бесполезно. Существует и некоторая промежуточная группа фонем, достаточно вокализованных, но в то же время имеющих значительную шумовую составляющую.

Вычисления фонем повторяются циклически для всех последующих сегментов данных из речевого сигнала $X(t)$, причем повторятся «нарастающим итогом» для переменного значения $R = 2, 3, \ldots$ . Каждый очередной сегмент данных сопоставляется по правилу одновременно со всеми $R$ множествами $\{X_r\}$ из текущего списка фонем. При этом не исключается возможность объединения одного и того же сегмента данных с элементами одновременно нескольких разных множеств. В результате будем иметь список фонем с некоторым фиксированным числом элементов $R^*$. Это важная характеристика как речевого сигнала, так и самого диктора. Чем больше значение $R^*$ для конкретного диктора, тем богаче с фундаментальной, фонетической точки зрения его речь.

В данном выводе и состоят, по-видимому, главный смысл и назначение фонетического анализа речи (ФАР). Однако здесь же присутствует и очевидная проблема: чрезмерно большое число фонем в речи диктора – это признак ее нечеткости, или не информативности. С точки зрения качества устной речи первостепенный интерес, безусловно, представляет собой множество четких МЗЕ. Его, в таком случае, и следует считать основным итогом ФАР. Поэтому логика подсказывает: после выполнения всех перечисленных выше вычислений некоторые «фонемы» из окончательного списка можно исключить как маргинальные.

Добавим к сказанному, что предложенный алгоритм имеет множество разнообразных модификаций за счет, главным образом, применения рекуррентных вычислительных процедур корреляционно-спектрального анализа [3, с. 24–33]. Среди них наибольший интерес представляет метод обеляющего фильтра (МОФ) [4, с. 26–31], основанный на авторегрессионной модели МЗЕ.

В работе [5, с. 297–303] было показано, что в асимптотике, когда $n \to \infty$, и при гауссовом распределении речевого сигнала $P_r = N(K_r)$ с обратной АКМ ленточной структуры выражение для оптимальной решающей статистики сводится к виду

$$\rho_{x,r} = \frac{1}{F+1} \sum_{f=0}^{F} \frac{\left| 1 + \sum_{m=1}^{p} a_r(m) e^{-j\pi m f/F} \right|^2}{\left| 1 + \sum_{m=1}^{p} a_x(m) e^{-j\pi m f/F} \right|^2} - 1 \geq 0.$$

Здесь $\{a_x(m)\}, \{a_r(m)\}$ – два вектора АР-коэффициентов: входного сигнала и $r$-го эталона, оба одного порядка $p > 1$. Это стандартная формулировка МОФ в частотной области. Преимуществом данной интерпретации критерия МИР является, прежде всего, возможность его эффективной реализации в адаптивном варианте на основе быстрых вычислительных процедур АР-анализа, таких как метод Берга и др. [4, с. 26–31]. Именно такой вариант МОФ был реализован в дальнейшем для проведения его экспериментальных исследований в типовой задаче ФАР.

Следует обратить внимание на то, что вокализованные фрагменты речи имеют явно выраженный периодический (колебательный) характер. Период колебаний и характер колебаний весьма и весьма индивидуальны. В этом легко удостовериться, сравнивая внутренние колебания одинаковых вокализованных участков речи для одного и того же человека с другим человеком.

Формы внутренних колебаний периодических переходных процессов для одного человека на одном фрагменте одной и той же фразы очень похожи. В частности, практически совпадают число внутренних колебаний, постоянная их затухания и период повторения колебательных процессов (период основного тона). У другого человека оказываются существенно иными и период основного тона и форма внутренних колебаний переходных процессов. Все это свидетельствует о близости частотных спектров голосовых фраз одного человека и существенном их отличии от спектра аналогичной фразы, но произнесенной другим человеком.

Индивидуальные различия распределения мощности сигнала по спектру положены в основу первых систем биометрической аутентификации человека по голосу. Они строятся на базе гребенки узкополосных фильтров, выделяющих из голоса колебания разных частот. Заметим, что полосы пропускания разделяющих фильтров подбираются при проектировании биометрической системы, но полосовые фильтры не могут быть слишком узкими. Система не должна быть чувствительной к собственным вариациям частотного спектра голоса человека. С другой стороны, информации о распределении спектральной плотности должно быть достаточно для уверенной идентификации человека. Обычно используют гребенку из 16 фильтров, которые по аналогии с гребенкой вокодеров расширяются по мере роста значений выделяемой частоты. Это связано с тем, что высокие частоты менее стабильны по энергии в сравнении с низкими частотами.

Системы спектрального анализа голоса обучаются периодически запоминая распределение энергий по 16 каналам. Периодичность опроса каналов составляет порядка 35 мс (миллисекунд). В итоге получается достаточно большой массив данных, соответствующий анализируемому слову (фразе). Если этого типа системы воспроизводятся программно, то стараются использовать входные данные, снятые с частотой 16 кГц 16 разрядным АЦП, что связано с

особенностями реализации гребенки цифровых фильтров. Решение об эквивалентности полученной фразы эталону принимается любым известным на сегодня аппаратом. Может быть использован классический аппарат математической статистики или та же самая задача может быть решена в нейросетевом базисе. Все определяется традициями и взглядами разработчика биометрической системы. Независимо от используемого математического инструмента, при корректном его использовании конечные результаты оказываются сопоставимы.

**Программа экспериментальных исследований.**

Эксперимент состоял из двух этапов.

На *первом этапе* были выбраны 20 наиболее распространенных фонем русского языка: «а», «о», «у», «э», «ш», «щ», «р», «с», «в», «з», «ж», «и», «л», «л'», «ф», «х», «ч», «е», «ы», «м». Все они последовательно во времени, многократно (в разных реализациях) проговаривались в микрофон группой из 10 дикторов, все разного возраста, мужчины и женщины, в режиме продолжительного (до 1 с), достаточно информативного звучания. Полученные сигналы через АЦП (частота дискретизации 8 кГц) были записаны в память ПК в виде соответствующих звуковых файлов для последующего анализа.

На *втором этапе* идентификация дикторов осуществлялась по требованиям в соответствии с ГОСТ 16600–72 «Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений». В соответствии с ГОСТ 16600–72 были выбраны тексты фраз и команд последовательно во времени, многократно (в разных реализациях) проговаривались в микрофон группой из 10 дикторов, все разного возраста, мужчины и женщины, в режиме продолжительного (до 1 мин), достаточно информативного звучания. Полученные сигналы через АЦП (частота дискретизации 8 кГц) были записаны в память ПК в виде соответствующих звуковых файлов.

Для реализации предложенных экспериментальных исследований был разработан лабораторный образец информационной системы фонетического анализа слитной речи (ИС ФАР). Данная система представляет собой фонетический анализатор. Варианты применения такого анализатора можно привести из самых различных областей. Это может быть, например, задача анализа качества речи по ее фонетическому составу как для отдельного диктора, так и для идентификации диктора по голосу. В качестве прикладной задачи можно привести текстонезависимую идентификацию разных дикторов по голосу в режиме реального времени.

ИС обеспечивает выполнение следующих возможностей:

1) автоматическое выделение фонем из входных данных;

2) обработка фонем;

3) хранение фонем;

4) визуализация полученных результатов;

5) текстонезависимая идентификация дикторов по голосу.

Ниже представлена блок-схема работы ИС ФАР (рис. 3).

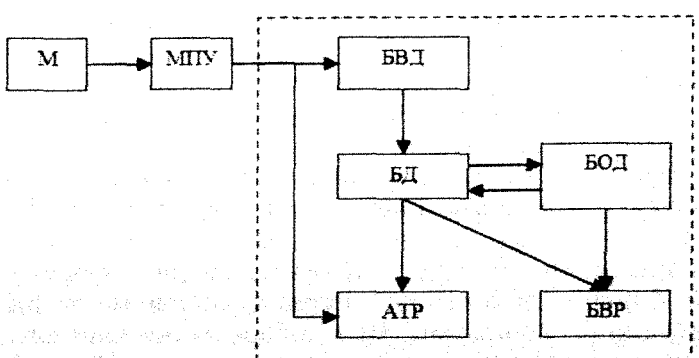



Рис. 3. Блок-схема работы ИС ФАР

Здесь М – динамический микрофон AQG D77 S, МПУ – микрофонный ламповый предусилитель со встроенным аналого-цифровым преобразователем, БВД – блок ввода данных, БВР – блок вывода результатов, БД – база данных, БОД – блок обработки данных, АТР – подсистема автоматического транскрибирования речевых сигналов. Блоки, ограниченные штриховой линией, выполнены в виде соответствующих программных модулей и составляют собственно информационную систему. Звуковой сигнал поступает с микрофона М на предусилитель МПУ, который осуществляет его усиление и преобразование в цифровой вид. Преобразованный таким образом сигнал поступает по шине USB в персональный компьютер, где осуществляется его запись в звуковой файл. Этот файл считывается БВД, где осуществляются его предварительная обработка, анализ и запись полученных результатов в базу данных в соответствии с выбранным режимом обработки.

БВР осуществляет извлечение данных из БД, соответствующих требуемому критерию, и отображение их в виде, удобном для пользователя. БОД предназначен для организации возможности работы с группами дикторов и формирования входных данных для БВР.

Подсистема АТР позволяет производить отображение в различных режимах и автоматическую разметку входного сигнала на фонемы в соответствии со списком фонем какого-либо диктора из БД. Кроме того, возможно озвучивание выбранных фрагментов сигнала, сохранение результатов транскрибирования в текстовый файл и анализ получаемых результатов.

Информация, содержащаяся в БД, может быть как непосредственно считана БВР, так и поступать в БВР через БОД.

Интерфейс ИС ФАР состоит из главной формы, на этой форме отображаются дикторы, внесенные в БД и главное меню программы. При выборе любого диктора из списка в правой части окна отображается краткая информация о нем. Кроме того, при помощи имеющегося меню

можно выбирать различные режимы работы, загрузки, сохранения и отображения данных. Ниже представлен общий вид интерфейса ИС ФАР (рис. 4).

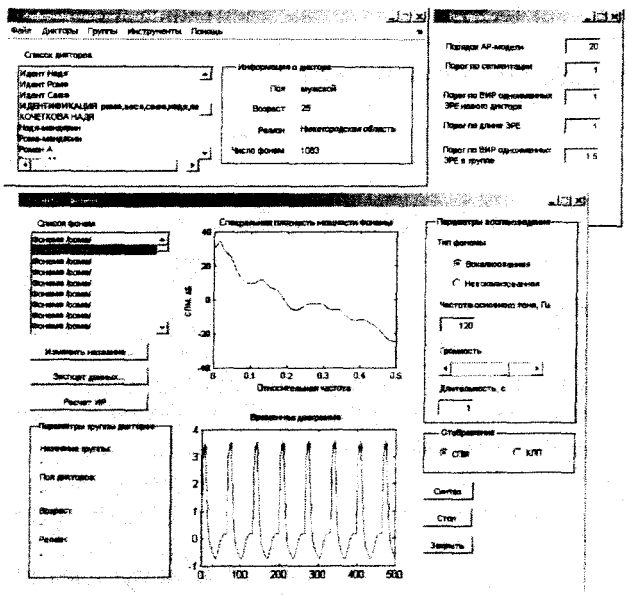



Рис. 4. Общий вид интерфейса ИС ФАР

В процессе эксперимента на сегментирование подавались фразы отдельных дикторов и производилась идентификация конкретного диктора посредством подсчета распознанных фонем. Решение о принадлежности произнесенной фразы конкретному диктору принимается автоматически после подсчета всех распознанных фонем и вычисления доминирующих фонем среди всех остальных, что представлено ниже (рис. 5).

На рисунке видно, что в произнесенной фразе всего выделено 759 фонем, из них 609 фонем принадлежат диктору «роман», а 150 фонем распознаны как «ложные» фонемы, похожие на фонемы других дикторов. Таким обра-

зом, по большему количеству принадлежащих определенному диктору фонем можно идентифицировать, кто произнес фразу. При этом в системе «ИСФАР» нет привязки к произнесенным командам и фразам и осуществляется автоматическая текстонезависимая идентификация диктора.

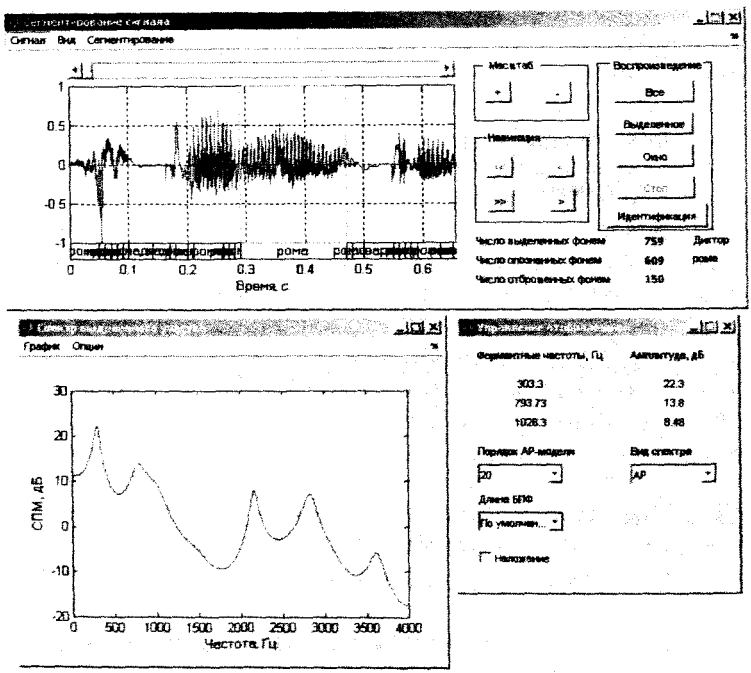



Рис. 5. Окно выполнения идентификации диктора по количеству фонем

В ходе решения поставленной задачи были получены следующие результаты:

• благодаря применению МОФ в задаче ФАР удается резко сократить вычислительную сложность решаемой задачи идентификации и одновременно в полной мере использовать оптимальные свойства решающей статистики МИР;

• проанализирован процесс речеобразования и исследована работа артикуляторного аппарата человека, в результате чего выработаны пути построения модели идентификации голосового сообщения;

• произведен обзор и анализ методов, которые могут использоваться при идентификации голосового сообщения – нейросети, частотные цифровые фильтры, Фурье-анализ, кепстральный анализ, методы машинного обучения, векторное квантование, гауссовы смеси и вейвлет-анализ. Показана предпочтительность выбора Фурье-анализа как основы построения модели;

• построена структурная схема модели идентификации голосового сообщения по фонемной составляющей и индивидуальным характеристикам голоса;

• спроектирована структура базы данных голосовых сообщений для тестирования и статистической оценки качества работы предложенной модели.

Исследования осуществлены в терминах универсального теоретико-информационного подхода и информационной теории восприятия речи [1, с. 3–9]. Их *главная цель* – создание необходимой методологической и программной базы для дальнейшей конструкторской разработки системы идентификации диктора по голосу.

**Литература**

1. *Савченко В. В.* Информационная теория восприятия речи // Известия высших учебных заведений России. Радиоэлектроника. – 2007. – Вып. 6. – ISSN 1993-8985.

2. *Савченко В. В., Акатьев Д. Ю., Карпов Н. В.* Автоматическое распознавание элементарных речевых единиц методом обеляющего фильтра // Известия высших учебных заведений России. Радиоэлектроника. – 2007. – Вып. 4. – ISSN 1993-8985.

3. *Савченко В. В.* Теоретико-информационное обоснование гауссовой модели сигналов в задачах автоматического распознавания речи // Известия высших учебных заведений России. Радиоэлектроника. – 2007. – Вып. 1. – ISSN 1993-8985.

4. *Савченко В. В., Губочкин И. В.* Оптимизация авторегрессионной модели сигналов в задаче автоматического распознавания

речи // Известия высших учебных заведений России. Радиоэлектроника. – 2007. – Вып. 2. – ISSN 1993-8985.

5. *Савченко В. В., Карпов Н. В.* Анализ фонетического состава речевых сигналов методом переопределенного дерева // Системы управления и информационные технологии. – 2008. – Вып. 2. – ISSN 1729-5068.

6. *Савченко В. В., Губочкин И. В.* Фонетический анализ речи методом переменного дерева // Известия высших учебных заведений России. Радиоэлектроника. – 2007. – Вып. 3. – ISSN 1993-8985.

УДК 004.056

**А. Ю. Кузнецов**

Санкт-Петербургский национальный
исследовательский университет
информационных технологий, механики и оптики

# СИСТЕМА РАННЕГО ОБНАРУЖЕНИЯ ЦИФРОВЫХ ДИКТОФОНОВ

Все современные диктофоны можно разделить на две большие группы: кинематические и цифровые. К первой группе относятся устройства, работающие по принципу записи звуковой информации на магнитный носитель. Данные диктофоны в качестве средств негласного съема информации потеряли свою актуальность, так как для них уже существует достаточно много систем противодействия. Ко второй группе относятся устройства, построенные на принципе записи электрических сигналов в кристалл микросхемы памяти в цифровом виде. Конструктивно цифровые диктофоны могут быть выполнены в двух вариантах:

1) устройства, в которых функция диктофона является основной;

2) устройства, в которых функция диктофона является дополнительной.

Ко второй группе относятся устройства:

1) сотовые телефоны (большинство моделей);

2) смартфоны и КПК;

3) MP3-плейеры с возможностью записи.

Все электронные устройства являются источниками побочного электромагнитного излучения. По характеру ПЭМИ цифровые диктофоны можно разделить на следующие подгруппы.

1. Диктофоны, имеющие импульсный преобразователь напряжения, например, если в качестве источника питания использована одна батарея напряжением 1,5 V.

2. Диктофоны, имеющие съемную конструкцию флэш-памяти.

3. Диктофоны, осуществляющие сжатие речевой информации посредством специализированного сигнального процессора.

4. Диктофоны, имеющие жидкокристаллический дисплей.

5. Диктофоны, имеющие различные подключенные устройства, такие как выносной микрофон, пульт дистанционного управления и т. д.

6. Диктофоны, имеющие корпус, способный экранировать излучение диктофона.

Современные системы обнаружения диктофонов работают по принципу анализа побочного электромагнитного излучения. По исследованиям, максимальный уровень излучения для всех цифровых диктофонов лежит в диапазоне от 20 до 120 кГц. Для диктофонов с импульсным преобразователем напряжения наиболее сильный уровень наблюдается на частоте преобразования. Дистанция обнаружения таких диктофонов – более метра. Дистанция обнаружения диктофонов со съемной флэш-памятью лежит в диапазоне от 50 см до 1 м. В устройствах с жидкокристаллическим дисплеем последний также является источником образования электромагнитного поля. Причем энергия растет с размерами дисплея, а в особенности, если он графический и цветной. Наличие таких дисплеев характерно для приборов, у которых функция диктофона является дополнительной: сотовые телефоны, КПК, смартфоны и т. д.

Дальность обнаружения таких устройств может превысить 1 м. Для диктофонов с подключенным выносным микрофоном или пультом дистанционного управления соединительный кабель является дополнительным относительно мощным источником излучения. Дальность излучения таких диктофонов превышает 1 м. Для диктофонов в экранированных корпусах дальность обнаружения резко падает, так как излучение экранируется корпусом и в зависимости от качества экранировки составляет менее 30 см. Данные устройства относятся к классу спецтехники и специально разрабатываются с целью минимизации излучения.

Таким образом, мы получаем, что существующие средства обнаружения диктофонов бессильны против современных цифровых диктофонов со следующими конструктивными особенностями.

1. Имеют встроенный аккумулятор.
2. Имеют встроенную флэш-память.
3. Не имеют графического дисплея.
4. Не имеют дополнительных функций, не относящихся к записи и обработке речи.
5. Имеют экранированный металлический корпус.
6. Имеют небольшие размеры.

Для своевременного обнаружения таких устройств есть предложение создать систему, основанную на принципе нелинейной локации и детекции металлов.

Практика работы с нелинейным локатором позволяет сделать вывод, что скорость перемещения антенны вдоль поверхности обследуемого объекта, а также расстояние до объекта поиска для всех нелинейных локаторов приблизительно одинаковы, поэтому объективное сравнение моделей нелинейных локаторов можно было бы осуществлять по максимальной дальности обнаружения некоторого эталонного нелинейного отражателя. К сожалению, это практически невозможно из-за организационных сложностей согласования конструкции такого отражателя с производителями аппаратуры и проведения регулярных сравнительных испытаний.

Свойства нелинейных объектов рассеивать зондирующий сигнал на $n$-й гармонике количественно оценивается нелинейной эффективной поверхностью рассеяния (НЭПР) – $\sigma_n$. Оценка НЭПР объекта поиска в силу объективных обстоятельств невозможна. Рабочий диапазон частот объекта поиска не совпадает с частотой зондирующего сигнала и частотой отклика, поэтому провести оценку эффективности антенны объекта, как правило, не представляется возможным. Нелинейные отражатели отличаются большим разнообразием схемных и конструктивных решений, и оценить уровень сигнала, выделяемого на нелинейном элементе, затруднительно.

Модель взаимодействия НЛ с объектом поиска – нелинейным отражателем в упрощенном виде описывается выражением

$$P_{пр} = \sigma_2 \left( \frac{P_{пер} \cdot G_{пер}}{4\pi R^2} \right)^2 \frac{G_{пр}}{4\pi R^2},$$

где $P_{пер}$ – мощность зондирующего сигнала НЛ на входе передающей антенны;

$G_{пер}$ – коэффициент усиления передающей антенны;

$G_{пр}$ – коэффициент усиления приемной антенны;

$P_{пр}$ – мощность второй гармоники на входе приемника НЛ;

$\sigma_2$ – нелинейная эффективная поверхность рассеяния (НЭПР) объекта поиска на частоте второй гармоники.

Если в последнем выражении положить:

$$P_{пр} = P_{про},$$

где $P_{про}$ – пороговая чувствительность приемника (НЛ), то получим:

$$R_{max} = \sqrt[6]{\sigma_2} \cdot \sqrt[6]{\left( \left( \frac{P_{пер} \cdot G_{пер}}{4\pi} \right)^2 \cdot \frac{G_{пр}}{4\pi \cdot P_{про}} \right)},$$

где $R_{max}$ – максимальная дальность обнаружения гипотетического нелинейного объекта.

Введем в качестве обобщенного показателя эффективности НЛ коэффициент $K_{эф}$, кратный максимальному расстоянию обнаружения нелинейного отражателя любого варианта исполнения и определяющего его потенциальные возможности по выявлению нелинейных отражателей:

$$K_{эф} = \sqrt[3]{\left(P_{пер} \cdot G_{пер}\right)} \cdot \sqrt[6]{\left(\frac{G_{пр}}{P_{про}}\right)}.$$

В соответствии с данными формулами был произведен анализ рынка современных нелинейных локаторов. Выбор был сделан в пользу импульсного локатора NR-900EMS.

Конструктивно система раннего обнаружения средств звукозаписи может быть выполнена в виде классической рамки (аналог рамки металлодетектора).

Эта конструктивная особенность позволяет установить нелинейный локатор непосредственно в одну из панелей металлодетектора или на малом расстоянии от нее, что, в свою очередь, увеличит возможности всей системы и позволит бороться против средств звукозаписи в экранированном корпусе. К основным требованиям для металлодетектора, применяемого в системе обнаружения диктофонов, относятся:

- обеспечение селективности по отношению к металлическим предметам, разрешенным к проносу на охраняемый объект;
- надежное обнаружение объекта поиска;
- обеспечение помехоустойчивости;
- обеспечение специальной безопасности;
- высокая чувствительность.

После проведенных испытаний система раннего обнаружения диктофонов показала высокие результаты по обнаружению миниатюрных средств звукозаписи как в пластиковом корпусе, так и в экранированном (в испытаниях принимала участие система, состоящая из металлодетектора и нелинейного локатора). Однако стоит отметить, что при проведении опыта на человеке, проходящем через ме-

таллодетектор, не было посторонних металлических предметов. Если срабатывание нелинейного локатора говорит о наличии на теле человека (злоумышленника) электронных устройств, то срабатывание металлодетектора говорит о наличии либо закамуфлированных средств звукозаписи, либо о наличии посторонних металлических предметов. Из этого следует, что при применении данной системы в реальных условиях металлодетектор будет часто срабатывать ложно. Поэтому окончательный осмотр проходящего через систему человека остается за оператором данной системы.

УДК 004.056

**О. Н. Жданов, В. А. Чалкин**

Сибирский государственный
аэрокосмический университет
им. акад. М. Ф. Решетнева

# ОПИСАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ КЛЮЧЕВОЙ ИНФОРМАЦИЕЙ ПРИ ПЕРЕДАЧЕ СООБЩЕНИЙ ПО КАНАЛУ «ЗЕМЛЯ–БОРТ»[1]

**Понятие и базовые типы аутентификации.**

Аутентификация – это проверка принадлежности субъекту доступа предъявленного им идентификатора. Как известно, все механизмы аутентификации основаны на предъявлении пользователем системе специальной информации (помимо идентификатора), на основании которой модуль аутентификации выносит решение о том, считать ли данного пользователя легитимным или признать, что произошла попытка (возможно, неумышленная) подмены пользователя. В ряде случаев требуется и взаимная аутентификация – когда оба участника информационного обмена проверяют подлинность идентификаторов друг друга.



[1] Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России на 2009–2013 годы».

Существует естественное деление механизмов аутентификации на локальную (в рамках локализованной информационной системы) и удаленную (при передаче информации по каналу связи).

В случае удаленной аутентификации существует проблема передачи аутентификационной информации по недоверенным каналам связи, так как возникает угроза перехвата аутентификационной информации злоумышленником с целью дальнейшего использования для атаки на систему защиты. Чтобы сохранить в тайне уникальную информацию, при пересылке по таким каналам используются различные протоколы аутентификации [1, с. 52].

**Основные требования к системе аутентификации сторон при передаче сообщений по спутниковому каналу.**

В общем случае при передаче сообщений по спутниковому каналу «Земля–борт» механизм аутентификации решает следующую основную задачу: предоставить способ подтверждения того, что сообщение передано с земли на борт легитимным передающим центром. Аутентификация борта в большинстве случаев не требуется.

Вследствие особенностей спутникового канала связи можно выделить следующие основные требования к данной системе.

1. Устойчивость к атакам при помощи перехвата сообщений (вследствие общедоступности среды передачи) на протяжении срока службы борта.

2. Высокая скорость работы на аппаратной платформе бортового комплекса управления (предполагается, что земля способна обеспечить необходимые вычислительные ресурсы; «узкое место» возникает именно вследствие ограниченности вычислительных ресурсов борта). Процесс аутентификации не должен вызывать больших задержек в процессе передачи сообщений (длительность процедуры аутентификации не должна превышать минимальное время отклика борта).

3. Минимальное число и объем сообщений, передаваемых между Землей и бортом; в идеале, должно переда-

ваться единственное сообщение вместе с полезной информацией (в одном кадре данных).

В настоящее время аппаратные реализации симметричных криптографических систем по скорости работы значительно превосходят реализации асимметричных систем. Кроме того, в силу меньшей сложности (сравнительно с реализациями асимметричных систем) у аппаратных реализаций симметричных систем при сравнимой криптостойкости больше вероятность безотказной работы в течение заданного времени, т. е. выше надежность. Поэтому для применения в системе «борт–Земля» предпочтительной является аппаратная реализация симметричной криптосистемы.

Недостатком многих широко распространенных протоколов является тот факт, что аутентификация будет успешна только в том случае, если секретный ключ известен обеим сторонам информационного обмена. При этом в случае многократного перехвата злоумышленником данных, передаваемых между сторонами, возникает угроза атаки на шифр на основе данных об открытых и шифрованных текстах с последующим получением информации о ключе. Таким образом, очевидно, что секретные ключи шифрования в такой схеме необходимо периодически менять. Периодичность смены ключей зависит от критичности возможной компрометации системы и предполагаемой стойкости используемого шифра к различным методам криптоанализа.

Исходя из вышеперечисленных требований для системы передачи сообщений по каналу «Земля–борт» наиболее приемлемым способом аутентификации является режим вычисления имитовставки алгоритма блочного шифрования.

**Режим имитовставки ГОСТ 28147–89.**

Данный режим криптографического преобразования предусмотрен в российском стандарте ГОСТ 28147–89 для решения задачи обнаружения искажений в зашифрованном массиве данных с заданной вероятностью. Имито-

вставка – это контрольная комбинация, зависящая от открытых данных и секретной ключевой информации.

Ключевым свойством процедуры вычисления имитовставки является тот факт, что для потенциального злоумышленника две следующие задачи практически неразрешимы, если он не владеет ключевой информацией:

- вычисление имитовставки для заданного открытого массива информации (что делает возможным использование ее как механизма аутентификации);
- подбор открытых данных под заданную имитовставку (что делает возможным использование ее как механизма проверки целостности данных).

Алгоритм выработки имитовставки (рис. 1) основывается на том же преобразовании в ходе раунда шифрования, что и в режиме шифрования стандарта ГОСТ 28147–89. Отличие заключается только в том, что вместо 32 раундов используются только 16 и определенным образом изменен порядок использования подключей раундов.

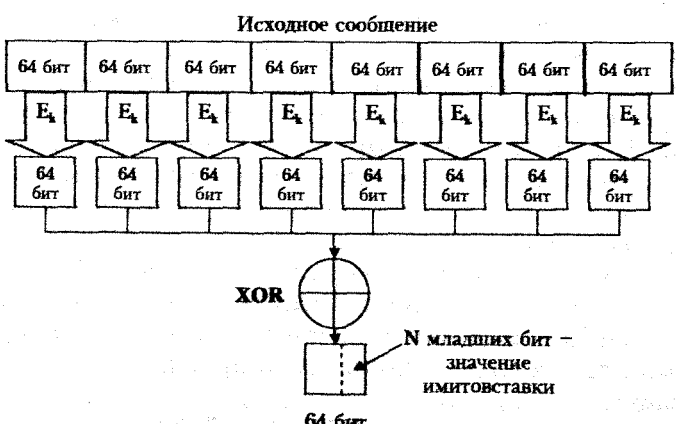



Рис. 1. Схема режима имитовставки ГОСТ 28147–89

В качестве имитовставки берется часть блока, полученного на выходе, обычно 32 его младших бита. При выборе размера имитовставки $N$ считается, что вероятность успеш-

ного навязывания ложных данных равна величине $2^{-N}$ на одну попытку подбора. При использовании имитовставки размером 32 бита эта вероятность равна $2^{-32} \approx 0{,}23 \cdot 10^{-9}$.

**Протокол ESA.**

В соответствии с протоколом передачи телеметрической информации ESA (European Space Agency – Европейского космического агентства) аутентификация Земли при передаче разовой команды на борт осуществляется по значению поля аутентификации длиной 40 байт, вставляемого в передаваемый кадр. Возможности для двухстороннего обмена сообщениями, таким образом, в данном случае не предусмотрены. Поэтому оптимальным решением для аутентификации в данном случае будет использование процедуры выбора имитовставки для передаваемого сообщения.

При этом может быть использован как стандартный режим выработки имитовставки по ГОСТ 28147–89, так и любой другой блочный симметричный итерированный шифр, например, AES – современный стандарт блочного шифрования США, несмотря на различия в алгоритмах ГОСТ и AES. В этом случае в поле аутентификации записывается XOR-сумма шифртекстов, полученных при шифровании разбитого на блоки передаваемого сообщения (аналогично тому, как это происходит в ГОСТ 2814789).

В силу того, что операции, используемые в ГОСТ 2814789 и AES, эффективно реализуются на любых 32-разрядных аппаратных платформах общего назначения, требование высокой скорости работы алгоритмов на борту будет удовлетворено.

С точки зрения криптографической стойкости при данном подходе опасность возникает по причине того, что по открытому спутниковому каналу передаются пары «открытый текст – шифрованный текст», что позволяет аналитику проводить более эффективные атаки на шифры. Несмотря на высокую практическую стойкость алгоритмов ГОСТ 2814789 и AES, знание большого количества таких пар может дать аналитику противника возможность делать предположения о вероятных значениях битов ключа.

Для защиты от такой атаки необходимо разработать эффективную схему управления ключевой информацией, предполагающую регулярную смену используемых для вычисления имитовставки ключей шифрования [2, с. 214].

**Схема управления ключевой информацией.**

Для устранения угрозы компрометации системы, связанной с возможностью перехвата передаваемых сообщений с целью криптоаналитической атаки, предлагается использование двухуровневой системы управления ключевой информацией.

В этом случае используются два вида ключей: долговременные и сеансовые. Долговременные ключи генерируются из отрезков псевдослучайной последовательности бит необходимой длины на этапе разработки системы (до запуска борта) с последующим тестированием на отсутствие статистических закономерностей по известным методикам. Затем они записываются в энергонезависимую память бортового комплекса управления и сохраняются в памяти передающего центра на Земле. При этом долговременные ключи должны быть недоступными третьим лицам, так как именно ими обеспечивается криптостойкость аутентификации. Число необходимых долговременных ключей зависит от срока службы борта и частоты смены ключей. Достаточной частотой смены представляется 1 раз в год. Таким образом, необходим 1 ключ на каждый год работы системы передачи сообщений между бортом и Землей.

Долговременные ключи не используются непосредственно для выработки имитовставки. Они применяются для получения гаммы шифра, отрезки которой становятся сеансовыми ключами, которые используются при вычислении значения имитовставки. В случае использования алгоритма ГОСТ 28147–89 применяется гаммирование, определяемое Стандартом (с минимальным периодом, равным $2^{64}$ различных ключей), при использовании шифра иностранного происхождения можно вырабатывать гамму по стандарту ANSI X9.17, применяя любой блочный шифр. Таким образом, для выработки гаммы и для вычисления

имитовставки используется один и тот же модуль шифрования, что упрощает аппаратную реализацию системы аутентификации.

Сеансовый ключ вырабатывается каждый раз на Земле перед отправкой телекоманды на борт и на борту – перед выполнением процедуры аутентификации полученного кадра.

Таким образом, каждый новый сеанс передачи телекоманды аутентифицируется новым ключом, что делает такую систему устойчивой к атакам на блочные шифры на основе анализа пар «открытый текст – шифрованный текст» (при условии секретности долговременных ключей).

Смена долговременных ключей осуществляется по команде с Земли следующим образом. В ПЗУ борта зафиксировано начальное значение синхропосылки, использованное для шифрования и выработки имитовставки первого кадра. По Стандарту рекуррентный генератор, используемый для выработки очередных значений синхропосылок, из которых затем вырабатывается гамма шифра, имеет период $(2^{64} - 2^{32}) \approx 1{,}8 \cdot 10^{19}$. Поэтому начальная синхропосылка повторится через $1{,}8 \cdot 10^{19}$ циклов работы рекуррентного генератора, значит, одного значения синхропосылки достаточно для получения $1{,}8 \cdot 10^{19}/4 \approx 4{,}5 \cdot 10^{18}$ различных сеансовых ключей (так как длина ключа ГОСТ 28147–89 – 256 бит, а каждый цикл генератора дает после зашифрования 64-битный отрезок гаммы). При скорости передачи 4,5 кбит/с, если каждый новый ключ будет вырабатываться для каждых 512 бит, этого количества ключей хватит для работы защищенного канала в течение $1{,}6 \cdot 10^{10}$ лет непрерывной работы, т. е. период гаммы более чем достаточный.

При необходимости смены долговременного ключа по запросу системы управления (или по команде ЦУП) модуль шифрования на Земле прерывает последовательность вырабатываемых рекуррентным генератором синхропосылок и передает на борт очередной кадр, зашифрованный с использованием начальной синхропосылки, которая, как

было сказано выше, хранится в памяти борта. Борт, каждый раз выполняющий сравнение синхропосылки с этим значением, получает признак необходимости смены долговременного ключа. Смена ключа производится не для того кадра, который принят с начальной синхропосылкой, а для следующего за ним, после расшифрования кадра и проверки имитовставки, и в случае корректности на Землю передается стандартное подтверждение приема команды, которое становится для модуля шифрования на Земле сигналом к смене долговременного ключа.

Такая схема позволяет отказаться от введения дополнительного признака (флага) или команды смены ключа и обеспечить невозможность рассинхронизации смены долговременного ключа между Землей и бортом. Смены таблицы замен при этом не требуется, так как это усложнило бы аппаратную реализацию модуля шифрования без увеличения стойкости.

**Генерация элементов ключевой информации.**

Как известно, для всех современных итерированных блочных шифров, таких как ГОСТ 28147–89 и AES, ключ шифрования представляет собой последовательность бит определенной длины. Надежность шифрования определяется, в частности, качеством этой последовательности с точки зрения криптостойкости.

Общепринятыми для всех блочных шифров требованиями к ключам шифрования являются следующие.

- Ключ должен являться массивом битов, принимающих с равной вероятностью значения 0 и 1.
- Между битами ключа не должно быть явной или легко обнаруживаемой зависимости, иными словами, в массиве бит должны отсутствовать статистические закономерности.

Для тестирования ключей на соответствие требованиям 1 и 2 используются различные статистические критерии.

1. Тест Чезаро – используется для проверки близости набора чисел к случайному. Данный тест основан на известной теореме Чезаро: вероятность того, что два произ-

вольно выбранных натуральных числа являются взаимно простыми, равна $6/\pi^2$.

Для проверки случайности ключа шифрования при помощи теста Чезаро ключ как последовательность бит разбивается на несколько равных по длине битовых векторов, каждый из которых переводится в числовую форму, после чего каждая пара чисел из полученного набора проверяется на взаимную простоту, вычисляется значение характеристики теста и по нему делается вывод о степени близости всего набора чисел, а значит, и ключа шифрования к случайной последовательности.

2. Критерий Пирсона (хи-квадрат) – используется для проверки равновероятности распределения битов ключа. Данный тест основан на широко применяемом в математической статистике критерии соответствия значений в статистической выборке определенному закону распределения (в данном случае – закону распределения «хи-квадрат»).

Для проверки ключа шифрования по критерию Пирсона он разбивается на отрезки длиной $k$ бит каждый ($k$ = 1, 2, 4, 8, ...). При $k$ = 1 проверяется равновероятность появления значений 0 и 1, при $k$ = 2 – значений 00, 01, 10 и 11 и т. д.

3. Критерий серий – используется для проверки независимости битов ключа друг от друга.

Наиболее распространенными на сегодняшний день методами генерации ключей шифрования для блочных шифров являются следующие.

1. Использование аппаратного датчика истинно случайных чисел – самый эффективный метод с точки зрения качества ключевой информации, однако он далеко не всегда приемлем по экономическим соображениям и вследствие низкой производительности.

2. Использование метода «электронной рулетки», когда очередная получаемая порция случайных битов зависит от момента времени нажатия оператором некоторой клавиши на клавиатуре компьютера или от положения

курсора на экране. Подходит для генерации небольшого по объему массива ключевой информации, однако требует наличия оператора и обязательной проверки полученной последовательности на случайность и отсутствие статистических закономерностей.

3. Использование гаммы шифра блочного алгоритма шифрования, когда в качестве ключа используется гамма шифра, полученная при определенном открытом значении синхропосылки и секретном значении ключа шифрования. Данный подход обеспечивает достаточное качество ключевой информации, так как криптографическая гамма обладает необходимыми статистическими характеристиками. Так, гамма шифра алгоритма ГОСТ 28147–89 обладает периодом повторения 64-битных блоков, равным $(2^{64}-2^{32})$. Недостаток такого подхода: он требует дополнительных вызовов процедур шифрования, что не всегда приемлемо в случае аппаратной реализации.

4. Использование стандарта генерации ключей ANSI X9.17. Данный стандарт предусматривает генерацию ключа по алгоритму, схема которого приведена на рис. 2, с использованием функции зашифрования произвольного блочного шифра с длиной блока 64 бит.

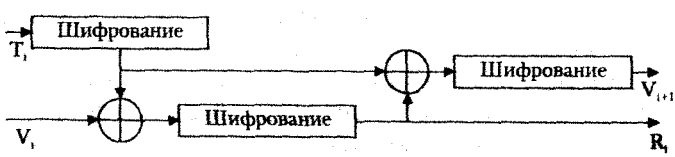



Рис. 2. Схема генерации ключа по стандарту ANSI X9.17

В целом данный подход имеет те же достоинства и недостатки, что и предыдущий, однако следует отметить, что генерация 64 бит ключа требует трех вызовов процедуры зашифрования, что делает такой способ генерации ключа весьма ресурсоемким в случае аппаратной реализации.

5. Использование алгоритмического генератора псевдослучайных чисел. В этом случае к генератору предъяв-

ляется требование криптостойкости: степень трудоемкости определения отсутствующих членов генерируемой им последовательности должна быть не меньшей, чем степень трудоемкости атаки на шифр, для которого генерируется ключ.

Одним из наиболее стойких к криптографическим атакам является алгоритм Блюма-Блюма-Шуба (BBS). Главное его достоинство состоит в том, что строго доказано, что не существует алгоритма с полиномиальной оценкой времени его выполнения, который по любым $k$ битам выходной последовательности может предсказать ее $(k+1)$-й бит с вероятностью, существенно большей, чем 0,5.

Алгоритм BBS при корректном выборе начальных параметров удовлетворяет всем статистическим критериям, предъявляемым к псевдослучайным последовательностям. Однако вследствие наличия в алгоритме операции умножения чисел алгоритм BBS может быть эффективно реализован далеко не на всех аппаратных платформах, поэтому он является наиболее подходящим для программных систем шифрования.

Наиболее предпочтительным для генерации долговременных ключей в рассматриваемой системе представляется применение генератора BBS с последующим тестированием методами, изложенными выше (тест Чезаро, критерии Пирсона и серий).

**Выводы.**

В рамках проекта по разработке системы аутентификации сторон по спутниковому каналу «Земля–борт» в [3–5] получены следующие результаты.

1. Проведено исследование и сравнительный анализ различных подходов к формированию ключевой информации для алгоритмов блочного шифрования. Разработана методика оценки зависимости криптостойкости шифрования по алгоритму ГОСТ 28147–89 от выбранной ключевой информации. Данная методика позволяет выбирать таблицы замен (S-блоки), обеспечивающие устойчивость к наиболее распространенным методам криптоанализа (линей-

ный и дифференциальный криптоанализ). Разработанная методика после несущественных изменений может быть применена для выбора и тестирования ключа алгоритма AES.

2. Программно реализованы:

- алгоритм BBS;
- тест Чезаро, критерии Пирсона и серий;
- алгоритм построения таблиц замен и ключей для алгоритма ГОСТ 28147–89, описанный в [4] и [5]. На программу получено авторское свидетельство [7].

3. На основе полученных результатов аппаратно реализован алгоритм выработки имитовставки по ГОСТ 28147–89 [6].

Реализация выполнена на базе программируемой логической интегральной схемы (ПЛИС) в виде netlist'a. Разработка произведена на отладочной плате Terasic DE-0 FPGA Altera Cyclone III. Среда разработки Quartus 11 v11.0. Язык разработки VHDL. Разработка осуществлялась в контексте общей схемы взаимодействия космического аппарата (КА) с наземным комплексом управления (рис. 3).

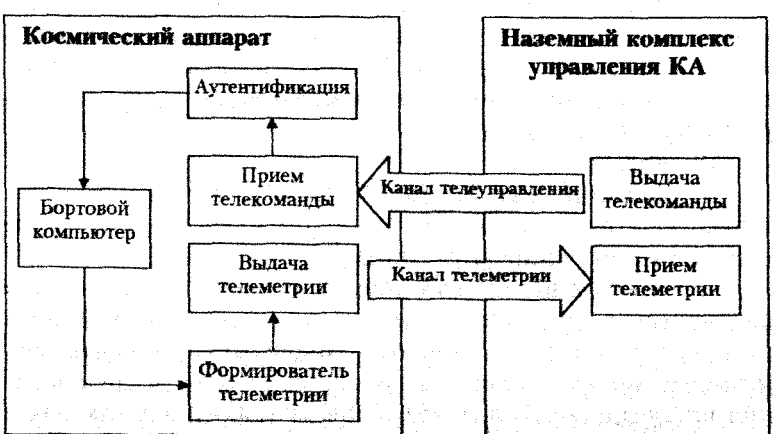



Рис. 3. Общая схема взаимодействия космического аппарата и наземного комплекса управления

Управление КА осуществляется через тракт телеуправления, структурная схема которого представления на рис. 4. Аутентификация производится после кадровой синхронизации до начала работы вычислителя.

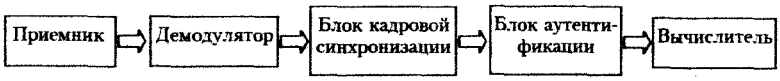



Рис. 4. Структурная схема тракта телеуправления

После приема команды телеуправления происходит аутентификация: сверка полученного значения имитовставки с расчетным. В случае совпадения команда передается на вычислитель, в противном случае команда не выполняется. В штатном режиме вычислитель (Leon 3) обращается к ведомым устройствам через внутрикристальную шину (AMBA). Поэтому блок аутентификации выполнен в качестве ведомого slave устройства шины AMBA.

Предложено использование резервного контура обработки команд телеуправления без участия вычислителя (в случае его отказа). Для этого используется жесткая привязка блока аутентификации к блоку кадровой синхронизации и резервному контроллеру. В будущем предполагается использование сетевого режима на базе шинно-сетевой архитектуры SpiceWire (рис. 5).

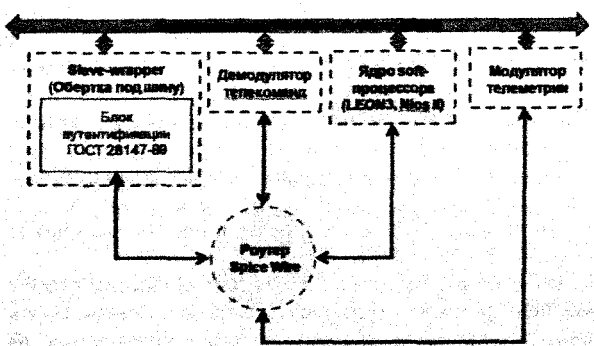



Рис. 5. Связь блока аутентификации с другими блоками

Основными функциональными возможностями блока аутентификации являются:

1) управление через шину AMBA;

2) управление через сетевой интерфейс (SpiceWire);

3) расчет сеансового ключа из долговременного;

4) расчет имитовставки для команды телеуправления;

5) сравнение расчетной имитовставки с полученной.

Блок аутентификации состоит из контроллера, вычислителя криптопреобразования, интерфейса внешней памяти.

Контроллер отвечает за вычисление нового сеансового ключа, запись новых значений ключа и таблиц замен в регистрах вычислителя, выполняет сверку расчетной имитовставки с полученной и в случае успешной аутентификации инициирует передачу команды вычислителю.

Описанная аппаратная реализация алгоритма аутентификации удовлетворяет как требованиям надежности (проведены доказательства оценок), так и требованию к скорости работы.

**Литература**

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2003. – 816 с.

2. *Жданов О. Н., Золотарев В. В.* Методы и средства криптографической защиты информации. – Красноярск: СибГАУ, 2008. – 253 с.

3. *Чалкин Т. А., Волощук К. М.* Алгоритм построения узлов замен алгоритма шифрования ГОСТ 28147–89 // Вестник СибГАУ им. акад. М. Ф. Решетнева. Вып. 1(22): В 2 ч. Ч. 2 / Под общ. ред. Г. П. Белякова; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2009. – С. 46–50.

4. *Чалкин Т. А.* Разработка методики выбора параметров для алгоритма построения узлов замен блочного шифра ГОСТ 28147–89 // Актуальные проблемы безопасности информационных технологий: Материалы III Междунар. науч.-практ. конф. / Под общ. ред. О. Н. Жданова, В. В. Золотарева; Сиб. гос. аэрокосм. ун-т. – Красноярск, 2009. – С. 33–38.

5. *Жданов О. Н., Чалкин Т. А.* Аутентификация сторон при передаче сообщений по спутниковому каналу «Земля–борт» // Информационные технологии моделирования и управления. № 5(64). – С. 656–662.

6. *Жданов О. Н.* и др. Аутентификации канала телеуправления малым спутником аппаратными криптографическими средствами // Сб. докл. VII Междунар. науч.-практ. конф. «Электронные средства и системы управления» ТУСУР. – Томск, 2011. – С. 215–220.

7. Свидетельство о государственной регистрации программ для ЭВМ № 2011613877. Программный комплекс построения и тестирования ключевой информации для шифрования данных по алгоритму ГОСТ 28147–89 // Чалкин Т. А., Жданов О. Н.

УДК 004.056

**А. В. Генк**

Санкт-Петербургский государственный инженерно-экономический университет

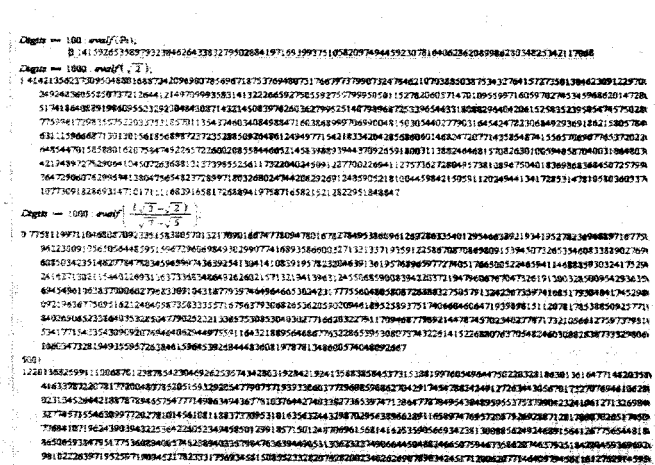
# О ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ МАТЕМАТИЧЕСКИХ ПРОГРАММ «MAPLE» И «MATHEMATICA» В СИСТЕМАХ ЗАЩИТЫ И ШИФРОВАНИЯ ДАННЫХ

Математические пакеты «Maple» и «Mathematica» [1, 2] являются общепризнанными мировыми лидерами в области систем компьютерной алгебры, позволяющими работать с аналитическими выражениями в виде формул. Одним из следствий такой возможности уже в области численных расчетов является уникальное свойство этих пакетов – расчет с произвольной, задаваемой пользователем, точностью. По умолчанию расчеты выполняются с 10 десятичными разрядами, но можно задать, например, точность 50, 100, 1000, 10000 и т. д. знаков. Разработчики систем утверждают даже, что на современных персональных компьютерах возможны вычисления с заданием до миллиона значащих цифр! При этом целочисленные расчеты (например, вычисление факториалов, биномиальных коэффициентов и т. п.) выполняются абсолютно точно, с любым количеством цифр (ограничиваемым только размером оперативной памяти).

Приведем несколько примеров вычислений в пакете «Maple-11» (рисунок). В 1-м примере вычислено значение

числа $\pi$ со 100 знаками после запятой, во втором – квадратный корень из 2-х уже с 1000 знаками, в 3-м – некоторое выражение из 4-х иррациональных чисел с той же точностью и в 4-м вычислено значение факториала 500 (ответ содержит более 1000 цифр). Все эти вычисления система производит очень быстро, практически мгновенно.

Отмеченную особенность пакетов «Maple» и «Mathematica» можно, на наш взгляд, плодотворно использовать в системах защиты и шифрования данных. В простейшем варианте применяется парольная защита файлов, допускающая очень длинные (например, из 1000 цифр) пароли. Пользователь должен помнить только небольшое 4–6-значное целое число и одно или несколько действий с ним (например, возведение в некоторую степень, а в более сложном варианте – и используя некоторую алгебраическую формулу), а также принятую точность результата. На компьютере должен быть установлен пакет «Maple» или «Mathematica» (можно даже в одной из устаревших версий). В пакете производится требуемое вычисление, и результат копируется в окно пароля (рисунок).



Примеры вычислений в пакете «Maple»

Очевидно, что вскрыть такой пароль (типа выражения (3) на рисунке) каким-либо перебором абсолютно невозможно, но остается возможность каким-либо образом получить его, используя разного рода шпионские программы, заражающие компьютер.

В более сложных системах шифрования данных можно использовать заранее обусловленное многозначное число, вычисляемое отправителем и получателем в пакетах «Maple» или «Mathematica» как основу для кодирования (декодирования) данных. При этом номер символа в какой-либо простой кодировке (пусть это, например, 89, которому соответствует, скажем, буква «п») кодируется множеством *разных* пар чисел, являющихся трехзначными *порядковыми номерами* цифр 8 и 9 в принятом базовом (опорном) числе. Например, в числе (3) на рисунке символ 89 сначала кодируется как 004007 (или как 994996), затем (когда он снова встретится в тексте) – как 015008 (или как 004008) и т. д. Для числа (3) на рисунке общее число вариантов кодировки одного символа (с номером 89) составит примерно 100×100 = 10000 (поскольку в нем примерно 100 цифр «8» и 100 цифр «9». Если использовать трехзначную базовую кодировку символа, то количество вариантов его кодировки с использованием 1000-значного опорного числа составит примерно 1 млн (а для 10000-значного опорного числа – 1 млрд).

С учетом множества вариантов выбора исходного числа, формул его обработки в пакетах и количества знаков результата общее число вариантов кодировки легко может быть доведено в этой системе до $10^{20}$–$10^{23}$ и более. Следовательно, степень защищенности данных при таком способе кодирования будет чрезвычайно высока (полный перебор всех вариантов становится безнадежным делом даже с использованием сверхмощных компьютеров), хотя конкретная удобная его программная реализация будет, видимо, достаточно сложной. Принципиально важно отметить, что в таком способе кодирования практически не будет повторяющихся групп цифр, несущих реальную ин-

формацию о символе (так как один символ при его повторах в тексте кодируется огромным множеством *разных* чисел). Поэтому становятся совершенно неэффективными все методы дешифровки, использующие анализ файла на повторяющиеся числа. Такие системы будут обнаруживать только *случайно* повторяющиеся группы цифр (по 2, 3, 4 и т. д.), которые не несут абсолютно никакой информации о реальных закодированных символах.

Автор благодарит профессоров кафедры вычислительных систем и программирования М. В. Буйневича, Е. В. Стельмашонок, а также Р. А. Пермякова (г. Новосибирск) за обсуждение и полезные замечания.

**Литература**

1. *Дьяконов В. П.* Maple 10/11/12/13/14 в математических расчетах. – М.: ДМК-пресс, 2011.

2. *Васильев А. Н.* Mathematica. Практический курс с примерами решения прикладных задач. – СПб.: Корона-ВЕК, 2008.

УДК 004.056

**О. Н. Жданов**

Сибирский государственный
аэрокосмический университет
им. акад. М. Ф. Решетнева

## ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

**Общие положения.**

Электронная цифровая подпись (ЭЦП) для сообщения является числом, зависящим от самого сообщения и от секретного ключа, известного только подписывающему. Важное требование: подпись должна допускать проверку без знания секретного ключа. При возникновении спорной ситуации, связанной с отказом от факта подписи либо с возможной подделкой подписи, третья сторона должна иметь возможность разрешить спор.

Задачи, которые решает подпись:

- осуществить аутентификацию источника сообщения;
- установить целостность сообщения;
- обеспечить невозможность отказа от факта подписи конкретного сообщения.

Для реализации схемы ЭЦП необходимы два алгоритма: алгоритм генерации подписи и алгоритм проверки. Надежность схемы ЭЦП определяется сложностью следующих задач:

- *подделки подписи*, т. е. нахождения правильного значения подписи для заданного документа;
- *создания подписанного сообщения*, т. е. нахождения хотя бы одного сообщения с правильным значением подписи;
- *подмены подписи*, т. е. нахождения двух различных сообщений с одинаковым значением подписи.

Заметим, что между ЭЦП и собственноручной подписью имеются различия, хотя они и служат для решения одинаковых задач. Так, ЭЦП зависит от подписываемого текста, различна для разных тестов. Кроме того, ЭЦП требует дополнительных механизмов, реализующих алгоритмы ее вычисления и проверки. Наконец, принципиальной сложностью, возникающей при использовании ЭЦП, является необходимость создания инфраструктуры открытых ключей. Эта инфраструктура состоит из центров сертификации открытых ключей и обеспечивает возможность своевременного подтверждения достоверности открытой информации, необходимой для проверки ЭЦП, что необходимо для предотвращения подделки подписи.

**Некоторые наиболее употребительные схемы ЭЦП.**

В настоящее время имеется большое количество различных схем ЭЦП, обеспечивающих тот или иной уровень стойкости. Существующие схемы можно классифицировать таким образом.

- **Схемы на основе систем шифрования с открытыми ключами.**
- **Схемы со специально разработанными алгоритмами вычисления и проверки подписи.**

• Схемы на основе симметричных систем шифрования. Рассмотрим некоторые схемы.

**1. *Схема Эль-Гамаля.***

Безопасность схемы основана на трудности вычисления дискретных логарифмов в конечном поле. Для генерации пары ключей выбирается простое число $p$ и два случайных числа, $g$ и $x$, оба меньше $p$. Затем вычисляется $y = g^x \bmod p$. Открытым ключом является набор чисел $y$, $g$, $p$. При этом $p$ и $g$ можно сделать общими для группы пользователей. Секретным ключом является $x$. Чтобы подписать сообщение $M$, сначала выбирается случайное число $k$, взаимно простое с $p - 1$. Затем вычисляется $a = g^k \bmod p$. Далее с помощью расширенного алгоритма Евклида для нахождения $b$ решается следующее уравнение:

$$M = (xa + kb) \bmod (p - 1).$$

Подписью является пара чисел: $a$ и $b$. Для проверки подписи нужно убедиться, что

$$y^a \cdot a^b \bmod p = g^M \bmod p.$$

*Первое замечание.* Число $k$ должно храниться в секрете и уничтожаться сразу после вычисления подписи, так как знание $k$ и значения подписи позволяет легко вычислить секретный ключ $x$. И тогда подпись будет полностью скомпрометирована. Кроме того, $k$ должно быть действительно случайным и не должно повторяться для различных подписей, полученных на одном секретном ключе. Если злоумышленник сможет получить два сообщения, подписанных с помощью одного и того же значения $k$, то он сможет раскрыть $x$, даже не зная значение $k$.

*Второе замечание.* При вычислении подписи целесообразно использовать хэш-образ сообщения, а не само сообщение $M$. Это защитит схему подписи от возможности подбора сообщений с известным значением подписи. Это распространенная практика.

Схема Эль-Гамаля послужила образцом для построения большого семейства во многом сходных по своим свойствам схем подписи.

**Пример**. Выберем $p = 11$ и $g = 2$, а секретный ключ $x = 8$. Вычислим: $y = g^x \bmod p = 2^8 \bmod 11 = 3$.

Открытым ключом являются $y = 3$, $g = 2$ и $p = 11$. Чтобы подписать $M = 5$, сначала выберем случайное число $k = 9$, убеждаемся, что НОД (9,10) = 1. Вычисляем: $a = g^k \bmod p = 2^9 \bmod 11 = 6$.

Далее с помощью расширенного алгоритма Евклида находим $b$: $M = (ax + kb) \bmod (p - 1)$, $5 = (8 \cdot 6 + 9 \cdot b) \bmod 10$.

Решением будет $b = 3$, а подпись представляет собой пару чисел: $a = 6$ и $b = 3$.

Для проверки подписи убедимся, что:

$$y^a \cdot a^b \bmod p = g^M \bmod p,$$

т. е.

$$3^6 \cdot 6^3 \bmod 11 = 2^5 \bmod 11.$$

**2. *Алгоритм подписи DSA.***

В августе 1991 г. NIST (National Institute of Standards and Technology) в своем стандарте цифровой подписи DSS (Digital Signature Standard) предложил для использования алгоритм цифровой подписи DSA (Digital Signature Algorithm). В алгоритме используются следующие параметры:

$p$ – простое число длиной $L$ битов, где $L$ принимает значение, кратное 64, в диапазоне от 512 до 1024 (в первоначальном стандарте размер $p$ был фиксирован и равен 512 битам. Это ограничение вызвало множество критических замечаний, и NIST отменил его);

$q$ – 160-битовый простой множитель $p - 1$;

$g = h^{(p-1)/q} \bmod p$, где $h$ – любое число, меньшее $p - 1$, для которого $h^{(p-1)/q} \bmod p > 1$, $x < q$, $y = g^x \bmod p$.

В алгоритме также используется однонаправленная хэш-функция $H(M)$. Стандарт определяет использование алгоритма SHA.

Первые три параметра, $p$, $q$ и $g$, открыты и могут быть общими для пользователей сети. Секретным ключом является $x$, а открытым – $y$. Чтобы подписать сообщение $M$:

1) пользователь А генерирует случайное число $k$, меньшее $q$;

2) **A** вычисляет:

$$r = (g^k \bmod p\ ) \bmod q,\ s = (k^{-1}(H(M) + xr)) \bmod q;$$

3) его подписью служат параметры $r$ и $s$, которые он посылает **B**;

4) **B** проверяет подпись, вычисляя:

$$w = s^{-1} \bmod q,\ u_1 = (H(M)\cdot w) \bmod q,\ u_2 = (rw) \bmod q;$$
$$v = ((g^{u_1} \cdot y^{u_2}) \bmod p) \bmod q.$$

Если $v = r$, то подпись правильна.

**3. *ЭЦП на эллиптических кривых.***

В настоящее время в России действует стандарт подписи на эллиптических кривых. Поэтому нам представляется логичным более подробно остановиться на этой схеме.

*Предварительные сведения.* Любая эллиптическая кривая над полем $K$ характеристики $\neq 2,3$ изоморфна кривой вида

$$y^2 = x^3 + ax + b.$$

Особый интерес для криптографии представляет объект, называемый эллиптический группой по модулю $p$, где $p$ является простым числом. Такая группа определяется следующим образом. Выберем два неотрицательных целых числа, $a$ и $b$, которые меньше $p$ и удовлетворяют условию

$$4a^3 + 27b^2 \pmod p \neq 0.$$

Элементами эллиптической группы по модулю $p$ являются пары $(x,y)$ неотрицательных целых чисел, которые меньше $p$ и удовлетворяют условию $y^2 = x^3 + ax + b \pmod p$ вместе с «точкой в бесконечности» $O$.

Несколько слов о «точке в бесконечности» $O$. По определению, это нейтральный элемент группового закона. В графической интерпретации следует себе представлять ее расположенной на оси $y$ в предельном направлении, определяемом все более «крутыми» касательными к кривой. Она является «третьей точкой пересечения» с кривой для

любой вертикальной прямой: такая прямая пересекается с кривой в точках вида $(x_1,y_1)$, $(x_1,-y_1)$ и в точке $O$.

Определим групповую операцию. Суммой точек $P(x_1,y_1)$ и $Q(x_2,y_2)$ назовем точку $(x_3,y_3)$, где

$$x_3 = \lambda^2 - x_1 - x^2 \pmod p;$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p;$$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, \text{если} \quad P \neq Q; \\ \dfrac{3x_1^2 + a}{2x_1}, \text{если} \quad P = Q. \end{cases}$$

Кратные точки. Если $k$ – целое число, то, как и в любой абелевой группе, $k \cdot P$ обозначает сумму $k$ точек $P$ при $k > 0$ и сумму $|k|$ точек $-P$, если $k < 0$.

Рассмотрим алгоритм вычисления точки $kP$. Представим число $k$ в двоичном виде

$$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \ldots + k_r \cdot 2^r, \qquad k_i \in \{0,1\}.$$

Далее, положим $P_0 = P$, $P_1 = 2P_0$, ..., $P_r = 2P_{r-1} = 2^rP$.

Откуда $kP = \Sigma P_i$. Таким образом, мы можем вычислить $kP$ *самое большее за* $2\log_2 k$ шагов, каждый из которых представляет собой сложение точек на кривой.

**Пример**. Чтобы найти $100P$, представляем 100 в виде $100 = 2^6 + 2^5 + 2^2$. Далее, $P_0 = P$, $P_1 = 2P_0 = 2P$, $P_2 = 2P_1 = 2^2P$, $P_3 = 2P_2 = 2^3P$, $P_4 = 2P_3 = 2^4P$, $P_5 = 2P_4 = 2^5P$, $P_6 = 2P_5 = 2^6P$. Теперь $100P = P_6 + P_5 + P_2$. Мы нашли точку $100P$, произведя 6 удвоений и 2 сложения точек на кривой.

Замечание. Приведенная оценка времени работы не является наилучшей, особенно для конечных полей характеристики $p = 2$.

***Порядком*** $n$ точки $P$ на эллиптической кривой называется такое наименьшее натуральное число, что $nP = O$, разумеется, такого конечного $n$ может и не существовать, в этом случае мы будем говорить о точке ***бесконечного порядка***.

Пусть $E$ – эллиптическая кривая над полем $F_p$ и $P$ – точка на $E$. Задачей дискретного логарифмирования на $E$ (с основанием $P$) называется задача нахождения для данной точки $Q \in E$ такого целого числа $n$ (если оно существует), что $nP = Q$.

Стойкость криптографических систем, определенных на эллиптических кривых, определяется сложностью решения задачи дискретного логарифмирования в группе ее точек. Задача дискретного логарифмирования на эллиптической кривой является более трудной для решения, чем задача дискретного логарифмирования в конечных полях.

*Цифровая подпись на эллиптических кривых.* В качестве международного стандарта принят американский алгоритм цифровой подписи на эллиптических кривых (ECDSA). В этом стандарте используются эллиптические кривые над полем характеристики 2. Однако криптографически стойких кривых над полем такой характеристики сравнительно мало. Поэтому мы рассмотрим ЭЦП на эллиптических кривых, заданных над полем большей характеристики.

Замечание. В России официально принят стандарт ЭЦП на эллиптических кривых над полем большей характеристики – ГОСТ 34.10–2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». Выбор кривой и точки на ней подразумевает решение ряда вспомогательных задач. Прежде всего, это подсчет количества точек на кривой. Если $N$ – количество точек на $E(F_p)$, то должны выполняться следующие условия:

$$\begin{cases} p+1-2\sqrt{p} \le N \le p+1+2\sqrt{p}, & (1) \\ G \in E(F_p) \Rightarrow N \cdot G = O. & (2) \end{cases}$$

Таким образом, чтобы отсеять лишние числа из интервала $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$, можно проверять условие (2) для разных точек $G$. Единственное оставшееся число и будет искомым порядком кривой.

Для получения криптографически стойкой системы ЭЦП должны выполняться следующие условия.

Порядок точки $G$, используемой в системе ЭЦП, должен быть простым числом $n$, $n > \max\{2^{160}, 4\sqrt{p}\}$.

- $N \neq p$ и $N \neq p + 1$, где $N$ – порядок кривой;
- $pk \neq 1 \pmod{n}$ для всех $k = 1, ..., C$, где $C$ настолько велико, что вычислить дискретный логарифм в $F_{p^c}$ за приемлемое время невозможно.

Замечание. В настоящее время значение $C = 20$ считается достаточным.

Возможный способ защититься от известных атак и от возможных атак для специальных классов кривых, которые могут быть обнаружены в будущем, – выбирать кривую $E$ случайным образом так, чтобы выполнялись указанные условия.

После того, как порядок $N$ кривой определен, требуется найти большой простой делитель $n$ порядка кривой. Такой делитель может не существовать, и тогда потребуется повторять процедуру выбора кривой до тех пор, пока не будут выполнены все требуемые условия. Поиск числа $n$ может потребовать как разложения на множители числа $N$, так и доказательства простоты числа $n$. Точку $G$ можно выбрать следующим образом. Найдем случайную точку $G' \in E(F_p)$ и вычислим $G = \frac{N}{n} G'$. Если $G \neq O$, то требуемая точка найдена, если $G = O$, то выбираем другую точку $G'$.

Описанные параметры могут быть общими для всех пользователей. Для генерации и проверки подписи требуются еще и индивидуальные параметры пользователя – это секретный и открытый ключи. Ключ подписи (секретный ключ) – это случайное число $d$, $0 < d < n$. Ключ проверки подписи (открытый ключ) – это точка эллиптической кривой $Q = d \cdot G$. Алгоритм ЭЦП также использует хеш-функцию, обозначаемую $h$.

*Генерация подписи.* Входные данные: сообщение $M$, исходные параметры и ключ подписи. Выходные данные: подпись $(r,s)$.

Алгоритм.

Выбрать случайное число $k$ в интервале $(1, n-1)$.

1. Вычислить $(x, y) = d \cdot G$.
2. Вычислить $r = x \bmod n$.
3. Если $r = 0$, то вернуться к шагу 1.
4. Вычислить $z = k^{-1} \bmod n$.
5. Вычислить $e = H(M)$.
6. Вычислить $s = z(e + dr) \bmod n$.
7. Если $s = 0$, то вернуться к шагу 1.
8. Вывести пару $(r,s)$ – подпись к $M$.

Замечания.

• При $r = 0$ результат вычисления $s$ не зависит от секретного ключа $d$.

• При $s = 0$ необходимого для проверки подписи числа $s^{-1} \bmod n$ не существует.

• В качестве хеш-функции $H$ на шаге 6 в стандартах ANSI X9F1 и IEEE P1363 используется SHA-1, в российском стандарте ГОСТ Р 34.10–2001 – хеширование по стандарту ГОСТ Р 34.11–94.

*Пример генерации подписи.* Наша цель – показать особенности алгоритма, не зависящие от разрядности чисел. Пусть используется эллиптическая кривая $E_{751}(-1,1)$ и генерирующая точка $G = (384, 475)$ порядка $n = 13$ (13 – наибольший из делителей порядка кривой $N = 728$). Предположим, абонент подписывает личным секретным ключом $d = 12$ сообщение, хеш-свертка которого равна $e = 12$.

Пусть абонент, подписывающий сообщение, выбрал случайное $k = 3$. Тогда он вычисляет $kG = (x,y) = 3 \cdot (384,475) = (596,318)$ и затем $r = x \bmod n = 596 \bmod 13 = 11$. Используя расширенный алгоритм Евклида, определяем $z = k^{-1} \bmod n = 3^{-1} \bmod 13 = 9$ (так как $3 \cdot 9 = 27 \equiv 1 \pmod{13}$). Наконец, $s = z(e + dr) \bmod n = 9(12 + 12 \cdot 11) \bmod 13 = 9$. Таким образом, $(r,s) = (11,9)$ – цифровая подпись данного абонента для сообщения.

В реально использующихся системах ЭЦП по российскому стандарту числа имеют порядка 60 десятичных знаков.

*Проверка подписи.* Входные данные: сообщение $M$, исходные параметры, ключ проверки подписи и подпись к $M$. Выходные данные: заключение о подлинности или фальсификации подписи.

Алгоритм.

1. Если хотя бы одно из условий $1 \le r \le n-1$, $1 \le s \le n-1$ нарушается, то подпись фальшивая и работа алгоритма закончена.

2. Вычислить $e = H(M)$.

3. Вычислить $v = s^{-1} \bmod n$.

4. Вычислить $u_1 = ev \bmod n$.

5. Вычислить $u_2 = rv \bmod n$.

6. Вычислить $X = u_1 \cdot G + u_2 \cdot Q = (x,y)$.

Если $r = x \bmod n$, то подпись действительная, иначе – подпись фальшивая.

Доказательство корректности алгоритма генерации и алгоритма проверки подписи достаточно просто.

**Классификация атак на схемы электронной подписи и арбитраж.**

Стойкость схемы электронной подписи зависит от стойкости используемых криптоалгоритмов и хеш-функций и определяется относительно пары «угроза–атака». Приведем классификацию атак на схемы электронной подписи:

• *атака на основе известного открытого ключа* (***key-only attack***) – самая слабая из атак, практически всегда доступная противнику;

• *атака на основе известных подписанных сообщений* (***known-message attack***) – в распоряжении противника имеется некоторое число пар ($p'$, $s$), где $p'$ – некоторое сообщение, а $s$ –допустимая подпись для него, при этом противник не может влиять на выбор $p'$;

• *простая атака с выбором подписанных сообщений* (***generic chosen-message attack***) – противник имеет возможность выбрать некоторое количество подписанных сооб-

щений, при этом открытый ключ он получает после этого выбора;

• направленная атака с выбором сообщений (directed chosen-message attack) – выбирая подписанные сообщения, противник знает открытый ключ;

• *адаптивная атака с выбором сообщений* (*adaptive chosen-message attack*) – противник знает открытый ключ, выбор каждого следующего подписанного сообщения он может делать на основе знания допустимой подписи предыдущего выбранного сообщения.

Каждая атака направлена на достижение определенной цели. Можно выделить следующие виды *угроз для схем электронной подписи* (в порядке возрастания силы):

• *экзистенциальная подделка* (*existential forgery*) – создание противником подписи для какого-нибудь, возможно бессмысленного, сообщения $M'$, отличного от перехваченного;

• *селективная подделка* (*selective forgery*) – создание подписи для заранее выбранного сообщения;

• *универсальная подделка* (*universal forgery*) – нахождение эффективного алгоритма формирования подписи, функционально эквивалентного исходному;

• *полное раскрытие* (*total break*) – вычисление секретного ключа, возможно, отличного от $k_A^{secret}$, соответствующего открытому ключу $k_A^{public}$, что дает возможность формировать подписи для *любых* сообщений.

Наиболее надежными являются схемы, стойкие против самой слабой из угроз на основе самой сильной из атак, т. е. против экзистенциальной подделки на основе атаки с выбором подписанных сообщений. Справедливо следующее утверждение. *Схемы ЭЦП, стойкие против экзистенциальной подделки на основе атаки с выбором подписанных сообщений существуют тогда и только тогда, когда существуют односторонние функции.*

*Процедура разрешения споров.*

Для практического применения схем ЭЦП помимо алгоритмов формирования подписи и ее верификации тре-

буется процедура арбитража. Арбитраж необходим, когда один из абонентов, например, получатель **B** предъявляет сообщение и подпись ($p'$, $s$), утверждая, что эта пара сообщение–подпись была получена от **A**, и **A** отказывается признавать эту подпись своей. С юридической точки зрения основанием для разрешения подобных споров в суде является подписание (обычным способом) каждым пользователем при подключении к системе специального документа, в котором пользователь принимает все «правила игры», вплоть до судебной ответственности. При разборе дела в суде арбитр выступает в качестве эксперта, дающего заключение о подлинности ЭЦП.

*Алгоритм арбитража.*

1. Абонент **B** предъявляет арбитру электронный документ и подпись.

2. Арбитр требует от абонента **A** предъявления своего секретного ключа. Если **A** отказывается, арбитр дает заключение, что подпись подлинная.

3. Арбитр выбирает из сертифицированного справочника открытый ключ абонента **A** и проверяет его соответствие секретному ключу, предъявленному **A**. Если они совпадают, арбитр переходит к шагу 5.

4. При обнаружении факта несоответствия ключей арбитр обращается в центр сертификации и требует предоставления заверенного абонентом **A** документа, содержащего его открытый ключ. Если выясняется, что открытый ключ, взятый из справочника, не совпадает с указанным в документе, арбитр признает подпись, предъявленную **B**, подлинной, при этом все издержки такого решения компенсируются за счет центра. Если открытые ключи в справочнике и документе совпадают, т. е. абонент **A** предъявил некорректный секретный ключ, арбитр признает подлинность ЭЦП.

5. Арбитр проверяет соответствие друг другу подписи и документа. При положительном результате проверки подпись признается подлинной, в противном случае отвергается.

Задача арбитража значительно сложнее, чем кажется на первый взгляд. Арбитраж и решение споров в суде невозможны в следующих случаях:

• секретный ключ сформирован не самим абонентом **A**, а специальным центром генерации ключей;

• аппаратура, на которой выполняется алгоритм генерации или проверки подписи, содержит какие-либо элементы, не контролируемые пользователем («черные ящики», защищенные участки памяти и т. п.).

Наконец, возможны безвыходные ситуации, в которых арбитр не может принять никакого обоснованного решения. Например, абонент **B** предъявляет $s$ и утверждает, что это подпись под документом $p'$. Абонент **A** признает, что это его подпись, но под документом $p \neq p'$, при этом выясняется, что хеш-образы этих документов совпадают, т. е. $H(p) = H(p')$. Арбитр понимает, что кто-то из двоих нашел коллизию для применяемой в схеме электронной подписи хеш-функции. Выход из положения возможен только в том случае, если заранее обговорен порядок разрешения спора в такой ситуации.

**Особые схемы электронной подписи.**

В некоторых ситуациях могут потребоваться схемы электронной подписи, отличные от рассмотренных классических схем. Известны следующие специальные схемы электронной подписи:

• *схема подписи «вслепую»*, когда абонент **A** подписывает документ, не зная его содержимого (см. «электронные деньги»);

• *схема групповой подписи*, которая позволяет верификатору убедиться в принадлежности полученного сообщения некоторой группе претендентов, но кто именно из членов группы подписал документ, верификатор определить не в состоянии;

• *схема разделяемой подписи*, которая формируется только при участии определенного количества участников протокола, иначе говоря, данная схема является объедине-

нием классической схемы подписи и *схемы разделения секрета*;

• *схема конфиденциальной (неотвергаемой) подписи*, которая не может быть проверена без участия сформировавшего ее участника протокола;

• *схема неоспоримой подписи*, в которой подделка подписи может быть доказана.

*Электронные деньги как пример «слепой» подписи.* В настоящее время электронный документооборот распространяется все больше. В современных платежных системах весь процесс происходит в электронной (цифровой) форме. При этом для обеспечения безопасности и признания законности используются криптосистемы с открытым ключом при формировании ЭЦП.

Учитывая, что традиционные денежные купюры – это защищенный от подделки документ, логичным представляется переход к использованию *электронных денег.* Защиту от подделки при этом может обеспечить ЭЦП банка, которая имеет большую надежность, чем традиционные водяные знаки, металлические полосы и т. п.

При осуществлении платежей с помощью кредитной карточки где-то в базе данных делается отметка об этом событии. Соединив вместе эти в отдельности малозначимые данные, можно собрать большое количество информации об отдельном человеке. Необходимо реализовать такую систему доступа к ресурсам и услугам, в которой одновременно решены задачи идентификации и анонимности. Другими словами, возникает задача обеспечения неотслеживаемости электронных документов, в частности электронных денег.

Электронные деньги – это информация о реально существующих средствах. Более полно, *электронные деньги – это бессрочные денежные обязательства банковской или иной структуры, представленные в электронной форме, сопровождаемые ЭЦП выдавшей их структуры и погашаемые в момент предъявления обычными денежными средствами.*

Для того, чтобы сделать электронную купюру эквивалентной обычной бумажной купюре того же номинала, Д. Шаум (основатель фирмы DigiCash и крупный специалист в области криптографии) предложил *протокол слепой подписи (blind signature)*.

Рассмотрим пример слепой подписи по схеме RSA. Банк **C** выбирает два секретных больших числа $p$ и $q$, вычисляет их произведение $n = pq$, а также находит $e$ и $d$ – соответственно, открытый $k_C^{(public)}$ и секретный $k_C^{(secret)}$ ключи банка, такие, что $ed = 1 \bmod \varphi(n)$, где $\varphi(n)$ – функция Эйлера, т. е. количество чисел, меньших $n$ и взаимно простых с $n$. В данном случае $\varphi(n) = (p - 1)(q - 1)$. Выбирается односторонняя функция $f$: $Z_n \to Z_n$.

Числа $n$, $e$ и функция $f$ публикуются. При этом пара ключей $(e,d)$ используется банком для создания купюр одного фиксированного номинала. Для создания купюр другого номинала используется своя пара ключей.

*Протокол транзакции заказа электронной наличности (снятия со счета) с использованием слепой подписи.*

1. Клиент **A** выбирает случайное число (по сути, номер купюры) $x \in Z_n$ и вычисляет $f(x)$.

2. Клиент **A** инициирует начало протокола слепой подписи, выбирая случайное число $r \in Z_n$, $r \neq 0$. Клиент **A** вычисляет $y = f(x)r^e \bmod n$, где $r^e$ – так называемый затемняющий множитель, и посылает запрос $y$ абоненту **C**.

3. Банк **C** подписывает купюру, вычисляя $y^d \bmod n$, и посылает полученное значение $(f(x))^d \cdot r \bmod n$ клиенту **A**.

4. Клиент **A** «снимает» действие затемняющего множителя и получает подписанную купюру $(x, (f(x))^d \bmod n)$, где $s = (f(x))^d \bmod n$ – подпись банка **C**.

Примечание. В полном протоколе используются дополнительно шаги формирования и проверки подписи клиента **A** на запросе $y$.

*Протокол транзакции платежа с использованием электронной наличности.*

1. Покупатель **A** передает продавцу **B** электронную купюру $(x,s)$.

2. Продавец **B** посылает $(x, s)$ банку **C**.

3. Банк **C** вычисляет $f(x)$ и проверяет свою подпись, убеждаясь в справедливости равенства $f(x) = s^e \bmod n$.

4. Банк **C** проверяет, не была ли купюра с данным номером потрачена ранее, и, если нет, перечисляет на счет клиента **B** сумму, равную номиналу купюры, и уведомляет его об этом.

Примечание. В полном протоколе используются дополнительно шаги формирования и проверки подписи клиента **B** на пересылаемом документе $(x,s)$.

Рассмотренная система платежей, требующая участия банка во всех транзакциях, называется *централизованной*. В отличие от последней, *автономная система платежей* предполагает, что продавец **B** сам, без обращения к банку **C**, проверяет подлинность предъявленной покупателем **A** электронной наличности. В этом случае банк идет на определенный риск, так как используемые схемы обеспечивают обнаружение злоупотреблений со стороны **A** постфактум. Основная идея соответствующих протоколов – однозначно идентифицировать нарушителя.

### Литература


1. *Алферов А. П.* и др. Основы криптографии: Учеб. пособие. – М.: Гелиос АРВ, 2001. – 480 с.

2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2003. – 816 с.

3. *Иванов М. А.* Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

4. *Жданов О. Н., Чалкин Т. А.* Эллиптические кривые и их применение в криптографии: Учеб. пособие. – Красноярск: СибГАУ, 2011. – 131 с.

УДК 004.056

**И. В. Поночевная, А. М. Петрова**

Санкт-Петербургский государственный инженерно-экономический университет

# АКТУАЛЬНЫЕ АСПЕКТЫ ОРГАНИЗАЦИОННО-ПРАВОВОЙ СОСТАВЛЯЮЩЕЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

В настоящее время во всем мире резко повысилось внимание к проблеме СИБ – системы информационной безопасности. Это обусловлено процессами стремительного расширения потоков развития информационных ресурсов в глобальной компьютерной сети Интернет, пронизывающих все сферы жизни общества и государства. К значительной части информационных ресурсов глобальной компьютерной сети Интернет предъявляются требования по обеспечению определенной степени конфиденциальности.

Отличительной особенностью информационных объектов является комплексное использование на них информационных и телекоммуникационных систем, т. е. инфокоммуникационных систем, что вызывает необходимость применения более широкого спектра составляющих для защиты информационного ресурса в информационном пространстве.

Рассматриваемые в работе декомпозиции составляющих СИБ могут оказаться совершенно бесполезными, если не будет соблюден надлежащий действующий пакет политик.

Действующий пакет политик включает в себя концепцию пакета политик безопасности (КППБ) и является в совокупности с составляющими СИБ основным документом, определяющим защищенность информационного пространства от внутренних, внешних и комбинированных «субъектов угроз».

Полезные рекомендации на этот счет содержатся в международных стандартах, в частности в международном стандарте безопасности информационных систем ISO 17799–2005[1].

Решение данной задачи предполагает, что защищенность может быть обеспечена только соблюдением концепции пакета политик безопасности, на основе комплексного подхода, реализация которого начинается с *организационно-правовых,* инженерно-технических и технологических составляющих на единой концептуальной основе.

Инженерно-техническое направление защиты формируется программно-аппаратными средствами защиты. Это направление формирует единую инженерно-техническую политику безопасности в части выбора средств защиты и текущее состояние системы безопасности.

Под программным средством защиты следует понимать совокупность специальных программ, реализующих функции безопасности и режима функционирования системы.

К аппаратным средствам защиты относятся механические, оптические, лазерные, радиотехнические, биометрические и др.

Технологическое направление защиты. Система безопасности должна быть эффективной, устойчивой к воздействиям, обеспечивать прозрачность, т. е. соответствовать требованиям международных и отечественных стандартов.

***Организационно-правовое направление защиты*** основано на нормативно-правовой основе, предполагающей, что разглашение, утечка ценной информации и несанкционированный доступ или взлом или подбор пароля в систему будет невозможным или существенно затруднен за счет проведения организационных мероприятий.

---

[1] Международный стандарт построения эффективной системы безопасности разработан в 2000 г. Международной организацией по стандартизации. Этот стандарт является официальным документом, описывающим комплексный подход к вопросам безопасности и рассматривающим в качестве элементов управления как технические, так и организационно-административные меры, обеспечивающие конфиденциальность, целостность, доступность и достоверность информации.

Одним из основных компонентов организационного направления является служба информационной безопасности. Основная цель функционирования службы информационной безопасности, использующей комплекс средств защиты, – избежать или свести до минимума возможность нарушения, или вовремя заметить и устранить последствия дестабилизирующих факторов по отношению к системе.

В работе предполагается, что организационно-правовая составляющая пакета политик играет первостепенную роль, так как эффективность самых дорогостоящих и сложных средств защиты сводится к нулю, если пользователи системы будут игнорировать элементарные правила работы.

Таким образом, если система будет соответствовать стандартам, то она будет прозрачна для взаимодействия с любой другой системой, которая соответствует также стандартам. Это относится к средствам криптографической защиты, к средствам защиты от несанкционированного воздействия, к средствам антивирусной защиты и т. д. Обобщающий мировой опыт международных стандартов в этой области является результатом развития национальных стандартов.

Особенно актуальны эти требования для инфокоммуникационных систем специального назначения, поскольку они предназначены, как правило, для передачи информационного ресурса, составляющей государственную тайну.

Вместе с развитием способов и методов передачи и преобразования информационного ресурса постоянно развиваются и методы обеспечения ее безопасности. Современный этап развития этой проблемы характеризуется переходом от традиционного ее представления как проблемы защиты информации к более широкому пониманию – проблеме информационной безопасности (инфобезопасности), заключающейся в комплексном ее решении по двум основным составляющим.

К первой составляющей можно отнести защиту государственной тайны и конфиденциальных сведений, обеспе-

чивающую главным образом невозможность несанцкионированного доступа к ним. При этом под конфиденциальными сведениями понимаются сведения ограниченного доступа общественного характера (коммерческая тайна, и т. д.), а также личная конфиденциальная информация (интеллектуальная собственность, персональные данные и т. д.).

Ко второй составляющей относится защита от информационного воздействия на человека, общество и государство, которая в последнее время приобретает международный масштаб и стратегический характер.

Исходя из вышесказанного, в последнее время проблема защиты информации рассматривается как проблема системы информационной безопасности как неотъемлемой составной части национальной безопасности Российской Федерации. Это ясно определяется концепцией национальной безопасности Российской Федерации и Доктриной информационной безопасности Российской Федерации, так как система национальных интересов России определяется совокупностью основных интересов личности, общества и государства.

Информационная безопасность Российской Федерации определяется в Доктрине как состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационном пространстве заключаются в реализации конституционных прав человека и гражданина на доступ к информации, использовании ее в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационном пространстве заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового соци-

ального государства, достижении и поддержании общественного согласия.

Интересы государства заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод граждан в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности; защиты информационных ресурсов государства от несанкционированного доступа; обеспечения безопасности информационных и телекоммуникационных систем России.

Из вышесказанного среди всей совокупности средств и методов обеспечения информационной безопасности организационно-правовая специфика стоит на особом месте, так как играет одну из наиболее важных ролей в создании и функционировании прочной системы защиты информации в информационном пространстве.

Это направление обусловливается тем, что возможности несанкционированного использования конфиденциальной информации в значительной мере зависят не от технических аспектов защиты, а от злоумышленных, небрежных и халатных действий пользователей системы и персонала объекта обработки информационного ресурса. Влияние этих аспектов практически невозможно избежать с помощью технических и программных средств защиты. Для этого необходимо организационное обеспечение системы информационной безопасности (инфобезопасности) – регламентация деятельности по обработке и защите конфиденциального информационного ресурса и взаимоотношений обслуживающего персонала на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к информационному ресурсу становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий.

Вышеизложенное говорит о том, что работоспособность системы информационной безопасности должна ба-

зироваться на концепции пакета политик, так как важность этой проблемы подчеркивает такой факт, как создание по инициативе Президента Российской Федерации «Доктрины информационной безопасности», и выделены общие методы обеспечения информационной безопасности: организационно-правовые, технические и экономические. «Доктрина информационной безопасности Российской Федерации» является основой для формирования государственной политики в области обеспечения информационной безопасности России.

**Литература**

1. Доктрина информационной безопасности РФ от 9 сентября 2000 г. № Пр-1895.

УДК 004.056.5

**Р. А. Пермяков**

Новосибирский государственный университет

## О ПОСТРОЕНИИ МОДЕЛИ НАРУШИТЕЛЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Проблемам информационной безопасности сегодня уделяется большое внимание как со стороны бизнеса, так и со стороны государства. Государственные инициативы, нашедшие отражение в последних изменениях правового поля в области информатизации, показывают важность обеспечения безопасности информации на всех уровнях общества. За последние годы тема безопасности персональных данных стала одной из ключевых в сообществе профессионалов в области информационной безопасности.

С другой стороны, бизнес-сообщество осознает важность защиты нематериальных активов, представляющих собой, в том числе и know-how, оперативную отчетность и состояние бизнеса, сведения о контрагентах [1].

Исходя из вышесказанного, бизнес предъявляет следующие требования к современным информационным системам.

1. Коммуникации с мобильными сотрудниками для информационной поддержки выполнения ими своих должностных обязанностей. Данный вид коммуникаций характеризуется тем, что мобильному пользователю в общем случае необходим полный доступ к информационным ресурсам компании в соответствии с его уровнем доступа. Опыт показывает, что частичное решение возможно через введение двух политик безопасности для пользователя с существенным ограничением возможности доступа к информационным ресурсам с мобильных устройств [2, 3]. Таким образом, мы сталкиваемся с ситуацией, когда установление каких-либо жестких требований со стороны службы безопасности к программному и/или аппаратному обеспечению противоречит не только потребностям объекта защиты, но и создает новый набор угроз для непрерывности процессов, проходящих в объекте. Фактически служба безопасности предприятия сталкивается с проблемой неконтролируемого использования программно-аппаратных средств пользователями, существующей в силу объективных причин, связанных с изменением бизнес-среды, возрастающей конкуренцией и сокращением времени принятия решения.

2. Коммуникации с контрагентами организации. Ведение современного бизнеса невозможно без информационного обмена с контрагентами, в том числе с участием информации ограниченного распространения. В общем случае при обмене информацией мы можем на уровне договоров требовать соблюдения режима коммерческой тайны, но при этом не вправе определять политику контрагента в отношении полученной информации, а также требовать применения каких-либо конкретных программных или технических решений. Проблема несоответствия политик безопасности между двумя организациями рассматрива-

лась в [4, 5], однако сегодня требования к функциональной независимости этих систем возросли многократно.

3. Информационный обмен с клиентами компании, физическими лицами. При рассмотрении информационного обмена между компанией и ее клиентом ситуация оказывается несколько лучше, поскольку в данном случае служба информационной безопасности имеет возможность навязать определенный регламент информационного обмена и в какой-то мере определить требования к программно-аппаратному обеспечению клиента. Однако мы не можем определять частные параметры системы защиты информации на стороне клиента, например, мы не можем требовать установки конкретной версии антивирусного программного обеспечения или соблюдения требования не посещать определенные сайты в Интернете [6].

Утечки информации данной категории становятся заметными в современном мире, требующем от бизнеса адекватной реакции в короткие сроки.

Исходя из требований, мы можем определить современные задачи информационной системы как:

- обеспечение информационной поддержки принятия решения в короткие сроки, независимо от местоположения;
- информационное обеспечение бизнес-процесса, доведение управляющих воздействий до исполнителя;
- информационное сопровождение коммуникаций организаций (B2B, B2C, B2G, G2C, G2G);
- обеспечение прозрачности принимаемых решений;
- обеспечение широкого информационного присутствия.

Таким образом, традиционные методы защиты информации, основанные на создании замкнутого периметра защиты, не позволяют эффективно использовать все возможности современных информационных систем. Более того, современное правовое поле запрещает использование мобильных клиентов при обработке персональных данных и другой охраняемой законом информации [7].

Для обоснованного изменения парадигмы защиты необходимо изучить новые возможности нарушителей. Традиционно модель нарушителя участвует при создании системы защиты информации как формальное представление интегратора о системе ограничений нарушителя естественного или искусственного характера [8].

При разработке системы защиты информации учитываются следующие параметры:

- классификация ресурсов;
- модель актуальных угроз;
- актуальная модель нарушителя.

Поскольку сегодня нет достоверного исследования взаимосвязи между классом нарушителя (в терминах любой известной модели) и классом информационных ресурсов, данный вопрос отдается на решение экспертам, что довольно часто приводит к необоснованно завышенной, в случае перестраховки экспертов, или необоснованно заниженной, в случае экономии ресурсов, оценке [9].

Кроме того, с учетом процессов усиления информационной связанности бизнеса [1] в традиционную классификацию нарушителя по критериям «внешний–внутренний» мы должны включить категорию «сотрудник контрагента», принимающую два значения:

- лояльный сотрудник контрагента, выполняющий распоряжение своего руководства по сбору критической информации в информационной системе организации и имеющий доступ в систему на основании договора между организациями;
- инсайдер контрагента, выполняющий распоряжения третьих лиц по сбору информации как в информационной системе контрагента, так и информационной системе организации.

Данный класс нарушителей не учитывается, например, в моделях ФСТЭК [8–10].

Очевидно, что данная ситуация будет сохраняться в силу естественного отставания распорядительных доку-

ментов от реального состояния дел. Для решения этой проблемы целесообразно изучить возможность широкого применения математических моделей при разработке нормативно-правовых актов в области информационной безопасности.

Рассмотрим один из возможных подходов к построению такой модели нарушителя. Далее будем руководствоваться следующими принципами.

1. Нарушителю в общем случае неизвестна организационно-техническая структура системы. Несмотря на то, что данное утверждение противоречит второму принципу Керкгоффса [11], учитывая принцип несовместимости, утверждающий, что высокая точность системы несовместима с большой сложностью, можно утверждать, что практически всегда внешний (относительно системы) наблюдатель не знает полностью ее внутреннюю структуру.

2. Нарушитель ограничен рамками естественной природы, которые можно выразить алгебраически.

3. Нарушитель старается выбрать по возможности оптимальный путь.

4. Цель нарушителя в общем случае сводится к снятию неопределенности о системе (в шенноновском смысле) с целью получения контроля над системой или ее частью. Под контролем мы будем понимать возможность перевода нарушителем системы в заранее определенное состояние с использованием как ресурсов атакуемой системы, так и сторонних ресурсов.

Таким образом, мы можем определить следующие множества:

*$S$ – множество состояний системы;*

*$S^{\text{ч}}$ – множество разрешенных политикой безопасности состояний системы;*

*$S^{\text{н}}$ – множество запрещенных политикой безопасности состояний системы, при этом очевидно, что $S = S^{\text{ч}} \cup S^{\text{н}}$;*

*$V$ – множество уязвимостей системы, при этом следует понимать, что под уязвимостью мы понимаем как не-*

*достатки и ошибки программного обеспечения, так и ошибки конфигурирования информационной системы;*

*$A$ – множество откликов системы (образующих алфавит) на сформированные запросы $Q$ нарушителя. При этом мы можем утверждать, что событие $a_i$ зависимо от $q_i$ и $s_i$ в силу природы исследуемого объекта. В силу этого мы можем определить аналогично два множества: $A = A^t \cup A^u$;*

*$T = S \cdot A \cdot Q \cdot S$ – множество возможных переходов в системе, аналогично мы можем выделить: $T = T^t \cup T^u$.*

Нарушитель осуществляет выбор запроса $q_i$, такого, что $card(T^t) \to min$.

Таким образом, мы можем определить энтропию информационной системы относительно нарушителя как взаимную энтропию атакуемой системы и хакера:

$$H(AQ) = H(A) + H(A|Q).$$

Применение понятия взаимной энтропии дает интересные результаты при исследовании информационных систем как объекта защиты. Так, например, широко используемый прием разделения базы данных (с целью понижения класса) на обезличенную и индекс к первой базе обеспечивают адекватный уровень защиты при следующем условии:

$$H(T_1 \cdot T_2) = H(T_1) + H(T_2);$$

очевидно, что данное требование выполняется, если:

$$(T^t \cup T^u) \cap T = \varnothing.$$

Таким образом, мы можем утверждать, что для понижения класса системы должны быть информационно изолированными.

**Литература**

1. *Пермяков Р. А., Помешкин А. А.* О требованиях к системам защиты информации в современных информационных системах //

Материалы XIII Всерос. науч.-практ. конф. «Проблемы информационной безопасности государства, общества и личности». – Томск, 2012. – С. 109–111.

2. *Anup K. Ghosh.* Software security and privacy risks in mobile e-commerce / Anup K. Ghosh, Tara M. Swaminatha // Communications of the ACM. Vol. 44. Is. 2. 2001. Feb. – P. 51–57.

3. *Jiejun Kong.* Providing robust and ubiquitous security support for mobile ad-hoc networks / Jiejun Kong, Petros Z., Haiyun Luo, Songwu Lu, Lixia Zhang // Network Protocols. 2001. Ninth International Conference, 14–14 Nov. 2001.

4. *Chuchang Liu.* Trust in Secure Communication Systems – The Concept, Representations, and Reasoning Techniques / Chuchang Liu, Maris A. Ozols // Proceeding AI '02 Proceedings of the 15-th Australian Joint Conference on Artificial Intelligence: Advances in Artificial Intelligence. – P. 60–70.

5. *George Coulouris.* Secure Communication in Non-Uniform Trust Environments [Электронный ресурс] / George Coulouris, Jean Dollimore, Marcus Roberts. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.56.8790 (дата обращения: 01.10.2012).

6. *Michael E. Porter.* Strategy and the Internet [Электронный ресурс] // Harward Busines Review OnPoint. URL: https://140.78.51.40/static/0855380/files/strategy%20and%20the%20internet.pdf (дата обращения: 01.10.2012).

7. *Лукацкий А.* Доступ с мобильных устройств и регуляторы [Электронный ресурс]. URL: http://lukatsky.blogspot.ru/2012/11/blog-post_12.html (дата обращения: 01.10.2012).

8. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации / Гостехкомиссия при Президенте РФ, 30.03.92.

9. Министерство связи и массовых коммуникаций РФ. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли [Электронный ресурс]. URL: http://minsvyaz.ru/common/upload/publication/1410065MC.pdf (дата обращения: 01.10.2012).

10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных / ФСТЭК России, 14.02.08.

11. *Kerckhoffs A.* La Cryptographie Militaire. – France, 1883.

УДК 65.012.7-65.012.8

**М. В. Буйневич**
Санкт-Петербургский государственный инженерно-экономический университет
**Олаоде А. Джон**
Санкт-Петербургский государственный университет телекоммуникаций

# СОСТАВ И СОДЕРЖАНИЕ ЭЛЕМЕНТОВ МОДЕЛИ ОЦЕНКИ УСТОЙЧИВОСТИ И БЕЗОПАСНОСТИ ТКС

Телекоммуникационные сети (ТКС) постоянно совершенствуются в направлении оказания все более широкого спектра услуг и предоставления новых инфокоммуникационных продуктов. Побочным эффектом является расширение списка новых угроз устойчивости функционирования и безопасности [1]. В этих условиях операторы должны перманентно принимать обоснованные решения для минимизации возможного ущерба. И главным инструментом здесь выступает адекватная модель оценки соответствующих показателей, определяющих степень обоснованности решений.

Предлагается некий универсальный набор взаимосвязанных элементов модели, отождествляющих собой все значимые объекты информационной безопасности.

1. **Оператор** – это субъект или организация, которые создают ТКС из уникального набора телекоммуникационного *оборудования* с тем, чтобы обеспечить конечного пользователя устойчивым и безопасным набором услуг и инфо-продуктов.

2. **Оборудование** – собственно телекоммуникационные (и иные необходимые) устройства и их специализированное программное обеспечение, необходимые и достаточные для организации ТКС. Оборудование прописано в паспорте оператора, обладает уникальным набором *уязвимостей* и располагается в одной из *зон безопасности*.

3. **Зона безопасности** – логическая конструкция, ограничивающая оборудование в пределах некого периметра (сетевой границы), характеризующегося уникальным набором *источников угроз* и, соответственно, уникальным уровнем сетевой безопасности.

4. **Источник угрозы** – кто-то или что-то (человек, программа, явление, процесс), способное использовать *уязвимость* оборудования для реализации *угрозы* безопасности.

5. **Уязвимость** – слабое место в *оборудовании* (или его архитектурном построении), наличие которого может привести к возникновению *угрозы* безопасности при соответствующем ее *источнике*.

6. **Угроза** – потенциальный ущерб *активам*, наносимый *источником угрозы* в результате использования им *уязвимости*.

7. **Актив** – нечто, представляющее ценность для *оператора* и потому подлежащее защите. Согласно подавляющему большинству авторитетных источников сферы информационной безопасности, ТКС характеризуется конфиденциальностью, целостностью и доступностью.

Представляется, что предложенный набор элементов (во взаимосвязи) является необходимым и достаточным для решения широкого класса задач безопасности ТКС, начиная от выбора актуальной темы научного исследования и заканчивая разработкой автоматизированной системы поддержки принятия количественно обоснованных решений.

Рассмотрим, например, решение задачи определения взаимосвязи требований и нарушений на сетях связи общего пользования. В [2] с позиций системного и причинно-следственного анализа разработан методологический подход, связывающий требования к оператору (в части требований к устойчивости функционирования и защите ТКС от несанкционированного доступа) с нарушениями целостности, устойчивости функционирования и безопасности сетей связи общего пользования, суть которого состоит в следующем:

– государством (в лице регулятора) к оператору предъявляются некие требования, которые реализуются им в виде защитных мер и мероприятий, направленных на минимизацию или устранение источников угроз и уязвимостей, обусловленных наличным операторским оборудованием и зоной его расположения;

– оператор определяет состав защитных мер и мероприятий, исходя из баланса их стоимости и ценности защищаемых активов, определяемого при помощи методов и средств оценки рисков;

– выполнение требований, предъявляемых к оператору, проверяется с помощью соответствующих методов и средств;

– источник угроз (при наличии соответствующей уязвимости) потенциально ведет к реализации угроз, создающих опасность нанесения ущерба конфиденциальности, целостности и доступности операторских активов, который, в свою очередь, кумулятивно и взвешенно ведет к нарушениям устойчивости и безопасности функционирования сетей связи общего пользования.

Таким образом, по установленной причинно-следственной цепочке невыполнение оператором предъявляемых ему требований ведет к предпосылкам соответствующих нарушений.

Следующим примером может служить анализ государственных и международных стандартов по безопасности, а также BestPractices (лучших практик безопасности ведущих операторов), описывающих специфические особенности компонентов (элементов и связей) модели.

**Литература**

1. *Буйневич М. В.* и др. Исследование и моделирование угроз безопасности цифровой телекоммуникационной сети: Отчет о НИР. Шифр «Цифровая угроза-2012» / Науч. рук. С. М. Доценко. Рег. № 047-12-054. – СПб.: СПбГУТ, 2012. – 219 с.

2. *Буйневич М. В.* и др. Разработка предложений по организационно-техническому обеспечению устойчивости функционирования сетей связи, защиты сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации, мето-

дов проверки и определение перечня нарушений целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации: Отчет о НИР / Науч. рук. С. М. Доценко. Рег. № 034-12-054. – СПб.: СПбГУТ, 2012. – 177 с.

УДК 004.056

**А. С. Куракин**

Санкт-Петербургский национальный
исследовательский университет
информационных технологий, механики и оптики

# МЕТОД ФОРМИРОВАНИЯ ПЕРЕЧНЯ ТРЕБОВАНИЙ, ПРЕДЪЯВЛЯЕМЫХ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Технические и организационные методы и средства, используемые для защиты обрабатываемых в информационной системе ПДн от угроз НСД, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации [1]. В силу этого перед проведением конкретных мероприятий по защите ПДн от НСД необходимо определить перечень организационно-технических требований, которым используемые средства должны удовлетворять.

Формализация данных требований, как правило, проводится на основе приказа ФСТЭК «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» [2]. Согласно данному документу, мероприятия по защите ПДн реализуются в рамках подсистем: управления доступом, регистрации и учета, обеспечения целостности, криптографической защиты, антивирусной защиты, обнаружения вторжений. Кроме этого, в ИСПДн должен проводиться контроль на наличие недекларированных возможностей в программном и программно-аппаратном обеспечении и анализ защищенности системного и прикладного программного обеспечения.

Порядок организации обеспечения безопасности ПДн в ИСПДн должен предусматривать:

- оценку обстановки;
- обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;
- разработку замысла обеспечения безопасности ПДн;
- выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты;
- решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;
- обеспечение реализации принятого замысла защиты;
- планирование мероприятий по защите ПДн;
- организацию и проведение работ по созданию системы защиты персональных данных (СЗПДн) в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в ИСПДн, а также решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;
- разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн;
- развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;
- доработку СЗПДн по результатам опытной эксплуатации.

При этом должны быть определены мероприятия по:

- выявлению и закрытию технических каналов утечки ПДн в ИСПДн;
- защите ПДн от несанкционированного доступа и неправомерных действий;
- установке, настройке и применению средств защиты.

Необходимо заметить, что набор требований к системе защиты, приводимый в документе [2], может оказаться избыточным для конкретной организации. Кроме того, затра-

ты, необходимые для выполнения всех требований, могут превышать бюджет, выделяемый в организации на СЗПДн.

Предлагаемый метод позволяет на основании документа [2] выбрать оптимальный перечень требований, позволяющий построить адекватную систему защиты ИСПДн организации, включающую мероприятия по защите от НСД и неправомерных действий к ПДн при их обработке и передаче по техническим каналам.

Требования к мероприятиям по организации и обеспечению безопасности ПДн формулируются на основе анализа и оценки полного множества угроз безопасности ПДн. При этом должны быть рассмотрены требования к системе защиты по каждой угрозе.

Формирование данного перечня осуществляется на основе значений следующих параметров:

- актуальность рассматриваемой угрозы – $A$;
- категория ИСПДн – $K$;
- исходная оценка защищенности ИСПДн – $E$.

Пусть $M$ – множество требований по документу [2]. Зададим функцию, которая, используя определенные в данном методе параметры, сформирует на основе этого множества $M'$ перечень оптимальных требований:

$$f(M, K, E, A) = M',$$

где $M' \subset M$.

Параметр $K$ может принимать 4 значения: $K_1$, $K_2$, $K_3$, $K_4$ (в соответствии с существующими классами ИСПДн). В зависимости от этого значения во множестве требований $M$ выделяются подмножества требований $M_{K1} \subset M_{K2} \subset M_{K3} \subset \subset M_{K4}$, где $M_{K1} = M$, при этом выполнение требований из этих подмножеств обеспечивает построение ИСПДн в защищенном режиме в соответствии с ее классом. Таким образом, по значению параметра $K$ определяется подмножество требований $M' = M_K \subset M$.

Параметр $E$ определяет исходную защищенность ИСПДн, и по его значению можно сделать вывод, какие требования уже выполнены и могут не включаться в опре-

деляемый перечень. Оставшиеся требования составляют подмножество $M_E \subset M$. При этом, чтобы избежать избыточности при построении СЗИ, необходимо исключить уже выполненные требования из строящегося подмножества:

$$M' = \frac{M'}{M_E}.$$

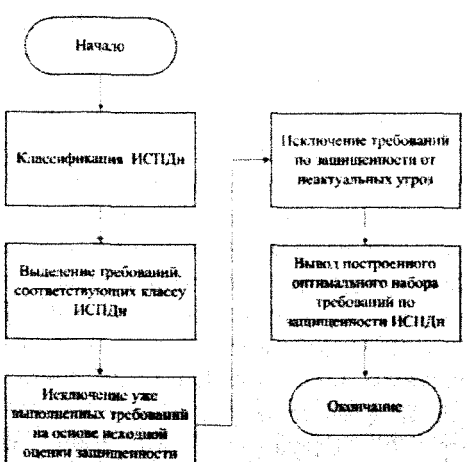
Пусть построено полное множество угроз $T = (t_1, t_2, ..., t_n)$, где $n$ – мощность множества $T$. Для каждой угрозы $t_i$ определим актуальность $a_i$ следующим образом:

$$a_i = \begin{cases} 1, \text{ если угроза актуальна для данной ИСПДн;} \\ 0, \text{ если угроза не актуальна для данной ИСПДн.} \end{cases}$$

Таким образом, параметр $A$ будет представлять собой множество значений $A = (a_1, a_2, ..., a_n)$.

Тогда подмножество $M'$ переопределится следующим образом: требование $mi \in M'$, если $a_i = 1$, $i = 1, ..., n$.

В результате построенное подмножество $M' \subset M$ является оптимальным набором требований к защищенности ИСПДн от НСД. Метод построения приведен ниже (рисунок).




**Метод формирования требований к защищенности ИСПДн от НСД**

После того, как перечень требований построен, согласно ему средства защиты информации, применяемые в ИСПДн, в установленном порядке должны проходить процедуру оценки соответствия. Поэтому следующей задачей в рамках построения ИСПДн в защищенном исполнении является выбор методов и средств защиты, применяемых в системе, удовлетворяющих разработанным требованиям.

**Литература**

1. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий: Руководящий документ ФСТЭК России, 2003.

2. Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных: Приказ Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. № 58 // Российская газета. 2010. 5 март.

УДК 004.056

**О. А. Теплоухова, А. С. Куракин**

*Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики*

# К ВОПРОСУ О ВЫБОРЕ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ НСД

Выбор в пользу тех или иных средств при проектировании информационных систем персональных данных (ИСПДн), обрабатывающих конфиденциальную информацию и ПДн, – ключевая процедура, определяющая будущий уровень не только надежности и защищенности системы, но и легитимности дальнейшей эксплуатации с точки зрения российского законодательства.

Задача по выбору технических средств защиты, как правило, является итерационной задачей управления рис-

ками, т. е. поиска решения, удовлетворяющего заданному критерию, такому как величина остаточного риска. Фактически вероятность возникновения угрозы информационной безопасности (далее – риск) представляет собой интегральную оценку того, насколько эффективно существующие средства защиты способны противостоять информационным атакам.

Метод оценки рисков информационной безопасности базируется на определении вероятности реализации атак, а также уровней их ущерба [1]. Для оценки данных величин могут использоваться статистические методы, методы экспертных оценок или элементы теории принятия решений [2].

По результатам анализа оценки рисков разрабатывается комплекс мер и средств, обеспечивающих выполнение требований в отношении величины остаточного риска. В случае ИСПДн достаточность принятых мер определяется оператором.

Проблема минимизации расходов на обеспечение защиты при соблюдении требований защиты ПДн является многосторонней задачей, решение которой может быть основано на выполнении задачи выбора СЗИ по результатам оценки информационной безопасности ИСПДн, согласно следующим критериям [3]:

- надежности СЗИ;
- суммарной стоимости применяемых средств защиты от НСД.

Надежность средств защиты от НСД определяется вероятностью безотказной работы системы защиты за время межрегламентного периода [4] (под регламентом понимается проведение работ, в состав которых входит проведение тестов и контролей, выявляющих отказавшие элементы для их последующего ремонта или замены).

Вероятность безотказной работы системы $P(t)$ за время $t$ вычисляется по формуле:

$$P(t) = 1 - P_{отк}(t),$$

где $P_{отк}(t)$ – вероятность отказа системы за время $t$. Величина $P_{отк}(t)$, в свою очередь, определяется в соответствии с формулой:

$$P_{отк}(t) = e^{-X(t)},$$

где $X(t)$ – интенсивность отказов системы за время $t$.

Суммарная стоимость $C_\Sigma$ определяется значением суммы цен и затрат на амортизацию (обслуживание) применяемых средств защиты.

Суммарная стоимость рассчитывается по следующей формуле:

$$C_\Sigma = \sum_{j=1} C_j \cdot A_j,$$

где $n$ – суммарное количество всех применяемых средств защиты в рассматриваемой ИСПДн;

$C_j$ – цена $j$-го средства защиты;

$A_j$ – амортизационные затраты $j$-го средства защиты.

Таким образом, на вход алгоритма по выбору СЗИ поступают только сертифицированные средства, удовлетворяющие критерию надежности согласно документам по технической эксплуатации.

**Постановка задачи.**

Рассмотрим математическую постановку данной задачи выбора СЗИ для построения ИСПДн в защищенном режиме.

Пусть $U = \{u_1, u_2, ..., u_N\}$ – полное множество угроз для данного класса ИСПДн; $N$ – мощность этого множества. Тогда каждому СЗИ можно поставить в соответствие вектор $\vec{Z} = \{z_1, z_2, ..., z_N\}$, где

$$z_i = \begin{cases} 0, \text{ если данное СЗИ нейтрализует угрозу } u_i; \\ 1, \text{ если данное СЗИ не может нейтрализовать угрозу } u_i. \end{cases}$$

Каждое СЗИ также характеризуется своей стоимостью $C_{\vec{z}i}$, определяемой значением цены и затрат на амортизацию (обслуживание) данного средства.

Покрытием $P = \{\vec{Z}_1, \vec{Z}_2, ..., \vec{Z}_k\}$ назовем такое множество векторов $\vec{Z}_i$, для которого выполняются следующие условия:

1) $C_\Sigma \leq C_{max}$, где $C_{max}$ – максимальная стоимость выбранных СЗИ;

2) $\vec{Z}_1 \vee \vec{Z}_2 \vee ... \vee \vec{Z}_k = \vec{E}$, где $\vec{E} = (1, 1, \ldots, 1)$ – единичный вектор.

Тогда в качестве решения рассматриваемой задачи выбора СЗИ необходимо найти покрытие $P$, т. е. такой набор СЗИ, совместное применение которых нейтрализует как можно большее количество угроз из множества $U$, но их суммарная стоимость не превышает допустимое значение $C_{max}$.

При этом необходимо отметить, что накладываемое ограничение на стоимость выбранных средств может не позволить найти покрытие $P$, для которого выполнится второе свойство (т. е. в результате дизъюнкции векторов $\vec{Z}_i$ не будет получен единичный вектор). В этом случае решением задачи будет такое множество векторов $\vec{Z}_i$, дизъюнкция которых даст вектор максимального веса. Под весом вектора подразумеваем вес Хэмминга $w(\vec{Z}_i)$ – число единиц (ненулевых компонент) в векторе. Чем больше вес, тем больше угроз покрывает данный вектор $\vec{Z}_i$.

В такой формулировке поставленная задача похожа на классическую комбинаторную задачу о покрытии множеств [5], в которой исходными данными являются конечное множество $M$ и семейство $S$ его подмножеств. Покрытием называют семейство $P \subseteq S$ наименьшей мощности, объединением которых является $M$. Вопросом данной задачи является существование покрывающего множества мощности $k$ или менее.

Одним из самых популярных способов решения задачи является «жадный» алгоритм, согласно которому множества в набор выбирают, руководствуясь следующим правилом: на каждом этапе выбирается множество, покрывающее максимальное число еще не покрытых элементов.

Отличием от классической задачи о покрытии множеств в нашей задаче является тот факт, что каждому СЗИ поставлена в соответствие его стоимость, и ограничивающим условием задачи является максимальная допустимая стоимость выбранных СЗИ. Поэтому классические методы для решения задачи о покрытии в исходном виде здесь не применимы.

**Описание алгоритма.**

Решим поставленную задачу, используя «жадный» алгоритм, модифицированный под сформулированные выше условия.

На предварительном этапе необходимо применить операцию дизъюнкции ко всем векторам $\bar{Z}_i$, $i = 1, ..., n$, где $n$ – количество всех СЗИ, которые можно применить для рассматриваемой ИСПДн. Если в результате этой операции не будет получен единичный вектор $\bar{E}$, то имеют место быть угрозы, которые не способны нейтрализовать ни одно из предлагаемых средств. В этом случае защиту от таких угроз необходимо строить на основе регламентных мер, принимаемых в организации.

Исключим данные угрозы из математической постановки задачи. Таким образом, мы знаем, что существует полное покрытие всего множества угроз $U$. Но есть вероятность, что точное решение задачи так и не будет найдено, если ограничивающее условие на стоимость применяемых СЗИ слишком строго.

На следующем шаге «жадного» алгоритма определим веса каждого вектора $\bar{Z}_i$. Далее начинаем формировать покрытие $P$. Первым выбираем вектор наибольшего веса и на каждом следующем шаге выбираем вектора, покрывающие наибольшее число еще не покрытых элементов. Если несколько векторов покрывают одинаковое количество непокрытых элементов, выбираем наименьшее по стоимости.

После каждого добавления вектора $\bar{Z}_i$ в покрытие $P$ определяем стоимость этого покрытия. Если сформировано полное покрытие множества угроз $U$ и стоимость этого по-

крытия $C_P$ не превышает $C_{max}$, объявляем это решением и завершаем алгоритм. Если на очередном шаге максимальная стоимость оказалась превышена, возвращаемся на шаг назад и запоминаем предыдущее покрытие. Далее начинаем алгоритм заново, выбирая новый начальный вектор, следующий по весу.

Если алгоритм перебрал все вектора в качестве начальных, а решение так и не было найдено, значит, ограничение на стоимость слишком строгое и точного решения найти невозможно. В этом случае решением объявляется то покрытие $P$ из запоминаемых на каждой неудачной ветке алгоритма, объединение векторов в котором покрывает большее число угроз множества $U$.

В результате алгоритм выбора средств защиты информации на основе «жадного» алгоритма выглядит следующим образом:

*Входные данные:*

- формируемое покрытие $P = \varnothing$,
- множество средств защиты $\{\vec{Z}_1, \vec{Z}_2, ..., \vec{Z}_n\}$ и их стоимости $\{\vec{C}_1, \vec{C}_2, ..., \vec{C}_n\}$;
- множество угроз $U = \{u_1, u_2, ..., u_N\}$;
- максимальная суммарная стоимость выбранных СЗИ $C_{max}$;
- счетчик $i = 0$.

*Выход:* покрытие $P = \{\vec{Z}_1, \vec{Z}_2, ..., \vec{Z}_k\}$, удовлетворяющее условиям:

1) $C_\Sigma \le C_{max}$;

2) $\vec{Z}_1 \vee \vec{Z}_2 \vee ... \vee \vec{Z}_k = \vec{E}$, где $\vec{E} = (1, 1, ..., 1)$ – единичный вектор.

Шаг 1. Проверяем: $i \le n$. Если да, идем на шаг 2. Если нет, идем на шаг 9.

Шаг 2. Выбираем начальный $\vec{Z}_{i0}$, удовлетворяющий условию:

$$w(\vec{Z}_{i0}) \ge w(\vec{Z}_j), \ \forall j \ne i_0.$$

Шаг 3. Добавляем выбранный $\bar{Z}_i$ к покрытию: $P = P \cup \bar{Z}_i$; если сформированное покрытие – полное, выход.

Шаг 4. Проверяем суммарную стоимость выбранных средств: $C_{\Sigma P} \leq C_{max}$. Если нет, идем на шаг 8.

Шаг 5. Выбираем очередной $\bar{Z}_i$, удовлетворяющий условиям:

1) $\bar{Z}_i$ покрывает наибольшее количество непокрытых элементов;

2) если первому условию удовлетворяют несколько векторов, выбираем $\bar{Z}_j$, для которого $C_j \leq C_k$, $\forall\ \bar{Z}_k$, удовлетворяющих условию 1.

Шаг 6. Добавляем выбранный $\bar{Z}_j$ к покрытию: $P = P \cup \bar{Z}_j$; если сформированное покрытие – полное, выход.

Шаг 7. Проверяем суммарную стоимость выбранных средств: $C_{\Sigma P} \leq C_{max}$. Если да, идем на шаг 5. Если нет, идем на шаг 8.

Шаг 8. Удаляем последний добавленный $\bar{Z}_j$ из покрытия: $P = P/\bar{Z}_j$, и запоминаем очередное неполное покрытие $P$; увеличиваем счетчик: $i = i + 1$, и идем на шаг 1.

Шаг 9. Из запоминаемых на неудачных ветках алгоритма решений $P$ выбираем то, которое образует наиболее полное покрытие множества угроз $U$.

**Сложность алгоритма.**

Вычислительная сложность предлагаемого алгоритма выбора СЗИ составляет $O(H(w))$, где $w$ – наибольший из весов векторов $\{\bar{Z}_1, \bar{Z}_2, ..., \bar{Z}_n\}$; $H(n)$ – сумма первых $n$ членов гармонического ряда:

$$H(n) = \sum_{k=1} \frac{1}{k} \leq \ln n + 1.$$

В рамках поставленной задачи мы рассматриваем только сертифицированные средства защиты, которые могут применяться в рассматриваемой ИСПДн. Поэтому

размерность задачи будет очень небольшой ($n \approx 10$). Соответственно, ее вычислительная сложность также невелика.

Таким образом, применение данного алгоритма выбора СЗИ требует проведения предварительного сбора информации о рассматриваемой ИСПДн и построения модели угроз НСД. Далее, по результатам применения алгоритма, необходимо проанализировать эффективность использования выбранных СЗИ и получить оценку качества уровня ИБ в ИСПДн.

Предложенный алгоритм является оптимальным решением задач по выбору технических СЗИ, обеспечивающих ИБ ИСПДн, и обладает следующими преимуществами:

- позволяет строить решение по выбору средств защиты от угроз НСД на основе метода оценки рисков информационной безопасности, учитывая вероятность реализации угроз и уровень ущерба;
- учитывает такой критерий технических средств, как надежность, т. е. вероятность безотказной работы за время межрегламентного периода;
- позволяет выбирать комплекс средств, оптимальных по объему нейтрализуемых угроз, не выходя за рамки суммарной стоимости всего комплекса;
- обладает малой вычислительной сложностью, что позволяет применять данный алгоритм на стандартном персональном компьютере (ПК) за приемлемое время.

Так, можно сделать вывод, что разработанный алгоритм позволяет решить задачу выбора технических СЗИ для обеспечения ИБ ИСПДн.

**Литература**

1. *Куракин А. С.* Алгоритм выбора средств защиты информационных систем персональных данных от несанкционированного доступа // Информационные технологии в профессиональной деятельности и научной работе: Сб. материалов Всерос. науч.-практ. конф.: В 2 ч. Ч. 1. Йошкар-Ола: Марийский государственный технический университет, 2011. – С. 68–74.

2. *Сердюк В. А.* Аудит информационной безопасности – основа эффективной защиты предприятия // BYTE. Россия. – 2006. № 4(92). – С. 32–35.

3. *Смирнов С. Н.* Вероятностные модели обеспечения информационной безопасности автоматизированных систем // Безопасность информационных технологий. – 2006. № 2. – С. 12–17.

4. *Прытков С. Ф., Горбачева В. М., Борисов А. А.* Надежность ЭРИ: Справочник // 22 ЦНИИИ МО РФ, 2006. – 674 с.

5. Задача о покрытии множества [Электронный ресурс] // Википедия – свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Задача_о_покрытии_множества (дата обращения: 15.09.2012).

УДК 65.012.7-65.012.8

**К. Е. Израилов**

Санкт-Петербургский государственный университет телекоммуникаций

# ФУНКЦИОНАЛЬНЫЙ МОДУЛЬ АВТОМАТИЗИРОВАННОЙ МЕТОДИКИ ОЦЕНКИ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТИ СВЯЗИ

Передача данных в современном мире целиком осуществляется с помощью сетей связи. По причине критичности нарушения конфиденциальности, целостности и доступности (далее – КЦД) передаваемой информации сами сети должны удовлетворять ряду условий для предотвращения этих нарушений [1–2]. Данные условия могут быть отражены в виде набора требований, используемых для оценки сети связи. Требования, как правило, могут быть обязательными или рекомендованными согласно действующим и планируемым для принятия нормам безопасности. Факт наличия нарушения является свершившимся событием и поэтому может быть использован лишь для минимизации его последствия. Напротив, факт невыполнения требований говорит о потенциальной возможности нару-

шения. С этой позиции проверка выполнения требований к сети связи позволяет оценивать уровень КЦД передаваемой информации, что может сигнализировать о необходимости принятия необходимых превентивных мер. Таким образом, проверка требований является более предпочтительным способом борьбы с рисками информационной безопасности, чем диагностика и последующая ликвидация нарушений.

Для осуществления проверки требований необходимо применение соответствующей методики, логично состоящей из следующих этапов: сбор информации о сети связи, создание списка соответствующих для нее требований, корректировка требований, проведение проверки требований, вычисление предпосылок к нарушениям и заключение о проверке. Входными данными методики будет собранная, проанализированная и формализованная информация о сети связи. Выходными же данными будет оценка предпосылок к нарушениям КЦД информации. Для получения выходных данных из входных удобно применять алгоритм, использующий математический аппарат на базе объектов безопасности, таких как источник, уязвимость, угроза, актив, требования (включая результат проверки их выполнения) и нарушение.

Поскольку прямая связь между конкретной конфигурацией сети связи фактами невыполнения требований и предпосылками к нарушениям отсутствует, а косвенная по причине сложных конфигураций реальных сетей слишком нетривиальна, то целесообразна автоматизация методики оценки с помощью программного средства.

Структура такого предлагаемого средства состоит из следующих модулей:

- интерфейсный, предоставляющий пользовательский интерфейс;
- функциональный, реализующий выполнение алгоритма методики;
- информационный, осуществляющий хранение данных, их редактирование и обмен с другими модулями.

И если интерфейсный и информационный модули строятся по стандартным шаблонам проектирования (первый – с использованием строителей графических интерфейсов, а второй – строителей баз данных), то функциональный является узкоспециализированным, так как должен соответствовать алгоритму конкретной методике оценки.

Функциональный модуль удобно описать с помощью двух представлений: потока управления и потока данных.

Представление потока управления описывает алгоритм модуля и соответствует технологической карте методики. Диаграмма такого представления показана на рис. 1. Блоки диаграммы на рис. 1 определяют действия алгоритма (соответствующие операциям технологической карты), нумерация в названиях блоков задает базовый порядок их выполнения, а линии указывают на использование данных одного модуля в другом.

Согласно алгоритму, вначале осуществляется ввод данных об инспектируемой сети (1 и 2), включающих в себя выбор типа оператора (3), проверяемых зон безопасности (4) и используемого для функционирования сети типа оборудования (5). Варианты выбора в каждом пункте зависят от выбора предыдущего. Выбранные зоны безопасности ведут к созданию списка связанных с ними источников угроз (7), а тип используемого оборудования – списка уязвимостей (8). Алгоритм содержит дополнительные шаги для их принудительной актуализации (7.1 и 8.1). Списки источников и уязвимостей используются для генерации единого списка требований (9), предъявляемых к сети связи. Проверка выполнения требований из данного список осуществляется на следующем шаге алгоритма (10). Поскольку причиной нарушения являются угрозы активам сети, которые определяются комбинацией актуальных источников и уязвимостей, а отсутствие последних обеспечивается благодаря применению защитных мер (контролируемых выполнением соответствующих требований), то элементы сгенерированного списка напрямую влияют на предпосылки к нарушениям.

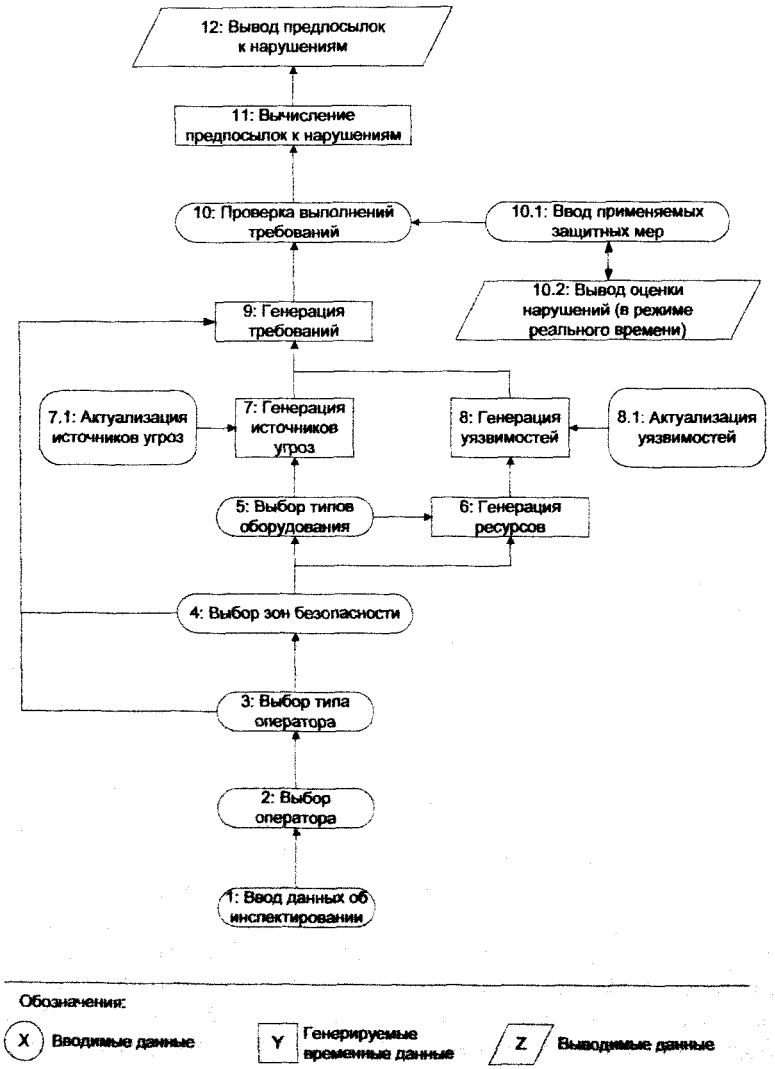



Рис. 1. Диаграмма потока управления

На шаге ввода данных о проверке выполнения требований имеется возможность в режиме реального времени давать текущую оценку нарушениям (10.1 и 10.2). Заключительными шагами алгоритма являются итоговое вычисление предпосылок к нарушениям (11) и вывод окончательного отчета о проведенной проверке (12).

Представление потока данных описывает функциональные зависимости значений, вычисляемых в модуле. Диаграмма такого представления показана на рис. 2.

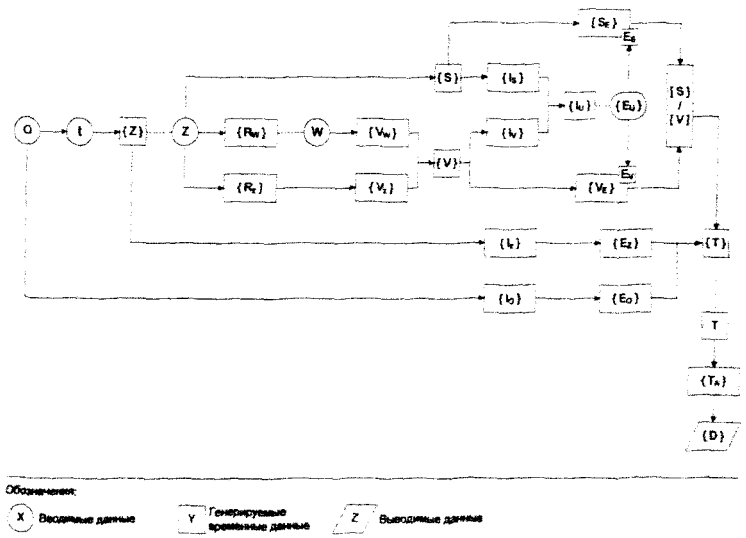



Рис. 2. Диаграмма потока данных

Блоки диаграммы на рис. 2 определяют вводимые, временные и выводимые данные. Линии на рисунке указывают зависимости в вычислениях одних данных через другие. Обозначения, принятые на рис. 2, представлены в таблице.

**Обозначения на диаграмме потока данных**

| Обозначение | Описание |
|---|---|
| O | оператор сети связи |
| t | тип оператора |

Окончание

| Обозначение | Описание |
|---|---|
| { Z } | список зон оператора с типом t |
| Z | зона оператора с типом t |
| { S } | список источников |
| { $R_W$ } | список оборудования оператора в зоне Z |
| { $R_Z$ } | список постоянных ресурсов оператора в зоне Z |
| W | тип оборудования |
| { $V_W$} | список уязвимостей, связанных с оборудованием |
| { $V_Z$ } | список уязвимостей, связанных с постоянными ресурсами |
| { V } | набор всех уязвимостей |
| { $I_S$ } | список требований по устранению источников S |
| { $I_V$ } | список требований по устранению уязвимостей V |
| { $I_Z$ } | список требований, обязательных для данной зоны оператора |
| { $I_O$ } | список требований, обязательных для оператора |
| { $I_U$ } | набор всех требований по устранению источников S и уязвимостей V |
| { $S_E$ } | список источников, существующих в результате невыполнения требований |
| { $V_E$ } | список уязвимостей, существующих в результате невыполнения требований |
| { $E_S$ } | список – подтверждение выполнения требования { $I_S$ } |
| { $E_U$ } | список – подтверждение выполнения требования { $I_U$ } |
| { $E_V$ } | список – подтверждение выполнения требования { $I_V$ } |
| { $E_Z$ } | список – подтверждение выполнения требования { $I_Z$ } |
| { $E_O$ } | список – подтверждение выполнения требования { $I_O$ } |
| [S]/[V] | таблица угроз, реализуемых источником S с помощью уязвимости V; включает способ определения актуальности угрозы (т. е. обязательность или рекомендуемость к устранению) согласно минимизации источников S и уязвимостей V |
| { T } | список угроз, реализуемых источником I с помощью уязвимости V |
| { $T_A$ } | список угроз соответствующим активам |
| { T } | угроза; сопоставляется с коэффициентом (1 для обязательных к устранению, [0.75, 0.5, 0.25] для рекомендуемых) |
| { D } | набор нарушений; с каждым нарушением D сопоставляется коэффициент, равный 1 в случае реализации любой обязательной угрозы и среднему арифметически взвешенному рекомендуемых к устранению угроз, в случае нарушений только их |

Упомянутая методика, ее технологическая карта и вариант автоматизированного средства (включаю архитектуру модулей и их программную реализацию) были разработаны и апробированы в рамках научно-исследовательской работы [3]. Использованные подходы и идеи могут быть применены для решения подобных задач в области автоматизации проверки сетей связи на предмет их соответствия требованиям безопасности.

**Литература**

1. ГОСТ Р 52448–2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.

2. ГОСТ Р 53110–2008. Система обеспечения информационной безопасности сети связи общего пользования. Общие положения.

3. *Буйневич М. В.* и др. Разработка предложений по организационно-техническому обеспечению устойчивости функционирования сетей связи, защиты сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации, методов проверки и определение перечня нарушений целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации: Отчет о НИР / Науч. рук. С. М. Доценко; рег. № 034-12-054. – СПб.: СПбГУТ, 2012. – 177 с.

# *РАЗДЕЛ 3*

# УПРАВЛЕНИЕ И ЭКОНОМИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056

**В. Н. Бугорский, Е. В. Стельмашонок**

Санкт-Петербургский государственный
инженерно-экономический университет

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИРМЫ В УСЛОВИЯХ ИНФОРМАЦИОННОЙ ЭКОНОМИКИ

Традиционно информационная безопасность фирмы трактуется как состояние защищенности ее информационной среды. Столь же традиционно обеспечение этого состояния достигается путем ограничения и жесткого контроля доступа посторонних лиц к информационной среде фирмы.

Такой подход полностью оправдывал себя на прежних стадиях развития экономики и технологий, поскольку позволял минимизировать риски нанесения ущерба фирмы из-за несанкционированного доступа к ее информационной среде. Однако в современных условиях такая модель обеспечения информационной безопасности оказывается неадекватной.

Дело в том, что ранее информационная среда фирмы существовала внутри нее и была слабо связана с внешним миром (вероятно, на этом этапе говорить об информационной среде фирмы преждевременно – скорее, речь может идти об информационном аспекте ее деятельности). Информация хранилась на традиционных носителях (в виде «бумажных») документов, доступ к которым было легко контролировать и практически невозможно осуществить извне, а сотрудники фирмы принимали на себя обязатель-

ства по неразглашению (соблюдение этих обязательств было также сравнительно легко контролировать, кроме того, у сотрудников было мало возможностей их нарушить). Ограничение доступа к внутрифирменной информации требовало определенных затрат, однако работе фирмы не препятствовало.

В современных же условиях фирма сама в значительной степени превратилась в информационный объект (благодаря активному использованию информационных технологий в управлении предприятием, сети Интернет и переводу внутрифирменной информации в цифровую форму). Она (как и ее информационная среда) плотно интегрирована в глобальное информационное пространство (Всемирную паутину), и ведет непрерывный обмен информационными потоками со своей внешней средой – не только активно собирая поступающую информацию, но и генерируя ее. От того, насколько правильно выбрана модель распространения информации, во многом зависит успех современного предприятия на рынке. Более того, успех во многом определяется тем, насколько непрерывно происходит обмен этой информацией с внешней средой (очевидно, что достаточно на некоторое время заблокировать работу сайта интернет-магазина, чтобы нанести его оператору значительный ущерб).

В силу этих изменений внутренняя информационная среда фирмы тесно связана с ее внешней информационной средой, а ограничение этой связи чревато потерями для бизнеса. Благодаря этому факту мы можем утверждать, что понятия «информационная безопасность» и «непрерывность бизнеса» не противопоставляются, а, скорее, определяют их сущность как двух аспектов одной комплексной задачи – обеспечение непрерывной и защищенной связи внутренней информационной среды фирмы с ее внешней информационной средой как ключевого условия рыночного успеха.

Таким образом, фирма сталкивается с важным противоречием – наиболее эффективным способом защиты ин-

формационной среды является ограничение доступа к ней, однако тесная интеграция фирмы во всемирную паутину препятствует таким ограничениям. Задача защиты информационной среды трансформируется из задачи обеспечения наиболее эффективного ограничения доступа в задачу обеспечения устойчивой связи внешней и внутренней информационной среды компании и защиты информации в условиях непрерывно нарастающего риска несанкционированного доступа к информационной среде фирмы (из-за непрерывного роста числа и количества информационных потоков, которыми фирма обменивается с внешней средой).

Отдельно следует учесть тот факт, что столь же плотно интегрированы в глобальное информационное пространство и сотрудники предприятия (в частности, благодаря социальным сетям), что многократно увеличивает их возможности по непреднамеренному разглашению информации.

По этой причине можно утверждать, что изменение задачи требует радикального изменения инструментов (комплекса средств защиты информации), используемых подразделениями информационной безопасности предприятия. Отказ от таких изменений чреват значительными потерями. Естественно, использование систем информационной безопасности предприятия должно сопровождаться достаточным экономическим обоснованием целесообразности их разработки и внедрения.

Существует ряд достаточно известных мер, направленных на предупреждение преступлений, связанных с нарушениями в сфере информационной безопасности предприятий.

Укрупненно можно выделить меры программно-технического характера, организационные и правовые.

В зависимости от видов нарушений могут использоваться различные группы мер и средств, но их применение для защиты информации на предприятии всегда будет связано с определенными, как правило, достаточно большими, затратами.

К мерам технического характера можно отнести средства технической защиты, такие как:

- установка оборудования для тушения пожаров;
- установка резервных систем электропитания;
- установка сигнализаций.

Программно-аппаратные средства защиты предназначены для защиты от несанкционированного доступа к информации.

К организационным мерам относятся:

- организация охраны информационных систем защиты;
- работа с персоналом;
- исключение случаев ведения особо важных работ только одним работником;
- разработка плана восстановления работоспособности системы после выхода ее из строя;
- передача работы по обслуживанию системы информационной безопасности предприятия на аутсорсинг;
- возложение ответственности на специально выделенных работников, которые должны обеспечить безопасность работы предприятия;
- страхование информационных рисков;
- резервирование информации и др.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства и судопроизводства в части информационного сектора в экономике.

Показатели, которыми характеризуют экономическую эффективность любой информационной деятельности, нужно искать в областях применения информации. Таким образом, эффективность системы защиты информации можно определить как степень ее соответствия своему назначению. Различают экономическую и функциональную эффективность систем защиты информации.

Основным показателем экономической эффективности системы защиты информации является годовой экономический эффект (экономическая прибыль).

Для расчета этого показателя необходимо уметь определять:

- величину убытков предприятия в результате хищения информации и последствий реализации других угроз;
- размеры затрат на создание и эксплуатацию комплекса средств защиты информации на предприятии.

Далее, для экономической оценки комплекса средств защиты, необходимо оценить эффективность его функционирования, сопоставляя затраты на создание системы и результаты, полученные от ее эксплуатации.

Показатели экономической эффективности для различных вариантов организации комплексной защиты информации на предприятии могут быть положены в основу выбора оптимального варианта, так как требуется не только обеспечить информационную безопасность предприятия любыми средствами, но и разумно увеличивать дополнительные расходы на эти цели.

*Капитальные* затраты в сфере защиты информации представляют собой затраты на организацию и функционирование соответствующих служб и подразделений по защите информации. Эти затраты носят разовый характер и направляются в основные и оборотные средства, т. е. в средства производства услуг по защите информации.

Свою стоимость они переносят на продукцию по частям за счет амортизационных отчислений. Капитальными их называют потому, что они не утрачиваются, а воспроизводятся.

*Эксплуатационные затраты*, в отличие от единовременных, являются повторяющимися. Они повторяются в каждом цикле производства, а рассчитываются в сумме за год. Эксплуатационные затраты осуществляются синхронно с производством. Эксплуатационные затраты составляют часть себестоимости продукции или услуг.

Наибольший удельный вес в эксплуатационных затратах принадлежит:

- заработной плате;
- амортизационным отчислениям;
- техническому обслуживанию.

В качестве экономического эффекта от применения средств защиты информации может выступать величина возможного ущерба от последствий компьютерных нарушений.

Ущерб в этом смысле определяется стоимостью всех утраченных технических и программных средств и живого труда, необходимого для ремонта, настройки, восстановления работоспособности системы.

Кроме того, стоимость вышеприведенного ущерба может быть откорректирована с учетом простоев других пользователей и долгосрочных последствий компьютерных нарушений, а также частоты возникновения ущерба.

УДК 004.056

**И. Н. Васильева**

Санкт-Петербургский государственный инженерно-экономический университет

## КОНЦЕПЦИИ GOVERNANCE И GRC В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

В последнее время бурное развитие получили стандарты управления (менеджмента) информационной безопасности (ИБ). Такие стандарты приняты в большинстве развитых западных стран, наиболее известны национальные стандарты Британии (BS 7799), Германии (BSI 100 [10]) и США (NIST 800 [13]), а также серия международных стандартов ISO/IEC 27000 [4].

Международные стандарты ISO определяют систему менеджмента информационной безопасности (СМИБ) как

часть общей системы менеджмента компании, базирующуюся на оценке бизнес-рисков, необходимую для создания, внедрения, функционирования, мониторинга, пересмотра, поддержки и улучшения информационной безопасности.

СМИБ объединяет воедино людей (персонал), процессы и ИТ-системы. СМИБ обеспечивает слаженную работу службы безопасности, ИТ-отдела и руководства компании.

Вместе с тем стандарт ISO 27001 лишь указывает, что «на проектирование и внедрение СМИБ организации влияют потребности и цели организации», однако не раскрывает вопросов интеграции задач обеспечения ИБ в корпоративный менеджмент.

Поэтому наряду с этими стандартами, ориентированными на внедрение защитных мер, получили развитие и другие документы, более понятные неспециалистам (например, руководителям компаний или бизнес-подразделений) и ориентированные на достижение бизнес-целей [3].

ISM3 делает акцент на достижение бизнес-целей и согласование целей ИБ с потребностями бизнеса (рис. 1).

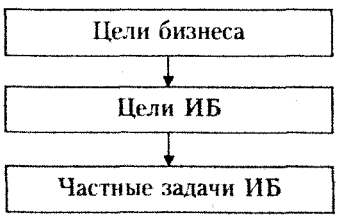



Рис. 1. Согласование целей ИБ с потребностями бизнеса

ISM3 рассматривает несколько уровней управления ИБ [9] (рис. 2):

- стратегический – направление и обеспечение: координация с целями бизнеса, определение целей ИБ, политика безопасности, выделение ресурсов;
- тактический – внедрение и оптимизация: разработка СМИБ и управление ресурсами;

• операционный – выполнение и отчетность: технические процессы.


Рис. 2. Уровни управления ИБ согласно ISM3

Процессы ISM3 делятся на 4 группы:

• общие практики (управление знаниями, аудит СМИБ, построение и развитие СМИБ);

• стратегические практики ИБ (отчетность перед заинтересованными сторонами, координация, определение стратегии, определение правил распределения обязанностей, выделение ресурсов);

• тактические практики ИБ (отчетность перед стратегическим менеджментом, управление выделенными ресурсами, определение тактических задач и целей безопасности, построение инфраструктуры ИБ, обучение персонала и т. д.);

• операционные практики (отчетность перед тактическим менеджментом, приобретение средств ЗИ, контроль доступа и физического окружения, обеспечение доступности, тестирование и проверка, мониторинг событий, обработка инцидентов).

Вместе с тем стандарт ISM3 совместим с другими методологиями и стандартами ИБ. В частности, СМИБ, построенные с использованием ISM3, соответствуют требованиям ISO 27001.

Другой стандарт, реализующий бизнес-подход к ИБ, – Cobit (Control Objectives for IT and related Technology), разработан Международной ассоциацией аудиторов информационных систем ISACA.

Методология Cobit ориентирована на бизнес [11] и предназначена не только для сервис-провайдеров ИТ, конечных пользователей и аудиторов, но и для менеджмента и владельцев бизнес-процессов. Управление и контроль над информацией являются основой методологии Cobit и помогают соответствовать целям бизнеса (рис. 3).

В основе Cobit лежит система сбалансированных показателей – концепция переноса и декомпозиции стратегических целей для планирования операционной деятельности и контроля их достижения.

Таким образом, Cobit является связующим звеном между целями бизнеса (бизнес-рисками), задачами управления и технической инфраструктурой. Он представляет лучшие практики, объединенные в структуру доменов (групп ИТ-процессов) и процессов, которые позволяют оптимизировать инвестиции в ИТ и предоставляют критерии для оценки эффективности управления ИТ.

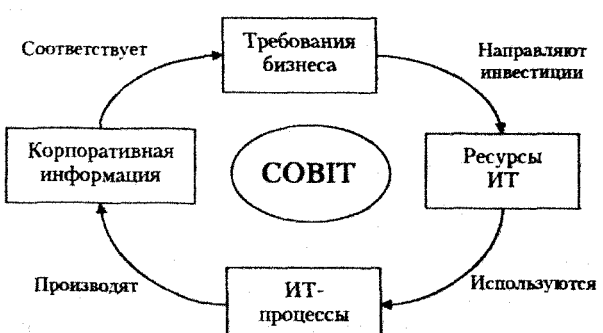



Рис. 3. Основной принцип методологии Cobit

**Цели ИТ и система сбалансированных показателей, отражающая их достижение, определяются целями бизнеса в ИТ-сфере и в конечном счете корпоративной стратегией.**

Среди процессов, описываемых Cobit 4.1, – обеспечение непрерывности ИТ-сервисов, обеспечение безопасности систем, управление проблемами (инцидентами), управление физической безопасностью и защитой от воздействия окружающей среды.

В апреле 2012 г. была принята новая, пятая, версия Cobit, существенно отличающаяся от предыдущей. Был сформулирован ряд новых принципов, заметно обновлена процессная модель, полностью переработана модель зрелости процессов.

Каскад целей: бизнес-цели → цели ИТ → Цели ИТ-процессов (внутренние цели ИТ), – представленный в COBIT 4.1, стал важнейшей частью COBIT5. При этом добавился верхний уровень потребностей заинтересованных сторон (Stakeholder Needs) – рис. 4.


Рис. 4. Каскад целей Cobit 5

Любое предприятие существует для того, чтобы создавать некоторую ценность для заинтересованных сторон (владельцев, акционеров, пользователей, органов власти, подрядчиков, заказчиков и общества в целом). Поэтому задача стратегического управления любым предприятием – коммерческим или государственным – формирование ценности, что подразумевает получение выгоды за счет оптимизации стоимости ресурсов и оптимизации рисков. Эти потребности заинтересованных сторон должны быть преобразованы в действенную, реализуемую на практике стратегию компании.

Cobit 5 включает ряд документов, часть из которых еще находится в разработке. В июле 2012 г. вышло руководство Cobit 5 for Information Security [12], хотя и в базовом руководстве вопросы ИБ освещены достаточно подробно (через соответствующие процессы, такие как управление безопасностью, управление сервисами безопасности и др.). При разработке COBIT 5 учитывались такие стандарты ИБ, как ISO 27001/27002 и NIST SP800-53 rev1.

Cobit 5 for Information Security рассматривает следующие принципы ИБ.

- Поддержка бизнеса:
  - фокус на бизнес;
  - предоставление качества и ценности для заинтересованных лиц;
  - соответствие требованиям регуляторов;
  - предоставление своевременной и точной информации о состоянии ИБ;
  - оценка текущих и будущих угроз ИБ;
  - постоянное совершенствование.
- Защита бизнеса:
  - использование риск-ориентированного подхода;
  - защита конфиденциальной информации;
  - концентрация на критичных для бизнеса системах;
  - внедрение надежных систем.
- Поощрение ответственного поведения в сфере ИБ:
  - ориентир на профессиональную этику;
  - формирование положительной культуры ИБ.

Методология Cobit 5 строится на следующих пяти основных принципах.

- Фокус на удовлетворение потребностей заинтересованных сторон.
- Полное покрытие деятельности компании.
- Единая комплексная методология.
- Обеспечение целостного подхода.
- Разграничение зон стратегического управления (бизнес-управления, корпоративного управления, Governance) и регулярного/текущего управления (Management).

Таким образом, управление ИБ в организации имеет несколько уровней (рис. 5) и определяется в конечном счете потребностями бизнеса.

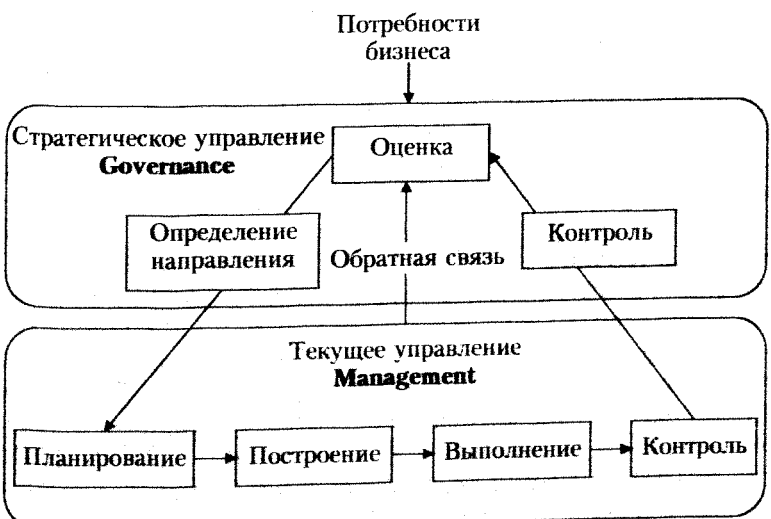



Рис. 5. Разделение уровней корпоративного управления Cobit 5

Согласно Cobit 5, под стратегическим управлением (бизнес-управлением, корпоративным управлением, Governance) понимается управление на уровне высшего

руководства, направленное на достижение целей предприятия. В сферу стратегического управления входят:

- оценка потребностей всех заинтересованных сторон, условий и возможностей (Evaluate);
- определение стратегического направления путем установки приоритетов и принятия решений (Direct);
- контроль продуктивности, выполнения требований и решения задач в рамках выбранного направления (Monitor).

В сферу менеджмента (регулярного, текущего управления, Management) входит планирование (Plan), построение (Build), выполнение (Run) и проверка (Monitor) отдельных видов деятельности в соответствии со стратегическим направлением, установленным высшим руководством компании для достижения бизнес-целей.

Уровень текущего управления (Management) соответствует, с некоторыми изменениями, модели непрерывного совершенствования PDCA.

Governance означает процесс принятия стратегических управленческих решений, глубоко влияющих на достижение бизнес-целей организации. Governance можно сформулировать как управление с позиций высшего руководства компании: указание целей и контроль их достижения.

В литературе можно встретить следующие переводы слова Governance на русский язык: «стратегическое управление» (Cobit 4.1 [11]), «руководство» (Cobit 5 [12]), «корпоративное управление» (проект ISO 27014 [5]).

Концепция Governance, подобная рассмотренной в Cobit, описывается проектом стандарта ISO/IEC 27014 Governance of Information Security [5], посвященного корпоративному управлению ИБ. В стандарте ISO/IEC 27014 выделяются следующие пять основных областей охвата системы корпоративного управления ИБ:

- согласованность стратегии ИБ и бизнеса;
- оценка эффективности;
- менеджмент рисков;
- управление ресурсами;
- увеличение стоимости.

Стандарт рассматривает возможное взаимодействие областей бизнеса и информационной безопасности для этих задач (рис. 6).

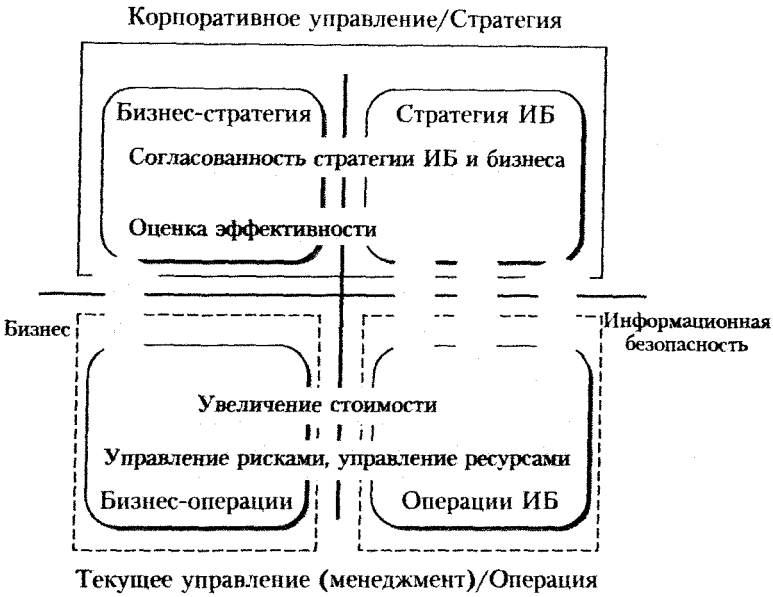



Рис. 6. Сопоставление задач ИБ и бизнеса

*Согласование стратегии ИБ и бизнеса.* Рассматриваются вопросы, необходимые для согласования информационной безопасности с целями бизнеса на стратегическом уровне.

*Увеличение стоимости.* Рассматриваются вопросы системы корпоративного управления ИБ, касающиеся инвестиций в информационную безопасность и их «возврата» (прибыли) в абсолютных или условных значениях, согласованности СМИБ организации с международными стандартами и другие вопросы. При рассмотрении данных вопросов организацией определяется, как добиться эффективности для бизнеса от инвестиций в обеспечение ИБ.

*Управление рисками.* Решение вопросов, рассмотренных в рамках данной задачи системы корпоративного управления ИБ, обеспечивает снижение влияния от инцидентов информационной безопасности до приемлемого уровня.

*Управление ресурсами.* Рассматриваются вопросы, связанные с выделением необходимых ресурсов для обеспечения ИБ, определением затрат и выгод от технологий информационной безопасности.

*Оценка эффективности.* Рассматриваются вопросы, связанные с мониторингом и оценкой эффективности ИБ организации. Оценка эффективности ИБ должна проводиться с учетом потребностей бизнеса.

Таким образом, стратегическое управление ИБ (Security Governance) обеспечивает связь между бизнесом и ИБ, выступая как связующее звено между текущим управлением (менеджментом) ИБ, инициативами соответствия (compliance), управлением рисками и корпоративной бизнес-стратегией (рис. 7) [6; 7].


Рис. 7. Роль стратегического управления ИБ как связующего звена

Рассмотренная связь нашла отражение еще в одной концепции и соответствующем классе поддерживающих ее инструментальных средств – GRC (Governance, Risk, Compliance).

GRC – это взгляд на управление чем-либо с трех точек зрения: высшего руководства (Governance), управления рисками (Risk Management) и соответствия требованиям (Compliance). Любую деятельность можно разложить по этим трем составляющим [1; 2; 8].

Действительно, сначала компании определяют цели, которых собираются достичь. Затем инициируют некую деятельность для их достижения. Пока деятельность выполняется, они хотят ее контролировать, получая своевременную, объективную и достоверную информацию о ходе выполнения. Это и есть функции высшего руководства (Governance) – указание целей и контроль их достижения.

Затем компании продумывают риски, которые могут встретиться на пути к поставленной цели. Для этого они выясняют, какие препятствия могут стать причиной нарушения сроков или сделать цель недостижимой, а также что компания рискует потерять на пути к цели. Выявленные риски обрабатываются, и в дальнейшем эта процедура периодически повторяется. Это функция управления рисками (Risk Management), которая, к сожалению, во многих российских компаниях носит пока недостаточно системный характер.

Кроме того, планируя и исполняя свою деятельность, компании заботятся о соблюдении множества внешних и внутренних правил. На них оказывают влияние законы, отраслевые стандарты и договорные обязательства. К тому же в компаниях имеются собственные нормативные документы, учитывающие их опыт и описывающие требования к выполняемым бизнес-процессам. Исполнение всех этих требований является функцией управления соответствием (Compliance).

Концепция GRC крайне актуальна и для ИБ. Несогласованность ИБ со стратегическими целями бизнеса и недостаточное осознание проблем ИБ со стороны руководства зачастую приводят к нехватке бюджетов на необходимую защиту, перерасходу на решение неактуальных задач и потерям, связанным с происходящими инцидентами. Внедрение в компании концепции GRC и поддерживающих ее ИТ решений – это прекрасная возможность для

того, чтобы вывести управление информационной безопасностью на качественно новый уровень.

Основа GRC – это доведение до сведения высшего руководства информации о рисках и исполнении требований, а информационная безопасность как раз и занимается снижением информационных рисков и исполнением требований отраслевых стандартов. Таким образом, система класса GRC при успешном внедрении может оказаться инструментом прямого общения топ-менеджмента с ИБ-подразделением, повысить статус этого подразделения и обеспечить лучшее взаимопонимание.

Стоит также отметить и пользу информационной безопасности для GRC. Ведь именно она обеспечивает целостность и доступность информации, необходимой для высшего руководства, т. е. принимает немалое участие в реализации корпоративного управления (функции Governance).

Эффективная модель GRC включает персонал, процессы, технологии и организационные факторы. Пример модели GRC приведен на рис. 8 [14].


Рис. 8. Модель GRC

Многие авторы также отмечают, что важным шагом в принятии концепции GRC является развитие моделей зрелости процессов, которые рассматриваются как международными стандартами (ISO/IEC 15504, ISO/IEC 21827), так и ISM3 и Cobit.

**Литература**


1. *Безгодов Е.* Концепция GRC [Электронный ресурс]. URL: http://ru.deiteriy.com/grc_concept (дата обращения: 12.06.2012).

2. *Безгодов Е.* Что такое GRC и чем это может быть полезно для ИБ? [Электронный ресурс] // Information Security = Информационная безопасность. – 2011. № 4. URL: http://www.itsec.ru/articles2/control/chto-takoe-grc-i-chem-eto-mojet-bit-polezno-dlya-ib (дата обращения: 12.06.2012).

3. *Васильева И. Н.* Развитие стандартов информационной безопасности // Информационные аспекты экономики: Материалы науч.-практ. конф. 2 дек. 2011 г. – СПб.: СПбГИЭУ, 2012. – С. 90–94.

4. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. – М., 2008.

5. *Курило А. П., Голованов В. Б.* Созидатели стандарта [Электронный ресурс] // Информационная безопасность банков. BIS-Journal: Отраслевой интернет-журнал. 26.07.2011. URL: http://www.ib-bank.ru/bis/a/98 (дата обращения: 26.08.2012).

6. *Лукацкий А.* Как в пылу борьбы за R и C не забыть, что такое G? [Электронный ресурс]. 29.09.2009. URL: http://www.slideshare.net/lukatsky/c-r-g (дата обращения: 26.08.2012).

7. *Лукацкий А.* Управление ИБ как Governance и как Management: небо и земля [Электронный ресурс]. 07.10.2008. URL: http://www.slideshare.net/lukatsky/security-governance-presentation?type=powerpoint (дата обращения: 26.08.2012).

8. *Шепелявый Д.* Концепция GRC стала очередным этапом развития рынка ИБ [Электронный ресурс] // Средства защиты информации и бизнеса 2008: Обзор CNewsAnalitics. URL: http://www.cnews.ru/reviews/free/security2008/articles/grc.shtml (дата обращения: 12.06.2012).

9. *Aceituno V.* ISM3: A Standard for Information Security Management // ISSA Journal. 2006. October. – P. 22–25.

10. BSI: BSI-Standards [Электронный ресурс]. URL: https://www.bsi.bund.de/EN / Publications/BSIStandards/BSIStandards_node.html; jsessionid=CD1A6E25A248B1F54558D20F25729009.2_cid244 (дата обращения: 01.02.2012).

11. CobiT 4.1. Российское издание. – М.: Аудит и контроль информационных систем, 2008.

12. Cobit 5 for Information Security Introduction [Электронный ресурс]. URL: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf (дата обращения: 29.08.2012).

13. NIST. Computer Security Resource Center. Special Publications (800 Series) [Электронный ресурс]. URL: http://csrc.nist.gov/publications/ PubsSPs.html (дата обращения: 27.08.2012).

14. *Sam Jr.* ECM as a Foundation for GRC [Электронный ресурс]. 30.11.2010. URL: http://paperfreetech.com/ecm-as-a-foundation-for-grc (дата обращения: 12.06.2012).

УДК 004.056

**Е. В. Стельмашонок, В. В. Тарзанов**

Санкт-Петербургский государственный инженерно-экономический университет

# ИМИТАЦИОННАЯ МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Имитационная модель функционирования системы защиты информации предназначена для осуществления комплексной оценки предполагаемых к использованию мер и средств защиты информации предприятия. Целью разработки является оценка общего коэффициента информационной защищенности, а также расчет суммарного риска, характеризующего величину ущерба от удачных попыток атак. Имитационную модель возможно использовать на любых объектах, где планируется внедрение (модернизация) системы защиты информации.

Современный уровень развития информационных технологий приводит к появлению ряда угроз, которые могут оказать сильное неблагоприятное воздействие на предприятие. Одной из наиболее существенных угроз является угроза информационной безопасности, как намеренная, так и случайная. Раскрытие или утрата ценной информации может существенным образом повлиять на работу организа-

ции. Для предотвращения этой угрозы создаются сложные и дорогие системы защиты информации, обеспечивающие защиту от несанкционированного доступа, перехвата информации при ее передаче, защиту от случайных помех и сбоев, а также защиту от информационного вмешательства в бизнес-процессы.

Ввиду высокой стоимости некоторых компонент системы и сложности построения такой системы необходимо заранее представлять, какой риск может последовать за реализацией той или иной угрозы. Зная заранее возможные риски и требуемый уровень защищенности, можно построить оптимальную систему защиты информации и свести возможность реализации угрозы к минимуму.

Для этой цели разработана имитационная модель, которая позволяет произвести оценку предполагаемых к использованию мер и средств защиты, оценить величину ущерба от удачных попыток атак. Попытки возможных атак имитируются в виде дискретно поступающих транзактов, целью которых является захват некоторого информационного ресурса. В качестве таких ресурсов могут выступать бухгалтерские, коммерческие, финансовые элементы информации, документы планирования, а также информация, циркулирующая в сети.

Имитационная модель реализована в системе *Arena 14.0 Professional* и состоит из блока имитации субъектов защиты, блока имитации мер и средств защиты и блока имитации объектов защиты. Блок имитации мер и средств защиты реализован в виде модулей защиты от несанкционированного доступа (НСД), от перехвата информации, от сбоев и от вмешательства в бизнес-процессы предприятия.

Основные ограничения и допущения, принятые в модели:

- предполагается, что возможны следующие типы угроз: несанкционированный доступ к информации, перехват информации при ее передаче (получении), уничтожение (повреждение) информации в результате различных видов сбоев в информационной инфраструктуре, несанкционированное вмешательство в бизнес-процесс;

• каждая атака может иметь целью некоторый информационный ресурс или их комбинацию;

• потоки транзактов-атак являются пуассоновскими с известными законами распределения времени между двумя транзактами потока;

• время захвата информационного ресурса является случайной величиной с известным законом распределения;

• величина возможного ущерба в случае доступа на определенное время к конкретному информационному ресурсу является константой.

Модуль защиты от НСД имеет следующие ограничения и допущения:

• возможными нарушителями являются нарушитель из числа штатного персонала и (или) специальное программное средство;

• целью нарушителей является получение доступа к ресурсам информационной системы для считывания информации;

• для достижения цели, нарушители совершают попытки подбора санкционирующего пароля;

• влияние организационных мер защиты на действия нарушителей не учитывается.

Входной информацией для имитационной подмодели защиты от НСД к данным является:

• максимальное время действий нарушителя ($t_{max}$);

• среднее время набора одной комбинации пароля ($t_{он}$);

• возможное число наборов комбинаций пароля до срабатывания ограничителя ($N_в$);

• общее число возможных комбинаций пароля ($N$);

• число разрешенных комбинаций пароля ($\chi$).

Аналитически, одним из способов оценки эффективности парольных систем является метод прямого вычисления вероятности НСД при использовании тотального перебора злоумышленником (в том числе специальным программным средством).

Модуль имитации защиты от перехвата имеет следующие ограничения и допущения:

• перехвату подлежит любая информация, циркулирующая в сети;

• перехват в сети полностью определяется вероятностью перехвата, имеющей известный закон распределения.

Основу модуля имитации защиты от перехвата составляет моделирование трафика в сети организации.

Модуль имитации защиты от сбоев основан на следующих ограничениях и допущениях:

• возможны сбои в информационном, программном и техническом обеспечении;

• вероятности возникновения сбоя каждого типа являются известной величиной;

• в системе присутствуют восстановительные резервы по каждому типу сбоя;

• любой тип сбоя влияет на все информационные ресурсы инфраструктуры.

Модуль имитации защиты от сбоев оценивает возможность прохождения транзакта-сбоя в блок объектов защиты. При этом учитываются возможности восстановительных резервов с учетом вероятности возникновения того или иного типа сбоя. В случае прохождения сбоя все доступные информационные ресурсы «захватываются» транзактом-сбоем на время, необходимое для восстановления работоспособности системы.

Модуль имитации защиты от вмешательства в бизнес-процесс имеет следующие ограничения и допущения:

• пресечение попытки вмешательства в бизнес-процесс осуществляется только организационными мерами защиты;

• на предприятии создана система организационного контроля за нормальным ходом протекания всех бизнес-процессов;

• после доступа нарушителя к соответствующим информационным ресурсам пресечение доступа невозможно.

Модуль имитации защиты от вмешательства в бизнес-процесс отслеживает игровую ситуацию, при которой игрок-злоумышленник пытается превысить свои полномочия (своей роли) в бизнес-процессе путем доступа к соответствующим информационным ресурсам. При этом другой игрок, отождествляемый с соответствующими организационными мерами защиты, в плановом порядке контролирует нормальный ход процесса.

Транзакты-атаки, прошедшие к объектам защиты, «захватывают» соответствующие информационные ресурсы на время, необходимое для совершения соответствующих действий с этими ресурсами. Это же время является аргументом функции вычисления риска, который может быть нанесен при удачном осуществлении атаки. Таким образом, суммарный (совокупный) риск вычисляется как сумма частных рисков по всем атакованным информационным ресурсам.

Попытки возможных атак имитируются в виде дискретно поступающих сущностей (транзактов-атак), целью которых является захват информационных ресурсов. Совокупность поступающих сущностей создает входные потоки попыток атак на объекты защиты. При этом существенными свойствами потоков являются:

- тип источника атаки;
- время поступления транзактов-атак, подчиняющееся заданному закону распределения;
- максимально возможное число атак;
- время поступления первого транзакта-атаки;
- число одновременно поступающих транзактов-атак.

Таким образом, основными выходными параметрами модели являются:

- число удачных попыток атак на информационную инфраструктуру предприятия;
- коэффициент доступа к каждому типу информационного ресурса;
- обобщенный коэффициент информационной безопасности;

• суммарный риск, характеризующий величину ущерба от удачных попыток атак.

При этом обобщенный коэффициент информационной безопасности определяется из выражения

$$K_{ИБ} = \frac{\Sigma_i^S A_i}{\Sigma_j^Q A_j}, \qquad (1)$$

где $A_i$ – $i$-я сорванная атака;

$A_j$ – $j$-я атака;

$S$ – общее число сорванных (предотвращенных) атак;

$Q$ – общее число атак.

Суммарный риск, характеризующий величину ущерба от удачных попыток атак, определяется с использованием самих функциональных возможностей *Arena*:

$$\begin{aligned} &ResBusyCost(Buhgalt\ doc) + ResBusyCost(Business\ doc) + \\ &+ ResBusyCost(Finance\ doc) + ResBusyCost(Plan\ doc), \end{aligned} \qquad (2)$$

где *ResBusyCost(Resource)* – встроенная функция расчета стоимости при условии, что ресурс захвачен.

Кроме того, выходная информация формируется в стандартных отчетах после завершения прогона имитационной модели, которые предоставляют исчерпывающую информацию о моделируемой системе защиты информации.

УДК 004.942

**О. В. Ивочкина**

Санкт-Петербургский государственный университет телекоммуникаций

## ANYLOGIC VS BCP – ИМИТАЦИОННОЕ ПРОЕКТИРОВАНИЕ НЕПРЕРЫВНОСТИ БИЗНЕС-ПРОЦЕССОВ

Прибыль любой компании и ее существование на рынке зависят от ресурсов, персонала и непрерывного вы-

полнения повседневных задач. У большинства компаний есть материальные ресурсы, интеллектуальная собственность, компьютеры, коммуникационные каналы, здания. Если хотя бы что-то одно из этого перечня повреждено или недоступно по той или иной причине, компании может быть нанесен ущерб. Если повреждено или недоступно более одного пункта из этого списка, в компании может возникнуть чрезвычайная ситуация. Если такая ситуация продолжается длительное время, это может стать катастрофой для компании. Многие компании уже никогда не восстанавливаются после катастроф. Однако компании, которые надлежащим образом подготовились к ним, имеют гораздо больше шансов продолжить свой бизнес и остаться на рынке после чрезвычайных ситуаций и катастрофы.

Что есть в офисах компаний на случай непредвиденной или экстремальной ситуации – отказа компьютерной сети, пожара, наводнения и тому подобного? Максимум – план эвакуации, телефоны службы спасения. Хорошо, если имеется страховка, которая позволит возродить бизнес из «пепелища». Поэтому все более остро встает вопрос о подготовке компании к «катастрофической», критической ситуации.

Сегодня в современном мире становится все более актуальной проблема обеспечения непрерывности бизнес-процессов. Всерьез об этом заговорили после террористических актов 11 сентября 2001 г. в США, когда «Башни-близнецы» – символ Нью-Йорка – один из центров деловой активности мира рухнул в считанные минуты.

В настоящее время обеспечение непрерывности бизнеса является одним из важнейших направлений стратегического и оперативного менеджмента. Понятно, что использование планов непрерывности бизнеса (Business Continuity Plan, BCP) требует дополнительных затрат компании. Однако вместе с этим каждая компания получает ряд существенных преимуществ, к которым относятся:

- быстрое и эффективное восстановление бизнеса в чрезвычайных ситуациях;

• минимизация финансовых потерь;

• удовлетворение требований клиентов, акционеров, руководства, аудиторов и других заинтересованных структур;

• уменьшение стоимости страховых контрактов и пр.

Непрерывность бизнеса можно планировать и обеспечивать как самостоятельно, так и прибегнув к услугам консалтинговых компаний. Здесь для российских компаний возможны следующие сценарии сотрудничества с поставщиками услуг в области планирования и поддержки непрерывности бизнеса:

• компания своими силами развивает BCP;

• BCP разрабатывает специализированная компания, а организация его поддерживает (частично внешние, частично внутренние разработки);

• BCP полностью разрабатывается и поддерживается специализированной компанией.

Крупнейшими консалтинговыми компаниями на рынке создания корпоративных программ непрерывности бизнеса являются EMC, Accenture, IBM, San Microsystems, HP, Symantec, E&Y, PWC, Deloitte, KMPG и пр.

В любом случае, будет ли данной проблемой заниматься сама компания или консалтинговая фирма, корпоративная программа управления непрерывностью бизнеса (Business Continuity Management, BCM) должна включать в себя следующие этапы:

• анализ бизнес-процессов предметной области (Business Environment Analysis, BEA) – выделение и ранжирование значимых для бизнеса процессов и определение требований к ним по непрерывности;

• анализ рисков (Risk Analysis, RA) – оценка и ранжирование значимых угроз и уязвимостей непрерывности бизнес-процессов, а также оценка достаточности существующих организационных и технических мер предупреждения прерываний бизнеса;

• оценка воздействия на бизнес (Business Impact Analysis, BIA) – анализ влияния бизнес-процессов на весь бизнес в целом и определение целей восстановления каж-

дого бизнес-процесса вместе с поддерживающей его инфраструктурой;

• определение стратегии непрерывности бизнеса (Business Continuity Strategy Definition) – фиксация целевого времени восстановления (Recovery Time Objective, RTO) и целевой точки восстановления (Recovery Point Objective, RPO) для каждого бизнес-процесса, выбор соответствующих организационных и технических решений;

• разработка и сопровождение BCP и восстановление инфраструктуры в чрезвычайных ситуациях (Disaster Recovery Plan, DRP) для документального оформления надлежащих решений;

• создание технической и организационной систем управления непрерывностью бизнеса;

• формирование адекватной программы сопровождения и эксплуатации корпоративной программы BCM, в частности определение программы осведомленности по вопросам обеспечения непрерывности бизнеса.

В том или ином виде все эти этапы описываются в стандартах BCM, принятых в различных странах: практики непрерывности бизнеса Британского института BCI (Business Continuity Institute), американских институтов DRI (Disaster Recovery Institute) и SANS (SysAdmin, Audit, Network, Security Institute); стандарты и спецификации Британского института стандартов (British Standard Institute, BSI); руководства Австралийского национального агентства аудита (ANAO); раздел международного стандарта по информационной безопасности ISO/IEC 27001; стандарты и библиотеки COBIT, ITIL, MOF в части непрерывности бизнеса и др.

Одним из средств для достижения поставленной целей BCP является инструментарий имитационного моделирования. Цель построения имитационной модели – решение некоторой проблемы реального мира, которую дорого либо невозможно решать, экспериментируя с реальными объектами.

Повышение производительности и надежности, уменьшение стоимости и рисков, оценка чувствительности

системы к изменениям параметров, оптимизация структуры – все эти проблемы встают при проектировании ВСР. Трудность понимания причинно-следственных зависимостей в сложной бизнес-системе приводит к ее неэффективной организации, ошибкам в их проектированиях, большим затратам на устранение ошибок. Сегодня имитационное моделирование становится практически единственным эффективным средством нахождения путей оптимального решения проблем в сложных бизнес-системах – средством поддержки принятия ответственных решений в сфере обеспечения устойчивости и непрерывности бизнеса.

Программная среда имитационного моделирования Anylogic, разработанная российской компанией XJ Technologies, позволяет построить требуемую модель бизнес-системы, так как поддерживает все подходы к моделированию как чисто информационных, так и бизнес-процессов: процессно-ориентированный (дискретно-событийный), системно-динамический и агентный, а также любую их комбинацию.

Уникальность, гибкость и мощность языка моделирования, предоставляемого Anylogic, позволяет учесть любой аспект моделируемой бизнес-системы с любым уровнем детализации. Графический интерфейс Anylogic, инструменты и библиотеки позволяют быстро создавать модели для широко спектра задач – от моделирования производства, логистики, бизнес-процессов до стратегических моделей развития компании и рынков.

Среда имитационного моделирования позволяет построить модель организации, как она есть сейчас, а после сбора и анализа результатов «прогона» сымитировать комплекс мероприятий по реинжинирингу «слабого» бизнес-процесса с акцентом на обеспечение его непрерывности, построить модель заново & vv, т. е. осуществить проектирование более устойчивой бизнес-системы.

С учетом вышеизложенного можно предположить потенциально высокую эффективность Anylogic как средства проектирования ВСР (в совокупности с традиционными средствами).

УДК 004.942

**А. Ю. Васильева**

Санкт-Петербургский государственный
университет телекоммуникаций

# К ВОПРОСУ ПРИМЕНЕНИЯ СИСТЕМЫ ПОДДЕРЖКИ И ПРИНЯТИЯ РЕШЕНИЙ В СФЕРЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

В одном ряду с экспертными системами и автоматизированными системами управления выделяют такой класс систем, как системы поддержки и принятия решений (далее – СППР). Их целью является помощь людям в выработке решения в сложной ситуации путем предоставления необходимой информации для возможности произведения полной и объективной оценки сложившихся условий в конкретной предметной области.

Выработка решения является итерационным процессом (рис. 1), в котором участвуют:

- СППР в качестве вычислительного и управляющего функциональных блоков;
- человек как управляющее звено, корректирующее входные данные и оценивающее полученный в ходе вычислений результаты.


Рис. 1. Процесс поддержки и принятия решений

В настоящее время СППР стали активно применяться в сфере бизнеса в качестве систем, используемых на любом уровне управления и способных координировать лиц, принимающих решения, как на одном уровне управления,

так и на разных. В таблице приведены уровни управления предприятием, где используется СППР.

**Использование СППР на различных уровнях управления**

| Уровень управления | Задачи | Исполнители |
|---|---|---|
| Стратегический | Стратегическое планирование деятельности организации (внутренняя и внешняя политики фирмы) | Менеджеры высшего звена |
| Тактический | Тактическое управление организацией при решении основных функций | Менеджеры среднего звена |
| Операционный | Оперативное реагирование на изменение ситуации, локальные решения | Менеджеры низшего звена |

В связи с тем, что СППР вынуждена решать такой широкий и разнообразный круг задач, она должна обладать следующими характеристиками:

- ориентация на решение плохо структурированных задач;
- сочетание традиционных методов доступа и обработки компьютерных данных с возможностями математических моделей и методами решения задач на их основе;
- направленность на непрофессионального пользователя компьютера;
- высокая адаптивность, обеспечивающая возможность приспосабливаться к особенностям имеющегося технического и программного обеспечения, а также требованиям пользователя.

Перечисленные характеристики необходимы всем СППР и на данный момент идет активное использование и внедрение такого рода систем на предприятиях, занимающихся различной деятельностью. СППР помогают в решении задач логистики, финансовых, бухгалтерских и прочих задач. Также стоит отметить отдельный род задач, где необходимо применение СППР, – это задачи обеспечения безопасности предприятия.

Очень часто, говоря о СППР в сфере обеспечения безопасности, предполагается, что СППР лишь предоставляет пользователю наборы регламентов на случай возникновения той или иной ситуации и возможность контролировать их выполнение, а расчет надежности и безопасности системы с точки зрения возможных угроз и уязвимостей рассматривают как отдельную задачу, не включая ее в СППР.

На рис. 2 отображены основные функциональные блоки, из которых должна состоять СППР, используемая в целях обеспечении безопасности предприятия.

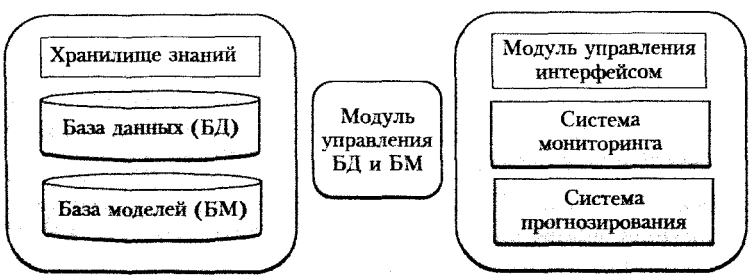



Рис. 2. Функциональная схема СППР

База данных содержит документы, актуальную информацию и прочие данные, пополняемые и отображаемые с помощью систем управления БД и системы мониторинга, в то время как базы моделей должны содержать совокупность модулей и процедур, реализующих математические методы (например, статистический анализ данных, методы оценки надежности системы и т. п.) и используемых в системах прогнозирования.

Система мониторинга отображает актуальную информацию в режиме реального времени, а также архив данных, в то время как система прогнозирования должна дать возможность пользователю самостоятельно смоделировать надежную и безопасную систему на основании актуальных данных, оценить возможные риски, надежность и безопасность системы, а также смоделировать возможные тенденции развития системы.

На сегодняшний день существует множество программных продуктов, позволяющих рассчитать надежность системы, как отечественных (АРБИТР, АРМ Надежность, АСОНИКА-К, Any-Graph, CRISS), так и зарубежных (BlockSim, ItemSoftware, Reliability Workbench, Windchill). Все они отвечают заявленным задачам: позволяют прогнозировать надежность системы на этапе проектирования, а также оценивать количественные показатели надежности спроектированной системы на этапе испытаний и эксплуатации, но при этом данные системы являются отдельным продуктом, не интегрированным в СППР. Также необходимо отметить, что эти системы адресованы опытным инженерам, а не простым пользователям. Также перечисленные системы оперируют абстрактными сущностями и позволяют производить только статическое моделирование, без возможности изменения системы в связи с актуализацией данных.

Решением могла бы стать разработка СППР с интегрированным модулем расчета надежности и безопасности системы, предоставляющая пользователю не только актуальную информацию от системы мониторинга и регламенты действий, но и систему моделирования надежности и безопасности системы с точки зрения наличия в ней ряда угроз и уязвимостей.

УДК 004.056

**И. В. Поночевная, Н. Н. Махальцева**

Санкт-Петербургский государственный
инженерно-экономический университет

## ОЦЕНКА ЗАТРАТ ПРИ ПРОЕКТИРОВАНИИ, ВНЕДРЕНИИ И ЭКСПЛУАТАЦИИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Качество управления современным предприятием напрямую зависит от эффективности применяемой КИС (корпоративной информационной системы), работа кото-

рой во многом определяется уровнем безопасности этой системы. Разработка и внедрение защиты требует определенных затрат сил и средств. Рассмотрим, как формируется оценка затрат для реализации парольной защиты на всех стадиях жизненного цикла КИС.

Представим систему информационной безопасности в виде модели, состоящей из уровневой защиты (Y_(z) = = 0,1,2,3,...n)). Уровень защиты характеризуется устойчивостью к внутренним, внешним, комбинированным (D(v_y)) и прочим воздействиям на систему и скоростью реагирования уровневой защиты в случае дестабилизирующего воздействия «субъектов угроз» на ценный информационный ресурс.

На первом этапе для «субъекта угроз» необходимо получить доступ к уровню защиты, т. е. подбор соответствующего пароля в систему. В рамках данного этапа осуществляется попытка проникновения на соответствующий уровень защиты с подключением к объектам КИС.

На втором этапе, взломав соответствующий уровень защиты и получив доступ к объектам КИС, «субъект угроз» может реализовать следующие дестабилизирующие воздействия угроз: попытка сканирования сервера; попытка получить доступ в систему, как законный пользователь; попытка внедрения вредоносных программ с целью нарушения ценности информационного ресурса; попытка перехвата, блокирования, утечки, модификации или уничтожения информации.

В техническом задании заказчика должны быть отражены величины показателей информационного ресурса, которые определят уровень СИБ для данного объекта КИС (рис. 1).

Ценность информационного ресурса при нарушении функционирования системы защиты должна сохранять свою доступность – **dustup_**; достоверность – **dostover_**; содержательность – **soderjat_**; точность – **tochnost_**; конфиденциальность – **konfid_**; достаточность – **dostatoch_**; актуальность – **actual_**; своевременность – **svoevrem_**;

ценность – **cenost**, т. е. не должна претерпевать существенных изменений. Ценность информации может быть оценена подобно материальным ресурсам.


Рис. 1. Предполагаемые уровни защиты заказчика

**Предполагаемый уровень защиты зависит от величины показателей информационного ресурса (Pok_(i_r) = = 0,1,2,3,...n), а величины показателей зависят от ценности информационного ресурса Sen_(i_r) (рис. 2).**

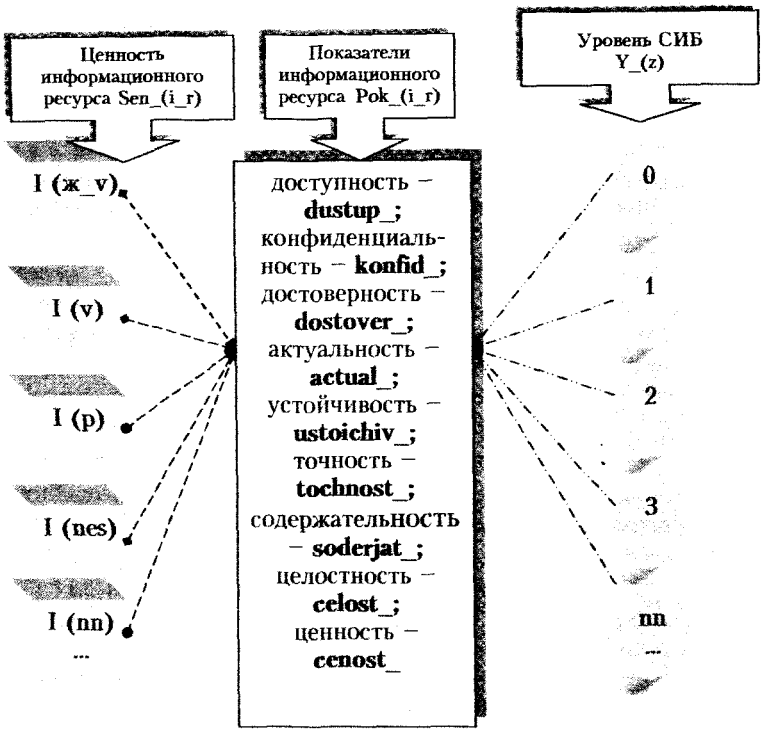



Рис. 2. Показатели, характеризующие уровневую защиту СИБ

Исходя из заданной классификации информации (I (nes) – несущественная; I (p) – полезная; I (v) – важная; I(ж_v) – жизненно-важная) и набора критериев (dustup_; dostover_; soderjat_; tochnost_; dostatoch_; actual_; svoevrem_; cenost_; celost_) представим матрицу соотношения величины показателя Pok_(i_r) от степени ценности информационного ресурса Sen_(i_r), где:

1) значения критериев показывают лишь относительную важность критерия;

2) все критерии ведут себя одинаково: либо все возрастают, либо все вместе убывают в зависимости от повы-

шения степени ценности информационного ресурса. В нашем случае удобнее, чтобы все показатели возрастали, т. е.

$$Krit\_{}_{i+1} > Krit\_{}_{i},$$

где Krit_ – критерий;

i – степень ценности информационного ресурса;

3) чем ценнее информационный ресурс, тем больше весовой коэффициент значимости критерия:

$$Krit\_{}_{i+1} - Krit\_{}_{i} > Krit\_{}_{i} - Krit\_{}_{i+1};$$

4) чем весомей коэффициент значимости критерия, тем больше влияние критерия на процесс проектирования, внедрения и эксплуатацию СИБ:

$$Krit\_{}_{i\,(max)} > Krit\_{}_{j\,(max)}.$$

Для наглядности данную зависимость можно представить в виде графика (рис. 3).

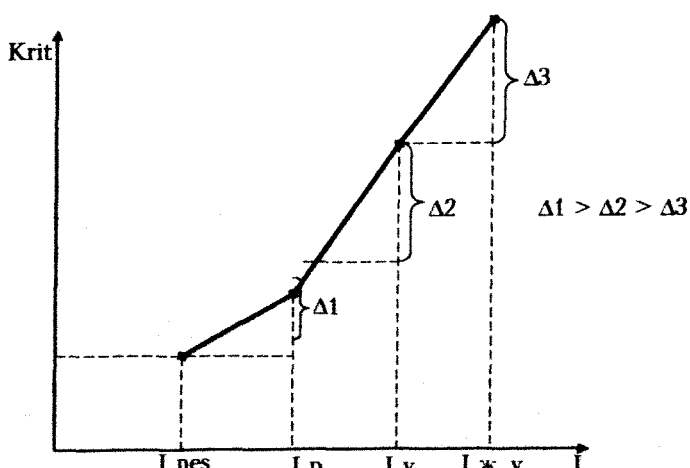



Рис. 3. Влияние критерия на процесс проектирования

Таким образом, не показатели задают уровень СИБ, а структура информационного ресурса, т. е. каждой степени ценности информационного ресурса соответствует свой

уровень безопасности. Таким образом, сначала должна быть задана степень ценности информационного ресурса, а потом даны значения критериям, из чего ясно, что критерий может принимать разные значения, величина которых будет определять право доступа различных пользователей системы к информации.

Поскольку уровень СИБ задавался количеством символов в пароле, то можно условно представить следующим образом:

$$N = f(I),$$

где N – количество символов в пароле;

I – ценность информационного ресурса.

Таким образом в матрице можно дополнить строки количества символов в пароле и соответствующих затрат на уровень СИБ, представим матрицу в виде таблицы.

**Матрица затрат**

| Информация / Критерий | I (nes) – несущественная | I (p) – полезная | I (v) – важная | I (ж_v) – жизненно-важная |
|---|---|---|---|---|
| dustup_ | [a, b] | [b + 1; c] | [c + 1; d] | [d + 1; e] |
| dostover_ | ..... | ..... | ..... | ..... |
| soderjat_ | Интервалы значений | | | |
| tochnost_ | | | | |
| dostatoch_ | ..... | ..... | ..... | ..... |
| actual_ | ..... | ..... | ..... | ..... |
| N | $N_0$ | $N_1$ | $N_2$ | $N_3$ |
| Затраты | $Z_0$ | $Z_1$ | $Z_2$ | $Z_3$ |

Далее рассмотрим структурную классификацию элементов затрат системы информационной безопасности и расходов «субьекта угроз».

Предлагаются следующие элементы затрат:

- затраты капитальные (фиксированные или единовременные);
- затраты эксплуатационные (текущие);
- расходы «субьекта угроз» нарушителя системы.

Рассмотрим состав элементов затрат, включенных в структурную классификацию СИБ, и соответствующих расходов «субъекта угроз».

1. Затраты капитальные (единовременные) включают:

• затраты на организационную составляющую (Z(org), т. е. привлечение дополнительных кадровых ресурсов;

• затраты на инженерно-техническую составляющую (Z(in_tex), к ним можно отнести: средства защиты (SZ_fs); средства защиты рабочих станций (SZ_rs); средства криптографической защиты (SZ_k); средства резервного копирования (S_rk); средства восстановления данных (S_bd); средства аутентификации и идентификации (S_a_i); средства контроля целостности (S_k_c); chtlcndf rjynhjkz ljcnegyjcnb (S_k_d);

• затраты на правовую составляющую (Z(prav): законодательные документы (Z_doc); нормативно-правовые документы (N_prav_doc); положения, приказы, распоряжения, инструкции, требования (Ras_instr_prik);

• затраты на технологическую составляющую (Z_texno): научно-исследовательские работы по формированию средств и методов защиты (N_I_R); разработка своих достижений в области аппаратных и программных средств защиты с последующей ее стандартизацией и сертификацией (Ann_Pr_sr).

Надо отметить, что капитальные затраты в последующем при эксплуатации системы существенно влияют на величину эксплуатационных затрат системы, так как от платформы капитальной в дальнейшем зависят и эксплуатационные вложения на соответствующий уровень средств системы безопасности.

2. Затраты эксплуатационные (текущие) (Tek_zatrat) включают:

• совершенствование системы кадровых ресурсов: совершенствование уровня подготовки ПС в области безопасности (Sov_urov_nodg); повышение квалификационного уровня (Pov_kval_urov); тестирование на соответствие

данному квалификационному уровню (Tes_dan_kval_urov); привлечение доп._персон (Dop_Per), периодич_аттестация_(Att);

• совершенствование аппаратных и программных средств защиты: средства серверов (SZ_fs); средства защиты рабочих станций (SZ_rs); средства криптографической защиты (SZ_k); средства резервного копирования (S_rk); средства восстановления данных (S_bd); средства аутентификации и идентификации (S_a_i);

• совершенствование правовой базы: нормативно-правовые документы (N_prav_dok); положения, приказы, распоряжения, инструкций, требования (Ras_instr_prik).

• совершенствование технологической базы: научно-исследовательские работы по формированию средств и методов защиты (N_I_R); разработку своих достижений в области аппаратных и программных средств защиты с последующей ее стандартизацией и сертификацией (App_Pr_sr).

Представленная структурная классификация позволяет оценить затраты капитальные, эксплуатационные и затраты «субъекта угроз» в зависимости от уровня защиты системы безопасности. Данная структура, с одной стороны, отвечает определенному уровню защиты системы, с другой стороны, уровень защиты влияет на поведение «субъекта угроз» и принятие соответствующего решения о денежных средствах, которые он должен затратить на взлом системы.

Защита должна отвечать соответствующему уровню безопасности системы, а уровень защиты определяется величиной эксплуатационных и капитальных затрат.

Эксплуатационные затраты для соответствующего уровня защиты могут характеризоваться явными и неявными затратами.

• Явные затраты: складываются из затрат на поддержку дополнительных инструкций или распоряжений пакета политик.

• Неявные (скрытые) затраты вытекают из явных затрат в связи с соответствующим дополнением (рекоменда-

цией) по соответствующему уровню безопасности для пакета политик.

Средства защиты оцениваются на основе стоимостных и функциональных критериев. При этом весьма желательно учитывать не только закупочную цену средств защиты на безопасность, но и расходы на обучение, содержание обслуживающего персонала, техническую поддержку, обновление парка оборудования.

3. Расходы «субъектов угроз» системы зависят от взлома или от невозможности взлома системы информационной безопасности, определяемого соответствующим уровнем средств защиты, и от значимости или незначимости информационного ресурса КИС.

Затраты нарушителя системы (Tv) могут характеризоваться прямыми (видимые) и косвенными (невидимые) затратами.

$$Tv = Pп + Kη.$$

Прямые затраты характеризуются первоначальными затратами нарушителя системы защиты **(Рп)**: затраты на нарушение действующего пакета политик безопасности **(Рп1)**; затраты на подбор структуры паролей для соответствующего уровня системы защиты **(Рп2)**; затраты на неоднократную попытку взлома пароля соответствующего уровня системы защиты, определяемые временными характеристиками уровня системы защиты **(Рпз)**:

$$Pп = Pп1 + Pп2 + Pп2 + .... + Pп(n).$$

Косвенные затраты обусловлены затратами в связи с подключением дополнительного «субъекта угроз» в процессе взлома системы для соответствующего уровня системы защиты **(Kη)**.

Косвенные затраты нарушителя ведут к дополнительному росту затрат: затраты на внедрение дополнительных технических средств, для взлома в случае непреодоления уровня системы защиты **(Kη1)**; затраты на подключение соответствующих технических средств, взлома в случае

непреодоления уровня системы защиты **(Kη2)**; затраты на увеличение парка компьютеров для взлома системы защиты **(Kη3)**; затраты на подключение и ввод в курс действий другого нарушителя **(Kη4)**:

$$K\eta = K\eta 1 + K\eta 2 + K\eta 3 + K\eta 4 + \ldots + K\eta(m).$$

Все вышепредставленные затраты «субъекта угроз» в совокупности выливаются в соответствующую стоимостную сумму.

Затраты на средства защиты на стадии создания системы безопасности играют немаловажную роль по снижению эксплуатационных затрат, так как чем выше капитальные вложения на стадии внедрения, тем ниже эксплуатационные расходы на стадии функционирования системы в течение определенного периода (например, года).

Устойчивость составляющих СИБ определяется уровнем защиты ценного информационного ресурса

$$Fсз = \hbar(y0; y1; y2; y3; \ldots y(n)),$$

где $\hbar$ – уровень защиты информационного ресурса:

y0 – доступности **(dustup_)**; y1 – целостности **(celost_)**; y2 – конфиденциальности **(konfid_)**; y3 – достоверности **(dostover_)**; y4 – актуальности **(actual_)**; y6 – точности **(tochnost_)**; y7 –содержательности **(soderjat_)**; y8 – ценности **(cenost)_**.

Затраты на средства защиты на стадии создания системы безопасности играют немаловажную роль по снижению эксплуатационных затрат, так как чем выше капитальные вложения на стадии внедрения, тем ниже эксплуатационные расходы на стадии функционирования системы в течение определенного периода (например, года).

Динамическое равновесие между средствами защиты системы безопасности и средствами для взлома информационной системы позволяет оценить стоимость взлома системы, которая может оказаться значительно выше, чем стоимость информационного ресурса. В то же время оно предполагает, что чем выше уровень защиты системы

безопасности, тем ниже вероятность того, что «субъекту угроз» не удастся атаковать и взломать соответствующий уровень защиты и нарушить тем самым достоверность, доступность, целостность и конфиденциальность объектов КИС. Уровень защиты системы безопасности влияет на поведение нарушителя и принятие соответствующего решения. Защита должна отвечать соответствующему уровню безопасности системы, а уровень защиты определяется величиной эксплуатационных и капитальных затрат.

Предложенные оценки всех составляющих элементов затрат системы информационной безопасности и расходов «субъекта угроз» позволят создателям корпоративной информационной системы определить и оценить затраты для выстраивания системы информационной безопасности необходимого уровня защиты.

# СОДЕРЖАНИЕ

*Раздел 2*

## ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

## *Раздел 3*

## УПРАВЛЕНИЕ И ЭКОНОМИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*НАУЧНОЕ ИЗДАНИЕ*

# АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник научных трудов

Редактор *А. В. Алехина*
Корректор *Е. Г. Закревская*
Компьютерная верстка *Т. А. Бойченко*

---

ИД № 00918 от 02.02.2000 г.
Подписано в печать 20.12.12. Формат 60×84 1/16. Бумага типогр. № 1.
Печать цифровая. Усл.-печ. л. 15,81. Уч.-изд. л. 15,84. Изд. № 113. Тираж 100 экз. Заказ 791.

---

СПбГИЭУ. 191002, Санкт-Петербург, ул. Марата, 27.
ИзПК СПбГИЭУ. 192102, Санкт-Петербург, ул. Касимовская, 5.