ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
Государственное образовательное учреждение высшего профессионального образования
«**ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**»

Р.В. Мещеряков

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ ЭВМ

Учебное пособие

Издательство
Томского политехнического университета
2008

УДК 681.3.067(075.8)
ББК 32.81я73
М56

Мещеряков Р.В.

М56 Информационная безопасность и защита информации в сетях ЭВМ: учебное пособие / Р.В. Мещеряков. – Томск: Изд-во Томского политехнического университета, 2008. – 147 с.

ISBN 5-98298-198-2

В учебном пособии изложены теоретические вопросы курса информационной безопасности и защиты информации в сетях ЭВМ, рассмотрена государственная система защиты информации в Российской Федерации, представлены основные модели защиты и их практическая реализация в информационных системах.

Пособие соответствует программе дисциплины «Информационная безопасность и защита информации в сетях ЭВМ» и предназначено для бакалавров и магистрантов, обучающихся по направлению «Информатика и вычислительная техника», а также представляет интерес и для студентов технических вузов, ведущих подготовку специалистов в области информационных технологий.

УДК 681.3.067(075.8)
ББК 32.81я73

Рекомендовано к печати Редакционно-издательским советом
Томского политехнического университета

Рецензент

Доктор технических наук, профессор, заведующий кафедрой автоматизации систем управления Томского государственного университета систем управления и радиоэлектроники

А.М. Кориков

ISBN 5-98298-198-2

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

В учебном пособии рассматриваются ключевые разделы курса «Информационная безопасность и защита информации в сетях ЭВМ», предусмотрены как теоретические разделы, так и практические, направленные на развитие навыков анализа информационной безопасности объектов, а также путей их совершенствования.

Целями дисциплины являются:

1) приобретение студентами знаний по информационной безопасности и о направлениях ее развития;
2) ознакомление с возможными нарушениями информационных систем, овладение основными принципами построения и функционирования современных защищенных информационных систем;
3) освоение и приобретение навыков работы со средствами защиты.

Учебное пособие ориентировано на подготовку магистрантов по программе 552813 «Сети ЭВМ и телекоммуникации».

В учебном пособии рассмотрен ряд важных практических направлений, по которым автор проводил исследования при работе в Центре технологий безопасности Томского государственного университета систем управления и радиоэлектроники. Необходимо отметить, что ряд разделов настоящего пособия были взяты из работы Белова Е.Б., Лося В.П., Мещерякова Р.В., Шелупанова А.А. «Основы информационной безопасности» [20].

ВВЕДЕНИЕ

Теория защиты информации [20, 27] определяется как система основных идей, относящихся к защите информации, дающая целостное представление о сущности проблемы защиты, закономерностях ее развития и существенных связях с другими отраслями знания, формирующаяся на основе опыта практического решения задач защиты и определяющая основные ориентиры в направлении совершенствования практики защиты информации.

Составными частями теории являются:

- полные и систематизированные сведения о происхождении, сущности и содержании проблемы защиты;
- систематизированные результаты анализа развития теоретических исследований и разработок, а также опыта практического решения задач защиты;
- научно обоснованная постановка задачи защиты информации в современных системах ее обработки, полно и адекватно учитывающая текущие и перспективные концепции построения систем и технологий обработки, потребности в защите информации и объективные предпосылки их удовлетворения;
- общие стратегические установки на организацию защиты информации, учитывающие все многообразие потенциально возможных условий защиты;
- методы, необходимые для адекватного и наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные прикладные методы решения;
- методологическая и инструментальная база, содержащая необходимые методы и инструментальные средства для решения любой совокупности задач защиты в рамках любой выбранной стратегической установки;
- научно обоснованные предложения по организации и обеспечению работ по защите информации;
- научно обоснованный прогноз перспективных направлений развития теории и практики защиты информации.

Информационная безопасность определяется способностью государства, общества, личности:

- обеспечивать с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности, устойчивого функционирования и развития;
- противостоять информационным опасностям и угрозам, негативным информационным воздействиям на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические источники информации;
- вырабатывать личностные и групповые навыки и умения безопасного поведения;
- поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно ни было навязано.

Информационная война – действия, принимаемые для достижения информационного превосходства в интересах национальной военной стратегии, осуществляемые путем влияния на информацию и информационные системы противника при одновременной защите собственной информации своих информационных систем.

1. ОБЩИЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информация – это сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), отраженные на материальных носителях, используемые в целях получения знаний и практических решений. Наиболее важными в практическом плане свойствами информации являются: ценность, достоверность, своевременность. Ценность информации определяется обеспечением возможности достижения цели, поставленной перед получателем.

Достоверность – соответствие полученной информации действительной обстановке.

Своевременность – соответствие ценности и достоверности определенному временному периоду.

Эффективность принимаемых решений определяется, кроме того, системой факторов, характеризующих показатели информации. Среди них можно выделить такие как:

- внутренние свойства (достоверность и кумулятивность), сохраняющиеся при переносе данных в другую среду (систему);
- внешние свойства (временные свойства и свойства защищенности, которые характерны для данных, находящихся (используемых) в определенной среде (системе), и которые исчезают при их переносе в другую систему.

Достоверность. В свойстве достоверности выделяются безошибочность и истинность данных. Под безошибочностью понимается свойство данных не иметь скрытых случайных ошибок. Случайные ошибки в данных обусловлены, как правило, ненамеренными искажениями содержания сведений человеком или сбоями технических средств при переработке данных в информационной системе (ИС). При анализе истинности данных рассматривают преднамеренные искажения данных человеком – источником сведений (в том числе и из-за неумения или непонимания сути вопроса) или искажения, вносимые средствами обработки информации.

Кумулятивность. Кумулятивность определяет такие понятия как гомоморфизм (соотношение между объектами двух множеств, при котором одно множество является моделью другого) и избирательность.

Данные, специально отобранные для конкретного уровня пользователей, обладают определенным свойством – избирательностью. Это социальная составляющая кумулятивности.

Временные свойства. Временные свойства определяют способность данных отображать динамику изменения ситуации (динамичность). При этом можно рассматривать или время запаздывания появления в данных соответствующих признаков объектов, или расхождение реальных признаков объекта и тех же признаков, отображаемых в данных. Соответственно можно выделить:

- актуальность – свойство данных, характеризующих текущую ситуацию;
- оперативность – свойство данных, состоящее в том, что время их сбора и переработки соответствует динамике изменения ситуации;
- идентичность – свойство данных соответствовать состоянию объекта.

Нарушение идентичности связано с техническим (по рассогласованию признаков) старением информации, при котором происходит расхождение реальных признаков объектов и тех же признаков, отображенных в информации.

В плане социальных мотивов рассматриваются:

- срочность – свойство данных соответствовать срокам, определяемым социальными мотивами;
- значимость – свойство данных сохранять ценность для потребителя с течением времени, т. е. не подвергаться моральному старению.

Защищенность данных. При рассмотрении защищенности можно выделить технические аспекты защиты данных от несанкционированного доступа (свойство недоступности) и социально-психологические аспекты классификации данных по степени их конфиденциальности и секретности (свойство конфиденциальности).

Дополнительно можно выделить следующие свойства информации:

1. Общественная природа (источником информации является познавательная деятельность людей, общества).

2. Языковая природа (информация выражается с помощью языка, т. е. знаковой системы любой природы, служащей средством общения, мышления, выражения мысли. Язык может быть естественным, используемым в повседневной жизни и служащим формой выражения мыслей и средством общения между людьми, и искусственным, созданным людьми для определенных целей (например, язык математической символики, информационно-поисковый, алгоритмический и др.).

3. Неотрывность от языка носителя.

4. Дискретность (единицами информации как средствами выражения являются слова, предложения, отрывки текста, а в плане содержания – понятия, высказывания, описание фактов, гипотезы, теории, законы и др.).

5. Независимость от создателей.

6. Старение (основной причиной старения информации является не само время, а появление новой информации, с поступлением которой прежняя информация оказывается неверной, перестает адекватно отображать явления и закономерности материального мира, человеческого общения и мышления).

7. Рассеяние (т. е. существование в многочисленных источниках).

На сегодня рынок информации в России многообразен и динамичен. Активно используя самые совершенные технологии, он расширяется за счет формирования новых общественных потребностей и начинает доминировать в мировой экономике наряду с энергетическим рынком. Чтобы оценить масштабность рынка информации, достаточно посмотреть на его структуру. В число основных секторов этого рынка входят:

- традиционные средства массовой информации (телевидение, радио, газеты);
- справочные издания (энциклопедии, учебники, словари, каталоги и т. д.);
- справочно-информационные службы (телефонные службы, справочные бюро, доски объявлений и др.);
- консалтинговые службы (юридические, маркетинговые, налоговые и др.);
- компьютерные информационные системы;
- отраслевые базы данных;
- Internet.

Возможно, этот перечень не полон, однако основные направления он отражает.

Компьютерный сектор рынка имеет ряд особенностей, выделяющих его из всех остальных.

Во-первых, он дает новое качество информационных услуг – быстрый поиск в больших массивах информации. В Internet существуют различные поисковые системы информации.

Во-вторых, позволяет реализовать полный цикл технологии ввода, хранения, обновления и доставки информации потребителям с наиболее эффективными алгоритмическими решениями на отдельных этапах.

В-третьих, компьютерный сектор очень быстро развивается и начинает оказывать влияние на другие секторы информационного рынка. В первую очередь это относится к системам телетекста в сочетании с

обычным телевидением, а также к системам мультимедиа, которые начинают конкурировать с полиграфическими изданиями справочной и учебной литературы.

Источник информации – это материальный объект, обладающий определенными сведениями (информацией), представляющими конкретный интерес для злоумышленников или конкурентов.

В общем плане, без значительной детализации, можно считать источниками конфиденциальной информации следующие категории:

1. Люди (сотрудники, обслуживающий персонал, продавцы, клиенты и др.).
2. Документы самого различного характера и назначения.
3. Публикации: доклады, статьи, интервью, проспекты, книги и т. д.
4. Технические носители информации и документов.
5. Технические средства обработки информации: автоматизированные средства обработки информации и средства обеспечения производственной и трудовой деятельности, в том числе и средства связи.
6. Выпускаемая продукция.
7. Производственные и промышленные отходы.

Контрольные вопросы и упражнения

1.1. Что такое «информация»? Определите основные свойства, определяющие информацию как продукт.
1.2. Перечислите основные источники информации в информационных системах. Носители информации.
1.3. Каковы основные цели защиты информации?
1.4. Как влияют действия субъектов информационного обмена на информацию?
1.5. Охарактеризуйте показатели информации: важность, полнота, адекватность, релевантность, толерантность. Какое значение они имеют при защите информации? Приведите примеры.
1.6. Какова основная цель комплексного подхода к защите информации. Аргументируйте свой ответ. Приведите примеры.
1.7. Дайте определения каждого из следующих определений комплексности и укажите их сходства и различия: а) целевая; б) инструментальная; в) структурная; г) функциональная; д) временная.
1.8. Приведите основные стандарты международного обмена.
1.9. Что такое «средства защиты информации»? Основные характеристики. Приведите примеры.
1.10. Обоснуйте необходимость встраивания средств защиты информации в информационную систему.

2. ГОСУДАРСТВЕННАЯ СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

Информация как объект юридической защиты. Основные принципы засекречивания информации

Организационно-правовое обеспечение информационной безопасности представляет собою совокупность решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению информационной безопасности, так и создание и функционирование систем защиты информации на конкретных объектах. Поэтому организационно-правовая база должна обеспечивать выполнение следующих функций:

1) разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации;
2) определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране, и порядка регулирования деятельности предприятия и организации в этой области;
3) создание полного комплекса нормативно-правовых руководящих и методических материалов (документов), регламентирующих вопросы обеспечения информационной безопасности как в стране в целом, так и на конкретном объекте;
4) определение мер ответственности за нарушения правил защиты;
5) определение порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Под юридическими аспектами организационно-правового обеспечения защиты информации понимается совокупность законов и других нормативно-правовых актов. С помощью указанных аспектов достигаются следующие цели:

- все правила защиты информации являются обязательными для соблюдения всеми лицами, имеющими отношение к конфиденциальной информации;

---

[1] Приводится по работе [20]

- узакониваются все меры ответственности за нарушения правил защиты информации;
- узакониваются (приобретают юридическую силу) технико-математические решения вопросов организационно-правового обеспечения защиты информации;
- узакониваются процессуальные процедуры разрешения ситуаций, складывающихся в процессе функционирования системы защиты.

Разработка законодательной базы информационной безопасности любого государства является необходимой мерой, удовлетворяющей первейшую потребность в защите информации при развитии социально-экономических, политических, военных направлений развития этого государства. Особое внимание со стороны западных стран к формированию такой базы вызвано все возрастающими затратами на борьбу с «информационными» преступлениями. Все это заставляет страны Запада серьезно заниматься вопросами законодательства по защите информации. Так, первый закон в этой области в США был принят в 1906 г., а к настоящему времени уже имеется более 500 законодательных актов по защите информации, ответственности за ее разглашение и компьютерные преступления.

Определение основных принципов отнесения сведений, имеющих конфиденциальный характер, к защищаемой информации

Созданием законодательной базы в области информационной безопасности каждое государство стремится защитить свои информационные ресурсы. Информационные ресурсы государства в самом первом приближении могут быть разделены на три большие группы:

- информация открытая – на распространение и использование которой не имеется никаких ограничений;
- информация запатентованная – охраняется внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности;
- информация, «защищаемая» ее собственником, владельцем с помощью отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны. К этому виду относят обычно информацию, не известную другим лицам, которая или не может быть запатентована, или умышленно не патентуется с целью избегания или уменьшения риска завладения ее соперниками, конкурентами.

Защищают и охраняют, как правило, не всю или не всякую информацию, а наиболее важную, ценную для собственника, ограничение распространения которой приносит ему какую-то пользу или прибыль, возможность эффективно решать стоящие перед ним задачи.

Какую информацию относят к защищаемой?

Во-первых, *секретную* информацию. К секретной информации в настоящее время принято относить сведения, содержащие государственную тайну.

Во-вторых, *конфиденциальную* информацию. К этому виду защищаемой информации относят обычно сведения, содержащие коммерческую тайну, а также тайну, касающуюся личной (неслужебной) жизни и деятельности граждан.

Таким образом, под защищаемой информацией понимают сведения, на использование и распространение которых введены ограничения их собственником и характеризуемые понятием «тайна».

Применительно к органам государственной власти и управления под тайной понимается то, что скрывается от других, что известно определенному кругу людей. Иначе говоря, те сведения, которые не подлежат разглашению и составляют тайну.

Основное направление использования этого понятия – засекречивание государством определенных сведений, сокрытие которых от соперников, потенциального противника дает ему возможность успешно решать жизненно важные вопросы в области обороны страны, политических, научно-технических и иных проблем и с меньшими затратами сил и средств.

К подобному же виду тайны относится засекречивание предприятием, фирмой сведений, которые помогают ему эффективно решать задачи производства и выгодной реализации продукции.

Сюда же примыкают и тайны личной жизни граждан, обычно гарантируемые государством: тайна переписки, врачебная тайна, тайна денежного вклада в банке и др., представленные в табл. 1.

Таблица 1

Классификация информации

Вид информации	Защищаемая		Запатентованная		Открытая
Владелец	Секретная	Конфиденциальная	Патент	Авторское право	
Личность		Личная тайна. Персональные данные	Патент физического лица	Авторское право физического лица	
Общество		Коммерческая тайна	Патент юридического лица	Авторское право юридического лица	
Государство	Государственная тайна	Служебные сведения	Государственный патент		

… – *Обеспечивается защитой государства*

Защищают и охраняют, как правило, не всю или не всякую информацию, а наиболее важную, ценную для собственника, ограничение распространения которой приносит ему какую-то пользу или прибыль, возможность эффективно решать стоящие перед ним задачи. При этом различают признаки защищаемой информации:

- засекречивать информацию, т. е. ограничивать к ней доступ, может только ее собственник (владелец) или уполномоченные им на то лица;
- чем важнее для собственника информация, тем тщательнее он ее защищает. А для того, чтобы все, кто сталкивается с этой защищаемой информацией, знали, что одну информацию необходимо оберегать более тщательно, чем другую, собственник определяет ей различную степень секретности;
- защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства;
- секретная информация обладает определенным генетическим свойством: если эта информация является основанием для создания новой информации (документов, изделий и т. п.), то созданная на этой основе информация является, как правило, секретной.

Отличительным признаком защищаемой информации является то, что засекречивать ее может только ее собственник (владелец) или уполномоченные им на то лица.

Владельцами (собственниками) защищаемой информации могут быть:

- Государство и его структуры (органы). В этом случае к ней относятся сведения, являющиеся государственной, служебной тайной, иные виды защищаемой информации, принадлежащей государству или ведомству. В их числе могут быть и сведения, являющиеся коммерческой тайной.
- Предприятия, товарищества, акционерные общества (в том числе и совместные) и другие – информация является их собственностью и составляет коммерческую тайну.
- Общественные организации – как правило, партийная тайна, не исключена также государственная и коммерческая тайна.
- Граждане государства (их права – тайн переписки, телефонных и телеграфных разговоров, врачебная тайна, персональные данные и др. – гарантируются государством, личные тайны – их личное дело. Следует отметить, что государство не несет ответственность за сохранность личных тайн).

Понятие «государственная тайна» является одним из важнейших в системе защиты государственных секретов в любой стране. От ее пра-

вильного определения зависит и политика руководства в области защит секретов.

Определение этого понятия дано в Законе РФ «О государственной тайне»: «Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации».

Модель определения государственных секретов обычно включает в себя следующие существенные признаки:

1. Предметы, явления, события, области деятельности, составляющие государственную тайну.
2. Противник (данный или потенциальный), от которого в основном осуществляется защита государственной тайны.
3. Указание в законе, перечне, инструкции сведений, составляющих государственную тайну.
4. Наносимый ущерб обороне, внешней политике, экономике, научно-техническому прогрессу страны и т. п. В случае разглашения (утечки) сведений, составляющих государственную тайну.

Какие сведения могут быть отнесены к государственной тайне, определено в Указе Президента РФ от 30 ноября 1995 г. № 1203. К ним отнесены сведения (указаны лишь разделы): в областях военной, внешнеполитической и внешнеэкономической, экономической, научной, разведывательной, контрразведывательной и оперативно-розыскной деятельности.

Нельзя засекречивать информацию как имеющую статус государственной тайны:

- если ее утечка (разглашение и т. п.) не влечет ущерба национальной безопасности страны; в нарушение действующих законов;
- если сокрытие информации будет нарушать конституционные и законодательные права граждан;
- для сокрытия деятельности, наносящей ущерб окружающей природной среде, угрожающей жизни и здоровью граждан. Подробнее этот перечень содержится в ст. 7 Закона РФ «О государственной тайне».

Какие же используются критерии для отнесения сведений, во-первых, к государственной тайне, во-вторых, к той или иной степени секретности?

Ответ на этот вопрос дают Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности, указанные в постановлении Правительства РФ от 4 сентября 1995 г. № 870.

К сведениям *особой важности* следует относить сведения, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких областях.

К *совершенно секретным* сведениям следует относить сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики Российской Федерации в одной или нескольких областях.

К *секретным* сведениям следует относить все иные из числа сведений, составляющих государственную тайну. Ущерб может быть нанесен интересам предприятия, учреждения или организации.

Как видно из изложенного, разница между тремя степенями секретности зависит от величины ущерба.

Понятие, виды и размер ущерба разработаны пока еще недостаточно и, видимо, будут отличны для каждого конкретного объекта защиты – содержания сведений, составляющих государственную тайну, сущности отраженных в ней фактов, событий, явлений действительности. В зависимости от вида, содержания и размеров ущерба можно выделить группы некоторых видов ущерба при утечке (или возможной утечке) сведений, составляющих государственную тайну.

Политический ущерб может наступить при утечке сведений политического и внешнеполитического характера, о разведывательной деятельности спецслужб государства и др. Политический ущерб может выражаться в том, что в результате утечки информации могут произойти серьезные изменения в международной обстановке не в пользу Российской Федерации, утрата страной политических приоритетов в каких-то областях, ухудшение отношений с какой-либо страной или группой стран и т. д.

Экономический ущерб может наступить при утечке сведений любого содержания: политического, экономического, военного, научно-технического и т. д. Экономический ущерб может быть выражен прежде всего в денежном исчислении. Экономические потери от утечки информации могут быть прямыми и косвенными.

Так, прямые потери могут наступить в результате утечки секретной информации о системах вооружения, обороны страны, которые в результате этого практически потеряли или утратили свою эффективность и требуют крупных затрат на их замену или переналадку.

Косвенные потери чаще всего выражаются в виде размера упущенной выгоды: срыв переговоров с иностранными фирмами, о выгодных сделках с которыми ранее была договоренность; утрата приоритета в научном исследовании, в результате соперник быстрее довел свои исследования до завершения и запатентовал их и т. д.

Моральный ущерб, как правило, неимущественного характера наступает от утечки информации, вызвавшей или инициировавшей противоправную государству пропагандистскую компанию, подрывающую репутацию страны, приведшую к выдворению из каких-то государств наших дипломатов, разведчиков, действовавших под дипломатическим прикрытием и т. п.

Проблема засекречивания информации и определения степени секретности сведений, документов, изделий и работ является одной из стержневых во всей деятельности по защите информации. Она имеет большое государственное значение, определяет методологию и методику защиты информации, объем работ по ее защите и другие обстоятельства, связанные с деятельностью государственных органов, предприятий и организаций в этой области. Правила засекречивания информации определяют в конечном счете политику государства в области защиты секретов. Этим и объясняется, что в перечне сведений, составляющих государственную тайну, утверждающихся у нас в стране на самом высоком уровне, находит отражение концепция руководства страны в области защиты государственных секретов.

Засекречивать информацию имеют право органы власти, управления и должностные лица, наделенные соответствующими полномочиями. Они осуществляют политику государства в области защиты информации:

- определяют категории сведений, подлежащих защите и, следовательно, засекречиванию, и закрепляют это в законодательных актах;
- разрабатывают перечни сведений, подлежащих засекречиванию;
- определяют степени секретности документов, изделий, работ и сведений и проставляют на носителях защищаемой информации соответствующие грифы секретности.

Таким образом, *засекречивание информации* – это совокупность организационно-правовых мер, регламентированных законами и другими нормативными актами, по введению ограничений на распространение и использование информации в интересах ее собственника (владельца).

Обозначим кратко основные принципы засекречивания информации:

1. Законность засекречивания информации. Заключается в осуществлении строго в рамках действующих законов и других подзаконных нормативных актов. Отступление от этого принципа может нанести серьезный ущерб интересам защиты информации, интересам личности, общества и государства, в частности незаконным сокрытием от общества информации, не требующей засекречивания, или утечки важной информации.

2. Обоснованность засекречивания информации. Заключается в установлении путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экономических или иных последствий этого акта, исходя из баланса жизненно важных интересов личности, общества и государства. Неоправданно засекречивать информацию, вероятность раскрытие которой превышает возможность сохранения ее в тайне.

3. Своевременность засекречивания информации. Заключается в установлении ограничений на распространение этих сведений с момента их получения (разработки) или заблаговременно.

4. Подчиненность ведомственных мероприятий по засекречиванию информации общегосударственным интересам. Это в первую очередь относится к области защиты государственной тайны. Что касается коммерческой тайны, то предприятия наделены правами засекречивания информации, кроме оговоренных в законе случаев.

В Российской Федерации в соответствии с Законом «О государственной тайне» в настоящее время складывается следующая форма засекречивания информации. Закон определяет категории сведений, отнесенных к государственной тайне, затем Президент РФ на основе предложений Правительства РФ утверждает два перечня: Перечень должностных лиц органов государственной власти и управления, наделенных полномочиями по отнесению сведений к государственной тайне, и Перечень сведений, отнесенных к государственной тайне, – для осуществления единой государственной политики в области засекречивания информации.

Руководители, наделенные полномочиями по засекречиванию информации, утверждают своими приказами перечни сведений, подлежащих засекречиванию, в соответствии с их отраслевой, ведомственной или программно-целевой принадлежностью. Они же наделяются полномочиями распоряжения этими сведениями, пересмотра степени их секретности и рассекречивания.

Предприятия при определении степени (грифа) секретности документов, изделий, работ по-прежнему будут руководствоваться перечнями сведений, подлежащих засекречиванию. Таким образом, до исполнителей будут доводиться стратегические установки на применение режимных ограничений в конкретных ситуациях (рис. 1).

Степень секретности и конфиденциальности информации, отображенной в документах, изделиях и т. д., не остается постоянной. Она обычно уменьшается и реже (например, документы представляют историческую и иную ценность) может увеличиваться. Степень секретности и конфиденциальности информации периодически должна пересматри-

ваться. При этом она может быть увеличена, снижена до фактической, или рассекречена вообще.

Рис. 1. Порядок засекречивания информации, составляющей государственную тайну

Рассекречивание конфиденциальной и секретной информации, работ, документов, изделий – это деятельность предприятий по снятию (частичному или полному) ограничений на доступ к ранее засекреченной информации, на доступ к ее носителям, вызываемая требованиями законов и объективными факторами: изменением международной и внутригосударственной обстановки, появлением более совершенных видов определенной техники, снятием изделий с производства, передачей (продажей) научно-технических решений оборонного характера в народное хозяйство, продажей изделия за границу и т. д., а также взятием государства на себя международных обязательств по открытому обмену сведениями, составляющими в Российской Федерации государственную тайну.

Информация должна оставаться секретной или конфиденциальной до тех пор, пока этого требуют интересы национальной безопасности или конкурентной и коммерческой деятельности предприятия.

Принципиальные аспекты рассекречивания информации могут быть изложены в следующих основных положениях:

1. Информация не подлежит засекречиванию, а засекреченная должна быть рассекречена, если это сделано необоснованно и в нарушение действующих законов, в целях скрытия нарушений законности, в результате неумелого руководства и должностных ошибок, нарушения конституционных и других законодательных прав граждан.

2. Засекреченная информация рассекречивается не позднее сроков, установленных при ее засекречивании. Ранее этих сроков подлежит рассекречиванию лишь информация, которая попадает под действие взятых Российской Федерацией на себя международных обязательств по открытому обмену информацией, или процесс ее распространения вследствие разглашения не подлежит локализации. Срок засекречивания информации, отнесенной к государственной тайне, не должен превышать 30 лет. Правом продления сроков засекречивания информации наделяются руководители центральных органов федеральной исполнительной власти, осуществившие отнесение соответствующих сведений к государственной тайне.

3. Информация не подлежит засекречиванию, а засекреченная должна быть рассекречена, если содержащиеся в ней новые научные, проектные, технологические и т. п. разработки находятся ниже мирового технологического уровня или достаточно подробно раскрыты в опубликованной зарубежной или отечественной литературе; информация является общеизвестной, а также информация о событиях и явлениях, которые могут нанести ущерб здоровью людей или окружающей среде.

4. Рассекречиванию (разглашению) не подлежат сведения, затрагивающие личную (неслужебную) жизнь граждан страны, если на обратное не имеется согласия самих граждан, а в случае их смерти – их ближайших родственников. Иной порядок такого рассекречивания рассматривается через суд.

Государственная система правового обеспечения защиты информации в Российской Федерации

Второй функцией организационно-правового обеспечения информационной безопасности является определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране. Основой для создания государственной системы организационно-правового обеспечения защиты информации является

создаваемая в настоящее время государственная система защиты информации, под которой понимается совокупность федеральных и иных органов управления и взаимоувязанных правовых, организационных и технических мер, осуществляемых на различных уровнях управления и реализации информационных отношений и направленных на обеспечение безопасности информационных ресурсов.

Основные положения правового обеспечения защиты информации приведены в Доктрине информационной безопасности РФ, а также в других законодательных актах.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской

Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных принципах [1]:

- соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;
- открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;
- правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
- приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
- создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
- определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
- оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;

- координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;
- контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;
- предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
- развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
- организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;
- проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;
- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;
- защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;
- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
- совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;
- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Рассмотрим структуру государственной системы информационной безопасности и основные функции ее составных частей (рис. 2).

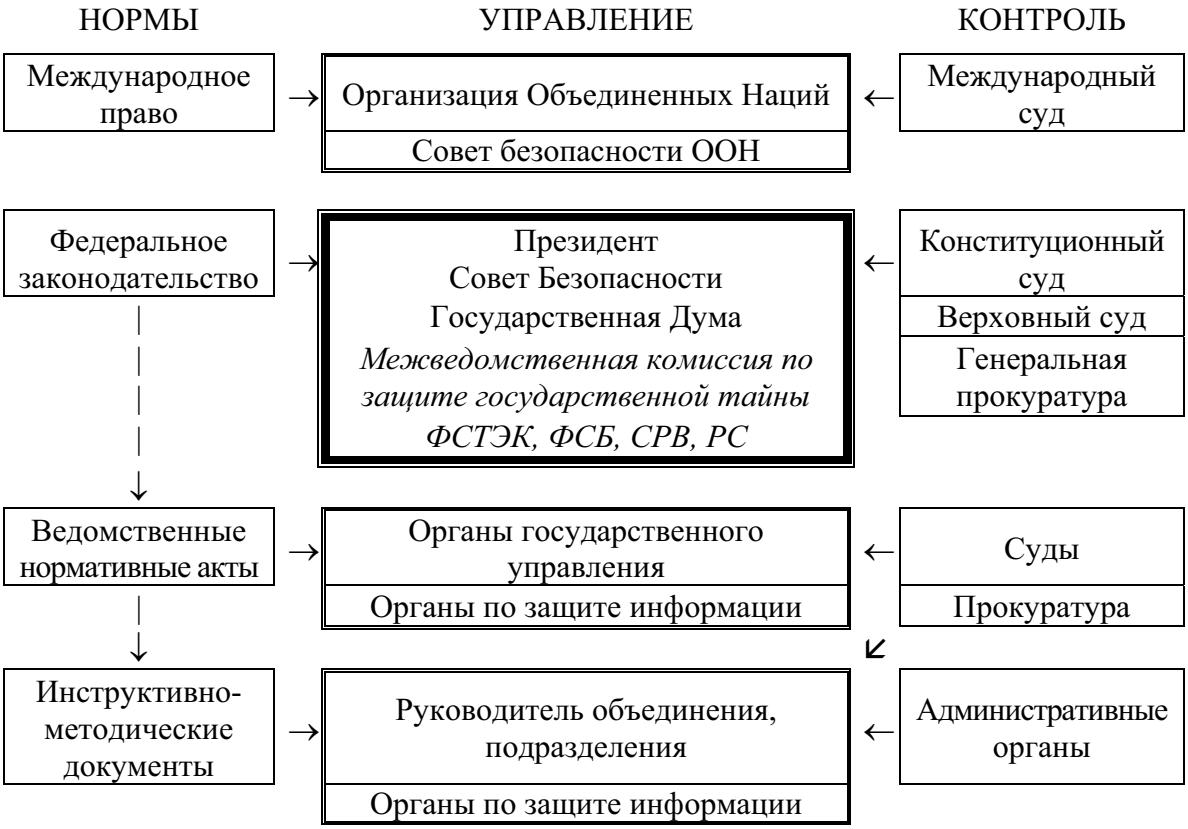


Рис. 2. Структура государственной системы информационной безопасности

Основным органом, координирующим действия государственных структур по вопросам защиты информации является *Межведомственная комиссия по защите государственной тайны*, созданная Указом Президента РФ от 8 ноября 1995 г. № 1108. Она действует в рамках государственной системы защиты информации от утечки по техническим каналам, положение о которой введено в действие постановлением Правительства РФ от 15 сентября 1993 г. № 912–51. В этом постановлении определены структура, задачи и функции, а также организация работ по защите информации применительно к сведениям, составляющим государственную тайну. Основной задачей государственной системы защиты информации является проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности страны.

Общая организация и координация работ в стране по защите информации, обрабатываемой техническими средствами, осуществляется коллегиальным органом – Федеральной службой по техническому и экспортному контролю (ранее в Российской Федерации функции выполняла *Государственная техническая комиссия России* – Гостехкомиссия). В ее состав входят руководители федеральных органов государственного управления, определяющих научно-техническую и фи-

нансовую политику по защите информации в политической, экономической, военной областях, или их первые заместители.

ФСТЭК России в пределах своей компетенции осуществляет следующие функции:

- формирует общую стратегию и определяет приоритетные направления защиты информации в жизненно важных сферах деятельности государства с целью предотвращения ущерба интересам страны;
- определяет основные требования исследований, рассматривает и утверждает концепции, требования, нормы и другие нормативно-технические и методические документы;
- рассматривает и предоставляет на утверждение правительству проекты государственных программ по защите информации;
- заслушивает руководителей министерств и ведомств, государственных предприятий и объединений, главных конструкторов по вопросам, связанным с защитой информации, и осуществляет другие важные функции.

Специальные центры при ФСТЭК осуществляют деятельность по организации работ и контролю эффективности защиты информации в пределах территориально-промышленных зон.

Федеральная служба безопасности (ФСБ) России осуществляет контроль за обеспечением в органах государственного управления и на предприятиях, ведущих работы по оборонной и другой секретной тематике, организационно-режимных мероприятий.

Федеральное агентство правительственной связи и информации организует и координирует в стране деятельность по созданию, оценке эффективности и эксплуатации криптографических средств защиты информации, обрабатываемой средствами вычислительной техники и передаваемой по каналам связи, а также организует работы по предотвращению ущерба за счет возможно внедренных в средства и объекты информатики закладных устройств. В марте 2003 г. ФАПСИ было упразднено, и его функции были переданы в ФСБ и ФСО, тем не менее, ряд нормативных актов действует в настоящее время.

Росстандарт выступает в качестве национального органа по стандартизации и сертификации продукции.

Другие органы государственного управления (министерства, ведомства) в пределах своей компетенции:

- определяют перечень охраняемых сведений;
- обеспечивают разработку и осуществление технически и экономически обоснованных мер по защите информации на подведомственных предприятиях;

- организуют и координируют проведение научно-исследовательских и опытно-конструкторских работ (НИОКР) в области защиты информации в соответствии с государственными (отраслевыми) программами;
- разрабатывают по согласованию с Гостехкомиссией отраслевые документы по защите информации;
- контролируют выполнение на предприятиях отрасли установленных норм и требований по защите информации;
- создают отраслевые центры по защите информации и контролю эффективности принимаемых мер;
- организуют подготовку и повышение квалификации специалистов по защите информации.

Для осуществления указанных функций в составе органов государственного управления функционируют научно-технические подразделения (центры) защиты информации и контроля.

На предприятиях, выполняющих оборонные и иные секретные работы, функционируют научно-технические подразделения защиты информации и контроля, координирующие деятельность в этом направлении научных и производственных структурных подразделений предприятия, участвующие в разработке и реализации мер по защите информации, осуществляющие контроль эффективности этих мер.

Кроме того, в отраслях промышленности и в регионах страны создаются и функционируют лицензионные центры, осуществляющие организацию и контроль за лицензионной деятельностью в области оказания услуг по защите информации, органы по сертификации средств вычислительной техники и средств связи, испытательные центры по сертификации конкретных видов продукции по требованиям безопасности информации, органы по аттестации объектов информатики.

Государственная система обеспечения информационной безопасности создается для решения следующих проблем, требующих законодательной поддержки:

- защита персональных данных;
- борьба с компьютерной преступностью, в первую очередь в финансовой сфере;
- защита коммерческой тайны и обеспечение благоприятных условий для предпринимательской деятельности;
- защита государственных секретов;
- создание системы взаимных финансовых расчетов в электронной форме с элементами цифровой подписи;
- обеспечение безопасности автоматизированных систем управления (АСУ) потенциально опасных производств;

- страхование информации и информационных систем;
- сертификация и лицензирование в области безопасности, контроль безопасности информационных систем;
- организация взаимодействия в сфере защиты данных со странами – членами СНГ и другими государствами.

Анализ современного состояния информационной безопасности в России показывает, что уровень ее в настоящее время не соответствует жизненно важным потребностям личности, общества и государства.

К негативным факторам, осложняющим решение задач обеспечения информационной безопасности, относятся:

- обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение;
- несовершенство нормативно-правовой базы, отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве;
- слабое обеспечение органов государственной власти и управления полной, достоверной и своевременной информацией, неразвитость информационных отношений в сфере предпринимательства;
- недостаточная защищенность государственного информационного ресурса и слабость мер по обеспечению сохранности государственных секретов в органах государственной власти и управления;
- необеспеченность прав граждан на информацию, манипулирование информацией, вызывающее неадекватную реакцию населения и ведущее в ряде случаев к политической нестабильности в обществе.

Такое положение дел в области обеспечения информационной безопасности требует безотлагательного решения ряда ключевых проблем:

1. Развитие концепции информационной безопасности, являющейся основой государственной политики в этой области.
2. Формирование законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, нормативного закрепления ответственности должностных лиц и граждан по соблюдению требований информационной безопасности.
3. Разработка механизмов реализации прав граждан на информацию.
4. Формирование системы информационной безопасности, обеспечивающей реализацию государственной политики в этой области.
5. Совершенствование методов и технических средств, обеспечивающих комплексное решение задач защиты информации.

6. Разработка критериев и методов оценки эффективности систем и средств информационной безопасности.
7. Исследование форм и способов цивилизованного воздействия государства на формирование общественного сознания.
8. Комплексное исследование деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.

Таким образом, очевидно, что для формирования эффективной системы правового обеспечения защиты информации необходима концепция, которая позволит проводить в стране единую, обеспечивающую сбалансированность интересов государства и личности, политику в области информационной безопасности.

Разработка правового обеспечения защиты информации идет по трем направлениям:

1. Защита прав личности на частную жизнь.
2. Защита государственных интересов.
3. Защита предпринимательской и финансовой деятельности.

Структура законодательной базы по вопросам информационной безопасности

Конституционные законы

Конституция РФ

Основные общие законы

– *О безопасности*
– *Об информации, информационных технологиях и защите информации*
– *Гражданский кодекс РФ*
– *Административный кодекс РФ*

Специальные законы

О защите государственной тайны

– *О государственной тайне*
– *Об участии в международном информационном обмене*

О защите интеллектуальной собственности

– *Об авторском праве и смежных правах*
– *Патентный закон*
– *О правовой охране программ для ЭВМ и баз данных*
– *О коммерческой тайне*

О защите персональных данных

– *О персональных данных*
– *Об электронной цифровой подписи*

Контрольные вопросы и упражнения

2.1. Определите понятие «государственная тайна». Обоснуйте назначение и необходимость введения нормативных документов, касающихся государственной тайны.
2.2. Перечислите сведения, составляющие государственную тайну. Почему они отнесены к ней? Конкретные сведения приводить не нужно.
2.3. Перечислите сведения, не подлежащие отнесению к государственной тайне и засекречиванию. Обоснуйте, приведите примеры.
2.4. Перечислите степени секретности сведений и грифы секретности носителей этих сведений. Чему должна соответствовать степень секретности сведений?
2.5. Какие органы защиты государственной тайны Вы знаете?
2.6. Чем отличается допуск физических лиц к работе с государственной тайной от допуска организаций?
2.7. Перечислите состав Межведомственной комиссии по защите государственной тайны. Какова ее структура?
2.8. Что предполагает собой наличие у предприятия лицензии по работе со сведениями, составляющими государственную тайну?
2.9. Перечислите сведения, относящиеся к сведениям конфиденциального характера.
2.10. Определите национальные интересы Российской Федерации в сфере информационной безопасности согласно Доктрине информационной безопасности Российской Федерации.
2.11. Какие виды угроз информационной безопасности Российской Федерации Вы знаете?
2.12. Рассмотрите источники угроз информационной безопасности Российской Федерации. Обоснуйте, приведите примеры.
2.13. Перечислите общие методы обеспечения информационной безопасности Российской Федерации. Приведете классификацию и примеры по всем указанным направлениям.
2.14. Как Вы считаете, могут ли результаты фундаментальных исследований быть угрозами национальной безопасности Российской Федерации? Обоснуйте свой ответ, приведите примеры.
2.15. Опишите право собственности на информационные системы, технологии и средства их обеспечения.
2.16. Перечислите цели защиты информации и прав субъектов в области информационных процессов и информатизации.
2.17. Укажите базовую структуру законодательной базы по вопросам информационной безопасности.

2.18. Опишите структуру государственной системы информационной безопасности.
2.19. Опишите области компетенции следующих органов по защите информации:
   а) Федеральная служба по техническому и экспортному контролю (ФСТЭК России);
   б) Федеральная служба безопасности Российской Федерации (ФСБ);
   в) Росстандарт;
   г) Министерство обороны Российской Федерации;
   д) Система внешней разведки Российской Федерации (СВР);
2.20. Деятельность в каких областях подлежит обязательному лицензированию? Приведите примеры.
2.21. Какие средства подлежат сертификации? Перечислите органы сертификации.
2.22. Подлежат ли сертификации средства иностранного производства, имеющие сертификаты стран-производителей?
2.23. Допускается ли использование несертифицированных средств защиты информации? Обоснуйте свой ответ.
2.24. Каким образом производится лицензирование в области защиты информации?
7.25. Каким образом производится сертификация в области защиты информации?
2.26. Необходимо ли сертифицировать программное обеспечение, если оно выполняет функции криптографических преобразований конфиденциальных сведений? Обоснуйте ответ.
2.27. Какие российские стандарты, действующие в области защиты информации Вы знаете?
2.28. Какие средства, имеющие сертификаты в области защиты информации Вы знаете? Приведите примеры и характеристики этих средств.
2.29. Какие условия необходимо выполнять для того, чтобы электронно-цифровая подпись на электронном документе являлась юридическим аналогом собственноручной подписи пользователя.
2.30. Какую информацию о себе Вы отнесли бы к конфиденциальной? Необходимо привести области, не приводя сами факты.

3. УГРОЗЫ БЕЗОПАСНОСТИ[2]

Угроза информации – возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию.

Виды угроз. Определив понятие «угроза государству, обществу и личности» в широком смысле, рассмотрим это понятие относительно непосредственного воздействия на конфиденциальную информацию, обрабатываемую на каком-либо объекте (кабинете, предприятии, фирме). Анализируя возможные пути воздействия на информацию, представляемую как совокупность информационных элементов, связанных между собой логическими связями.

Можно выделить основные нарушения:

1. Физической целостности (уничтожение, разрушение элементов).
2. Логической целостности (разрушение логических связей).
3. Содержания (изменение блоков информации, внешнее навязывание ложной информации).
4. Конфиденциальности (разрушение защиты, уменьшение степени защищенности информации).
5. Прав собственности на информацию (несанкционированное копирование, использование).

С учетом этого, для таких объектов систем угроза информационной безопасности представляет реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению, уничтожению конфиденциальной информации и сведений о самой системе, а также к прямым материальным убыткам. Обобщая рассмотренные угрозы можно выделить три наиболее выраженные для систем обработки информации:

1. подверженность физическому искажению или уничтожению;
2. возможность несанкционированной (случайной или злоумышленной) модификации;
3. опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначена.

---

[2] Приводится по работе [20]

Характер происхождения угроз

Угрозы безопасности информации в современных системах ее обработки определяются *умышленными (преднамеренные угрозы)* и *естественными (непреднамеренные угрозы* разрушающими и искажающими воздействиями внешней среды, надежностью функционирования средств обработки информации, а также преднамеренным корыстным воздействием несанкционированных пользователей, целью которых является хищение, уничтожение, разрушение, несанкционированная модификация и использование обрабатываемой информации. При этом под умышленными или преднамеренными понимаются такие угрозы, которые обуславливаются злоумышленными действиями людей. Случайными или естественными являются угрозы, не зависящие от воли людей. Приведем классификацию:

1. Умышленные факторы:
   1) хищение носителей информации;
   2) подключение к каналам связи;
   3) перехват электромагнитных излучений (ЭМИ);
   4) несанкционированный доступ;
   5) разглашение информации;
   6) копирование данных.
2. Естественные факторы:
   1) несчастные случаи (пожары, аварии, взрывы);
   2) стихийные бедствия (ураганы, наводнения, землетрясения);
   3) ошибки в процессе обработки информации (ошибки пользователя, оператора, сбои аппаратуры).

Источники угроз

Под источником угроз понимается непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию. Можно разделить на следующие группы:

- люди;
- технические устройства;
- модели, алгоритмы, программы;
- технологические схемы обработки;
- внешняя среда.

Предпосылки появления угроз

Существуют следующие предпосылки или причины появления угроз:

- объективные (количественная или качественная недостаточность элементов системы) причины, не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

- субъективные причины, непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

Рассмотрим некоторые определения:

Несанкционированный доступ – получение лицами в обход системы защиты с помощью программных, технических и других средств, а также в силу случайных обстоятельств доступа к обрабатываемой и хранимой на объекте информации.

Разглашение информации ее обладателем есть умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшие к не вызванному служебной необходимостью оглашению охраняемых сведений, в также передача таких сведений по открытым техническим каналам или обработка на некатегорированных ЭВМ.

Утечку информации в общем плане можно рассматривать как бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена.

Система защиты информации – совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

Классы каналов несанкционированного получения информации

Рассмотрим относительно полное множество каналов несанкционированного получения информации (КНПИ), сформированного на основе степени взаимодействия злоумышленника с элементами объекта обработки и самой информации (рис. 3). В соответствии с этим показателем КНПИ делятся на следующие классы:

1) от источника информации при несанкционированном доступе (НСД) к нему;
2) со средств обработки информаии при НСД к ним;
3) от источника информации без НСД к нему;
4) со средств обработки информации без НСД к ним.

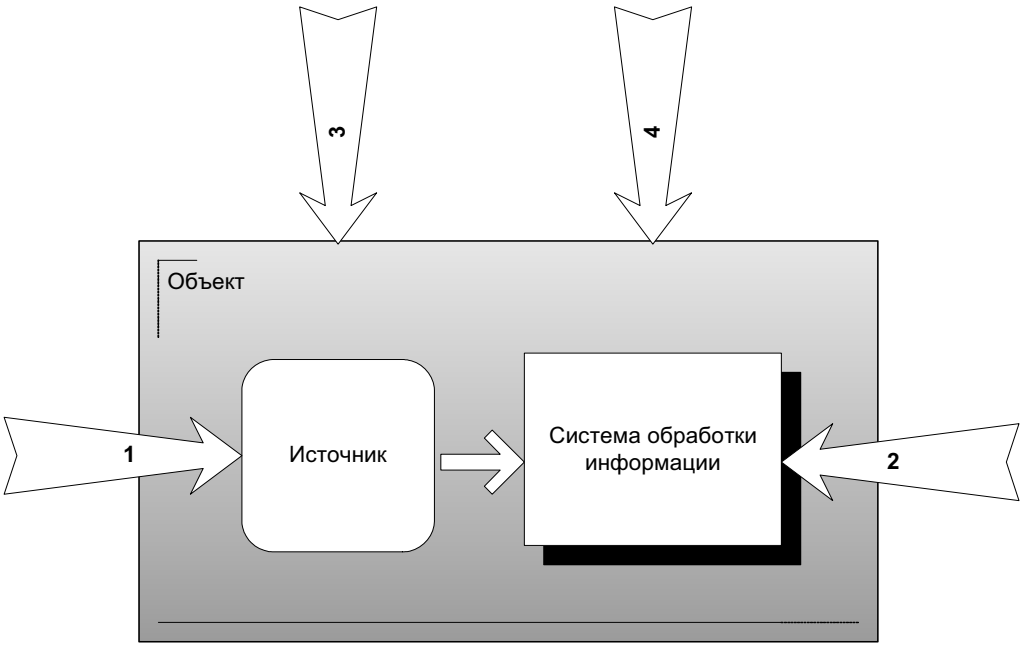


Рис. 3. Классификация КНПИ

К первому классу КНПИ относятся:

2.1. Хищение носителей информации.
2.2. Копирование информации с носителей (материально-вещественных, магнитных и т. д.).
2.3. Подслушивание разговоров (в том числе аудиозапись).
2.4. Установка закладных устройств в помещение и съем информации с их помощью.
2.5. Выведывание информации обслуживающего персонала на объекте.
2.6. Фотографирование или видеосъемка носителей информации внутри помещения.

Ко второму классу относятся:

2.1. Снятие информации с устройств электронной памяти.
2.2. Установка закладных устройств в СОИ.
2.3. Ввод программных продуктов, позволяющих злоумышленнику получать информацию.
2.4. Копирование информации с технических устройств отображения (фотографирование с мониторов и др.).

Третий класс составляют:

3.1. Получение информации по акустическим каналам (в системах вентиляции, теплоснабжения, а также с помощью направленных микрофонов).
3.2. Получение информации по виброакустическим каналам (с использованием акустических датчиков, лазерных устройств).

3.3. Использование технических средств оптической разведки (биноклей, подзорных труб и т. д.).
3.4. Использование технических средств оптико-электронной разведки (внешних телекамер, приборов ночного видения и т. д.).
3.5. Осмотр отходов и мусора.
3.6. Выведывание информации у обслуживающего персонала за пределами объекта.
3.7. Изучение выходящей за пределы объекта открытой информации (публикаций, рекламных проспектов и т. д.).

К четвертому классу относятся:

4.1. Электромагнитные излучения системы обработки информации (СОИ) (паразитные электромагнитные излучения (ПЭМИ), паразитная генерация усилительных каскадов, паразитная модуляция высокочастотных генераторов низкочастотным сигналом, содержащим конфиденциальную информацию).
4.2. Электромагнитные излучения линий связи.
4.3. Подключения к линиям связи.
4.4. Снятие наводок электрических сигналов с линий связи.
4.5. Снятие наводок с системы питания.
4.6. Снятие наводок с системы заземления.
4.7. Снятие наводок с системы теплоснабжения.
4.8. Использование высокочастотного навязывания.
4.9. Снятие с линий, выходящих за пределы объекта сигналов образованных на технических средствах за счет акустоэлектрических преобразований.
4.10. Снятие излучений оптоволоконных линий связи.
4.11. Подключение к базам данных и персональным ЭВМ по компьютерным сетям.

Причины нарушения целостности информации

В основу классификации причин нарушения целостности информации (ПНЦИ) положен показатель, характеризующий степень участия в этом процессе человека. В соответствии с таким подходом ПНЦИ делятся на два вида: объективные и субъективные:

1.1. Субъективные преднамеренные.
- 1.1.1. Диверсия (организация пожаров, взрывов, повреждений электропитания и др.).
- 1.1.2. Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации).

1.1.3. Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности психотропным оружием).

1.2. Субъективные непреднамеренные.

1.2.1. Отказы обслуживающего персонала (гибель, длительный выход из строя).

1.2.2. Сбои людей (временный выход из строя).

1.2.3. Ошибки людей.

2.1. Объективные непреднамеренные.

2.1.1. Отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

2.1.2. Сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

2.1.3. Стихийные бедствия (наводнения, землетрясения, ураганы).

2.1.4. Несчастные случаи (пожары, взрывы, аварии).

2.1.5. Электромагнитная несовместимость.

Угрозы безопасности информационных систем[3]

Угрозы информационной системе можно рассматривать с позиций их воздействия на ее характеристики, такие, в частности, как готовность системы, ее надежность и конфиденциальность.

Готовность – способность информационной системы обеспечить законным пользователям условия доступа к ресурсам в соответствии с принятым режимом работы.

Надежность – способность системы обеспечивать информационные потребности только законным пользователям в рамках их интересов.

Конфиденциальность – способность системы обеспечивать целостность и сохранность информации ее законных пользователей.

Угрозы могут также классифицироваться и по природе возникновения: стихийные бедствия, несчастные случаи (чрезвычайные происшествия), различного рода ошибки или злоупотребления, сбои и отказы оборудования и др.

Кроме того, угрозы могут быть классифицированы по ориентации на угрозы персоналу, материальным и финансовым ресурсам и информации, как составным элементам информационной системы.

---

[3] Приводится по работе [20]

Неоднократно предпринимались попытки описать различные виды угроз и воздействий на информационные системы, дать характеристику степени опасности каждой из них. Однако большинство таких попыток сводилось к описанию угроз на достаточно высоком уровне абстракции, так как описать угрозы на конкретном деятельном уровне просто не представляется возможным.

На стадии концептуальной проработки вопросов безопасности информационной системы представляется возможным рассмотрение общего состава потенциальных угроз. Конкретные перечни, связанные со спецификой информационной системы (ИС) и условий требуют определенной детализации и характерны для этапа разработки конкретного проекта системы безопасности ИС.

В общем плане к угрозам безопасности относятся:

- похищения и угрозы похищения сотрудников, персонала, членов их семей и близких родственников;
- убийства, сопровождаемые насилием, издевательствами и пытками;
- психологический террор, угрозы, запугивание, шантаж, вымогательство;
- грабежи с целью завладения денежными средствами, ценностями и документами.

Преступные посягательства в отношении помещений (в том числе и жилых), зданий и персонала проявляются в виде:

- взрывов;
- обстрелов из огнестрельного оружия, сигнальных ракетниц, ручных гранатометов;
- минирования, в том числе с применением дистанционного управления;
- поджогов, бросков канистр и иных емкостей с легко воспламеняющейся жидкостью;
- нападения, вторжения, захваты, пикетирования, блокирования;
- акты вандализма, повреждения входных дверей, решеток, ограждений, витрин, мебели, а также транспортных средств личных и служебных.

Цель подобных акций:

- откровенный террор в отношении коммерческого предприятия;
- нанесение серьезного морального и материального ущерба;
- срыв на длительное время нормального функционирования;
- вымогательство значительных сумм денег или каких-либо льгот (кредиты, отсрочка платежей и т. п.) перед лицом террористической угрозы.

Угрозы информационным ресурсам проявляются в овладении конфиденциальной информацией, ее модификации в интересах злоумышленника или ее разрушении с целью нанесения материального ущерба.

Осуществление угроз информационными ресурсами может быть произведено:

- через имеющиеся агентурные источники в органах государственного управления, коммерческих структур, имеющих возможность получения конфиденциальной информации;
- путем подкупа лиц, непосредственно работающих на предприятии или структурах, непосредственно связанных с его деятельностью;
- путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники, с помощью технических средств разведки и съема информации, несанкционированного доступа к информации и преднамеренных программно-математических воздействий на нее в процессе обработки и хранения;
- путем подслушивания конфиденциальных переговоров, ведущихся в служебных помещениях, служебном и личном автотранспорте, на квартирах и дачах;
- через переговорные процессы с иностранными или отечественными фирмами, используя неосторожное обращение с информацией;
- через инициативников из числа сотрудников, которые хотят заработать деньги и улучшить свое благосостояние или проявляют инициативу по другим моральным или материальным причинам.

К факторам, приводящим к информационным потерям и, как следствие, к различным видам убытков или ущерба можно отнести следующие причины и действия.

1. *Материальный ущерб,* связанный с несчастными случаями, вызывает частичный или полный вывод из строя оборудования или информационного ресурса. Причинами этого могут быть:

- пожары, взрывы, аварии;
- удары, столкновения, падения;
- воздействия твердых, газообразных, жидких или смешанных химических или физических сред;
- поломка элементов машин различного характера: механического, электрического, электронного и электромагнитного;
- последствия природных явлений (наводнения, бури, молнии, град, оползни, землетрясения и т. д.).

2. *Кража и преднамеренная порча материальных средств*. Воруют главным образом небольшие по габаритам аппаратные средства (мониторы, клавиатуру, принтеры, модемы, кабели и оргтехнику), инфор-

мационные носители (диски, дискеты, ленты, магнитные карты и др.) и различное другое имущество (документация, комплектующие и др.).

Посягательства и вредительские действия проявляются в самых различных формах: явные (например, оставленная отвертка внутри печатающего устройства, в корпусе вентилятора процессора) или скрытые (например, вредные химические вещества в помещениях и аппаратуре).

3. *Аварии и выход из строя аппаратуры, программ и баз данных*. Остановка или нарушение деятельности информационных центров не такие уж редкие события, а продолжительность этих состояний в основном небольшая. Но иногда прямые и косвенные последствия этих действий могут быть весьма значительными. Последствия этих действий к тому же не могут быть заранее предусмотрены и оценены.

4. *Убытки, связанные с ошибками* накопления, хранения, передачи и использования информации. Эти ошибки связаны с человеческим фактором, будь то при использовании традиционных носителей информации (дискеты, ленты) или при диалоговом обмене в режиме удаленного доступа.

При традиционных носителях цена обычной ошибки даже после уточнения может достигнуть 0,5 %. Формальный и информационный контроль позволяет уменьшить величину ущерба, но, тем не менее, число таких ошибок не уменьшается. Их последствия редко бывают весьма значительными, однако представляют собой достаточно постоянный поток и приносят постоянные потери, обусловленные поиском, устранением и последующим повторением действий, а это невосполнимые потери времени и денег.

При диалоговом режиме дополнительно прибавляются ошибки восприятия, чтения, интерпретации содержания и соблюдения правил.

Ошибки передачи зависят от используемой техники. Они могут быть простыми при использовании средств почтовой связи и чисто техническими (телепередача). В обоих случаях могут быть потери, ошибки неумения, оплошности, наличие помех, сбои и искажения отдельных букв или сообщений. Ошибки подобного рода оцениваются как потери предприятия. И хотя их трудно определить и оценить, но учитывать необходимо. Не следует недооценивать эту категорию угроз, хотя к ним довольно быстро привыкают.

5. *Ошибки эксплуатации*. Эти ошибки могут приобретать различные формы: нарушение защиты, переполнение файлов, ошибки языка управления данными, ошибки при подготовке и вводе информации, ошибки операционной системы, ошибки программы, аппаратные ошибки, ошибочное толкование инструкций, пропуск операций и т. д.

Диапазон ошибок людей значительный. Иногда трудно установить различие между ошибкой, небрежностью, утомлением, непрофессионализмом и злоупотреблением.

6. *Концептуальные ошибки и ошибки внедрения*. Концептуальные ошибки могут иметь драматические последствия в процессе эксплуатации информационной системы.

Ошибки реализации бывают в основном менее опасными и достаточно легко устранимыми.

7. *Убытки от злонамеренных действий в нематериальной сфере*. Мошенничество и хищение информационных ресурсов – это одна из форм преступности, которая в настоящее время является довольно безопасной и может принести больший доход, чем прямое ограбление банка. Между тем, учитывая сложность информационных систем и их слабые стороны этот вид действий считается достаточно легко реализуемым.

Нередко все начинается случайно, часто с небольшого правонарушения: обмана, воровства только для того, чтобы установить, что это не слишком трудное дело и в больших масштабах. Единственным препятствием остается только совесть. Мошенничество часто имеет внутренние побудительные мотивы или совершается в корыстных целях, по договоренности с третьими лицами (сотрудничество).

8. *Болтливость и разглашение*. Эти действия, последствия которых не поддаются учету, относятся к числу трудно контролируемых и могут находиться в рамках от простого, наивного хвастовства до промышленного шпионажа в коммерческой деятельности – таков их диапазон.

9. *Убытки социального характера*. Речь идет об уходе или увольнении сотрудников, забастовках и других действиях персонала, приводящих к производственным потерям и неукомплектованности рабочих мест. Опасность этих действий существует почти всегда.

Особо опасный вид угроз представляет промышленный шпионаж как форма недобросовестной конкуренции.

Промышленный шпионаж – это действия, наносящие владельцу коммерческой тайны ущерб, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, а также ее носителей лицом, не уполномоченным на это ее владельцем.

Контрольные вопросы и упражнения

3.1. Каковы основные виды угроз?
3.2. Приведите примеры нарушения физической целостности.
3.3. Является ли угрозой нарушение прав собственности на информацию? Почему?

3.4. Какие умышленные факторы происхождения угроз могут произойти в компьютерной системе?
3.5. Какие естественные факторы происхождения угроз могут произойти в компьютерной сети?
3.6. Возможно ли одновременное происхождение естественных и умышленных факторов происхождения угроз? Приведите примеры.
3.7. Кто может быть противником/злоумышленником?
3.8. Какие технологические схемы обработки банковской информации могут являться источниками угроз?
3.9. Приведите примеры нарушения конфиденциальности информации, источником которых являются компьютерные программы.
3.10. Определите каналы НСД, которые связаны непосредственно с источником информации.
3.11. К каким каналам НСД относится получение информации с монитора компьютера? Почему?
3.12. Являются ли отходы и мусор каналом НСД?
3.13. Можно ли по открытым публикациям и рекламным материалам определить область деятельности организации?
3.14. Составьте список классов каналов НСД к мобильным телефонам.
3.15. Какие причины нарушения целостности информации необходимо отнести к субъективным преднамеренным?
3.16. В каких случаях Вы отнесете пожар к каждой из категорий причин нарушения целостности информации?
3.17. Приведите примеры электромагнитной несовместимости, которая являлась бы причиной нарушения целостности банковской информации.
3.18. Чем определяются угрозы информационной системе?
3.19. Дайте определение для каждого из следующих терминов: готовность, надежность, конфиденциальность информационной системы.
3.20. В каких случаях при анализе угроз информационной системы необходимо учитывать конфиденциальность?
3.21. Что относится к угрозам безопасности сотрудников, работающих с информационной системой?
3.22. Является ли несоблюдение техники безопасности на рабочем месте угрозой информационной системе?
3.23. Какие угрозы могут быть отнесены к посягательствам на безопасность помещений, зданий?
3.24. Какова особенность угроз информационным ресурсам?
3.25. Что является материальным ущербом, связанным с несчастными случаями? Приведите список причин.
3.26. По отношению к каким элементам информационной системы производят кражи, преднамеренную порчу материальных средств?

3.27. Каковы характеристики аварий и выхода из строя аппаратуры информационной системы? Можно ли их предусмотреть?
3.28. Возможно ли оценить последствия действий аварий и выхода из строя аппаратуры? Приведите примеры для банковской сферы.
3.29. Приведите примеры ошибок, связанных с накоплением, хранением, передачей и использованием информации.
3.30. Зависят ли ошибки в информационной системе от используемой техники? В каких случаях.
3.31. Какие ошибки возникают при эксплуатации информационной системы?
3.32. Возможен ли контроль разглашения информации? Приведете примеры для сферы экономики.
3.33. Какие социальные факторы влияют на безопасность информационной системы?
3.34. Что такое промышленный шпионаж? Приведете примеры.
3.35. Какие, на Ваш взгляд, меры необходимо предпринимать в информационной системе для противодействия промышленному шпионажу?
3.36. Какие потери и угрозы информационной системе, на Ваш взгляд, являются наиболее продолжительными, после которых необходимо более длительное восстановление? Рассмотрите как материальную, так и нематериальную сферу, а также объективные и субъективные факторы.
3.37. Из каких составляющих раскладывается материальный ущерб, причиненный информационной системе?
3.38. Каковы виды дополнительных расходов, связанных с персоналом, необходимо учитывать при восстановлении работоспособности информационной системы?
3.39. Приведите примеры информационных инфекций информационной системы. Приведите описание возможных последствий.
3.40. Приведите причины остановок или выходы из строя информационных систем.
3.41. Возможно ли изменение информации в процессе передачи информации в информационной системе? Какие параметры линии передачи играют основную роль при данных нарушениях?
3.42. Опишите последовательность действий злоумышленника при маскараде в информационной системе. Для чего это нужно?
3.43. Приведите основные места вторжений в информационную систему. Какие методы вторжений вы знаете?
3.44. Приведите отличия пассивных вторжений в линии связи от активный вторжений.

4. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ[4]

Теоретические основы компьютерной безопасности являются довольно новой областью информационных технологий. Автоматизированным системам (АС) поручается решение важных для безопасности государства, общества и отдельного человека задач, например охрана государственных секретов, управление атомными станциями, электронные банковские расчеты. В связи с этим нет необходимости доказывать, что без решения комплекса задач защиты АС будут нести в себе постоянную угрозу.

Проблема защиты информации в АС с момента формулирования в середине 70-х годов до современного состояния прошла длительный и во многом противоречивый путь. Первоначально существовали два направления решения задачи поддержания конфиденциальности: использование криптографических методов защиты информации в средах передачи и хранения данных и программно-техническое разграничение доступа к данным и ресурсам вычислительных систем.

Позднее с появлением тенденции к распределенной обработке информации (проект ARPANET и последующие разработки) классический подход к организации разделения ресурсов и классические криптографические протоколы начинают постепенно исчерпывать себя и эволюционировать.

Проблематика защиты информации в середине 80-х все более явно разделяется на несколько направлений: формулирование и изучение свойств теоретических моделей безопасности АС – анализ моделей безопасного взаимодействия, рассматривающих различные аспекты криптографической защиты, теория создания качественных программных продуктов. На сегодняшний день такое положение продолжает сохраняться, а «лавинообразное» появление новых программных продуктов порождает определенный кризис в решении практических вопросов

[4] Приводится по работе [19]

при проектировании систем защиты. Так, новые технологические решения в АС (в первую очередь связанные с распределенностью), например механизм удаленного вызова процедур или технология типа «клиент-сервер», в теоретических работах пока отражены недостаточно.

В начале 80-х годов возникает ряд моделей защиты, основанных на декомпозиции автоматизированной системы обработки информации на субъекты и объекты, модели Белла-ЛаПадула (Bell-LaPadula), модель Take-Grant и т. д. В данных моделях ставятся и исследуются вопросы взаимодействия элементов системы с заданными свойствами. Целью анализа и последующей реализации модели является именно достижение таких свойств системы, как конфиденциальность и доступность. Как правило, та или иная модель безопасности исходит из априорной технологии работы с объектами (так, полномочное управление моделирует структуру секретного делопроизводства), которая может быть формализована и обоснована. При практической реализации данных моделей в конкретных АС встал вопрос о гарантиях выполнения их свойств (фактически это выполнение условий тех или иных утверждений, обосновывающих свойства формализованной модели). В связи с этим в зарубежной литературе формулируется понятие доверенной (достоверной) вычислительной базы (в английской транскрипции TCB), гарантирующей свойства системы.

Необходимо также упомянуть о том, что существующая методология проектирования защищенной системы представляет собой итеративный процесс устранения найденных слабостей, некорректностей и неисправностей.

С середины 80-х годов несовершенство западной методологии было замечено российскими специалистами и отражено в ряде работ. С этого времени намечается тенденция к появлению комплексных решений в области проектирования и реализации механизмов защиты АС.

В 1991 г. В.А. Герасименко предложил модель системно-концептуального подхода к безопасности, которая описывает методологию анализа и синтеза системы безопасности, исходя из комплексного взаимодействия ее компонентов, рассматриваемых как система. Результатам изучения является также совокупность системно-связанных рекомендаций по решению проблемы.

В 1996 г. в классической работе Грушо А.А. и Тимониной Е.Е. «Теоретические основы защиты информации» высказан и обоснован тезис о том, что гарантированную защищенность в автоматизированной системе следует понимать как гарантированное выполнение априорно заданной политики безопасности. В указанной работе также приведены примеры гарантированных политик. С другой стороны, в моделях АС,

как правило, редуцируется порождение субъектов, которому в реальных системах соответствует порождение процессов и запуск программ. Очевидно, что данное допущение в определенной степени снижает достоверность модели, поскольку порождение субъектов существенно влияет на свойства защищенности.

Математическая модель политики безопасности рассматривает систему защиты в некотором стационарном состоянии, когда действуют защитные механизмы, а описание разрешенных или неразрешенных действий не меняется. На практике АС обработки информации проходит путь от отсутствия защиты к полному оснащению защитными механизмами, при этом система управляется, т. е. разрешенные и неразрешенные действия в ней динамически изменяются.

Таким образом, основной особенностью информационной безопасности АС являлась, да и сейчас является, ее практическая направленность. Большинство положений сначала реализовывалось в виде конкретных схем и рекомендаций, а уж затем обобщалось и фиксировалось в виде теоретических положений или методических рекомендаций. Другой особенностью информационной безопасности АС была на первых этапах развития значительная зависимость теоретических разработок от конкретных способов реализации АС, определявшихся проектными программными или аппаратными решениями. Как можно заметить, данная особенность связана с предыдущей: особенности реализации той или иной АС определяют возможные виды атак, а следовательно, те или иные необходимые защитные меры. На настоящий момент эти две особенности АС в определенной степени нивелированы, что позволяет перейти к разработке системонезависимых теоретических положений, на основании которых будут реализовываться проекты различных АС.

Модель контроля целостности Кларка-Вилсона

Модель Кларка-Вилсона появилась в результате проведенного авторами анализа реально применяемых методов обеспечения целостности документооборота в коммерческих компаниях. В отличие от моделей Биба и Белла-Лападулы, она изначально ориентирована на нужды коммерческих заказчиков, и, по мнению авторов, более адекватна их требованиям, чем предложенная ранее коммерческая интерпретация модели целостности на основе решеток. Основные понятия рассматриваемой модели – это корректность транзакций и разграничение функциональных обязанностей. Модель задает правила функционирования компьютерной системы и определяет две категории объектов данных и два класса операций над ними.

Все содержащиеся в системе данные подразделяются на контролируемые и неконтролируемые элементы данных (constrained data items – CDI и unconstrained data items – UDI соответственно). Целостность первых обеспечивается моделью Кларка-Вилсона. Последние содержат информацию, целостность которой в рамках данной модели не контролируется (этим и объясняется выбор терминологии).

Далее, модель вводит два класса операций над элементами данных: процедуры контроля целостности (integrity verification procedures – IVP) и процедуры преобразования (transformation procedures – TP). Первые из них обеспечивают проверку целостности контролируемых элементов данных (CDI), вторые изменяют состав множества всех CDI (например, преобразуя элементы UDI в CDI).

Наконец, модель содержит девять правил, определяющих взаимоотношения элементов данных и процедур в процессе функционирования системы.

Правило C1. Множество всех процедур контроля целостности (IVP) должно содержать процедуры контроля целостности любого элемента данных из множества всех CDI.

Правило C2. Все процедуры преобразования (TP) должны быть реализованы корректно в том смысле, что не должны нарушать целостность обрабатываемых ими CDI. Кроме того, с каждой процедурой преобразования должен быть связан список элементов CDI, которые допустимо обрабатывать данной процедурой. Такая связь устанавливается администратором безопасности.

Правило E1. Система должна контролировать допустимость применения TP к элементам CDI в соответствии со списками, указанными в правиле C2.

Правило E2. Система должна поддерживать список разрешенных конкретным пользователям процедур преобразования с указанием допустимого для каждой TP и данного пользователя набора обрабатываемых элементов CDI.

Правило C3. Список, определенный правилом C2, должен отвечать требованию разграничения функциональных обязанностей.

Правило E3. Система должна аутентифицировать всех пользователей, пытающихся выполнить какую-либо процедуру преобразования.

Правило C4. Каждая TP должна записывать в журнал регистрации информацию, достаточную для восстановления полной картины каждого применения этой TP. Журнал регистрации – это специальный элемент CDI, предназначенный только для добавления в него информации.

Правило С5. Любая ТР, которая обрабатывает элемент UDI, должна выполнять только корректные преобразования этого элемента, в результате которых UDI превращается в CDI.

Правило Е4. Только специально уполномоченное лицо может изменять списки, определенные в правилах С2 и Е2. Это лицо не имеет права выполнять какие-либо действия, если оно уполномочено изменять регламентирующие эти действия списки.

Публикация описания модели Кларка-Вилсона вызвала широкий отклик среди исследователей, занимающихся проблемой контроля целостности. В ряде научных статей рассматриваются практические аспекты применения модели, предложены некоторые ее расширения и способы интеграции с другими моделями безопасности.

Роль каждого из девяти правил модели Кларка-Вилсона в обеспечении целостности информации можно пояснить, показав, каким из теоретических принципов политики контроля целостности отвечает данное правило. Напомним, что первые шесть из сформулированных выше принципов это:

1) корректность транзакций;
2) аутентификация пользователей;
3) минимизация привилегий;
4) разграничение функциональных обязанностей;
5) аудит произошедших событий;
6) объективный контроль.

Соответствие правил модели Кларка-Вилсона перечисленным принципам показано в табл. 2. Как видно из табл. 2, принципы 1 (корректность транзакций) и 4 (разграничение функциональных обязанностей) реализуются большинством правил, что соответствует основной идее модели.

Таблица 2

Правило модели Кларка-Вилсона	Принципы политики контроля целостности, реализуемые правилом
С1	1, 6
С2	1
Е1	3, 4
Е2	1, 2, 3, 4
С3	4
Е3	2
С4	5
С5	1
Е4	4

Теория безопасных систем (TCB)

Понятие «доверенная вычислительная среда» (trusted computing base – TCB) появилось в зарубежной практике обеспечения информационной безопасности достаточно давно. Смысл характеристики «доверенная» можно пояснить следующим образом.

Дискретная природа характеристики «безопасный» (в том смысле, что либо нечто является безопасным, полностью удовлетворяя ряду предъявляемых требований, либо не является, если одно или несколько требований не выполнены) в сочетании с утверждением «ничто не бывает безопасным на сто процентов» подталкивают к тому, чтобы вести более гибкий термин, позволяющий оценивать то, в какой степени разработанная защищенная АС соответствует ожиданиям заказчиков. В этом отношении характеристика «доверенный» более адекватно отражает ситуацию, где оценка, выраженная этой характеристикой (безопасный или доверенный), основана не на мнении разработчиков, а на совокупности факторов, включая мнение независимой экспертизы, опыт предыдущего сотрудничества с разработчиками, и в конечном итоге, является прерогативой заказчика, а не разработчика.

Доверенная вычислительная среда (TCB) включает все компоненты и механизмы защищенной автоматизированной системы, отвечающие за реализацию политики безопасности. Все остальные части АС, а также ее заказчик полагаются на то, что TCB корректно реализует заданную политику безопасности даже в том случае, если отдельные модули или подсистемы АС разработаны высококвалифицированными злоумышленниками с тем, чтобы вмешаться в функционирование TCB и нарушить поддерживаемую ею политику безопасности.

Минимальный набор компонентов, составляющий доверенную вычислительную среду, обеспечивает следующие функциональные возможности:

- взаимодействие с аппаратным обеспечением АС;
- защиту памяти;
- функции файлового ввода-вывода;
- управление процессами.

Дополнение и модернизация существующих компонентов АС с учетом требований безопасности могут привести к усложнению процессов сопровождения и документирования. С другой стороны, реализация всех перечисленных функциональных возможностей в рамках централизованной доверенной вычислительной среды в полном объеме может вызвать разрастание размеров TCB и, как следствие, усложнение доказательства корректности реализации политики безопасности. Так, опе-

рации с файлами могут быть реализованы в ТСВ в некотором ограниченном объеме, достаточном для поддержания политики безопасности, а расширенный ввод-вывод в таком случае реализуется в той части АС, которая находится за пределами ТСВ. Кроме того, необходимость внедрения связанных с безопасностью функций во многие компоненты АС, реализуемые в различных модулях АС, приводит к тому, что защитные функции распределяются по всей АС, вызывая аналогичную проблему.

Представляется оправданной реализация доверенной вычислительной среды в виде небольшого и эффективного (в терминах исполняемого кода) ядра безопасности, где сосредоточены все механизмы обеспечения безопасности. В связи с перечисленными выше соображениям, а также с учетом определенной аналогии между данными понятиями такой подход предполагает изначальное проектирование АС с учетом требований безопасности. При этом в рамках излагаемой теории определены следующие этапы разработки защищенной АС:

- определение политики безопасности;
- проектирование модели АС;
- разработка кода АС;
- обеспечение гарантий соответствия реализации заданной политике безопасности.

Понятие политики безопасности

Рассматривая вопросы безопасности информации в АС, можно говорить о наличии некоторых «желательных» состояний данных систем. Эти желательные состояния (представленные в терминах модели собственно АС, например в терминах субъектно-объектной модели, которая будет рассмотрена ниже) описывают «защищенность» системы. Понятие «защищенности» принципиально не отличается от любых других свойств технической системы, например «надежной работы», и является для системы внешним, априорно заданным. Особенностью понятия «защищенность» является его тесная связь с понятиями «злоумышленник» (как обозначение внешней причины для вывода системы из состояния «защищенности») или «угроза» (понятие, обезличивающее причину вывода системы из защищенного состояния действиями злоумышленника).

При рассмотрении понятия «злоумышленник» практически всегда выделяется объект его воздействия – часть системы, на которую направлены те или иные его действия («объект атаки»). Следовательно, можно выделить три компонента, связанные с нарушением безопасности системы:

- **«злоумышленник»** – внешний по отношению к системе источник нарушения свойства «безопасность»;

- **«объект атаки»** – часть, принадлежащая системе, на которую злоумышленник производит воздействие;
- **«канал воздействия»** – среда переноса злоумышленного воздействия.

Иногда удается достичь общепринятого понимания оптимальности принимаемого решения и доказать его существование. Например, в математической статистике для проверки простой гипотезы против простой альтернативы всеми признано понятие оптимального решения, которое минимизирует ошибку второго рода, а также доказано существование такого критерия (лемма Неймана-Пирсона). Однако, когда решение многоальтернативное, то общепринятого понимания оптимальности не получается, а в тех случаях, когда рассматривается вопрос об оптимальном в каком-то смысле решении, то его существование, чаще всего, удается доказать лишь в частных задачах.

Подобная ситуация существует в задачах защиты информации, поскольку неоднозначно решение о том, что информация защищена. Кроме того, система защиты – не самоцель и должна нести подчиненную функцию по сравнению с главной целью вычислительного процесса.

Результатом решения в задачах защиты информации является выбор правил распределения и хранения информации, а также обращения с информацией, что и называется политикой безопасности. Соблюдение политики безопасности должно обеспечить выполнение того компромисса между альтернативами, который выбрали владельцы ценной информации для ее защиты. Ясно, что, являясь результатом компромисса, политика безопасности никогда не удовлетворит все стороны, участвующие во взаимодействии с защищаемой информацией. В тоже время выбор политики безопасности – это окончательное решение проблемы: что хорошо и что плохо в обращении с ценной информацией. После принятия такого решения можно строить защиту, то есть систему поддержки выполнения правил политики безопасности. Таким образом, построенная система защиты информации хорошая, если она надежно поддерживает выполнение правил политики безопасности. Наоборот, система защиты информации – плохая, если она ненадежно поддерживает политику безопасности.

Такое решение проблемы защищенности информации и проблемы построения системы защиты позволяет привлечь в теорию защиты точные математические методы. То есть доказывать, что данная система в заданных условиях поддерживает политику безопасности. В этом суть доказательного подхода к защите информации, позволяющего говорить о «гарантированно защищенной системе». Смысл «гарантированной защиты» в том, что при соблюдении исходных условий заведомо выполняются все правила политики безопасности. Термин «гарантированная защита» впервые встречается в стандарте министерства обороны США на требования к защищенным системам («Оранжевая книга»).

Интегральной характеристикой защищаемой системы является **политика безопасности** – качественное (или качественно-количественное) выражение свойств защищенности в терминах, представляющих систему. Описание политики безопасности может включать или учитывать свойства злоумышленника и объекта атаки. Приведем пример. Наиболее часто рассматриваются политики безопасности, связанные с понятием «доступ». **Доступ** – категория субъектно-объектной модели, описывающая процесс выполнения операций субъектов над объектами.

Политика безопасности включает:

- множество возможных операций над объектами;
- для каждой пары «субъект, объект» (S_i, O_j) множество разрешенных операций, являющихся подмножеством всего множества возможных операций.

Операции связаны обычно с целевой функцией защищаемой системы (т. е. с назначением системы и решаемыми задачами). Например, операции «создание объекта», «удаление объекта», «перенос информации от произвольного объекта к предопределенному объекту» (операция «чтения») и т. д.

Можно сформулировать три аксиомы защищенных АС.

Аксиома 1. В защищенной АС всегда присутствует активный компонент (субъект), выполняющий контроль операций субъектов над объектами.

Этот компонент фактически отвечает за реализацию некоторой политики безопасности.

Аксиома 2. Для выполнения в защищенной АС операций над объектами необходима дополнительная информация (и наличие содержащего ее объекта) о разрешенных и запрещенных операциях субъектов с объектами.

Аксиома 3. Все вопросы безопасности информации в АС описываются доступами субъектов к объектам.

Важно заметить, что политика безопасности выражает в общем случае нестационарное состояние защищенности. Защищаемая система может изменяться, дополняться новыми компонентами (субъектами, объектами, операциями субъектов над объектами). Очевидно, что политика безопасности должна быть поддержана во времени, следовательно, в процесс изучения свойства защищаемой системы должны быть определены процедуры **управления безопасностью**.

С другой стороны, нестационарность защищаемой АС, а также вопросы реализации политики безопасности в конкретных конструкциях защищаемой системы (например, программирование контролирующего субъекта в командах конкретного процессора) предопределяют необхо-

димость рассмотрения задачи **гарантирования заданной политики безопасности**.

Будем следовать общепринятому определению политики безопасности (ПБ), приведенному в стандарте «Оранжевая книга» (1985 г.).

Определение. Политика безопасности – это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Полное описание ПБ достаточно объемно даже в простых случаях. Существуют два типа политики безопасности: дискреционная и мандатная.

Основой дискреционной (дискретной) политики безопасности является дискреционное управление доступом (Discretionary Access Control – DAC), которое определяется двумя свойствами:

- все субъекты и объекты должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила.

Термин «дискреционная политика» является дословным переводом Discretionary policy, еще одним вариантом перевода является следующий – разграничительная политика. Рассматриваемая политика – одна из самых распространенных в мире, в системах по умолчанию имеется ввиду именно эта политика.

К достоинствам дискреционной политики безопасности можно отнести относительно простую реализацию соответствующих механизмов защиты. Этим обусловлен тот факт, что большинство распространенных в настоящее время АС обеспечивают выполнение положений именно данной политики безопасности.

В качестве примера реализаций дискреционной политики безопасности в АС можно привести матрицу доступов, строки которой соответствуют субъектам системы, а столбцы – объектам; элементы матрицы характеризуют права доступа. К недостаткам относится статичность модели. Это означает, что данная политика безопасности не учитывает динамику изменений состояния АС, не накладывает ограничений на состояния системы.

Кроме этого, при использовании дискреционной политики безопасности возникает вопрос определения правил распространения прав доступа и анализа их влияния на безопасность АС.

Основу мандатной (полномочной) политики безопасности составляет мандатное управление доступом (Mandatory Access Control – MAC), которое подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- задан линейно упорядоченный набор меток секретности;

- каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации – его уровень секретности в АС;
- каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в АС – максимальное значение метки секретности объектов, к которым субъект имеет доступ; метка секретности субъекта называется его уровнем доступа.

Основная цель мандатной политики безопасности – предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнен доступа, т. е. противодействие возникновению в АС информационных каналов сверху вниз.

Чаще всего мандатную политику безопасности описывают в терминах, понятиях и определениях свойств модели Белла-ЛаПадула. В рамках данной модели доказывается важное утверждение, указывающее на принципиальное отличие систем, реализующих мандатную защиту, от систем с дискреционной защитой: если начальное состояние системы безопасно, и все переходы системы из состояния в состояние не нарушают ограничений, сформулированных политикой безопасности, то любое состояние системы безопасно.

Кроме того, по сравнению с АС, построенными на основе дискреционной политики безопасности, для систем, реализующих мандатную политику, характерна более высокая степень надежности. Таким образом, каналы утечки в системах данного типа не заложены в нее непосредственно, а могут появиться только при практической реализации системы вследствие ошибок разработчика. В дополнении к этому, правила мандатной политики безопасности более ясны и просты для понимания разработчиками и пользователями АС, что также является фактором, положительно влияющим на уровень безопасности системы. С другой стороны, реализация систем с политикой безопасности данного типа довольно сложна и требует значительных ресурсов вычислительной системы.

Политика MLS

Название происходит от аббревиатуры Multilevel Security и лежит в основе государственных стандартов оценки информации. Решетка строится как прямое произведение линейной решетки L и решетки SC подмножеств множества X, т. е. (α, β), (α', β') – элементы произведения, $\beta, \beta' \in L$ – линейная решетка, $\alpha, \alpha' \in SC$ – решетка подмножеств некоторого множества X. Тогда

$$(\alpha, \beta) < (\alpha', \beta') \Leftrightarrow \alpha \subseteq \alpha', \beta < \beta'.$$

Верхняя и нижняя границы определяются следующим образом:

$$(\alpha, \beta) \oplus (\alpha', \beta') \Leftrightarrow (\alpha \cup \alpha', \max\{\beta, \beta'\}),$$
$$(\alpha, \beta) \otimes (\alpha', \beta') \Leftrightarrow (\alpha \cap \alpha', \min\{\beta, \beta'\}).$$

Вся информация {объекты системы} отображается в точки решетки $\{(\alpha, \beta)\}$. Линейный порядок, как правило, указывает гриф секретности. Точки множества X обычно называются категориями.

Многоуровневая политика безопасности (политика MLS) принята всеми развитыми государствами мира. В повседневном секретном делопроизводстве госсектор России также придерживается этой политики.

Решетка ценностей *SC* является основой политики MLS. Другой основой этой политики является понятие информационного потока. Для произвольных объектов *X* и *Y* пусть имеется информационный поток $X \to \alpha Y$, где *X* – источник, *Y* – получатель информации. Отображение: $O \to SC$ считается заданным. Если $C(Y) > C(X)$, то *Y* – более ценный объект, чем *X*.

MLS политика в современных системах защиты реализуется через мандатный контроль (или, также говорят, через мандатную политику). Мандатный контроль реализуется подсистемой защиты на самом низком аппаратно-программном уровне, что позволяет эффективно строить защищенную среду для механизма мандатного контроля. Устройство мандатного контроля, удовлетворяющее некоторым дополнительным, кроме перечисленных, требованиям, называется монитором обращений. Мандатный контроль еще называют обязательным, так как его проходит каждое обращение субъекта к объекту, если субъект и объект находятся под защитой системы безопасности. Организуется мандатный контроль следующим образом. Каждый объект *O* имеет метку с информацией о классе $c(O)$. Каждый субъект также имеет метку, содержащую информацию о том, какой класс доступа $c(S)$ он имеет. Мандатный контроль сравнивает метки и удовлетворяет запрос субъекта *S* к объекту *O* на чтение, если $c(S) > c(0)$ и удовлетворяет запрос на запись, если $c(S) < c(O)$. Тогда согласно изложенному выше мандатный контроль реализует политику MLS.

Политика MLS создана, в основном, для сохранения секретности информации. Вопросы целостности при помощи этой политики не решаются или решаются как побочный результат защиты секретности.

Модель «Take-Grant»

Задача об условиях, при которых в системе некоторый субъект рано или поздно получит требуемый ему доступ, исследовалась в модели «take-grant», когда форма передачи или взятия прав определяются в виде специального права доступа.

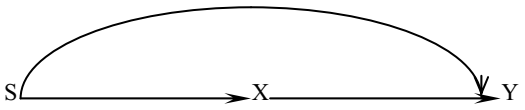
Описываем функционирование системы при помощи графов доступов G_t и траекторий в фазовом пространстве $\varsigma = \{G\}$. Единственное

дополнение – правила преобразования графов. Будем считать, что множество доступов $R = \{r, w, c\}$, где r – читать, w – писать, c – вызывать. Допускается, что субъект X может иметь права $\alpha \subseteq R$ на доступ к объекту Y, эти права записываются в матрице контроля доступов. Опишем еще два права: право take (t) и право grant (g), которые также записываются в матрицу контроля доступов субъекта к объектам. Можно считать, что эти права определяют возможности преобразования одних графов состояний в другие. Преобразование состояний, то есть преобразование графов доступов, проводятся при помощи команд. Существует 4 вида команд, по которым один граф доступа преобразуется в другой.

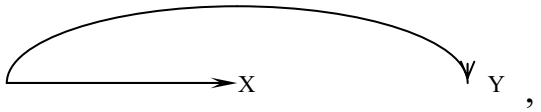
1. **Take.** Пусть S – субъект, обладающий правом t к объекту X и $\alpha \subseteq R$ некоторое право доступа объекта X к объекту Y. Тогда возможна команда «S take α for$Y$ from X». В результате выполнения этой команды в множество прав доступа субъекта S к объекту Y добавляется право α. Графически это означает, что, если в исходном графе доступов G был подграф

$$S \xrightarrow{t} X \xrightarrow{\alpha} Y ,$$

то в новом состоянии G', построенном по этой команде t, будет подграф

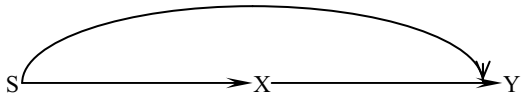


2. **Grant.** Пусть субъект S обладает правом g к объекту X и правом $\alpha \subseteq R$ к объекту Y. Тогда возможна команда «S grant α for Y to X». В результате выполнения этой команды граф доступов G преобразуется в новый граф G', который отличается от G добавленной дугой (X Y). Графически это означает, что если в исходном графе G был подграф



,

то в новом состоянии G' будет подграф



.

3. **Create.** Пусть S – субъект, $\beta \subseteq R$. Команда «S create P for new object X» создает в графе новую вершину X и определяет P как права доступов S к X. То есть по сравнению с графом G в новом состоянии G' добавляется подграф вида

$$S \xrightarrow{\beta} X.$$

4. **Remove.** Пусть S – субъект и X – объект, $\beta \subseteq R$. Команда «S remove P for X» исключает права доступа P из прав субъекта S к объекту X. Графически преобразования графа доступа G в новое состояние G' в результате этой команды можно изобразить следующим образом:

$$\underset{\text{в } G}{S \xrightarrow{p} X}, \quad \underset{\text{в } G}{S \xrightarrow{p/\beta} X}.$$

Модель Белла-ЛаПадула *(Б-Л)*

Модель Белла-Лападула препятствует чтению пользователей и процессов данных, имеющих уровень секретности выше их прав в системе.

Модель Б-Л построена для обоснования безопасности систем, использующих политику MLS. Пусть определены конечные множества S, O, R, L:

S – множество субъектов системы;

O – множество объектов, не являющихся субъектами;

R – множество прав доступа; R = {read (r), write(w), execute (e), append (a)};

L – уровни секретности.

Множество V состояний системы определяется произведением множеств:

$$V = B \times M \times F \times H ,$$

где сомножители определяются следующим образом. B – множество текущих доступов и есть подмножество множества подмножеств произведения $S \times O \times R$. Множество подмножеств будем обозначать $P(S \times O \times R)$ элементы множества B будем обозначать b и они представляют в текущий момент t графы текущего доступа (в каждый момент субъект может иметь только один вид доступа к данному объекту).

M – матрица разрешенных доступов, $M = |M_{ij}|$, $M_{ij} \subseteq R$. F – подмножество множества $L^s \times L^s \times L^0$, где каждый $f = (f_s, f_0, f_c), f \in F$, – вектор, который состоит из трех компонент, каждая из которых тоже вектор (или отображение); f_s – уровень допуска субъектов (это некоторое отображение f: S - >L); f_o – уровень секретности объектов (это некоторое отображение f: O – > L); f_c – текущий уровень секретности субъектов (это тоже некоторое отображение f_c: $S \rightarrow L$).

Элементы подмножества F, которые допущены для определения состояния, должны удовлетворять соотношению:

$$\forall S \in Sf_s(S) \geq f_c(S),$$

H – текущий уровень иерархии объектов, в работе McLean этот уровень не изменяется, совпадает с f_0 и далее не рассматривается.

Элементы множества V состояний будут обозначаться через v. Пусть определены множество Q – запросов в систему и множество D – решений по поводу этих запросов (D = {yes, no, error}). Определим множество W действий системы как

$$W \subseteq Q \times D \times V \times V = \{(q, d, v_2, v_1)\}.$$

Каждое действие системы (q, d, v_2, v_1) имеет следующий смысл: если система находилась в данный момент в состоянии v_1, поступил запрос q, то принято решение d и система перешла в состояние v_2.

Модель Biba

Одной из первых моделей была опубликованная в 1977 г. модель Biba. Согласно ей все субъекты и объекты предварительно разделяются по нескольким уровням доступа, а затем на их взаимодействия накладываются следующие ограничения:

1. Субъект не может вызывать на исполнение субъекты с более низким уровнем доступа;
2. Субъект не может модифицировать объекты с более высоким уровнем доступа.

Предположим, что опасности для нарушения секретности не существует, а единственная цель политики безопасности – защита от нарушений целостности информации. Пусть по-прежнему в информацию внесена решетка ценностей SC. В этой связи любой информационный поток $X \rightarrow Y$ может воздействовать на целостность объекта Y и совершенно не воздействовать на целостность источника X. Если в Y более ценная информация, чем в X, то такой поток при нарушении целостности Y принесет более ощутимый ущерб, чем поток в обратном направлении от более ценного объекта Y к менее ценному X. Biba предложил в качестве политики безопасности для защиты целостности следующее.

Определение. В политике Biba информационный поток $X \rightarrow \alpha Y$ разрешен тогда и только тогда, когда

$$c(Y) \leq c(X).$$

Можно показать, что в широком классе систем эта политика эквивалентна следующей.

Определение. Для систем с доступами w и r политика Biba разрешает доступ в следующих случаях:

$$S \xrightarrow{r} O \Leftrightarrow c(S) \le c(O),$$

$$S \xrightarrow{w} O \Leftrightarrow c(S) \ge c(O).$$

Очевидно, что для реализации этой политики также подходит мандатный контроль.

Модель Sutherland

Сазерлендская модель защиты, опубликованная в 1986 г., делает акцент на взаимодействии субъектов потоков информации. Используется машина состояний со множеством разрешенных комбинаций состояний и некоторым набором начальных позиций. В данной модели исследуется поведение множественных композиций функций перехода из одного состояния в другое.

Модель Low-Water-Mark (lwm)

Данная модель является конкретизацией модели Б-Л, а также дает пример того, что происходит, когда изменения уровня секретности объекта возможны. Политика безопасности прежняя: все объекты системы классифицированы по узлам решетки ценностей (MLS) и поток информации разрешен только «снизу вверх».

В рассматриваемой системе один объект (неактивный), три операции с объектом, включающие запросы на доступ: read, write, reset.

Эти операции используются несколькими субъектами (процессами), имеющими фиксированные уровни секретности (для простоты – классы секретности образуют линейный порядок). Напомним формальное требование политики о том, что информация может двигаться только «снизу вверх». Поток информации возможен тогда и только тогда, когда реализуется доступ субъекта к объекту вида *w* или *r*. При помощи r поток считается разрешенным, если $f_s(S) > f_o(0)$.

При команде w поток считается разрешенным, если субъект *S* не может прочитать информацию в объекте уровня $f_s(S) < f_0(0)$ и записать в объект, для которого $f_s(S) > f_0(O)$, хотя бы в одном из этих соотношений неравенство строгое (напомним, что по условию текущие уровни субъектов $f_c(S) = f_s(S)$ для любого *S*). Из этих свойств следует, что в системе должны выполняться условия *ss* и *. Условие *ds* автоматически выполняется, так как нет ограничений на доступ, кроме перечисленных выше.

Таким образом, условия ss в данной системе выглядят стандартно: если $X = w$ или *r*, то могут быть разрешены доступы (*S*, *O*, *X*) при выполнении $f_s(S) > f_0(O)$.

Условие *:

если $X = w$, то $f_s(S) = f_0(O)$,

если $X = r$, то $f_s(S) > f_o(O)$.

Контрольные вопросы и упражнения

4.1. Назовите основные положения и направления развития теории информационной безопасности информационных систем.
4.2. В каких случаях используются модели безопасности?
4.3. Перечислите базовые представления моделей безопасности.
4.4. Приведите основные положения дискреционной модели Харрисона-Руззо-Ульмана.
4.5. В чем проявилось развитие от модели Харрисона-Руззо-Ульмана к модели типизованной матрицы доступа?
4.6. Приведите основные положения модели распространения прав доступа Take-Grant.
4.7. Приведите основные положения модели Белла-ЛаПадула.
4.8. Приведите основные положения ролевой политики безопасности и критерий безопасности.
4.9. Какие ограничения должны быть учтены при применении формальных моделей безопасности?
4.10. Какие рекомендации Вы бы дали при использовании формальных моделей безопасности?

5. МЕТОДЫ ЗАЩИТЫ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ[5]

Для несанкционированного получения информации наиболее вероятными являются следующие варианты атак:

1. Атака целевым вирусом (закладкой).
2. Атака общим вирусом.

Против атак можно применить различные проверки целостности программного обеспечения (ПО), которые, в свою очередь, могут быть нейтрализованы стелс-механизмами вирусов, и т. д. Можно предложить универсальную закладку, работающую в защищенном режиме микропроцессора (МП), блокирующую всякого рода попытки программ пользователя переключиться в защищенный режим и эмулирующую все известные способы обращения к расширенной памяти. При таком подходе любые способы контроля целостности ПО не дадут корректного результата. Из вышесказанного следует:

Утверждение 1: гарантированно корректно работает та программа (закладка или средство защиты от нее), которая первой получает управление.

Для гарантированно корректной работы средств защиты от закладок необходимо проверять целостность программных файлов до начала работы программы первичного загрузчика.

Для обеспечения невозможности доступа к информации на компьютере применяют «электронные замки». В частности, фирмы-разработчики BIOS предлагают парольную защиту входа в компьютер, при этом пароль хранится в виде свертки в энергонезависимой памяти компьютера (CMOS). Такая защита неэффективна, так как в случае получения доступа к включенному компьютеру можно считать содержимое CMOS и тем самым получить доступ к информации о пароле. Отсюда следует:

Утверждение 2: для гарантированной работы электронного замка достаточно, чтобы программа защиты от закладок и свертка пароля были аппаратно защищены от чтения программными средствами во время работы компьютера.

---

[5] Приводится по работе [19]

Удаленный НСД по сети без доступа непосредственно к компьютеру

Во многих областях приходится пользоваться зарубежным программным обеспечением и аппаратными средствами передачи информации по сети с коммутацией пакетов. Ряд фирм (например HP) ставят связные сервера вместе с программным обеспечением «под ключ», при этом еще и блокируя интерфейс администратора. В этом случае для гарантированной защиты обрабатываемой информации важно, с одной стороны, чтобы управление средствами шифрования не зависело от импортного программного обеспечения, а с другой – чтобы средства защиты были по возможности «прозрачными» по отношению к средствам обработки информации.

При отсутствии отечественных операционных систем можно говорить лишь о передаче конфиденциальной информации по виртуальным сетям. Под виртуальной сетью понимается сеть, образованная множеством криптомаршрутизаторов, использующих Internet как транспортную среду передачи данных. Каждый криптомаршрутизатор защищает свою подсеть посредством зашифрования исходящих и расшифрования входящих пакетов. Криптомаршрутизаторы обмениваются информацией, зашифрованной на ключах парной связи между ними. Обмен ключами по сети отсутствует. Для закрытия информации эксплуатируется принцип инкапсуляции со скрытием внутренних адресов. Это означает, что выходящий пакет шифруется полностью вместе с заголовком на ключе парной связи текущего криптомаршрутизатора и криптомаршрутизатора, закрывающего подсеть, содержащую абонента. К этой криптограмме добавляется IP-заголовок, с адресом отправителя – внешний адрес текущего криптомаршрутизатора и с адресом получателя – адрес криптомаршрутизатора, закрывающего сеть корреспондента. Для прохождения полученного пакета через устройства маскировки топологии надсетей (NAT) необходимо к IP-заголовку добавить подзаголовок произвольного протокола, например UDP с некоторыми неиспользуемыми портами. Отсюда следует, что извне обмен информацией между защищаемыми подсетями выглядит как обмен UDP-пакетами между парой компьютеров.

Все попытки зондирования нарушителем внутренних подсетей будут неудачными, поскольку пришедший пакет не будет правильно расшифрован. Отсутствие необходимости поддерживать транспортный уровень стека протоколов TCP/IP приводит к недейственности атак на транспортный уровень, что повышает надежность работы криптомаршрутизаторов.

Очевидно, что при таком подходе получить доступ к открытой сети Internet невозможно, но защита такого рода будет надежной с точностью до стойкости алгоритма шифрования.

НСД к информации на отчуждаемых компонентах, т. е. съемных носителях и в канале связи с другими компьютерами

Для топологии сети «точка-точка» при возможном внедрении нарушителем произвольных закладок в программное обеспечение компьютеров и работе по коммутируемому или выделенному каналу по протоколу RS232 возможно применение наложенных средств шифрования канала. Если обеспечить включение алгоритмов шифрования в состав каналообразующей аппаратуры только при непосредственной передаче информации в линию и выключение при отсутствии передачи информации при конфигурировании модема, то вне зависимости от количества и агрессивности закладок, нарушитель:

- не оказывает асинхронное воздействие извне на программно-аппаратные комплексы;
- не получает открытую информацию, передаваемую по каналу при непосредственном съеме информации с линии;
- не получает открытую информацию при перенаправлении ее по коммутируемому каналу.

Вариант защиты от локального НСД

Рассмотрим пример построения комплекса средств защиты от НСД–1 для некоторой модели нарушителя.

Модель нарушителя (его возможности)

Установка системы защиты производилась в отсутствие нарушителя.

- Нарушитель не имеет информацию о пароле установки.
- Нарушитель не имеет информацию о пароле пользователя.
- Нарушитель не может вскрыть кожух компьютера.
- Нарушитель не имеет копию информации, записанной в носителе ключевой информации пользователя.
- Программы ROM BIOS не могут быть перезаписаны в процессе работы компьютера.

Очевидно, что программные средства защиты могут с той или иной степенью сложности быть обойдены при использовании механизма работы бутовых вирусов (вирусов, внедряющихся в программу начального загрузчика). Так, однажды внедренный вирус семейства OneHalf достаточно свободно чувствует себя в среде Windows NT Workstation 4.0. Аналогично, используя механизм работы микропроцессора 80386 и выше, можно создать закладку, обходящую все средства программного контроля целостности.

Отсюда следует, что в рамках данной модели нарушителя требуется только программно-аппаратная защита информации. При этом необходимо гарантировать чистоту операционной среды, т. е. загружаемого в начальный момент программного обеспечения. Дальнейший контроль может производиться программными средствами с использованием средств разграничения доступа.

Защита при загрузке операционной системы

Средства, гарантирующие защиту от НСД к информации при включении компьютера, гарантируют неизменность операционной среды в момент включения компьютера по отношению к состоянию ПО в момент установки средств защиты методом проверки имитозащитной приставки выбранных файлов при каждой загрузке компьютера.

Эти средства осуществляют защиту от НСД к информации, записанной на жесткий диск компьютера, путем запроса пароля, вводимого с клавиатуры, а также подключения элемента Touch Memory (ТМ), с которого считывается ключевая информация (КИ). После считывания КИ программа, записанная в ПЗУ, осуществляет проверку целостности выбранных при установке комплекса файлов. В случае положительного результата проверки происходит загрузка операционной системы. В ином случае повторно запрашивается пароль. Для блокирования доступа к информации о пароле при включенном компьютере программное обеспечение, находящееся на плате, исчезает из адресного пространства компьютера и не может быть считано никакими программными средствами без извлечения микросхемы ПЗУ из платы. Загрузка компьютера при отсутствии адаптера или при неисправном адаптере блокируется.

Алгоритм проверки целостности программного обеспечения основан на современных алгоритмах генерации имитозащитной приставки, что обеспечивает достаточное качество проверки. Ключевыми элементами являются: пароль пользователя, пароль установки, а также содержимое ТМ. В качестве примера конкретной реализации можно привести электронные замки «Аккорд» (ОКБ САПР) (www.accord.ru) и «Соболь» (НИП «Информзащита») (www.infosec.ru). К концу 2003 г. фирмой ОКБ САПР изготовлено более 100 тыс. штук электронных замков «Аккорд».

Таким образом, из вышесказанного можно сделать следующие выводы:

- программные комплексы без дополнительных апаратных и технических средств не обеспечивают защиту от НСД при наличии программных закладок и вирусов;
- для создания устойчивой и в то же время гибкой системы защиты от НСД следует применять программно-аппаратные комплексы;

- для обеспечения «чистоты операционной среды» сразу после загрузки ОС необходим контроль сохранности файлов ОС до момента выполнения любых участков кода, записанных на переписываемых носителях.

Вариант защиты от удаленного НСД

В настоящее время для передачи информации внутри контролируемой территории используются локальные вычислительные сети (ЛВС). Рассмотрим применение протокола TCP/IP для работы в ЛВС и предположим, что необходимо выполнить обмен информацией между несколькими ЛВС по каналам Internet.

Пусть модель нарушителя будет следующей.

- Нарушитель знает топологию всей сети.
- Нарушитель знает IP-адреса подсетей.
- Нарушитель имеет образцы программного обеспечения рабочих станций и серверов в подсетях и образцы аппаратуры.
- Нарушитель имеет информацию о внедренных в ПО программно-аппаратных закладках, отладочной информации, мастер-паролях и т. д.
- Нарушитель не имеет ключевой информации, т. е. сеансовых и базовых ключей.

Возможные средства защиты

Для решения задачи по защите информации в таких условиях предлагается применить разбиение всего пространства сети Internet на два непересекающихся по открытой информации подпространства: подпространство P – защищаемые подсети и подпространство C – остальная часть сети Internet. При этом подпространства P и C пересекаются только по открытой информации. Основные принципы, заложенные в работу устройства защиты – криптомаршрутизатора (КМ), состоят в следующем. Во-первых, внешний и внутренний интерфейсы должны быть разделены физически (например, две разные сетевые карты или разные каналы RS232). Во-вторых, вся исходящая информация должна преобразоваться КМ по определенным правилам.

Таким образом, достигается полная прозрачность КМ для любого сетевого программного обеспечения, работающего через стек протоколов TCP/IP в рамках внутренних подсетей. Адресное пространство внутренних подсетей не зависит от адресов в Internet. Устойчивость защиты информации в защищаемых подсетях равна стойкости криптосхемы, реализованной в КМ. Стойкость защиты информации, передаваемой по открытым каналам Internet, также равна стойкости криптосхемы.

При отсутствии воздействия противника на внутренние подсети, т. е. локального НСД к локальным сетям, защищенность информации в целом равна стойкости криптосхемы.

Надежность средств защиты

Рассмотренные выше три системы защиты информации от НСД позволяют в разных случаях решать задачу защиты информации с надежностью, соответствующей стойкости реализованных систем шифрования при заданных моделях нарушителя.

Несанкционированный доступ к информации на отчуждаемых компонентах может выступать в качестве НСД-1 (при атаках на информацию на съемных носителях) и НСД-2 (при атаках на информацию в коммутируемом канале связи).

Рассмотрим модель нарушителя в случае атаки на канал связи.

- Нарушитель имеет комплект оборудования.
- Нарушитель имеет исходные тексты всех программ и всю дополнительную информацию о них (пусть даже он является автором части программ).
- Нарушитель имеет запись всего материала, т. е. всей информации в канале связи за определенный промежуток времени.
- Нарушитель не имеет возможности оказывать влияние на работу и начальные условия работы компьютера в сети.

В этих условиях защитить информацию от НСД можно только криптографическими методами, т. е. шифрованием информации в канале связи. Это может быть реализовано методами защиты от НСД-2, описанными ранее.

Таким образом, обеспечить защиту информации от НСД на отчуждаемых компонентах с заранее заданной надежностью возможно только при хранении и передаче информации в зашифрованном виде. В этом случае вопрос о вычислении степени надежности защиты от НСД сводится к оценке стойкости используемого алгоритма шифрования.

В реальных условиях естественно считать возможными все атаки, т. е. попытки как НСД–1, так и НСД–2. При этом для защиты информации необходимо, во-первых, построить максимально реальную модель нарушителя, а во-вторых, обеспечить защиту информации на всех уровнях с заданной надежностью.

Защита от несанкционированного доступа

В общем случае несанкционированный доступ является реализацией преднамеренной угрозы информационной безопасности. С практической точки зрения можно выделить следующие варианты несанкционированного доступа:

- доступ к носителям информации;
- локальный доступ к отдельным персональным компьютерам;
- локальный доступ к ресурсам сети;
- удаленный доступ к отдельным компьютерам или ресурсам сети.

Предотвращение несанкционированного доступа к носителям информации обеспечивается физическими мерами защиты (пропускной режим, охрана, замки на дверях, сейфы и т. д.). Естественно, что ряд подобных мер используется и для защиты от несанкционированного доступа к компьютерам в организации. Однако здесь очень большое значение имеют и программно-технические способы защиты от несанкционированного доступа, которые мы кратко рассмотрим в этой главе.

Парольная защита с помощью стандартных системных средств

Методы, входящие в эту группу, представляют, так сказать, первый рубеж обороны от несанкционированного доступа. Как видно из названия, их особенностью является использование возможностей защиты, непосредственно встроенных в системные программы и операционные системы компьютеров. Поэтому использование этих методов не требует дополнительных затрат на приобретение специализированных программ или дополнительных технических средств.

Парольная защита отдельных персональных компьютеров

Основная задача этого вида парольной защиты – предотвратить доступ посторонних лиц к информации на вашем компьютере в ваше отсутствие. Здесь уместна аналогия с обычной квартирой – вряд ли кто в здравом уме оставит дверь нараспашку, уходя, например, на работу. Напротив, большинство старается поставить надежные замки. В то же время многие пользователи оставляют компьютер включенным и спокойно уходят обедать, предоставляя свою информацию в распоряжение всем желающим. А ведь кроме преднамеренных корыстных действий злоумышленника вполне возможны и проблемы, вызванные непреднамеренными действиями ваших коллег. Например, кому-то срочно потребовалось просмотреть файл, полученный из сторонней организации. Ваш компьютер включен и свободен. Человек вставляет дискету и от-

крывает файл в Word. Вот вирус и на вашем компьютере! Без вас кто-то по незнанию или по недоразумению может стереть или исказить файлы, да мало ли что еще может произойти. Впрочем, то же самое можно сказать и тогда, когда без присмотра остается даже выключенный компьютер, поскольку включить его может каждый. Для исключения подобных случаев и используется парольная защита.

В системных средствах компьютера существуют два вида парольной защиты: защита от включения компьютера и защита от доступа к включенному компьютеру в ваше отсутствие.

Защита от включения компьютера может быть реализована с помощью установки пароля в BIOS. В этом случае (после включения компьютера, перед началом загрузки операционной системы) на экран выводится запрос на ввод пароля. Пока не будет введен правильный пароль, компьютер не загрузится. Но, как и все известные методы защиты, пароль в BIOS не дает абсолютной гарантии от несанкционированного доступа. Посмотрим, что может сделать даже не очень квалифицированный взломщик.

Во-первых, имеется аппаратный способ отключения пароля в BIOS. Для этого достаточно вскрыть корпус системного блока и замкнуть определенные контакты на системной плате. Как это сделать, может узнать любой желающий. Однако в условиях учреждения выполнение подобной операции затруднено по понятным причинам – на виду у всех этого не сделаешь.

Во-вторых, во многих версиях BIOS имеются так называемые технологические пароли, введенные производителями. Списки этих паролей можно найти в Internet. Зная такой пароль, его можно ввести вместо установленного вами и произвести загрузку компьютера.

И, наконец, пароль можно подобрать или просто подсмотреть. Пользователи часто выбирают достаточно очевидные короткие пароли, мнемоника которых облегчает подбор. Очень часто это краткие имена пользователей (например, Vova, Nina и др.), имена родственников, даты рождения и пр. Специалисты службы информатизации установили пользователю пароль в BIOS. Чтобы не забыть этот пароль, пользователь записывает его на бумажке, которую приклеивает на собственный монитор... Иногда применяются достаточно наивные уловки: например, многие считают верхом находчивости приклеить такую бумажку к нижней стороне столешницы своего стола, не подозревая, что именно там и будет искать ее злоумышленник.

Тем не менее, при всей кажущейся простоте метод парольной защиты в BIOS является достаточно эффективным в условиях большинства обычных организаций. При правильном применении он позволит

практически отсечь попытки доступа к вашему компьютеру коллег и посетителей, не ставивших себе целью предварительные действия по взлому или краже пароля. Отметим, что пароль в BIOS предотвращает не только попытки несанкционированной загрузки компьютера с жесткого диска, но и попытки загрузиться с гибкого системного диска или CD-ROM при включении компьютера. Кроме того, он препятствует и изменению настроек BIOS.

В качестве дополнительного средства защиты можно использовать так называемый пароль Windows, который блокирует только загрузку операционной системы, уже установленной на вашем компьютере. Для более надежной защиты от несанкционированного включения компьютера в обоснованных случаях применяются специализированные программно-технические средства.

Очевидным путем предотвращения доступа к уже включенному компьютеру является выключение его на время вашего отсутствия. Однако это далеко не всегда удобно. Кроме того, частое включение/выключение снижает ресурс компьютера, поскольку возникающие при этом перепады температуры и напряжения отрицательно сказываются на электронных компонентах.

Одним из простейших способов предотвращения несанкционированного доступа к включенному компьютеру является установка паролей в программах, называемых хранителями экрана. Подобные программы (Screen Savers) входят в состав всех версий Windows.

Установка пароля в хранителе экрана не представляет проблем даже для начинающих пользователей. Для этого достаточно выполнить несложные операции при выборе так называемой заставки, которая определяет тип изображения, появляющегося на мониторе при работе хранителя экрана. Здесь же можно задать и время, через которое запускается хранитель экрана, если на компьютере не проводится действий с клавиатурой или мышью (обычно это время задается в интервале 3–5 минут). После запуска хранителя экрана рабочее изображение на экране монитора скрывается динамическим рисунком. Обычно работа хранителя экрана прекращается после первого нажатия на клавиатуру или перемещения мыши. Однако если пароль установлен, то доступ к рабочим программам можно получить только после его ввода. Разумеется, и эта защита не является абсолютной. Простейшим случаем ее преодоления является, например, перезагрузка путем выключения компьютера или нажатием клавиши «Reset». Поэтому важно, чтобы этот способ защиты сочетался с рассмотренной выше защитой от несанкционированного доступа при загрузке компьютера.

Парольная защита в локальных сетях

В локальных сетях парольная защита наряду с рассмотренными выше функциями выполняет и функции разграничения доступа пользователей к информационным ресурсам сети. Перед началом работы каждый пользователь вводит свое имя и соответствующий пароль, определяющий, например, к файлам каких сетевых дисков или каталогов имеет право доступа конкретный сотрудник. При этом может учитываться и способ доступа к файлам – только на чтение или и на чтение, и на модификацию файлов. Возможность установки подобного вида защиты заложена в стандартные средства известных операционных сред, например, Windows Vista/XP/NT и др.

Способ разграничения доступа определяется в процессе так называемого администрирования локальной сети. Грамотное администрирование сети требует, с одной стороны, определенных знаний, а с другой – наличия конкретных решений руководства организации или отдельного ее подразделения по разграничению доступа к информации. Если по недосмотру руководства или из-за недостаточной квалификации обслуживающего персонала все диски персональных компьютеров и серверов локальной сети выделены при администрировании в общий доступ, ваша информация практически не защищена. Все хранящиеся у вас на компьютере файлы доступны с любого компьютера сети, и ситуация ничем не лучше той, когда вы отставили без присмотра включенный компьютер. В некотором смысле она даже хуже, поскольку подходить к вашему компьютеру, чтобы «подсмотреть», скопировать или исказить вашу информацию, нет необходимости – это можно сделать даже из другой комнаты. Более того, это может быть сделано и в вашем присутствии, а вы ничего не заметите. Поэтому следует обязательно выяснить, какие диски и каталоги вашего компьютера являются доступными в сети и кому конкретно они доступны на чтение и/или изменение данных. Подобную информацию может предоставить системный администратор сети. В ряде случаев для повышения надежности защиты вашей информации ее целесообразно хранить непосредственно на сервере, доступ к которому ограничивается мерами физической защиты.

Однако даже правильно сконфигурированная сеть, информационные ресурсы сервера и персональных станций которой защищены паролями, не предоставляет, к сожалению, абсолютно надежной защиты информации. Дело здесь опять в том, что пароль можно «подсмотреть» (если он, например, записан на бумажке) или подобрать.

Защита от несанкционированного доступа с помощью специализированных программно-технических средств

Электронные замки

Эти средства обеспечивают идентификацию и аутентификацию пользователей для разрешения их доступа к компьютеру, а также могут выполнять целый ряд дополнительных функций.

Например, с помощью электронного замка «Соболь», созданного московской компанией «Информзащита», могут быть обеспечены следующие функции защиты:

- идентификация пользователей с помощью электронных идентификаторов типа Touch Memory;
- аутентификация пользователей по паролю;
- регистрация в специальной энергонезависимой памяти всех попыток включения компьютера и входов в систему;
- контроль целостности файлов и физических секторов жесткого диска с блокировкой компьютера при нарушении целостности контролируемых файлов;
- блокировка до 4-х устройств ввода-вывода (гибкий диск, CD-ROM, ZIP, LPT и др.);
- блокировка входа в систему зарегистрированного пользователя при превышении им заданного количества неудачных попыток входа.

Плата контроллера «Соболь» устанавливается в разъем PCI (ISA) системной платы компьютера, в комплект поставки входят, в частности, внешний считыватель Touch Memory и два электронных идентификатора с собственной памятью.

Для идентификации пользователю достаточно прикоснуться «таблеткой» электронного идентификатора к считывателю. Затем необходимо ввести пароль длиной до 16 символов. Контроль целостности реализован на аппаратном уровне и предназначен для того, чтобы убедиться, что системные программы и файлы компьютера не были модифицированы злоумышленником или посторонними программами.

Примерами электронных замков могут служить также аппаратно-программный комплекс «Криптон-Замок» зеленоградской фирмы «АНКАД» (www.ancud.ru) и комплекс «Аккорд 1.95» московской фирмы ОКБ САПР (www.accord.ru). В целом они выполняют сходные функции, однако имеют и определенные различия.

Например, с помощью электронного замка «Аккорд 1.95» могут быть выполнены следующие функции защиты:

- идентификация и аутентификация пользователей;

- ограничение «времени жизни» паролей и времени доступа пользователей к компьютеру;
- контроль целостности программ и данных, в том числе файлов ОС и служебных областей жесткого диска;
- разграничение доступа к информационным и аппаратным ресурсам компьютера;
- возможность временной блокировки компьютера и гашения экрана при длительной неактивности пользователя до повторного ввода идентификатора;
- исключение возможности несанкционированного выхода в операционную систему, загрузки с дискеты и прерывания контрольных процедур с клавиатуры.

Контроллер «Аккорда» имеет собственный процессор, который защищает от прочтения и модификации флэш-память, где хранятся ключи пользователей и контрольные суммы, а также обеспечивает выполнение проверки целостности конфигурации системы до загрузки операционной системы.

Отметим, что электронные ключи, как правило, являются одним из элементов целого семейства программно-аппаратных комплексов защиты информации, предлагаемых на рынке конкретной компанией.

Средства шифрования информации на диске

Задача подобных средств – создание специальной среды шифрования информации, работая с которой авторизованный пользователь видит дополнительный логический диск, на котором в зашифрованном виде представляется конфиденциальная информация. Информация обычно шифруется и расшифровывается «на лету», пользователь этого может и не замечать. Однако если кто-то, не имея идентификатора и не зная пароля, попытается работать с компьютером, этого диска он просто не увидит.

Примером подобного средства может быть, в частности, система защиты конфиденциальной информации Secret Disk московской компании «Аладдин» (www.aladdin.ru).

Secret Disk создает в компьютере «секретные» логические диски, при сохранении информации на которых она автоматически шифруется в «прозрачном» режиме. Чтобы получить доступ к такому диску, необходимо использовать электронный идентификатор и набрать пароль. Секретная информация хранится в специальном зашифрованном файле, который может располагаться на локальном или сетевом диске или на внешних носителях.

Система Secret Disk позволяет использовать самые различные виды электронных идентификаторов компании «Аладдин»:

- электронные ключи HASP, подключаемые к параллельному порту компьютера с сохранением возможности подключения к этому порту принтеров и других устройств;
- смарт-карты (для тех, кто о них не знает, скажем, что они похожи на проездные в метро для студентов);
- карты PCCard для ноутбуков;
- электронные брелки eToken, подключаемые к порту USB.

Система реализует ряд функций защиты, характерных и для электронных ключей, например, запуск хранителя экрана при отключении электронного идентификатора от компьютера, нажатии заданной комбинации клавиш или неактивности пользователя в течение определенного времени. Компьютер при этом блокируется и может быть разблокирован лишь вводом правильного пароля при подключенном электронном идентификаторе.

Кроме того, интерес представляют функции создания защищенных архивов и так называемый «вход по принуждению». На последней функции стоит остановиться особо.

Если кто-то, завладев электронным идентификатором, принуждает пользователя сообщить пароль, пользователь может указать злоумышленнику специальный пароль входа по принуждению. В этом случае система имитирует все характерные признаки системного сбоя или неисправности компьютера, а сама в это время в зависимости от настройки может стереть секретный диск или данные в электронном идентификаторе.

Определенный интерес имеет интеграция электронных брелков с сертифицированными средствами защиты «Crypto Pro CSP» (производитель компания «КриптоПро» – www.cryptopro.ru), что позволяет хранить сертификаты ключей непосредственно на электронном ключе.

Дактилоскопические системы защиты

Подобные устройства считаются сегодня одними из наиболее перспективных для идентификации пользователей компьютерных систем. Как правило, они состоят из дактилоскопического сканера, встраиваемого в переднюю панель компьютера, клавиатуру или (чаще всего) в мышь, и соответствующего комплекса программ.

Свет, отраженный от прижатого к поверхности сканера пальца, через оптическую систему попадает на светочувствительный датчик, который фиксирует узоры папиллярных линий. Это изображение оцифровывается, передается в компьютер и сравнивается с введенным ранее узором пальца-образца. По имеющейся статистике ложный допуск по отпе-

чатку пальца может произойти не чаще, чем в одном случае на миллион [19]. С функциональной точки зрения использование дактилоскопического идентификатора не отличается от ввода пароля или применения электронного идентификатора. Например, вместо ввода пароля нужно приложить палец к определенному месту мыши. Однако, с точки зрения пользователя, это гораздо более удобно, поскольку не нужно запоминать длинный пароль или носить с собой электронный идентификатор.

Устройства подобного типа сравнительно недавно появились на российском рынке и не получили пока большого распространения. Примерами таких устройств могут служить мыши с дактилоскопическим вводом UMATCH BioLink Mouse и EyeD Opti Mouse. При неплохих эргономических характеристиках эти средства не обеспечивают должной надежности хранения конфиденциальной информации. Управление системой защиты реализовано в них чисто программными средствами, а все атрибуты защиты хранятся в памяти компьютера. Поэтому сломать такой механизм защиты и получить доступ к защищаемой информации сравнительно нетрудно.

В целом использовать дактилоскопические мыши UMATCH BioLink Mouse и EyeD Opti Mouse в комплекте с поставляемыми программами как самостоятельное средство защиты от НСД целесообразно лишь в тех случаях, когда информация не представляет большой ценности и должна быть закрыта только от массовых пользователей, а не от специалистов по взлому защиты. Их лучше рассматривать как элемент комплексной системы защиты информации, в которой они выполняют только функции идентификации или аутентификации пользователей. При этом цифровые образы отпечатков должны храниться в труднодоступной для злоумышленника внутренней памяти системы защиты от НСД.

Контрольные вопросы и упражнения

5.1. Каково назначение защищенных компьютерных систем?

5.2. Приведете типовую архитектуру аппаратных средств от несанкционированного доступа к компьютерным системам. Приведите примеры.

5.3. Какие ключевые носители Вы знаете? Приведите примеры. Проведите их сравнительный анализ.

5.4. Приведите типовую схему идентификации и аутентификации пользователя в компьютерных системах. Каковы ее особенности?

5.5. Перечислите операционные системы, поддерживающие идентификацию пользователя в системе?

5.6. К каким элементам компьютерной системы необходимо разграничение доступа?
5.7. Каким образом определяется доступ к различным ресурсам компьютерной системы: внешним устройствам, оперативной памяти, дисковым накопителям, процессорному времени?
5.8. Какие средства операционной системы существуют для надежного выполнения более одного процесса, задачи; работы нескольких пользователей.
5.9. Поясните назначение систем резервного копирования. Приведите примеры.
5.10. Как часто необходимо делать резервирование данных? Какие носители информации требуются для резервного копирования, в чем их особенности? Приведите примеры.
5.11. Что Вы понимаете под целостностью данных?
5.12. Каким образом осуществляется проверка целостности баз данных? Логическая и физическая целостность.
5.13. Какие средства и способы существуют для проведения транзакции операций с распределенными базами данных?
5.14. Какие средства существуют для восстановления работоспособности компьютерных систем после сбоя?
5.15. Зачем необходимы средства самотестирования компьютерных систем? Приведите примеры.
5.16. Резервные источники питания. Определите назначение, характеристики. Приведите примеры.
5.17. Восстановление работоспособности компьютерных сетей. Рассмотрите случаи: обрыв линии, конфликт адресов.
5.18. Шифрование носителей информации. Определите назначение и приведите примеры.

6. ОСНОВЫ КРИПТОГРАФИИ[6]

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом волновала человеческий ум с давних времен. История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

Разные люди понимают под шифрованием разные вещи. Дети играют в игрушечные шифры и секретные языки. Это, однако, не имеет ничего общего с настоящей криптографией. Настоящая криптография (*strong cryptography*) должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки крупными организациями – такими как мафия, транснациональные корпорации и крупные государства. Настоящая криптография в прошлом использовалась лишь в военных целях. Однако сейчас, со становлением информационного общества, она становится центральным инструментом для обеспечения конфиденциальности.

По мере образования информационного общества, крупным государствам становятся доступны технологические средства тотального надзора за миллионами людей. Поэтому криптография становится одним из основных инструментов обеспечивающих конфиденциальность, доверие, авторизацию, электронные платежи, корпоративную безопасность и бесчисленное множество других важных вещей.

Криптография не является более придумкой военных, с которой не стоит связываться. Настала пора снять с криптографии покровы таинственности и использовать все ее возможности на пользу современному обществу. Широкое распространение криптографии является одним из немногих способов защитить человека от ситуации, когда он вдруг обнаруживает, что живет в тоталитарном государстве, которое может контролировать каждый его шаг.

---

[6] Приводится по работам [20, 30]

Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Начиная с послевоенного времени и по нынешний день появление вычислительных средств ускорило разработку и совершенствование криптографических методов.

Почему проблема использования криптографических методов в информационных системах (ИС) стала в настоящий момент особо актуальна?

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Internet, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем, еще недавно считавшихся практически не раскрываемыми.

Проблемой защиты информации путем ее преобразования занимается *криптология* (*kryptos* – тайный, *logos* – наука). Криптология разделяется на два направления: *криптографию* и *криптоанализ*. Цели этих направлений прямо противоположны.

Криптография занимается поиском и исследованием математических методов преобразования информации.

Сфера интересов *криптоанализа* – исследование возможности расшифровывания информации без знания ключей.

Современная криптография включает в себя четыре крупных раздела:

1. Симметричные криптосистемы.
2. Криптосистемы с открытым ключом.
3. Системы электронной подписи.
4. Управление ключами.

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Терминология

Итак, криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться *тексты*, построенные на некотором *алфавите*. Под этими терминами понимается следующее.

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст – упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных ИС можно привести следующие:

- алфавит Z_{33} – 32 буквы русского алфавита и пробел;
- алфавит Z_{256} – символы, входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит – $Z_2 = \{0,1\}$;
- восьмеричный алфавит или шестнадцатеричный алфавит;

Шифрование – преобразовательный процесс: *исходный текст*, который носит также название *открытого текста*, заменяется *шифрованным текстом*.

Дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство T [T_1, T_2, …, T_k] преобразований открытого текста. Члены этого семейства индексируются, или обозначаются символом k; параметр k является *ключом*. Пространство ключей K – это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на *симметричные* и системы *с открытым ключом*.

В *симметричных криптосистемах* и для шифрования, и для дешифрования используется *один и тот же ключ*.

В *системах с открытым ключом* используются два ключа – *открытый* и *закрытый*, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения [30].

Термины *распределение ключей* и *управление ключами* относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при

получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т. е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

- количество всех возможных ключей;
- среднее время, необходимое для криптоанализа.

Преобразование T_k определяется соответствующим алгоритмом и значением параметра k. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

Требования к криптосистемам

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т. д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
- число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;
- число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);
- знание алгоритма шифрования не должно влиять на надежность защиты;
- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;
- структурные элементы алгоритма шифрования должны быть неизменными;

- дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;
- длина шифрованного текста должна быть равной длине исходного текста;
- не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемых в процессе шифрования;
- любой ключ из множества возможных должен обеспечивать надежную защиту информации;
- алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Основные алгоритмы шифрования

Метод шифровки/дешифровки называют *шифром* (*cipher*). Некоторые алгоритмы шифрования основаны на том, что сам метод шифрования (алгоритм) является секретным. Ныне такие методы представляют лишь исторический интерес и не имеют практического значения. Все современные алгоритмы используют *ключ* для управления шифровкой и дешифровкой; сообщение может быть успешно дешифровано только если известен ключ. Ключ, используемый для дешифровки может не совпадать с ключом, используемым для шифрования, однако в большинстве алгоритмов ключи совпадают.

Алгоритмы с использованием ключа делятся на два класса: симметричные (или алгоритмы с секретным ключом) и асимметричные (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тот же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи, и ключ для дешифровки не может быть вычислен по ключу шифровки.

Симметричные алгоритмы подразделяют на *потоковые шифры* и *блочные шифры*. Потоковые позволяют шифровать информацию побитово, в то время как блочные работают с некоторым набором бит данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое.

Асимметричные шифры (также именуемые алгоритмами с открытым ключом, или – в более общем плане – криптографией с открытым ключом) допускают, чтобы открытый ключ был доступн всем (скажем,

опубликован в газете). Это позволяет любому зашифровать сообщение. Однако расшифровать это сообщение сможет только нужный человек (тот, кто владеет ключом дешифровки). Ключ для шифрования называют *открытым ключом*, а ключ для дешифрования – *закрытым ключом* или *секретным ключом*.

Таблица 3

Криптографическое закрытие информации

Вид преобразований	Способ преобразования	Разновидность способа	Способ реализации
Шифрование	Замена (подстановка)	Простая (одноалфавитная)	П
		Многоалфавитная одноконтурная обыкновенная	П
		Многоалфавитная одноконтурная монофоническая	П
		Многоалфавитная многоконтурная	П
	Перестановка	Простая	П
		Усложненная по таблице	П
		Усложненная по маршрутам	П
	Аналитическое преобразование	По правилам алгебры матриц	П
		По особым зависимостям	П
	Гаммирование	С конечной короткой гаммой	АП
		С конечной динной гаммой	АП
		С бесконечной гаммой	АП
	Комбинированные	Замена+перестановка	АП
		Замена+гаммирование	АП
		Перестановка+ гаммирование	АП
		Гаммирование+гаммирование	АП
Кодирование	Смысловое	По специальным таблицам (словарям)	П
	Символьное	По кодовому алфавиту	П
Другие виды	Рассечение-разнесение	Смысловое	АП
		Механическое	П
	Сжатие-расширение		

Примечание. Способ реализации: А – аппаратный, П – программный.

Современные алгоритмы шифровки/дешифровки достаточно сложны и их невозможно проводить вручную. Настоящие криптографические алгоритмы разработаны для использования компьютерами или специальными аппаратными устройствами. В большинстве приложений криптография производится программным обеспечением и имеется множество доступных криптографических пакетов.

Вообще говоря, симметричные алгоритмы работают быстрее, чем асимметричные. На практике оба типа алгоритмов часто используются вместе: алгоритм с открытым ключом используется для того, чтобы передать случайным образом сгенерированный секретный ключ, который затем используется для дешифровки сообщения.

Многие качественные криптографические алгоритмы доступны широко – в книжном магазине, библиотеке, патентном бюро или в Internet (табл. 3). К широко известным симметричным алгоритмам относятся DES и IDEA. Одним из наиболее криптостойких асимметричных алгоритмов является RSA. В России за стандарт шифрования принят ГОСТ 28147–89.

Цифровые подписи

Некоторые из асимметричных алгоритмов могут использоваться для генерирования *цифровой подписи*. Цифровой подписью называют блок данных, сгенерированный с использованием некоторого секретного ключа. При этом с помощью открытого ключа можно проверить, что данные были действительно сгенерированы с помощью этого секретного ключа. Алгоритм генерации цифровой подписи должен обеспечивать, чтобы было невозможно без секретного ключа создать подпись, которая при проверке окажется правильной.

Цифровые подписи используются для того, чтобы подтвердить, что сообщение пришло действительно от данного отправителя (в предположении, что лишь отправитель обладает секретным ключом, соответствующим его открытому ключу). Также подписи используются для проставления *штампа времени* (*timestamp*) на документах. Сторона, которой доверяем, подписывает документ со штампом времени с помощью своего секретного ключа и, таким образом, подтверждает, что документ уже существовал в момент, объявленный в штампе времени.

Цифровые подписи также можно использовать для удостоверения (*сертификации – to certify*) того, что документ принадлежит определенному лицу. Это делается так: открытый ключ и информация о том, кому он принадлежит подписываются стороной, которой доверяем. При этом доверять подписывающей стороне мы можем на основании того, что ее ключ был подписан третьей стороной. Таким образом возникает иерархия доверия. Очевидно, что некоторый ключ должен быть корнем иерархии (то есть ему доверяем не потому, что он кем-то подписан, а потому, что верим a-priori, что ему можно доверять). В *централизованной инфраструктуре ключей* имеется очень небольшое количество корне-

вых ключей сети (например, облеченные полномочиями государственные агентства; их также называют *сертификационными агентствами – certification authorities*). В *распределенной инфраструктуре* нет необходимости иметь универсальные для всех корневые ключи, и каждая из сторон может доверять своему набору корневых ключей (скажем своему собственному ключу и ключам, ею подписанным). Эта концепция носит название *сети доверия* (*web of trust*) и реализована, например, в PGP.

Цифровая подпись документа обычно создается так: из документа генерируется так называемый *дайджест* (*message digest*) и к нему добавляется информация о том, кто подписывает документ, штамп времени и прочее. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Получившийся зашифрованный набор бит и представляет собой подпись. К подписи обычно прикладывается открытый ключ подписывающего. Получатель сначала решает для себя доверяет ли он тому, что открытый ключ принадлежит именно тому, кому должен принадлежать (с помощью сети доверия или априорного знания), и затем дешифрует подпись с помощью открытого ключа. Если подпись нормально дешифровалась, и ее содержимое соответствует документу (дайджест и др.), то сообщение считается подтвержденным.

Свободно доступны несколько методов создания и проверки цифровых подписей. Наиболее известным является алгоритм RSA, ГОСТ 34.10–94, ГОСТ 34.10–2001.

Криптографические хеш-функции

Криптографические хеш-функции используются обычно для генерации дайджеста сообщения при создании цифровой подписи. Хеш-функции отображают сообщение в имеющее фиксированный размер *хеш-значение* (*hash value*) таким образом, что все множество возможных сообщений распределяется равномерно по множеству хеш-значений. При этом криптографическая хеш-функция делает это таким образом, что практически невозможно подогнать документ к заданному хеш-значению.

Криптографические хеш-функции обычно производят значения длиной в 128 и более бит. Это число значительно больше, чем количество сообщений, которые когда-либо будут существовать в мире.

Много хороших криптографических хеш-функций доступно бесплатно. Широко известные включают MD5 и SHA.

Криптографические генераторы случайных чисел

Криптографические генераторы случайных чисел производят случайные числа, которые используются в криптографических приложениях, например – для генерации ключей. Обычные генераторы случайных чисел, имеющиеся во многих языках программирования и программных средах, не подходят для нужд криптографии (они создавались с целью получить статистически случайное распределение, криптоаналитики могут предсказать поведение таких случайных генераторов).

В идеале случайные числа должны основываться на настоящем физическом источнике случайной информации, которую невозможно предсказать. Примеры таких источников включают шумящие полупроводниковые приборы, младшие биты оцифрованного звука, интервалы между прерываниями устройств или нажатиями клавиш. Полученный от физического источника шум затем «дистиллируется» криптографической хеш-функцией так, чтобы каждый бит зависел от каждого бита. Достаточно часто для хранения случайной информации используется довольно большой пул (несколько тысяч бит) и каждый бит пула делается зависимым от каждого бита шумовой информации и каждого другого бита пула криптографически надежным (*strong*) способом.

Когда нет настоящего физического источника шума, приходится пользоваться псевдослучайными числами. Такая ситуация нежелательна, но часто возникает на компьютерах общего назначения. Всегда желательно получить некий шум окружения – скажем, от величины задержек в устройствах, цифровой статистики использования ресурсов, сетевой статистики, прерываний от клавиатуры или чего-то иного. Задачей является получить данные, непредсказуемые для внешнего наблюдателя. Для достижения этого случайный пул должен содержать как минимум 128 бит настоящей энтропии.

Криптографические генераторы псевдослучайных чисел обычно используют большой пул (seed-значение), содержащий случайную информацию. Биты генерируется путем выборки из пула с возможным прогоном через криптографическую хеш-функцию, чтобы спрятать содержимое пула от внешнего наблюдателя. Когда требуется новая порция бит, пул перемешивается путем шифровки со случайным ключом (его можно взять из неиспользованной пока части пула) так, чтобы каждый бит пула зависел от каждого другого бита. Новый шум окружения должен добавляться к пулу перед перемешиваниями, дабы сделать предсказание новых значений пула еще более сложным.

Несмотря на то, что при аккуратном проектировании криптографически надежный генератор случайных чисел реализовать не так уж и трудно,

этот вопрос часто упускают из вида. Таким образом, следует подчеркнуть важность криптографического генератора случайных чисел – если он сделан плохо, он может легко стать самым уязвимым элементом системы.

Обеспечиваемая шифром степень защиты

Хорошие криптографические системы создаются таким образом, чтобы сделать их вскрытие как можно более трудным делом. Можно построить системы, которые на практике невозможно вскрыть (хотя доказать сей факт обычно нельзя). При этом не требуется очень больших усилий для реализации. Единственное, что требуется – это аккуратность и базовые знания. Нет прощения разработчику, если он оставил возможность для вскрытия системы. Все механизмы, которые могут использоваться для взлома системы, надо задокументировать и довести до сведения конечных пользователей.

Теоретически, любой шифровальный алгоритм с использованием ключа может быть вскрыт методом перебора всех значений ключа. Если ключ подбирается методом *грубой силы* (*brute force*), требуемая мощность компьютера растет экспоненциально с увеличением длины ключа. Ключ длиной в 32 бита требует 2^{32} (около 10^9) шагов. Такая задача под силу любому дилетанту и решается на домашнем компьютере. Системы с 40-битным ключом (например, экспортный американский вариант алгоритма RC4) требуют 2^{40} шагов – такие компьютерные мощности имеются в большинстве университетов и даже в небольших компаниях. Системы с 56-битными ключами (DES) требуют для вскрытия заметных усилий, однако могут быть легко вскрыты с помощью специальной аппаратуры. Стоимость такой аппаратуры значительна, но доступна для мафии, крупных компаний и правительств. Ключи длиной 64 бита в настоящий момент, возможно, могут быть вскрыты крупными государствами и уже в ближайшие несколько лет будут доступны для вскрытия преступными организациями, крупными компаниями и небольшими государствами. Ключи длиной 80 бит могут в будущем стать уязвимыми. Ключи длиной 128 бит вероятно останутся недоступными для вскрытия методом грубой силы в обозримом будущем. Можно использовать и более длинные ключи. В пределе нетрудно добиться того, чтобы энергия, требуемая для вскрытия (считая, что на один шаг затрачивается минимальный квантовомеханический квант энергии) превзойдет массу солнца или вселенной.

Однако, длина ключа это еще не все. Многие шифры можно вскрыть и не перебирая всех возможных комбинаций. Вообще говоря,

очень трудно придумать шифр, который нельзя было бы вскрыть другим более эффективным способом. Разработка собственных шифров может стать приятным занятием, но для реальных приложений использовать самодельные шифры не рекомендуется если не являетесь экспертом и не уверены на 100 % в том, что делаете.

Вообще говоря, следует держаться в стороне от неопубликованных или секретных алгоритмов. Часто разработчик такого алгоритма не уверен в его надежности, или же надежность зависит от секретности самого алгоритма. Вообще говоря, ни один алгоритм, секретность которого зависит от секретности самого алгоритма, не является надежным. В частности, имея шифрующую программу, можно нанять программиста, который дизассемблирует ее и восстановит алгоритм методом обратной инженерии. Опыт показывает, что большинство секретных алгоритмов, ставших впоследствии достоянием общественности, оказались до смешного ненадежными.

Длины ключей, используемых в криптографии с открытым ключом, обычно значительно больше, чем в симметричных алгоритмах. Здесь проблема заключается не в подборе ключа, а в воссоздании секретного ключа по открытому. В случае RSA проблема эквивалентна разложению на множители большого целого числа, которое является произведением пары неизвестных простых чисел. В случае некоторых других криптосистем, проблема эквивалентна вычислению дискретного логарифма по модулю большого целого числа (такая задача считается примерно аналогичной по трудности задаче разложения на множители). Имеются криптосистемы, которые используют другие проблемы.

Чтобы дать представление о степени сложности вскрытия RSA, скажем, что модули длиной 256 бит легко факторизуются обычными программистами. Ключи в 384 бита могут быть вскрыты исследовательской группой университета или компании. 512-битные ключи находятся в пределах досягаемости крупных государств. Ключи длиной в 768 бит, вероятно, не будут надежны продолжительное время. Ключи длиной в 1024 бит могут считаться безопасными до тех пор, пока не будет существенного прогресса в алгоритме факторизации; ключи длиной в 2048 бит большинство считает надежными на десятилетия.

Важно подчеркнуть, что *степень надежности криптографической системы определяется ее слабейшим звеном*. Нельзя упускать из вида ни одного аспекта разработки системы – от выбора алгоритма до политики использования и распространения ключей.

Криптоанализ и атаки на криптосистемы

Криптоанализ – это наука о дешифровке закодированных сообщений при отсутствии знаний о значении ключей. Имеется много криптоаналитических подходов. Некоторые из наиболее важных для разработчиков приведены ниже.

Атака со знанием лишь шифрованного текста (*ciphertext-only attack*). Это ситуация, когда атакующий не знает ничего о содержании сообщения, и ему приходится работать лишь с самим шифрованным текстом. На практике часто можно сделать правдоподобные предположения о структуре текста, поскольку многие сообщения имеют стандартные заголовки. Даже обычные письма и документы начинаются с легко предсказуемой информации. Также часто можно предположить, что некоторый блок информации содержит заданное слово.

Атака со знанием содержимого шифровки (*known-plaintext attack*). Атакующий знает или может угадать содержимое всего, или части зашифрованного текста. Задача заключается в расшифровке остального сообщения. Это можно сделать либо путем вычисления ключа шифровки, либо минуя это.

Атака с заданным текстом (*chosen-plaintext attack*). Атакующий имеет возможнот получить шифрованный документ для любого нужного ему текста, но не знает ключа. Задачей является нахождение ключа. Некоторые методы шифрования и, в частности, RSA, весьма уязвимы для атак этого типа. При использовании таких алгоритмов надо тщательно следить, чтобы атакующий не мог зашифровать заданный им текст.

Атака с подставкой (*Man-in-the-middle attack*). Атака направлена на обмен шифрованными сообщениями и, в особенности, на протокол обмена ключами. Идея заключается в том, что когда две стороны обмениваются ключами для секретной коммуникации (например, используя шифр Диффи-Хелмана – Diffie-Hellman), противник внедряется между ними на линии обмена сообщениями. Далее противник выдает каждой стороне свои ключи. В результате, каждая из сторон будет иметь разные ключи, каждый из которых известен противнику. Теперь противник будет расшифровывать каждое сообщение своим ключом и затем зашифровывать его с помощью другого ключа перед отправкой адресату. Стороны будут иметь иллюзию секретной переписки, в то время как на самом деле противник читает все сообщения.

Одним из способов предотвратить такой тип атак заключается в том, что стороны при обмене ключами вычисляют криптографическую хеш-функцию значения протокола обмена (или по меньшей мере значения ключей), подписывают ее алгоритмом цифровой подписи и посы-

лают подпись другой стороне. Получатель проверит подпись и то, что значение хеш-функции совпадает с вычисленным значением. Такой метод используется, в частности, в системе Фотурис (Photuris).

Атака с помощью таймера (*timing attack*). Этот новый тип атак основан на последовательном измерении времен, затрачиваемых на выполнение операции возведения в стенень по модулю целого числа. Ей подвержены по крайней мере следующие шифры: RSA, Диффи-Хеллман и метод эллиптических кривых.

Имеется множество других криптографических атак и криптоаналитических подходов. Однако приведенные выше являются, по-видимому, наиболее важными для практической разработки систем. Если кто-либо собирается создавать свой алгоритм шифрования, ему необходимо понимать данные вопросы значительно глубже.

Выбор для конкретных ИС должен быть основан на глубоком анализе слабых и сильных сторон тех или иных методов защиты. Обоснованный выбор той или иной системы защиты в общем-то должен опираться на какие-то *критерии эффективности*. К сожалению, до сих пор не разработаны подходящие методики оценки эффективности криптографических систем.

Наиболее простой критерий такой эффективности – *вероятность раскрытия ключа* или *мощность множества ключей (M)*. По сути это то же самое, что и *криптостойкость*. Для ее численной оценки можно использовать также и сложность раскрытия шифра путем перебора всех ключей.

Однако этот критерий не учитывает других важных *требований к криптосистемам*:

- невозможность раскрытия или осмысленной модификации информации на основе анализа ее структуры;
- совершенство используемых протоколов защиты;
- минимальный объем используемой ключевой информации;
- минимальная сложность реализации (в количестве машинных операций), ее стоимость;
- высокая оперативность.

Желательно конечно использование некоторых интегральных показателей, учитывающих указанные факторы.

Для учета стоимости, трудоемкости и объема ключевой информации можно использовать удельные показатели – отношение указанных параметров к мощности множества ключей шифра.

Часто более эффективным при выборе и оценке криптографической системы является использование экспертных оценок и имитационное моделирование.

В любом случае выбранный комплекс криптографических методов должен сочетать как удобство, гибкость и оперативность использования, так и надежную защиту от злоумышленников циркулирующей в ИС информации.

Контрольные вопросы и упражнения

6.1. Что такое криптографическое преобразование?
6.2. Приведите особенности симметричных шифров. Чем отличаются потоковые и блочные шифры. Приведите примеры.
6.3. Почему асимметричные шифры называют криптографией с открытым ключом? Приведите примеры асимметричных шифров.
6.4. В чем особенности реализации потоковых шифров?
6.5. Возможно ли совмещение алгоритмов шифрования данных и алгоритмов сжатия? Приведите примеры.
6.6. Шифр простой замены. Приведите блок-схему алгоритма. Каковы его слабые стороны?
6.7. Какой зависимостью связана длина ключа и скорость работы алгоритма? Проведите исследование на примере одного из шифров.
6.8. Повышает ли помехоустойчивость использование шифрования? Почему.
6.9. В чем особенность системы шифрования Вижинера? К какому виду алгоритмов она относится?
6.10. Зачем в криптографических системах необходимо использовать датчики случайных чисел? Приведите примеры.
6.11. К какому виду алгоритмов относятся следующие алгоритмы и в чем их особенности:
   а) ГОСТ 24147-89;
   б) DES;
   в) AES (IDEA);
   г) подстановка Цезаря;
   д) гаммирование;
   е) RSA;
   ж) PGP.
6.12. Каким образом можно генерировать ключи? Какие требования ставятся перед генератором ключей?

6.13. Что входит в распределение ключей в процессе управления ключами?
6.14. Что выполняет центр управления ключевой системой? Какие задачи и функции на него возложены?
6.15. Какие действия необходимо предпринять при компрометации ключа? Какие события относятся к компрометации ключа?
6.16. Что представляет собой электронно-цифровая подпись? Какое у нее назначение? На какие документы можно ее ставить?
6.16. Какие события происходят при определении электронно-цифровой подписи?
6.17. Какие отношения между участниками информационного обмена при использовании электронно-цифровой подписи возможны. Участники A, B, C, причем A передает сообщение B.
6.18. Что такое хеш-функция? Какое значение имеет хеш-функция в электронно-цифровой подписи.
6.19. В чем особенности стандарта шифрования ГОСТ 34.10-01?
6.20. Зачем нужна имитовставка?
6.21. Кто должен отвечать за ключевую информацию?
6.22. Что такое метод грубой силы для вскрытия шифрованного сообщения? Каким образом его применяют?
6.23. Зависит ли обеспечиваемая шифром степень защиты от длины ключа? Приведите пример на каком-либо алгороитме.
6.24. Что такое криптоанализ?
6.25. Приведите основные криптоаналитические подходы.
6.26. Есть ли возможность создания криптографической системы со 100 % надежностью от вскрытия?
6.27. Повышается ли надежность закрытия информации при последовательном применении двух алгоритмов шифрования?
6.28. Как Вы считаете что необходимо делать в первую очередь: шифровать, а затем подписывать документ, или наоборот: подписывать документ, а затем шифровать?

7. АРХИТЕКТУРА ЗАЩИЩЕННЫХ ЭКОНОМИЧЕСКИХ СИСТЕМ[7]

Принципы функционирования электронных платежных систем

Современная практика банковских операций, торговых сделок и взаимных платежей невозможна без использования в качестве платежного средства *пластиковых карт* (персонифицированных платежных инструментов). Они предоставляют пользующимся ими лицам возможность безналичной оплаты товаров и услуг и обналичивания в банковских автоматах и отделениях банков.

Совокупность методов и реализующих их субъектов, обеспечивающих применение этих карт, называют *электронной платежной системой* (ЭПС). С *организационной* точки зрения ее *ядром* является *ассоциация банков,* объединенная договорными обязательствами. Кроме того, в состав ЭПС входят *предприятия торговли и сервиса,* и *отделения банков,* принимающие карту в качестве платежного инструмента и образующие *приемную сеть точек обслуживания.* Для успешного функционирования ЭПС необходимы и *специализированные организации,* осуществляющие техническую поддержку обслуживания карт. Это процессинговые и коммуникационные центры, центры технического обслуживания и т. п.

Обобщенную схему функционирования ЭПС можно представить следующим образом. Банк, заключивший соглашение с ЭПС и получивший соответствующую лицензию, может выступать в двух качествах – как *банк-эмитент* (выпускающий смарт-карты и гарантирующий выполнение финансовых обязательств, связанных с их использованием как платежных средств) и как *банк-эквайер* (обслуживающий предприятия торговли и сервиса, принимающий к оплате карты как платежные средства, обналичивающий их в своих отделениях и через принадлежащие ему банкоматы). Банк-эквайер может делегировать *процессинговым цен-*

[7] Приводится по работам [12, 28]

трам технические атрибуты своей деятельности, такие как обработка запросов на авторизацию; перечисление на расчетные счета точек средств за товары и услуги, предоставленные по картам; прием, сортировка и пересылка документов, фиксирующих свершение сделок с использованием карт и т. п.

Существует два типа процедур приема платежа с помощью карты: неавтоматизированные, с помощью чеков-слипов; автоматизированные, с помощью торговых POS-терминалов и банкоматов.

В первом случае кассир должен проделать следующее:

1) прежде всего убедиться в подлинности карты;
2) при оплате с помощью копировальной машины-импринтера перенести реквизиты карты клиента на специальный чек, называемый *слипом*;
3) занести в него сумму, на которую была совершена покупка или оказана услуга;
4) получить подпись клиента.

В целях обеспечения безопасности операций ЭПС рекомендуется не превышать нижние лимиты сумм, по которым можно проводить расчеты без авторизации. При превышении лимитной суммы или в случае возникновения сомнения в личности клиента предприятию необходимо провести *процедуру авторизации.* При этом оно фактически получает доступ к информации о состоянии счета клиента и может установить принадлежность карты клиенту и его платежную способность в размере суммы сделки. Одна копия слипа остается на предприятии, вторая передается клиенту, третья доставляется в банк-эквайер и служит основанием для возмещения суммы платежа предприятию со счета клиента. Во втором случае широкую популярность приобрели POS-терминалы (Point-Of-Sale – оплата в точке продажи) и банкоматы. При использовании POS-терминалов нет необходимости в заполнении слипов, так как реквизиты пластиковых карт считываются с ее магнитной дорожки на POS-терминале считывателе. Клиент вводит в терминал свой PIN-код (Personal Identification Number – персональный идентификационный номер), известный только ему. Элементы PIN-кода включаются в общий алгоритм шифрования записи на магнитной полосе и служат электронной подписью владельца карты. На клавиатуре POS-терминала набирается сумма сделки. Если сделка осуществляется в отделении банка и в ее процессе происходит выдача клиенту наличных денег, помимо банковских POS-терминалов может быть использован электронный кассир-банкомат, который конструктивно представляет собой автоматизированный сейф со встроенным POS-терминалом. В этом случае POS-терминал через встроенный в сейф модем обращается за авторизацией в

соответствующую ЭПС. При этом используются мощности процессингового центра, услуги его предоставляются торговцу банком-эквайером.

Процессинговый центр (ПЦ) представлят собой специализированную сервисную организацию, которая обеспечивает обработку поступающих от банков-эквайеров (или непосредственно от точек обслуживания) как запросов на авторизацию, так и протоколов транзакций (представляющих собой зафиксированные данные о произведенных платежах и выдачах наличными посредством пластиковых карт). Для этого ПЦ ведет базу данных, содержащую данные о банках – членах ЭПС и держателях пластиковых карт, а также хранит сведения о лимитах держателей и выполняет запросы на авторизацию в том случае, если банк-эмитент не ведет собственной базы данных (off-line банк). Если ведет (on-line банк), то ПЦ пересылает полученный запрос об авторизуемой карте в банк-эмитент и затем посылает ответ банку-эквайеру. Каждый банк-эквайер осуществляет перечисление средств точкам обслуживания по платежам держателей карт банков-эмитентов, входящих в данную ЭПС, которые затем он сам должен получить от банков-эмитентов. Оперативное проведение взаиморасчетов между эквайерами и эмитентами обеспечивается наличием в ЭПС *расчетного банка,* в котором банки – члены ЭПС открывают корреспондентские счета. На основании накопленных за операционный день протоколов транзакций ПЦ готовит и рассылает итоговые данные для проведения взаиморасчетов между банками – участниками ЭПС, а также формирует и рассылает банкам-эквайерам и непосредственно в точки обслуживания стоп-листы (перечни карт, операции по которым по разным причинам приостановлены). Процессинговый центр может также обеспечивать потребности банков-эмитентов в новых картах, осуществляя их заказ на заводах и последующую персонализацию.

Особенностью продаж и выдач наличных по пластиковым картам является то, что эти операции осуществляются магазинами и банками «в долг». Гарантом выступает здесь банк-эмитент, выпустивший карты.

По виду расчетов с пластиковыми картами различают *кредитные* и *дебетовые* карты. Первые являются наиболее распространенным видом карт. При оплате с помощью кредитных карт банк покупателя открывает ему кредит на сумму покупки и через некоторое время (25 дней) присылает счет по почте, который покупатель, оплатив, должен вернуть обратно в банк. Естественно, что подобную схему банк может предложить только наиболее состоятельным и проверенным из своих клиентов, имеющих хорошую кредитную историю перед банком или солидные вложения в виде депозитов, ценностей или недвижимости. Держатель дебетовой карты должен заранее внести на свой счет в банке-эмитенте

определенную сумму, размер которой определяет лимит доступных средств. Контроль лимита выполняется при проведении авторизации. Как кредитная, так и дебетовая карты могут быть персональными, так и корпоративными.

В последние годы все большее внимание привлекают к себе ЭПС с использованием микропроцессорных карт (смарт-карт), принципиальным отличием которых является то, что они непосредственно несут информацию о состоянии счета клиента, являясь, в сущности, его транзитным счетом. Все транзакции здесь совершаются в режиме off-line в процессе диалога: карта-терминал или карта клиента – карта торговца. Такая система является почти полностью безопасной благодаря высокой степени защищенности кристалла с микропроцессором и полной дебетовой схеме расчетов. Кроме того, хотя смарт-карта дороже обычной, ЭПС оказывается дешевле в эксплуатации за счет того, что в режиме off-line нагрузки на телекоммуникации.

С точки зрения защиты информации в ЭПС существуют следующие уязвимые места:

1) пересылка платежных и других сообщений между банком и клиентом, между банками, между банком и банкоматом;
2) обработка информации внутри организаций отправителя и получателя сообщений;
3) доступ клиентов к средствам, аккумулированным на счетах.

Уязвимость пересылки определяется необходимостью защиты как оконечных систем, так и канала связи, через которые осуществляется взаимодействие отправителя и получателя электронного документа, что порождает следующие проблемы:

1) взаимное опознавание абонентов (взаимная аутентификация);
2) проблема обеспечения конфиденциальности и целостности документов при передаче по каналу связи;
3) проблема доказательства отправления и доставки документа;
4) обеспечение выполнения документа (проблема недоверия между отправителем и получателем из-за их независимости и принадлежности к разным организациям).

Для обеспечения функций защиты информации на отдельных узлах ЭПС должны быть реализованы следующие механизмы защиты:

1) управление доступом на оконечных системах;
2) контроль целостности сообщения;
3) обеспечение конфиденциальности сообщения;
4) взаимная аутентификация абонентов;
5) невозможность отказа от авторства сообщения;
6) гарантии доставки сообщения;

7) невозможность отказа от принятия мер по сообщению;
8) регистрация последовательности сообщений;
9) контроль целостности последовательности сообщений.

Качество решения обозначенных проблем определяется рациональным выбором криптографических средств при реализации механизмов защиты.

Электронные пластиковые карты

Одна из основных функций пластиковой карты стандартных размеров, изготовленной из специальной, устойчивой к механическим и термическим воздействиям пластмассы, заключается в обеспечении идентификации использующего ее лица как субъекта платежной системы (рис. 4). Для этого на карту наносят логотипы банка-эмитента и ЭПС, обслуживающую ее, имя держателя карты, номер его счета, срок действия карты и т. п. На карте могут присутствовать фотография держателя и его подпись. Алфавитно-цифровые данные – имя, номер счета и др. – могут быть эмбоссированы (нанесены рельефным шрифтом), что дает возможность при ручной обработке быстро перенести данные на чек с помощью устройства – импринтера, осуществляющего «прокатывание» карты с получением копии.

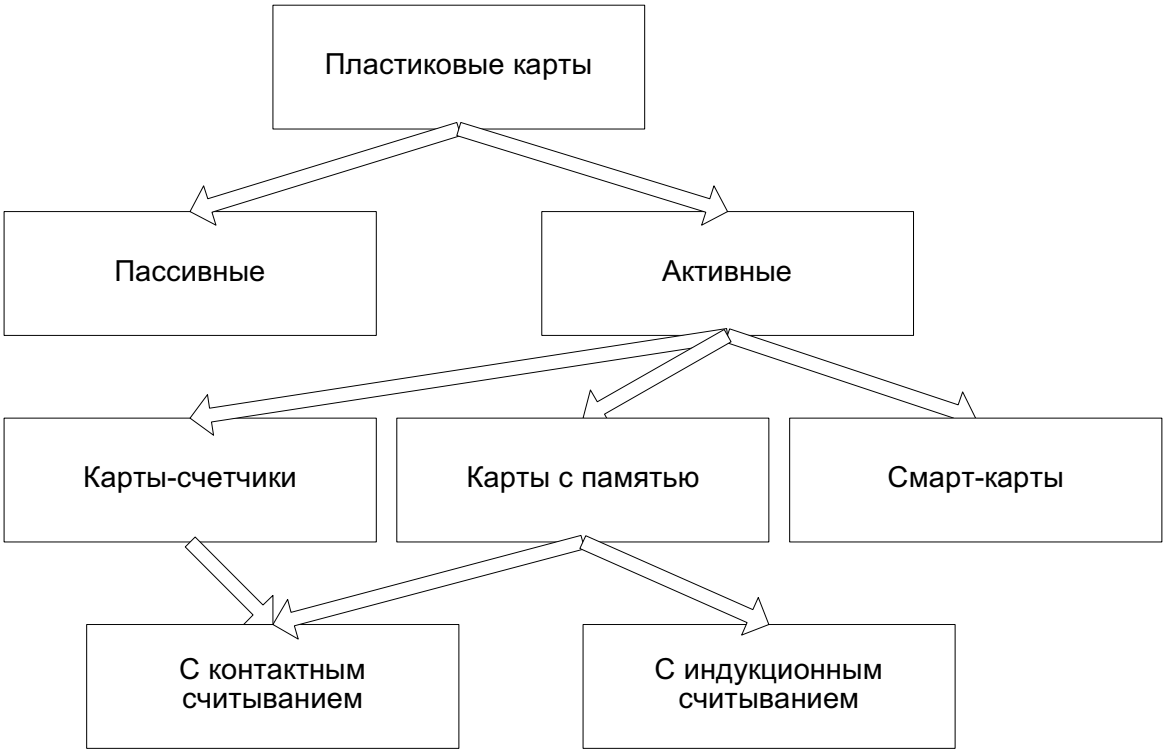


Рис. 4. Классификация пластиковых карт

Пассивные пластиковые карты всего лишь хранят информацию на том или ином носителе и представляют собой карты с магнитной полосой, которая располагается на обратной стороне карты. В соответствии со стандартом ISO 7811, она состоит из трех дорожек, первые две из которых предназначены для хранения идентификационных данных, а на третью дорожку можно записывать информацию, например текущее значение лимита дебетовой карты. Однако оперативная запись на магнитную полосу не практикуется (из-за невысокой надежности многократной записи-считывания), и эти карты используются только в режиме считывания информации.

Кроме того, эти карты уязвимы для мошенничества. Для повышения защищенности их фирмы *Visa* и *MasterCard/Europay* используют дополнительные графические средства защиты: голограммы и нестандартные шрифты для эмбоссирования. ЭПС с подобными картами требуют on-line авторизации в торговых точках и, как следствие, наличия разветвленных, высококачественных средств коммуникации (телефонных линий). Поэтому с технической точки зрения подобные системы имеют серьезные ограничения к применению в странах с широкоразвитыми системами связи.

Отличительная особенность *активных* карт – наличие встроенной в них микросхемы. *Карты-счетчики* используются в специализированных приложениях с предоплатой (за использование телефона-автомата, оплата автостоянки и т. п.), когда платежная операция требует уменьшения остатка на счете держателя карты на некоторую фиксированную сумму. Применение карт-счетчиков ограничено и не имеет большой перспективы (правда, не в России, где они только входят в моду).

Карты с памятью – это в сущности перезаписываемая карта-счетчик, в которой приняты меры, повышающие ее защищенность от атак злоумышленников. Объем памяти в них составляет от 32 байт до 16 Кбайт, которая реализуется или в виде ППЗУ (однократная запись и многократное считывание), или в виде электрически стираемого ППЗУ (ЭСППЗУ – многократная запись и считывание).

Эти карты можно разделить на два типа: с незащищенной (полнодоступной) и защищенной памятью. В картах первого типа нет никаких ограничений на чтение и запись данных, но их нельзя использовать в качестве платежных, так как специалист средней квалификации может достаточно просто их «взломать». Карты второго типа имеют две области: область идентификационных данных и одну или несколько прикладных областей. Первая допускает лишь однократную запись при персонализации и в дальнейшем доступна лишь для считывания. Доступ к прикладным областям регламентируется и осуществляется только при

выполнении определенных операций, в частности при вводе секретного PIN-кода.

Уровень защиты карт с памятью выше, чем у магнитных карт, и они используются в прикладных системах, в которых финансовые риски, связанные с мошенничеством, относительно невелики. Например, они используются в качестве платежного средства для оплаты таксофонов общего пользования, проезда на транспорте, в локальных платежных системах (клубные карты), в системах допуска в помещения и доступа к ресурсам компьютерных сетей (идентификационные карты). Карты с памятью имеют более низкую стоимость по сравнению со смарт-картами.

Смарт-карты (smart cards) или интеллектуальные карты представляют собой, по сути, микрокомпьютеры и содержат все основные аппаратные компоненты ЦП, ОЗУ, ПЗУ, ЭСППЗУ. Параметры их следующие:

1) ЦП с тактовой частотой 5 МГц;
2) ОЗУ емкостью до 256 байт;
3) ПЗУ емкостью до 10 Кбайт;
4) энергонезависимое ЗУ емкостью до 8 Кбайт.

В ПЗУ записан специальный набор программ, называемый COS *(Card Operation System),* который поддерживает файловую систему, базирующуюся в ЭСППЗУ и обеспечивающую регламентацию доступа к данным. При этом часть данных доступна только внутренним программам карточки.

Смарт-карта обеспечивает обширный набор функций:

1) разграничение полномочий доступа к внутренним ресурсам (благодаря работе с защищенной файловой системой);
2) шифрование данных с применением различных алгоритмов;
3) формирование ЭЦП;
4) ведение ключевой системы;
5) выполнение всех операций взаимодействия владельца карты, банка и торговца.

Некоторые смарт-карты обеспечивают режим «самоблокировки» (невозможность дальнейшей работы с ней) при попытке несанкционированного доступа. Смарт-карты позволяют существенно упростить процедуру идентификации клиента. Для проверки PIN-кода применяется алгоритм, реализуемый ЦП на карте, что позволяет отказаться от работы POS-терминала и банкомата в режиме реального времени и централизованной проверки PIN. Эти особенности делают смарт-карту высокозащищенным платежным инструментом, который может быть использован в финансовых приложениях, предъявляющих повышенные

требования к защите информации, именно поэтому они рассматриваются как наиболее перспективный вид пластиковых карт.

По принципу взаимодействия со считывающим устройством карта *с контактным считыванием* имеет на своей поверхности 8 – 10 контактных пластин. Карты ***с*** *индукционным считыванием* надежнее и долговечнее.

Персонализация и авторизация карт являются важными этапами подготовки и применения пластиковых карт. *Персонализация* карты осуществляется при ее выдаче клиенту, когда на карту заносятся данные, позволяющие идентифицировать карту и ее держателя, а когда необходимо осуществить проверку платежеспособности карты – при приеме ее к оплате в случае выдачи наличных денег. *Авторизация* – это процесс утверждения продажи или выдачи наличных денег по карте, который зависит от типа карты, схемы платежной системы (кредитная или дебетовая) и технической оснащенности точки обслуживания.

Способами персонализации являются следующие:

1. эмбоссирование;
2. кодирование магнитной полосы;
3. программирование ЭСППЗУ.

Исторически сложилось, что первоначально было эмбоссирование – процесс рельефного тиснения на пластиковой основе карты следующих данных: номер карты; дата начала и конца срока ее действия; фамилия и имя владельца. Эмбоссированная карта служит средством платежа при использовании импринтера. Кодирование магнитной полосы производится, как правило, на том же оборудовании, что и эмбоссирование. При этом часть информации о карте, содержащая номер карты и период ее действия, одинаковая как на магнитной полосе, так и на рельефе. Программирование микросхемы осуществляется обычным способом, но имеет некоторые организационные особенности, заключающиеся в том, что операции по программированию для повышения безопасности разнесены территориально и разграничены по правам различных сотрудников, участвующих в этом процессе. На первом рабочем месте выполняется активация карты (ввод ее в действие), на втором – операции, связанные с обеспечением безопасности, на третьем – производится собственно персонализация карты.

Персональный идентификационный номер

Испытанным средством идентификации банковской карты является использование секретного персонального номера PIN, значение которого должно быть известно только держателю карты. Длина PIN может

быть от 4 до 8 десятичных цифр. Чем больше цифра, тем меньше вероятность подобрать ее методом перебора, при этом вероятность возрастает, если подбор происходит подряд несколько дней. Поэтому банки вводят абсолютный предел на число неверных попыток, ликвидируя атаку подобного рода.

Значение PIN однозначно связано с соответствующими атрибутами банковской карты, поэтому трактуется как подпись держателя карты. Чтобы инициировать транзакцию, держатель карты, используя POS-терминал, вставляет свою карту в специальную щель считывателя и вводит свой PIN-номер на специальной клавиатуре терминала. Если значение PIN и номер счета клиента, записанный на магнитной полосе карты, согласуются между собой, тогда инициируется транзакция.

Защита PIN-номера является критичной для безопасности всей ЭПС. Банковские карты могут быть утеряны, украдены или подделаны. Тогда единственной контрмерой против несанкционированного доступа остается секретное значение PIN. Поэтому открытая форма РШ должна быть известна только законному владельцу карты. Она никогда не хранится и не передается в рамках ЭПС. Очевидно, что значение PIN необходимо держать в секрете в течение срока действия карты.

Метод генерации значения PIN оказывает существенное влияние на безопасность ЭПС. Вообще клиент различает два типа PIN:

1) назначенный ему банком;
2) выбираемый держателем карты самостоятельно.

Для первого типа есть два пути генерации:

1) выделение PIN номера криптографическим способом с помощью секретного ключа и крипто-алгоритма (например, DES) из номера счета держателя карточки;
2) банк выбирает значение PIN случайным образом, сохраняя его в виде криптограммы, и передает его держателям банковских карт, пользуясь защищенным каналом.

Использование PIN, назначаемого банком, неудобно, его трудно удержать в памяти. Для большего удобства клиента используют значение PIN, выбираемое им самим, что позволяет ему использовать один и тот же PIN для различных целей и для удобства запоминания задавать его как совокупность букв и цифр.

При идентификации клиентов по значению PIN и предъявленной карте используются два основных способа проверки: *неалгоритмический* и *алгоритмический.* Первый – не требует применения специальных алгоритмов и осуществляется непосредственным сравнением введенного клиентом PIN номера со значениями, хранимыми в базе данных (где эти номера зашифрованы методом прозрачного шифрования, что повы-

шает защищенность карты, не усложняя процесса сравнения). Второй способ заключается в том, что введенный клиентом PIN-номер преобразуют по определенному алгоритму с использованием секретного ключа и затем сравнивают со значением, хранящимся на карте.

Достоинства этого способа заключаются в следующем:

1) отсутствие открытой копии PIN на главном компьютере исключает его раскрытие персоналом банка;
2) отсутствие открытой передачи между главным компьютером и банкоматом или POS-терминалом (что исключает перехват или навязывание результатов сравнения);
3) отсутствие необходимости работы в реальном режиме времени (упрощается программирование) .

Обеспечение безопасности систем POS и банкоматов

Безопасность систем POS. Самым уязвимым местом систем POS являются ее POS-терминалы. Типичный POS-терминал снабжен устройствами считывания с любых пластиковых карт; энергонезависимой памятью; портами для подключения PIN-клавиатуры, принтера, модема, ПЭВМ или электронного кассового аппарата. Работать он может в режимах как реального времени (on-line) и с накоплением транзакций (off-line). Размеры и вес его сопоставимы с аналогичными параметрами телефонного аппарата, цена порядка 1,5 тысяч долларов США.

Изначально предполагается, что он не защищен от внешних воздействий. Угрозы для него связаны с возможностью раскрытия находящегося в нем секретного ключа и служащего для шифрования информации (передаваемой им в банк-эквайер), так как POS-терминалы устанавливаются в неохраняемых местах (магазины, автозаправочные станции и т. п.). Эти потенциальные угрозы получили название «обратное трассирование» (восстановление PIN в предыдущих транзакциях) и «прямое трассирование» (восстановление PIN в последующих транзакциях).

Для защиты от них предложены три метода, обеспечивающие смену ключа при каждой транзакции:

1) метод *выведенного ключа* (за счет генерации нового ключа с помощью однонаправленной функции из его текущего значения и некоторой случайной величины);
2) метод *ключа транзакции* (уникальный ключ, для генерации которого используют три составляющих – однонаправленную функцию от значения предыдущего ключа, содержание транзакции и информацию, полученная от карты);
3) метод *открытых ключей* (по аналогии со схемой Диффи-Хеллмана).

Безопасность банкоматов. Банкомат – это банковский автомат для выдачи и инкассирования наличных денег при операциях с пластиковыми картами. Кроме того, он позволяет держателю карты получать информацию о текущем состоянии счета, а также переводить операции по перечислению с одного счета на другой. Банкомат снабжен устройствами считывания с карт, клавиатурой для ввода PIN, ПЭВМ, платами X.25, а иногда и модемами. Денежные купюры размещаются в купюрах, хранящихся в специальном сейфе. Банкоматы монтируют капитально для пресечения возможных хищений, они имеют большие габариты и вес, размещают их как в охраняемых помещениях, так и непосредственно на улице. Работать они могут также в режимах (on-line) и (off-line).

В настоящее время распространенной формой эксплуатации банкоматов является *сеть банкоматов,* в которой участвуют несколько банков. Цель такой сети состоит в уменьшении стоимости операций, разделении затрат и риска для участников, преодолении географических ограничений и соответственно повышении субъективной ценности услуг для потребителей. Однако возникает серьезная проблема – защита конфиденциальности информации банков друг от друга (ключи шифрования, распределение ключей и т. п.)

Универсальная электронная платежная система UEPS

Ввиду недостаточного развития линий связи в России наиболее перспективны ЭПС, основанные на автономном принципе (off-line) обслуживания владельцев карточек в торговой точке или банкомате. Универсальная ЭПС (UEPS) отвечает этим требованиям и отличается высоким уровнем защищенности. Именно на основе этой технологии построена ЭПС «Сберкарт» с использованием смарт-карт в Сбербанке РФ. Концепция и технология UEPS разработана французской компанией NET I International.

Основным технологическим принципом UEPS является осуществление всех финансовых транзакций в режиме off-line при непосредственном взаимодействии двух смарт-карт. Алгоритмом шифрования служит DES. Высокая криптостойкость обеспечивается двойным шифрованием на ключах длиной 8 байт. В ЭПС, работающих в режиме off-line, большая часть функций обеспечения контроля по защите от мошенничества ложится на смарт-карту, как на базовый элемент UEPS.

В этой системе используются три основных смарт-карты:

1) служебные карты персонала банка;
2) торговые карты;
3) карты клиента.

В каждой из них 8-битовый микропроцессор. Основные характеристики: процессор – SGS – *Thompson,* 8 бит, система команд *Motorola* 6805; ОС – многозадачная операционная система чипа (MCOS); ОЗУ – 160 Кбайт; ПЗУ – 6 Кбайт; ЭСППЗУ – 2 Кбайта.

Особенности защиты UEPS заключаются в следующем:

1) конструкция и архитектура микропроцессора не позволяют осуществить механическое считывание информации путем спиливания кристалла по слоям, сканирования электронным микроскопом, воздействия ультрафиолетом и т. п. – при попытках совершить подобные операции микропроцессор полностью выходит из строя;
2) процессор контролирует доступ к защищенным областям памяти, передавая управление специальной прикладной программе UEPS;
3) вся информация поступает извне на карту (а также покидает ее) в зашифрованном виде и расшифровывается прикладной программой внутри самой карты с использованием ключей, хранящихся в защищенных областях памяти;
4) банковские ключи никогда не покидают карту в открытом виде;
5) схема распределения ключей и паролей системы UEPS тщательно проработана по картам банка, торговца и клиента.

Архитектура UEPS состоит из трех уровней:

1) центр эмиссии;
2) банки-участники;
3) операционные пункты.

Остановимся только на основном – центре эмиссии. Он выполняет следующие функции:

1) генерация генерального (мастер-ключа) и системообразующего ключей ЭПС;
2) первичная эмиссия смарт-карт – присвоение картам уникальных серийных номеров USN, занесение на карту общесистемной идентифицирующей и контрольной информации, а также генерального ключа системы;
3) ведение справочников участников расчетов, регистрация новых участников;
4) ведение справочников типов карт и кодов валют, используемых в системе;
5) ведение единой базы данных по заводским номерам и USN-номерам карт, имеющих хождение в системе.

Торговые учреждения и банковские пункты выдачи наличности оснащаются терминалами типа EFT-10 с программным обеспечением UEPS. Терминал имеет два считывателя для смарт-карт. В один в начале

рабочего дня вводится карта торговца, в другой – карта покупателя при оплате покупки.

Торговый терминал, постоянно находящийся вне банковского контроля, является с точки зрения безопасности одним из самых уязвимых элементов ЭПС. Он может подвергаться попыткам взлома (несанкционированного доступа) со стороны криминальных структур. Недопустимо доверять торговому терминалу секретную, критичную с точки зрения функционирования ЭПС информацию, т. е. банковские ключи и пароли, алгоритмы шифрования, списки финансовых транзакций и т. п. Поэтому он играет роль элемента, обеспечивающего интерфейс двух защищенных смарт-карт: клиента и торговца. Все платежные операции совершаются только в их диалоге. При этом вне карт вся информация всегда зашифровывается на базе сессионных (сеансовых) ключей. Сеансовый ключ вырабатывается также как парный ключ связи в схеме Диффи-Хеллмана и является уникальным для каждого сеанса связи карточек клиента и торговца. Кроме того, он находится только в памяти обеих карт и никогда их не покидает. На базе этого ключа зашифровываются все информационные потоки между картами, что делает бесполезными попытки перехвата сообщений в торговом терминале.

И, наконец, для обеспечения контроля безопасности и решения спорных ситуаций в ЭПС необходима эффективная схема организации сквозной уникальной нумерации и учета платежных транзакций, которая состоит из композиции следующих элементов:

1) уникальный серийный номер карты клиента в системе;
2) порядковый номер транзакции по списку транзакций на карте клиента;
3) уникальный серийный номер карты магазина в системе;
4) порядковый номер транзакции по списку транзакций на карте магазина;
5) порядковый номер инкассации карты магазина.

Реализация этой схемы позволяет однозначно проследить прохождение транзакции по всем элементам системы: Банк–Клиент–Магазин–Банк.

Обеспечение безопасности электронных платежей через сеть Internet

Сегодня Internet может рассматриваться как огромный рынок, способный охватить практически все население нашей планеты. Места совершения сделок постепенно перемещаются от традиционных рынков к более комфортным для потребителя – в дом или офис. Именно поэтому производители программных и аппаратных средств, торговые и финансовые организации активно развивают различные виды и методы ведения коммерческой деятельности в Internet – электронной торговли, проявляя надлежащую заботу об обеспечении ее безопасности.

Под термином «электронная торговля» понимают предоставление товаров и платных услуг через глобальные информационные сети. Основными видами электронной торговли являются:

1) продажа информации (например, подписка на базы данных, функционирующих в режиме on-line);
2) концепция «электронных магазинов» (Web-site, в котором имеется оперативный каталог товаров, виртуальная «тележка» покупателя и средства оплаты);
3) электронные банки, основным достоинством которых являются относительно низкая себестоимость и широкий охват клиентов (эти банки имеют свои собственные системы безопасности и защиты электронной информации, например, специальные карты-генераторы случайных паролей, синхронизируемых с паролем на банковском сервере, или персональные смарт-карты, также позволяющие генерировать сеансовые ключи).

Основные методы защиты электронной торговли должны обеспечивать немедленную авторизацию и шифрование финансовой информации в сети Internet, что позволяет обеспечить два типа протоколов: известный SSL и протокол SET (Secure Electronic Transactions). Последний предполагается использовать исключительно для шифрования финансовой информации.

Протокол SET должен гарантировать непременное соблюдение следующих условий:

1) абсолютная конфиденциальность информации;
2) полная сохранность данных (одним из средств, обеспечивающих это, является ЭЦП);
3) аутентификация счета владельца карточки и коммерсанта (это обеспечит, с одной стороны, сертификат владельца и ЭЦП, с другой – сертификат коммерсанта и ЭЦП).

Протокол SET гарантирует, что при взаимодействиях владельца карточки с коммерсантом через Internet информация о счете кредитной карточки будет оставаться конфиденциальной, так как для защиты транзакций используются процедуры шифрования и ЭЦП, при этом применяются криптосистемы обоих типов: симметричные и асимметричные. Правила SET предусматривают комбинированное шифрование сообщения: сначала с использованием случайным образом сгенерированного симметричного ключа, который для передачи по сети, в свою очередь, шифруется (а затем расшифровывается) по методу Диффи-Хеллмана. В результате образуется *электронный конверт.* Целостность информации и аутентификация участников транзакции гарантируются использованием ЭЦП.

Для защиты сделок от мошенничества и злоупотребления организованы специальные центры (агентства) сертификации в Internet, которые следят за тем, чтобы каждый участник электронной коммерции получал бы уникальный электронный сертификат, в котором с помощью секретного ключа сертификации зашифрован открытый ключ данного участника коммерческой сделки. Сертификат генерируется на определенное время и для его получения клиент должен представить в центр сертификации документ, подтверждающий личность участника. Затем, имея «на руках» открытый ключ центра сертификации, он может участвовать в сделках.

Технологические решения электронной торговли основаны на использовании следующих наборов компонент:

1) клиентский компьютер, имеющий доступ в Internet и Web-brouser;
2) сервер электронной торговли, на котором ведется каталог товаров и принимаются зашифрованные запросы клиентов на покупку тех или иных товаров;
3) средство для взаимной конвертации протоколов Internet и стандартных протоколов авторизации (ISO 8583 и др.).

Существуют различные технологические решения для электронной торговли:

1) адаптация технологии кредитных карт (существующих еще с 60-х гг.) к современным электронным технологиям;
2) внедрение концепции «чисто» *электронных денег;*
3) система с использованием специальных смарт-карт, предполагающих эмиссию электронных денег.

Электронные деньги представляют собой специальную последовательность электронных деноминаций и электронных подписей, подготовленных банками и приобретаемых за наличные. Клиент банка заводит виртуальный электронный «кошелек», поместив в него определенную сумму денег. В качестве эквивалента любой мелкой монеты используется 64-битовый номер, который переводится на жесткий диск конкретного пользователя. Дальнейшая оплата товаров и услуг осуществляется перечислением соответствующей битовой информации. Затем продавец, получив за оказанные услуги или покупку электронные деньги, возвращает электронную наличность банку в обмен на настоящие деньги.

Достоинствами такого типа технологии являются: конфиденциальность (движение электронной наличности невозможно проследить, и банк не связывает номера с каким-либо конкретным лицом, поэтому не может раскрыть инкогнито плательщика) и гарантированная безопасность для банков (любой покупатель может потратить только ту сумму, которую он имеет на счете). Недостатком является то, что электронные

деньги ничем не гарантированы. Например, если жесткий диск выходит из строя, или разоряется электронный банк, или кракеры расшифровывают номера электронной наличности, то во всех случаях нет никакого способа вернуть утраченную клиентом наличность, поскольку банк не связывает деньги с именем клиента и не может компенсировать потери клиента.

Контрольные вопросы и упражнения

7.1. Приведите методы формирований функций защиты.
7.2. Какие события возможны при воздействии негативных факторов на информацию?
7.3. Опишите, что относится к классу задач защиты информации уменьшения степени распознавания объектов? Приведите примеры экономических информационных систем.
7.4. Какие особенности классов задач защиты содержания обрабатываемой, хранимой и передаваемой информации? Приведите примеры банковских экономических систем.
7.5. Каким образом решаются задачи класса защиты информации от информационного воздействия? Приведите примеры информационных компьютерных систем.
7.6. Приведите состояние и функции системы защиты информации.
7.7. Что такое стратегия защиты информации? Какие стратегии защиты информации Вы знаете?
7.8. Какие способы и средства обеспечения безопасности Вы знаете? Приведите классификацию и примеры.
7.9. Из каких условий исходят при построении системы защиты информации?
7.10. Приведите требования к архитектуре системы защиты информации.
7.11. Какие общеметодологические принципы необходимо использовать при проектировании архитектуры защиты информации?
7.12. Из каких механизмов организационно должно состоять средство защиты информации?
7.13. Что такое «ядро средства защиты информации»? Каковы его цели и функции?
7.14. Какие ресурсы есть у средства защиты информации? Каким образом они взаимодействуют с ядром?
7.15. Что входит в организационное построение средства защиты информации?
7.16. Приведите особенности построения защищенных экономических систем.

7.17. Как взаимосвязаны принципы функционирования платежных систем с построением архитектуры средств защиты информации? Приведите примеры.
7.18. Каким образом функционирует пластиковая карта? Какие ядра пластиковых карт вы знаете?
11.19. Каковы особенности технологии работы с ключевыми носителями в платежных системах? Что такое сеансовый ключ?
7.20. Какова архитектура распределенных безопасных систем? В чем особенности ее построения?
7.21. Приведите примеры платежных систем. Какую защиту информации они предусматривают?
7.22. В чем особенности платежной системы S.W.I.F.T.?
7.23. В чем особенности платежной системы UEPS?
7.24. Какие средства предусматриваются для обеспечения безопасности банкоматов?
7.25. Каким образом обеспечивается безопасность электронных платежей через сеть Internet?
7.26. Приведите технологические решения для электронной торговли. Приведите примеры.
7.27. Какими последствиями грозит нарушение информационной безопасности экономических систем страны национальной безопасности?

8. БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И КОМПЬЮТЕРНЫХ СЕТЕЙ[8]

Компьютерные сетевые технологии и особенности безопасности сетей

Первая сетевая компьютерная технология – *централизованные* системы *доставки информации*, применявшиеся несколько лет назад, – позволяла сравнительно легко находить необходимые данные, однако в ней был затруднен обмен информацией, и централизованные компьютерные системы были сложны и дороги. Следующая технология *клиент-сервер* – получение информации из сети персональных компьютеров – оказалась дешевле, но пользователи ищут необходимые данные на множестве машин, среди большого числа приложений с различными интерфейсами. Однако она тоже не оправдала себя, т. к. заговорили всерьез о защите информации в компьютерных сетях.

В середине 90-х гг. появилась новая технология, заимствованная из организации глобальных компьютерных сетей Internet и представляющая собой *технологию универсального клиента* Web-сервиса. Оказалось, что Web-серверы и Web-навигаторы могут и должны использоваться не только для глобального обмена информацией со значительными информационными потоками, но Web-сервис – это сервис, необходимый каждой организации со сколько-нибудь заметными информационными потоками. Поэтому он сразу после возникновения стал использоваться не только в Internet – *глобальной вычислительной сети,* для которой и был создан, но и в рамках небольших *локальных вычислительных сетей,* разработанных по протоколу TCP/IP, т. е. в режиме своеобразно внутреннего Internet, или, как его называют теперь, – Intranet.

И, наконец, последнее достижение – *Java-технология,* при применении которой Web-сервис, и без того имевший огромную популярность в мире, получил как бы новый импульс. Миллион пользователей,

---

[8] Приводится по работам [19, 28]

уже привыкших в Internet работать с Web-страничками, где информация организована по принципу раскрывающихся гнезд на домашней страничке, с появлением *Java* просто получили крылья – теперь стало возможно творить все, не выходя из Web-браузера: запускать приложения, находящиеся на сервере, получать результаты прямо в HTML-страничку, не заботиться о клиентской части, распределенной среде, о доступе к различным базам данных. Открылись поистине безграничные возможности как в Internet, так и в Intranet-сетях.

Итак, современная компьютерная инфраструктура чаще всего ассоциируется с Internet и корпоративными Intranet-сетями. При этом Intranet-сети, используя разработанные в Internet Web-технологии, все более интегрируются с Internet. Последнее становится необходимым, так как вызвано появлением многочисленных услуг, которые предоставляет Internet: глобальная электронная почта, практически всемирная реклама, оперативное получение информационных новостей, доступ к современным информационным и программным ресурсам, оперативное получение консультаций квалифицированных специалистов, возможность организации совместной работы территориально разнесенных групп, электронная торговля, удаленный доступ к корпоративной сети, использование речевой и видеоинформации и т. п.

Базовую основу для Intranet-сетей составляют TCP/IP, NFS, Web-серверы, HTML-редакторы и e-mail. Такие сети и системы, создаваемые на основе стандартов Internet, отличаются относительной простотой настройки, низкой стоимостью, легко масштабируются, поддерживают распределенную обработку информации и обеспечивают быструю отдачу вложений. Основным сдерживающим препятствием развития Intranet являются общеизвестные факты нарушения безопасности в Internet и через Internet (согласно данным ФБР США ежегодный ущерб от компьютерных преступлений составляет около 7,5 млрд долларов и 80 % из них совершается через Internet). Отмеченная выше совместимость архитектурных концепций в различного класса сетях повлияла и на *обеспечение безопасности* обоих сетей. Теперь речь должна идти не о защищенности Internet, а об обеспечении принципа *разумной достаточности информационной безопасности* сети.

Под ним понимают следующее:

1) в сети не должна храниться информация, раскрытие которой приведет к серьезным последствиям;
2) в сети должна храниться информация, распространение которой желательно ее владельцу;
3) необходимо учитывать тот факт, что в любой момент хранимая в сети информация может быть перехвачена, искажена, стать недоступной.

Если речь идет как о безопасности Intranet-сетей, так и о передаче между ними информации через Internet, то естественно разумной достаточности информационной безопасности может не хватить, особенно в зависимости от критичности сети (ее типа и назначения). Поэтому необходимо применять специальные методы защиты для Intranet сетей и для них *проблемы безопасности выходят на первый план,* ибо помимо защиты информации в корпоративной сети необходимо учитывать возможность атак ее со стороны Internet.

Таким образом, особенности информационной безопасности сетей ЭВМ будут определяться прежде всего их типом, который зависит от того, где и с какой целью используются эти сети. Например, ясно, что Internet создавался как незащищенная система, не предназначенная для хранения и обработки конфиденциальной информации. Более того, защищенный Internet не смог бы стать той системой, которой он сейчас является, и не превратился бы в информационный образ мировой культуры, ее прошлого и настоящего. Именно поэтому развитие средств безопасности Internet должно войти в противоречие с ее назначением и речь должна идти не о защищенности Internet, а об обеспечении в ней упомянутого выше принципа разумной достаточности безопасности.

Защита информации в современных Intranet-сетях – информационных телекоммуникационных системах

Проблемы, связанные с защитой информации в современных информационных телекоммуникационных системах (ИТКС), как распределенных, так и локальных, которые сегодня и представляют собой сети Intranet, обычно включают в себя вопросы следующих компонентов:

1) информационных ресурсов локальной рабочей станции от НСД;
2) локальных сетей передачи данных;
3) межсетевого взаимодействия (реализуется созданием защищенных виртуальных сетей (VPN) на базе общедоступных сетей передачи данных; созданием защищенного взаимодействия между клиентом и сервером: обеспечением авторизованного доступа клиента к ресурсам, предоставляемым целевым сервером – например, защита при доступе к Web-серверам; обеспечением защиты информационных ресурсов корпоративной сети от атак извне; обеспечением защиты пользовательского взаимодействия, например, шифрование данных при обмене информации типа «точка-точка»);
4) электронной почты и документооборота;
5) электронных платежных систем (в том числе и осуществляющих платежные операции через Internet).

Реализация этих проблем определяется в соответствии с принятой политикой безопасности и выражается как в виде отдельных аппаратно-программных решений, так и в объединении организационно-административных мер и аппаратно-программных средств.

При этом на практике необходимо обеспечивать не только конфиденциальность, целостность и достоверность информации, но и ее доступность (включая доступность информационных ресурсов), или, другими словами, обеспечивать защиту от атак типа *отказ в обслуживании.*

Кроме того, при использовании криптографических алгоритмов особые требования выдвигаются к выбору ключевых систем, заключающиеся в следующем:

1) устойчивость к компрометации (компрометация ключа у одного пользователя не должна сказаться на работе всей системы в целом);
2) наличие у пользователей минимального числа ключей, защищенных особыми организационными (лучше техническими) мерами;
3) обеспечение защиты от копирования;
4) наличие механизмов плановой смены секретных ключей и сертификатов открытых ключей.

И, наконец, уровень безопасности и надежности системы защиты зависит не только от стойкости выбранных средств защиты информации (СрЗИ) или политики безопасности, но и от эффективности интеграции СрЗИ в целевую систему. Для аппаратных СрЗИ эта интеграция есть разработка и реализация процедур сопряжения (интерфейсов подключения устройств к рабочей станции, например RS-232, PCI-слот и т. п.). Для программных СрЗИ критичным становится вопрос о проверке среды (конкретно ОС) на наличие недокументированных возможностей и создании вариантов построения доверенной программной среды. Кроме того, встраивание программных СрЗИ может осуществляться одним из следующих споров: с использованием программных интерфейсов; с использованием криптосервера.

Программным интерфейсом (API) называется детальное описание функций и используемых ими параметров. Формат обращения к функциям (вызываемым и реализованным) поддерживает прикладное ПО, в которое интегрируется защитный механизм. Наиболее известные API – это CryptoAPI, GSS API и SSPI. *Криптосервер* локализует СрЗИ на особо выделенной рабочей станции и работает с критической к компрометации информацией (секретные ключи, пароли и т. п.). В прикладное ПО, работающее на другой (находящейся на связи) рабочей станции, встраиваются только вызовы функций, реализованных в ПО криптосервера.

Полная система защиты информации ИТКС в соответствии с рассмотренными в начале настоящего раздела основными компонентами должна состоять из пяти подсистем:

1) защиты локальных рабочих мест;
2) защиты локальных вычислительных сетей (ЛВС);
3) защиты межсетевого взаимодействия;
4) подсистемы аудита и мониторинга;
5) подсистемы технологической защиты.

Основными задачами первой подсистемы защиты являются:

1) разграничение доступа к ресурсам пользователей АРМ ИТКС;
2) криптографическая защита хранящейся на АРМ информации (обеспечение ее конфиденциальности и целостности);
3) аутентификация пользователей и авторизация их действий;
4) обеспечение невозможности влияния аппаратно-программного обеспечения АРМ на функционирование прикладных процессов ИТКС;
5) контроль целостности прикладного и системного ПО.

Любая защита в современных ИТКС должна начинаться с конкретного АРМ, т. е. с защиты информации в персональных ЭВМ. Задачи обеспечения защиты здесь осложняются тем, что функционирование СрЗИ происходит в так называемой *недоверенной программной среде,* для которой невозможно однозначно доказать отсутствие влияния программного окружения на функционирование СрЗИ. Защита реализуется применением СрЗИ типа *электронный замок*: средств абонентского шифрования, штатных и дополнительных средств разграничения доступа, входящих в состав программного обеспечения АРМа.

К отечественным криптографическим аппаратно-программным СрЗИ, широко применяемым сегодня для локальных станций, относятся следующие:

1) средства криптографической защиты семейства «Верба» (разработка «МО ПНИЭИ» – www.security.ru) подразделяются на два класса: «Верба» – с симметричными ключами и «Верба-О» – с открытыми ключами;
2) комплекс «Аккорд» (разработка «ОКБ САПР» и «Инфокрипт»), основу которого составляет аппаратный модуль доверенной загрузки;
3) комплексы «Криптон», «Криптон-Вето», «Crypton Lite» (разработка фирмы «Анкад»), в которых симметричный алгоритм шифрования реализован аппаратно на основе СБИС «Блюминг-1К» и конструктивно выполнен как слот компьютера типа IBM PC;
4) средства криптографической защиты «CryptoPro CSP» (crypto servers provider) (разработка «Крипто Про»), включающее сертифицированный Удостоверяющий центр;
5) комплексы «Континент» (разработка НИП «Информзащита»), выполненные как в аппаратном, так и программном исполнении.

Особенность программной среды этих комплексов заключается в том, что она разбивается на две области:

1) замкнутая программная среда (в ее рамках обеспечивается защита от негативного влияния программного и системного ПО, в котором могут быть источники потенциальной опасности внедрения программ-закладок, вирусов, программ-шпионов и т. п.);
2) доверенная программная среда (среда, проанализированная на наличие недокументированных возможностей и ошибок, способных оказать негативное влияние на безопасность функционирования СрЗИ).

Характерными задачами второй подсистемы защиты являются:

1) защита от НСД к информации и информационным ресурсам в рамках ЛВС;
2) криптографическая защита информации, передаваемой в ЛВС, на прикладном уровне, уровне ОС и уровне кабельной системы.

Основными задачами третьей подсистемы являются:

1) защита информации, передаваемой от ИТКС во внешнюю среду;
2) защита информации и ресурсов внутри ИТКС с помощью мониторинга и аудита событий, связанных с нарушением безопасности, от внешних негативных воздействий со стороны внешних сетей.

Главные задачи четвертой подсистемы состоят в следующем:

1) осуществление централизованного, удаленного, автоматизированного контроля работы серверов, АРМ и других объектов СЗИ;
2) централизованное ведение протокола всех событий, происходящих на тех же объектах;
3) выполнение автоматизированного анализа механизма принятия решений во внештатных ситуациях;
4) первичный контроль независимости выполнения основных технологических операций и правомерности событий, связанных с обеспечением безопасности.

Наконец, *основными задачами пятой подсистемы являются*:

1) выработка принципов построения технологического процесса обработки информации в ИТКС;
2) определение контрольных точек технологического процесса;
3) определение мест использования средств и методов защиты информации для регистрации, подтверждения и проверки прохождения информации через контрольные точки технологического процесса;
4) исключение сосредоточения полномочий у отдельных должностных лиц.

Особенности защиты на уровнях взаимодействия ISO/OSI

В зависимости от уровня взаимодействия открытых систем (OSI/ISO), когда в качестве основы взят стек протоколов TCP/IP, существуют свои наборы механизмов и служб обеспечения безопасности и соответственно свои угрозы. При этом каждый уровень с точки зрения реализации СрЗИ имеет свои преимущества и недостатки. Кроме того, атаки на каждом уровне проводятся с целью компрометации, изменения или уничтожения критических ресурсов данного уровня. Поэтому каждый уровень в соответствии с возможными угрозами должен быть защищен специальными средствами защиты, которые, взаимно дополняя друг друга, в совокупности обеспечат защиту системы в целом.

Физический и канальный уровни. Здесь в качестве механизмов защиты используется шифрование соединения или трафика (всего или его части), т. е. обеспечивается конфиденциальность передаваемой информации. В качестве вероятных угроз выделяются следующие:

1) несанкционированное подключение;
2) ошибочная коммутация;
3) прослушивание;
4) перехват;
5) фальсификация информации;
6) имитоатаки;
7) физическое уничтожение канала связи.

Для защиты на этих уровнях обычно применяют *скремблирование, шифрующие модемы, специализированные канальные адаптеры.*

Достоинства: простота применения, аппаратная реализация полная защита трафика, прозрачность выполнения СрЗИ своих функций. Недостатки: негибкость решения, низкая совместимость и высокая стоимость.

Сетевой уровень. Здесь решаются следующие задачи защиты информации:

1) защищаются непосредственно пакеты, передаваемые по сети;
2) в канале шифруется вся информация (защита трафика);
3) контролируется доступ к сети.

На данном уровне может быть реализована аутентификация рабочей станции, являющейся источником сообщений.

Угрозами могут являться:

1) анализ служебной информации сетевого уровня (топологии сети);
2) атаки на систему маршрутизации (модификация маршрутизационных таблиц через протоколы динамической маршрутизации и ICMP);

3) атаки на систему управления (фальсификация IP-адресов);
4) прослушивание, перехват и фальсификация информации;
5) имитоатаки.

К решениям, способным устранить угрозы, можно отнести:

1) пакетную фильтрацию;
2) административную защиту на маршрутизаторах;
3) протоколы зашиты информации сетевого уровня (защита и аутентификация трафика);
4) туннелирование;
5) векторизацию;
6) динамическое распределение сетевых адресов;
7) защиту топологии.

Достоинства: полнота контроля трафика, универсальность, прозрачность, совместимость, адаптивность к сетевой технологии. Кроме того, защита информации на этом уровне имеет ряд архитектурных преимуществ:

1) на сетевом уровне сеть становится полносвязанной системой, в то время как на более низких уровнях защита может быть реализована только как набор двухточечных звеньев защиты;
2) можно установить защищенное соединение между двумя компьютерами в любых точках сети;
3) появляется понятие топологии сети;
4) можно различить внутренние и внешние каналы и реализовать фильтрацию трафика между внутренней (корпоративной) и внешней (коммуникационной) сетью.

Недостатками являются:

1) неподконтрольность протоколов на транспортном и прикладном уровнях;
2) невозможно оказать существенное влияние на прикладные системы.

Транспортный уровень. На этом уровне опасными угрозами являются:

1) несанкционированные соединения и проведение разведки имеющихся приложений;
2) атаки на систему управления;
3) прослушивание, перехват и фальсификация информации;
4) имитоатаки.

Традиционные решения по защите от этих угроз:

1) защита в составе межсетевых экранов;
2) proxy-системы;
3) транспортные протоколы защиты и идентификация данных.

Достоинства: развитая функциональность и высокая гибкость защиты.

Недостатки: неполнота защиты и неподконтрольность событий в рамках прикладных и сетевых протоколов.

Прикладной уровень. Если необходимо применить к каким-то объектам этого уровня криптографические СрЗИ, то они должны продолжать действовать и на нижестоящих уровнях. Кроме механизмов обеспечения целостности и конфиденциальности, на прикладном уровне существует возможность обеспечить жесткую связь информации с породившим ее пользователем, т. е. обеспечить аутентификацию пользователя по созданной информации.

Основными угрозами на прикладном уровне следует считать:

1) НСД к данным;
2) разведку имен и паролей пользователей;
3) атаки на систему разграничения прав пользователей;
4) маскировку под легитимного пользователя;
5) атаки на систему управления и атаки через стандартные прикладные протоколы;
6) фальсификацию информации;
7) имитоатаки.

Защита на этом уровне может быть традиционна: встроенная защита приложений, межсетевые экраны с фильтрацией прикладных протоколов, proxy-системы и т. п.

Достоинства:

1) полнота и высокая функциональность в рамках конкретного приложения;
2) контроль на уровне действий конкретного процесса (пользователя).

Недостатки:

1) отсутствие универсальности;
2) ограниченность рамками заданного приложения;
3) неподконтрольность событий в нижележащих уровнях управления.

Криптографическая защита информации на этом уровне наиболее предпочтительна с точки зрения ее гибкости, однако ее аппаратно-программная реализация сложна.

Проблемы создания безопасных операционных систем сети

Цель нарушителей состоит в несанкционированном получении доступа к ресурсам Intranet-сети: транспортной среде, памяти адресному пространству. Основным назначением ОС сети является обеспечение корректного совместного использования прикладными программами

разнообразных ресурсов сети. Реализация *контроля безопасности информационных потоков* в системе обычно осложняется многообразием, разнородностью и многовариантностью путей информационного обмена, доступных для ОС. Особенности работы традиционных ОС заключаются в следующем.

Во-первых, традиционные ОС четко различают информационный обмен между процессами в системе (IPC) и доступ процессов к ресурсам ОС, под которыми здесь понимаются как аппаратные ресурсы (устройства ввода-вывода), так и программные (логические, виртуальные) ресурсы (файлы, процессы, семафоры). Большинство классических ОС опираются на различия между ресурсами и работают с каждым типом ресурсов по-своему.

Во-вторых, коммуникации между процессами очень многообразны и не подчиняются единой модели. Хотя и есть несколько общепринятых стандартов (RPC, программные каналы, сокеты), но в целом в каждой традиционной ОС используются свои специальные механизмы и протоколы обмена.

Популярный и проверенный метод «борьбы» со сложностью создаваемой системы – это применение объектно-ориентированного подхода при ее *анализе, проектировании (синтезе)* и *реализации,* с точки зрения которого термин *информационный обмен* представляет собой практически любые взаимодействия между сущностями в компьютерной системе, под которыми понимаются процесс, устройство, физический или логический ресурс, удаленный компьютер и т. д.

Некоторые попытки использования объектного подхода к проблеме доступа к ресурсу уже были приняты и реализованы в популярных ОС. В частности, в ОС UNIX дескриптор файла, устройства или сокета представляет собой относительно унифицированный интерфейс к ресурсу. В ОС Microsoft Windows NT используется, хотя и несколько ограниченная, но все же объектная модель ресурсов как на уровне приложений, так и на уровне самой ОС. В настоящее время отдельную нишу в рамках проблемы информационного обмена занимают объектные технологии DCOM, CORBA, JAVA и др. Данные технологии перспективны и заслуживают внимания, но большинство из них работает на более высоком уровне, чем ОС.

Поэтому для защиты сетей сегодня стоит задача создания защищенной ОС (ЗОС), которая должна строиться на объектной основе, регулировать доступ к системным ресурсам исходя из соображений не только их совместного использования конкурирующими приложениями, но и исходя из принятой в данной конкретной ЗОС политики безопасности. Эта политика должна оперировать абстрактными понятиями

субъекта и объекта, для которых на основании корректного набора правил делается вывод о предоставлении доступа субъекта к объекту (что и составляет модель безопасности).

Особенности функционирования межсетевых экранов

Многие задачи по отражению наиболее вероятных удаленных атак на Intranet со стороны Internet способен решать *межсетевой экран* (иностранные термины – *брандмауэр* – стена из огнеупорного материала – или *firewall*)**.** Межсетевой экран (МЭ) призван обеспечить безопасный доступ к Internet и ограничить доступ внешних пользователей к Intranet.

МЭ – это система межсетевой защиты, позволяющая разделить общую неоднородную сеть на две или более части и *реализовать набор правил,* определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Обычно МЭ защищают внутреннюю сеть предприятия от «вторжения» из глобальной сети Internet, однако они могут использоваться и для защиты от «нападений» из корпоративной Intenet-сети, к которой подключена локальная сеть предприятия.

МЭ пропускает через себя весь трафик, принимая для каждого проходящего пакета решение – пропускать его или отбросить. Для того чтобы МЭ мог это осуществить, ему необходимо определить набор правил фильтрации. Следует отметить, что ни один МЭ не гарантирует полной защиты внутренней сети при всех возможных обстоятельствах. Прежде чем перейти к основным компонентам МЭ, отметим «врожденные слабости» некоторых уже упоминавшихся распространенных служб Internet, для частичной ликвидации которых и применяются МЭ.

1. Прежде всего, это *набор протоколов управления* передачей сообщений TCP/IP, используемый в качестве межсетевого протокола и ставший *стандартом дефакто* для межсетевого взаимодействия. В заголовках пакетов TCP/IP указывается информация, на которую могут напасть *кракеры.* В частности, они могут подменить адрес отправителя в своих «вредоносных» пакетах, после чего они выглядят, как пакеты, передаваемые авторизованным клиентом.

2. Для простого *протокола передачи электронной почты* (Simple Mail Transfer Protocol – SMTP) одна из проблем безопасности заключается в том, что пользователь не может проверить адрес отправителя в заголовке сообщения электронной почты. В результате кракер может послать во внутреннюю сеть большое количество почтовых сообщений, что приведет к перегрузке и блокированию работы почтового сервера.

3. Популярная в Internet *программа электронной почты* – Sendmail – использует для работы некоторую сетевую информацию: IP-адрес отправителя. Перехватывая сообщения, отправляемые с помощью Sendmail, кракер может употребить информацию для нападений, например для *спуфинга* – подмены адресов.

4. *Протокол передачи файлов* (File Transfer Protocol – FTP) обычно рассматривают как один из методов работ с удаленными сетями. На FTP-серверах хранятся документы, программы, графики и другие виды информации. К ним нельзя обратиться напрямую, необходимо их сначала целиком переписать с FTP-сервера на локальный сервер. Некоторые из FTP-серверов ограничивают доступ пользователей к своим архивам данных с помощью паролей, а другие же предоставляют свободный доступ (так называемые анонимные FTP-серверы). Пользователь своего сервера, используя опции анонимного FTP, должен быть уверен, что там хранятся только файлы для свободного распространения.

5. *Служба сетевых имен* (Domen Name System – DNS) представляет собой распределенную базу данных, преобразующую имена пользователей и хост-компьютеров в IP-адреса (указываемые в заголовках пакетов), и наоборот. Для нее одной из проблем безопасности является то, что эту базу трудно «скрыть» от неавторизованных пользователей. В результате DNS часто используется кракерами как источник информации об именах доверенных хост-компьютеров.

6. *Служба эмуляции удаленного терминала* (TELNET). Пользователи, подключаясь к серверу TELNET (он используется для подключения к сети удаленных систем), должны регистрироваться на нем, вводя свое имя и пароль. Выйдя на сервер TELNET, кракер может сконфигурировать его программу так, чтобы она записывала имена и пароли пользователей.

7. *Всемирная паутина* (*World Wide Web* – WWW) – система, основанная на сетевых приложениях, позволяющих пользователям просматривать содержимое различных серверов в Internet или Intranet. Она дает пользователям возможность, используя гипертекстовые документы (в которых есть ссылки на другие документы и Web-узлы*),* легко переходить от одного узла к другому. Это полезное свойство WWW является и наиболее слабым ее местом, поскольку ссылки на Web-узлы содержат информацию о том, как осуществляется доступ к соответствующим узлам. Используя эту информацию, кракеры могут разрушить Web-узел или получить доступ к хранящейся в нем конфиденциальной информации.

К уязвимым службам и протоколам Internet относятся также протокол копирования UUCP, протокол маршрутизации RIP, графическая оконная система X Windows и др.

Рассматриваемый МЭ является набором компонентов, настраиваемых так, чтобы реализовать выбранную политику безопасности, принятую в защищаемой сети и определяет принимаемые решения по вопросу, фильтровать или нет с помощью МЭ конкретные протоколы. В частности, решает вопрос, будет ограничен доступ пользователей к определенным службам Internet на базе протоколов TCP/IP и если да, то до какой степени.

Сетевая безопасность предприятия должна содержать две политики:

1) политику доступа к сетевым сервисам;
2) политику реализации МЭ.

Политика доступа к сетевым сервисам обычно основывается на одном из следующих принципов: запретить доступ из Internet во внутреннюю сеть, но разрешить доступ из внутренней сети в Internet; разрешить ограниченный доступ во внутреннюю сеть из Internet, обеспечивая работу только отдельных «авторизованных» систем, например почтовых серверов.

В соответствии с политикой доступа определяется список сервисов Internet, к которым пользователи должны иметь ограниченный доступ, и задаются ограничения на методы доступа, например на использование протоколов SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Ограничение методов доступа необходимо для того, чтобы пользователи не могли обращаться к «запрещенным» сервисам Internet обходными путями. Например, если для ограничения доступа в Internet сетевой администратор устанавливает специальный шлюз (который не дает возможности пользователям работать в системе WWW), то они могут установить PPP-соединение с Web-серверами по коммутируемой линии.

Политика реализации МЭ определяет правила доступа к ресурсам внутренней сети. При этом прежде всего необходимо установить, насколько «доверительной» или «подозрительной» должна быть система защиты, т. е. правила доступа к внутренним ресурсам должны базироваться на одном из следующих принципов:

1) *запрещать все, что не разрешено в явной форме* (он обеспечивает значительную защищенность сети, однако реализация его обходится достаточно дорого и доставляет большие неудобства пользователям);
2) *разрешать все, что не запрещено в явной форме* (сеть менее защищена, но пользоваться ею удобней и требуются меньшие затраты при реализации).

Эффективность защиты внутренней сети с помощью МЭ зависит не только от выбранных политик, но и от рационального выбора и использования компонентов МЭ, функциональные требования к которым определяются:

1) фильтрацией на сетевом уровне;
2) фильтрацией на прикладном уровне;
3) настройкой правил фильтрации и администрированием;
4) средствами сетевой аутентификации;
5) ведением журналов и учетом.

Основные компоненты межсетевых экранов

Большинство компонентов МЭ относятся к одной из трех категорий:

1) фильтрующие маршрутизаторы (ФМ);
2) шлюзы сетевого уровня (ШСУ);
3) шлюзы прикладного уровня (ШПУ).

Их можно рассматривать как базовые компоненты реальных МЭ. Немногие МЭ включают в себя только одну из этих категорий.

Фильтрующие маршрутизаторы. Такой ФМ представляет собой работающую на сервере программу, которая способна фильтровать входящие и исходящие пакеты на основе информации, содержащейся в TCP- и IP-заголовках пакетов. Процесс инкапсуляции передаваемых данных и формирования TCP- и IP-заголовков в стеке протоколов TCP/IP известен и представлен на рис. 5.

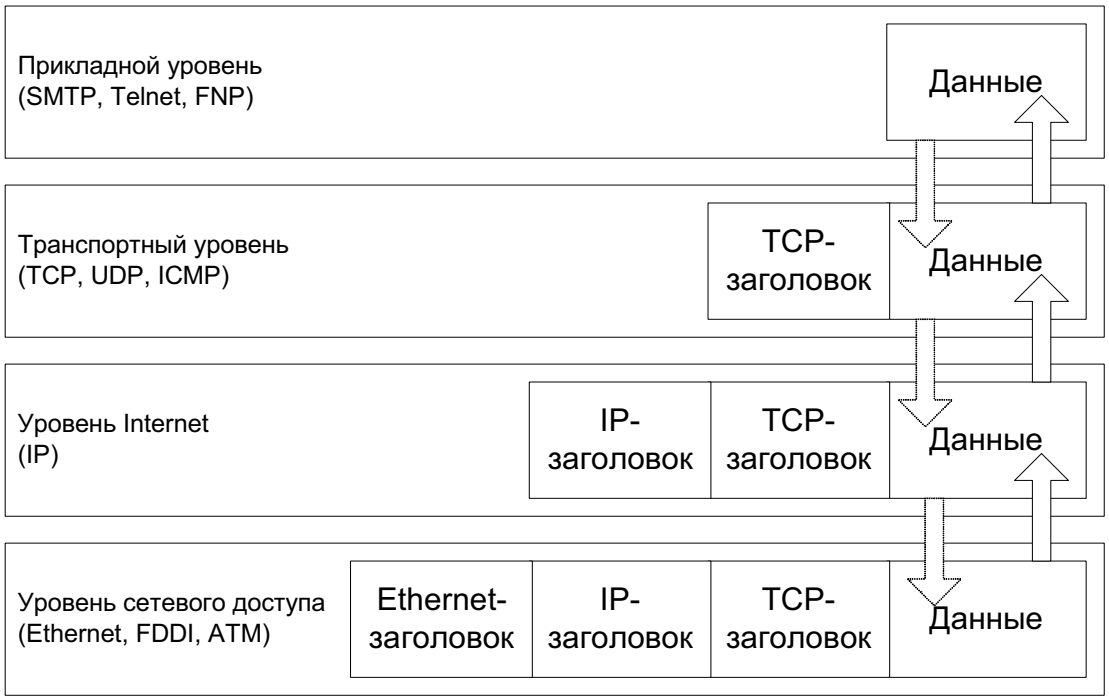


Рис. 5. Схема инкапсуляции данных в стеке протокола TCP/IP

Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы следующих полей заголовка пакета:

1) IP-адрес отправителя (адрес системы, которая послала пакет);
2) IP-адрес получателя (адрес системы, которая принимает пакет);

3) порт отправителя (порт соединения в системе-отправителе);
4) порт получателя (порт соединения в системе-получателе). Порт – программное понятие, используемое клиентом или сервером для посылки (приема) сообщений и идентифицируемое 16-ю битами.

В настоящее время не все ФМ фильтруют пакеты по TCP/UDP порту отправителя, однако многие производители ФМ начинают к этому стремиться. Некоторые ФМ проверяют, с какого сетевого маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации. Фильтрация может быть реализована различным образом для блокирования соединений с определенными хост-компьютерами или портами. Например, можно блокировать соединения от конкретных адресов сетей и хост-компьютеров, считающихся враждебными или ненадежными.

Добавление фильтрации по портам TCP и UDP к фильтрации по IP-адресам обеспечивает большую гибкость. Известно, что такие серверы, как демон TELNET, обычно связаны с конкретными портами (например, порт 23 протокола TELNET). Если же МЭ может блокировать соединение TCP (или UDP) с определенными портами или от них, то можно реализовать политику безопасности, при которой некоторые виды соединений устанавливаются только с конкретными хост-компьютерами. Например, внутренняя сеть Intranet может блокировать все входные соединения со всеми хост-компьютерами, за исключением некоторых. В частности, при фильтрации по портам TCP и UDP трафик SMTP будет пропущен ФМ (с возможностью фильтрации пакетов) в одну систему Intranet, трафик TELNET – в другую, а остальной трафик из Internet – в остальные системы Intranet.

В качестве простого примера работы фильтрующего маршрутизатора рассмотрим реализацию политики безопасности, допускающей определенные соединения сети Intranet с адресом 123.4.*.*. Соединения TELNET разрешаются только с одним хост-компьютером с адресом 123.4.5.6, который может быть прикладным TELNET-шлюзом, а SMTP-соединения – только с двумя хост-компьютерами с адресами 123.4.5.7 и 123.4.5.8, которые могут быть двумя шлюзами электронной почты. Обмен по NNTP (Network News Transfer Protokol) разрешается только на сервере новостей с адресом 129.6.48.264 и только с NNTP-сервером сети с адресом 123.4.5.9, а протокол NTP (сетевого времени) – для всех хост-компьютеров. Все другие серверы и пакеты блокируются. Соответствующий набор правил сведен в табл. 4.

Первое правило позволяет пропускать пакеты TCP из сети Internet от любого источника с номером порта, большим, чем 1023, к получателю с адресом 123.4.5.6 в порт 23. Порт 23 связан с сервером TELNET, а

все клиенты TELNET должны иметь непривилегированные порты с номерами не ниже 1024. Второе и третье правила работают аналогично и разрешают передачу пакетов к получателям с адресами 123.4.5.7 и 123.4.5.8 в порт 25, используемый SMTP. Четвертое правило пропускает пакеты к NNTP-серверу сети, но только от отправителя с адресом 129-6.48.254 к получателю с адресом 123.4.5.9 с портом назначения 119. Это единственный путь получения новостей внутренней сетью. Пятое правило разрешает трафик NTP, использующий протокол UDP вместо TCP, от любого источника к любому получателю Intranet. Шестое правило блокирует все остальные пакеты. Без него маршрутизатор мог бы блокировать, а мог бы не блокировать другие типы пакетов.

Таблица 4

Правила фильтрации

Тип	Адрес отправителя	Адрес получателя	Порт отправителя	Порт получателя	Действие
TCP	*	123.4.5.6	> 1023	23	Разрешить
TCP	*	123.4.5.7	> 1023	25	Разрешить
TCP	*	123.4.5.8	> 1023	25	Разрешить
TCP	*	123.4.5.9	> 1023	119	Разрешить
UDP	129.6.48.254	123.4.*.*	> 1023	123	Разрешить
*	*	*	*	*	Запретить

Правила фильтрации пакетов формулируются сложно, и обычно нет средств для тестирования их корректности, кроме медленного ручного тестирования. Даже если администратору удастся создать эффективные правила фильтрации, их возможности остаются ограниченными. Например, он задает правило, согласно которому ФМ будет отбраковывать все пакеты с неизвестным адресом отправителя. Однако кракер может использовать в качестве адреса отправителя в своем «вредоносном» пакете реальный адрес доверенного (авторизованного) пакета. В этом случае ФМ не сумеет отличить поддельный пакет от настоящего и пропустит его. Практика показывает, что такой вид атаки, называемый *подменой адреса,* широко распространен в Internet-сети и часто оказывается эффективным. Кроме того, обмануть МЭ с фильтрацией пакетов на сетевом уровне модели OSI-ISO несложно, достаточно кракеру создать IP-заголовок пакета (а только они и проверяются МЭ), удовлетворяющий разрешающим правилам фильтрации.

К *достоинствам* ФМ относят:

1) невысокую стоимость;
2) гибкость в определении правил фильтрации;
3) небольшую задержку при прохождении пакета.

Недостатками ФМ являются:

1) видимость внутренней сети (возможность изменения маршрута) из сети Internet;
2) сложность правил фильтрации, требующих хорошего знания TCP и UDP протоколов;
3) полная незащищенность либо недоступность всех компьютеров, стоящих за МЭ, при нарушении его работоспособности;
4) возможность подмены адреса,
5) отсутствие аутентификации на пользовательском уровне.

Шлюз сетевого уровня. Его называют иногда системой трансляции сетевых адресов или ШСУ модели OSI. Такой ШСУ исключает прямое взаимодействие между авторизованным (доверенным) клиентом и внешним хост-компьютером. Принимая запрос на конкретные услуги от доверенного клиента, он после проверки допустимости запрошенного сеанса устанавливает соединение с внешним хост-компьютером. После этого ШСУ копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Является ли запрашиваемый сеанс связи допустимым, ШСУ определяет с помощью следующей процедуры (рис. 6). Когда доверенный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли этот клиент базовым критериям фильтрации (например, может ли DNS-сервер определить IP-адрес клиента и ассоциированное с ним имя). Затем, действуя от имени клиента, ШСУ устанавливает соединение с внешним хост-компьютером и следит за выполнением процедуры квитирования по протоколу TCP, состоящей из обмена TCP-пакетами с флагами SIN (синхронизовать) и ACK (подтвердить).

<table>
<tr><th>Активная сторона</th><th></th><th>Пассивная сторона</th></tr>
<tr><td rowspan="4">Доверенный клиент</td><td>Запрос SIN (1000) →</td><td rowspan="4">Внешний хост-компьютер</td></tr>
<tr><td>← ACK (1001), SIN (2000) ответ</td></tr>
<tr><td>Подтверждение ACK (2001) →</td></tr>
<tr><td>← Соединение установлено (ACK, данные)</td></tr>
</table>

Рис. 6. Процедура проверки допустимости сеанса связи

Шлюз устанавливает соединение, когда он определил, что клиенты являются авторизованными участниками сеанса TCP, и проверил допустимость этого сеанса (т. е. числа, содержащиеся в TCP-пакетах, должны быть логически связаны).

Для копирования и перенаправления пакетов в ШСУ применяются специальные приложения, которые называются *канальными посредниками.* Они устанавливают между двумя сетями виртуальный канал и

разрешают пакетам, генерируемым приложениями TCP/IP, проходить по этому каналу.

Шлюз сетевого уровня выполняет еще одну важную функцию защиты: он используется в качестве *сервера-посредника,* выполняющего *процедуру трансляции адресов,* за счет которой происходит преобразование внутренних IP-адресов в один «надежный» IP-адрес. Этот «надежный» адрес ассоциируется с межсетевым экраном, из которого передаются все исходящие пакеты. В результате все исходящие пакеты оказываются отправленными из этого ШСУ, что исключает прямой контакт между внутренней (авторизованной) сетью и потенциально опасной внешней сетью, которая в этом случае видит только один активный IP-адрес ШСУ. Именно таким образом шлюз сетевого уровня и другие серверы-посредники *защищают внутренние сети от нападений типа подмены адресов.*

После установления связи ШСУ фильтруют пакеты только на сеансовом уровне модели OSI, т. е. они не могут проверять содержимое пакетов, передаваемых между внутренней и внешней сетью на уровне прикладных программ. Поэтому кракер, находящийся во внешней сети, может «протолкнуть» свои «вредоносные» пакеты через такой ШСУ, после чего он обратится напрямую к внутреннему Web-серверу, который сам по себе не сможет обеспечить функции МЭ. Чтобы фильтровать пакеты в соответствии с их содержимым, необходим шлюз прикладного уровня.

Шлюзы прикладного уровня. Для устранения некоторых недостатков, присущих ФМ и ШСУ, межсетевые экраны должны использовать дополнительные *программные средства для* фильтрации сообщений сервисов типа TELNET и FTP. Они называются *полномочными серверами-посредниками,* а выполняющий их хост-компьютер – *шлюзом прикладного уровня.*

Шлюз прикладного уровня (ШПУ) исключает прямое взаимодействие между авторизованным клиентом и внешним хост-компьютером и фильтрует все входящие и исходящие пакеты на прикладном уровне. Серверы-посредники, связанные с приложениями, переправляют через ШПУ информацию, генерируемую конкретными серверами. Для достижения более высокого уровня безопасности ШПУ и ФМ могут быть объединены в одном МЭ.

В качестве примера рассмотрим сеть, где с помощью ФМ допускается прохождение пакетов TELNET или FTP только к одному хост-компьютеру, являющемуся шлюзом прикладного уровня TELNET/FTP. Внешний пользователь, который хочет соединиться с некоторой системой в сети, сначала должен соединиться с ШПУ, а затем – с нужным внутренним хост-компьютером. Эта процедура осуществляется следующим образом:

1) внешний пользователь устанавливает TELNET-соединение с ШПУ с помощью протокола и вводит имя интересующего его внутреннего хост-компьютера;
2) ШПУ проверяет IP-адрес отправителя и разрешает или запрещает соединение в соответствии с тем или иным критерием доступа;
3) пользователю может потребоваться аутентификация (возможно с помощью одноразовых паролей);
4) сервер-посредник устанавливает TELNET-соединение между ШПУ и внутренним хост-компьютером;
5) сервер-посредник осуществляет передачу информации между этими двумя соединениями;
6) полномочный сервер-посредник (ШПУ) регистрирует соединение.

ШПУ имеют ряд серьезных преимуществ по сравнению с обычным режимом, при котором прикладной трафик пропускается непосредственно к внутренним хост-компьютерам. Они заключаются в следующем:

1. ШПУ пропускают только те службы, которые им поручено обслуживать, т. е., если ШПУ наделен полномочиями для служб FTP и TELNET, то в защищаемой сети будут разрешены только FTP и TELNET, а все остальные службы будут полностью блокированы. Для некоторых организаций такой вид безопасности имеет большое значение, так как он гарантирует, что через МЭ будут пропускаться только те службы, которые считаются безопасными,
2. ПШУ обеспечивают возможность фильтрации протокола. Например, некоторые МЭ, использующие ШПУ, могут фильтровать FTP-соединения и запрещать использование команды FTP *put,* что гарантированно не позволяет пользователям записывать информацию на анонимный FTP-сервер.
3. ШПУ может быть единственным хост-компьютером, имя которого должно быть известно внешним системам, т. е. имеет место невидимость структуры защищаемой сети из глобальной сети Internet.
4. Прикладной трафик может быть аутентифицирован прежде, чем он достигнет внутренних хост-компьютеров, и может быть зарегистрирован более эффективно, чем с помощью стандартной регистрации.
5. Защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, что снижает вероятность взлома с использованием «дыр» в программном обеспечении.
6. ШПУ позволяют обеспечить более высокий уровень защиты, поскольку взаимодействие с внешним миром реализуется через небольшое число прикладных полномочных программ-посредников, полностью контролирующих входящий и выходящий трафик.

Усиленная аутентификация. Одним из важных компонентов концепции МЭ является аутентификация, т. е. прежде чем пользователю будет предоставлено право воспользоваться тем или иным сервисом, необходимо убедиться, что он действительно тот, за кого себя выдает.

Одним из способов аутентификации является использование стандартных UNIX-паролей, однако так как они передаются открытым текстом, то такие пароли уязвимы – они могут быть перехвачены злоумышленниками, наблюдающими за каналами в сети Internet. Для ликвидации этого недостатка разработан ряд средств усиленной аутентификации, к которым относятся смарт-карты, персональные жетоны, биометрические механизмы и т. п. Общим для этих средств является то, что пароли, генерируемые этими устройствами, не могут быть повторно использованы нарушителем, наблюдающим за установлением связи.

Ряд наиболее популярных средств усиленной аутентификации, применяемых в настоящее время, называются *системами с одноразовыми паролями.* Например, смарт-карты или жетоны аутентификации генерируют информацию, которую аппаратное и программное обеспечения хост-компьютера используют вместо традиционного пароля. Этот пароль является уникальным (одноразовым) для каждого сеанса. Если он будет перехвачен, то второй раз его не используешь.

Так как МЭ могут централизовать управление доступом в сети, то они являются подходящим, более практичным местом для установки программ или устройств усиленной аутентификации. Сеансы TELNET или FTP, устанавливаемые со стороны сети Internet с системами подсоединяемой сети, должны проходить проверку с помощью средств усиленной аутентификации, прежде чем они будут разрешены. С другой стороны, системы подсоединяемой сети могут запрашивать для разрешения доступа и статические пароли, так как даже если их перехватит злоумышленник, то он не сможет ими воспользоваться, ибо средства усиленной аутентификации и другие компоненты МЭ предотвратят его проникновение или не дадут обойти экран.

Основные схемы сетевой защиты на базе межсетевых экранов

Перед администратором корпоративной или локальной сети при подключении ее к глобальной сети стоят следующие задачи:

1) защита от несанкционированного доступа со стороны глобальной сети;
2) скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;
3) разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой в глобальную.

Часто в корпоративной сети возникает потребность организации в ее составе нескольких сегментов с разными уровнями защищенности, например:

1) *свободно доступные сегменты* (например, рекламный WWW-сервер);
2) *сегменты с ограниченным доступом* (для доступа сотрудникам организации с удаленных узлов);
3) *закрытые сегменты* (финансовая локальная сеть предприятия).

Для защиты корпоративной (локальной) сети применяются следующие четыре основные *схемы организации* МЭ:

1. МЭ на основе ФМ;
2. МЭ на основе двухпортового шлюза;
3. МЭ на основе экранированного шлюза;
4. МЭ – экранированная подсеть.

МЭ на основе ФМ. Первая схема организации МЭ является самой распространенной и наиболее простой в реализации, конфигурируется для блокирования или фильтрации входящих и исходящих пакетов на основе анализа их адресов и портов. Компьютеры, находящиеся в защищаемой сети, имеют прямой доступ в сеть Internet, в то время как большая часть доступа к ним из Internet блокируется. Часто блокируются такие опасные службы, как X-Windows, NIS и FNS. В принципе можно реализовать любую из политик безопасности, упомянутых выше, однако если ФМ не будет фильтровать пакеты по порту источника и номеру входного или выходного порта, то реализация политики «запрещено все, что не разрешено в явной форме» может быть затруднена.

МЭ на основе ФМ имеют такие же недостатки, как и ФМ, причем они становятся более ощутимыми при ужесточении требований к безопасности защищаемой сети. Отметим дополнительно следующие недостатки:

1) сложность правил фильтрации для некоторой их совокупности может стать неуправляемой;
2) невозможность полного тестирования правил фильтрации приводит к незащищенности сети от непротестированных атак;
3) отсутствующая практически регистрация событий не позволяет администратору определить, подвергался ли МЭ атаке и скомпрометирован ли он;
4) каждый хост-компьютер, связанный с сетью Internet, нуждается в *своих средствах* усиленной аутентификации.

МЭ на основе двухпортового шлюза. Вторая схема организации МЭ построена на базе двухпортового ШПУ и включает в себя двухдомный хост-компьютер с двумя сетевыми интерфейсами, при передаче инфор-

мации между которыми и осуществляется основная фильтрация. Для обеспечения дополнительной защиты между ШПУ и сетью Internet обычно размещают ФМ, в результате чего между ШПУ и ФМ образуется внутренняя экранированная подсеть, которую можно использовать для размещения доступных извне информационных серверов.

В отличие от первой схемы МЭ вторая схема полностью блокирует трафик IP между сетью Internet и защищаемой сетью. Здесь только полномочные серверы-посредники ШПУ, могут предоставлять услуги и доступ пользователям. Такая схема МЭ полностью реализует упомянутую выше политику безопасности, обеспечивая высокий уровень безопасности, поскольку маршруты к защищенной подсети известны только МЭ и скрыты от внешних систем.

Вторая схема МЭ довольна проста и достаточно эффективна. Однако она не обладает достаточной гибкостью, требует от пользователей средств усиленной аутентификации, а также регистрации доступа, попыток зондирования и атак нарушителя, т. е. требует поддерживания безопасности ШПУ на высоком уровне (ибо любая брешь в его защите или компрометация дают возможность злоумышленнику проникнуть в защищаемую сеть).

МЭ на основе экранированного шлюза. Третья схема организации МЭ похожа на предыдущую, только ШПУ, реализуемый на хост-компьютере, имеет только один интерфейс. Здесь первичная безопасность обеспечивается ФМ, в котором пакетная фильтрация осуществляется одним из следующих способов:

1) разрешение внутренним хост-компьютерам открывать соединения с хост-компьютерами в сети Internet для определенных сервисов (средствами фильтрации);
2) запрещение всех соединений от внутренних хост-компьютеров (заставляя их использовать ШПУ).

МЭ, выполненный по третьей схеме, более гибок, но менее безопасен по сравнению со второй схемой. Это обусловлено тем что для третьей схемы существует потенциальная возможность передачи трафика в обход ШПУ непосредственно в системы локальной сети. Кроме того, здесь имеют место еще два недостатка: если атакующий нарушитель сумеет проникнуть в хост-компьютер или ФМ окажется скомпрометирован, то перед ним окажутся незащищенные системы внутренней сети. По этим причинам в последнее время все более популярной становится четвертая схема.

МЭ – экранированная подсеть. Четвертая схема организации МЭ представляет собой развитие третьей схемы. Здесь для создания экранированной подсети используются два ФМ – внешний (между сетью Inter-

net и экранируемой подсетью) и внутренний (между экранируемой подсетью и защищаемой сетью). Экранируемая подсеть содержит ШПУ и может включать информационные серверы и другие системы, требующие контролируемого доступа. Эта схема МЭ обеспечивает хорошую безопасность благодаря организации экранированной подсети, которая еще лучше изолирует внутреннюю защищаемую сеть от Internet.

Внешний ФМ защищает от сети Internet как экранированную подсеть, так и внутреннюю (локальную) сеть. Трафик пересылается им согласно следующим правилам: *разрешается трафик:* от объектов сети Internet к ШПУ и обратно; электронной почты от Internet к серверу электронной почты и обратно; FTP, Gopher и т. д. от Internet к информационному серверу; *запрещается остальной трафик.* Этот ФМ может быть использован также для блокирования других уязвимых протоколов, которые не должны передаваться к хост-компьютерам внутренней сети или от них.

Внутренний ФМ защищает внутреннюю сеть как от Internet, так и от экранированной подсети (в случае ее компрометации) – он управляет трафиком по следующим правилам: *разрешается график:* от ШПУ к системам внутренней сети и обратно; электронной почты от сервера электронной почты к системам внутренней сети и обратно; FTP, Gopher и т. д. от систем внутренней сети к информационному серверу и обратно.

Таким образом, для четвертой схемы МЭ ни одна система внутренней сети не достижима из Internet, и наоборот. Кроме того, четкое разделение функций между обоими ФМ и ШПУ позволяет достигнуть более высокой пропускной способности. ШПУ также может включать программы усиленной аутентификации.

Недостатки четвертой схемы МЭ в том, что пара ФМ требует особого внимания для обеспечения заданного уровня безопасности, ибо из-за ошибок при их настройке может возникнуть провал в безопасности защищаемой сети, при этом есть принципиальная возможность доступа в обход ШПУ.

Применение МЭ для организации виртуальных корпоративных сетей. Некоторые МЭ позволяют из сетей, подключенных к Internet, создавать виртуальную корпоративную сеть. Передача данных между локальными сетями, входящими в глобальную сеть, осуществляется через МЭ и производится прозрачным образом для пользователей локальных сетей. Конфиденциальность и целостность передаваемой информации обеспечиваются при помощи средств шифрования, использования ЭЦП и т. п., при этом могут шифроваться не только содержимое пакета, но и некоторые поля заголовка.

Программные методы защиты

SKIP-технология и SSL-протокол. К программным методам защиты в сетях относятся защищенные криптопротоколы (использующие асимметричную и симметричную криптографию), которые позволяют надежно защищать соединения в сетях. Основные подходы к протоколам, обеспечивающим защиту соединений, базируются на *SKIP-технологии* (Secure Key Internet Protocol – не путать со SKIP-протоколом управления криптографическими ключами, и на *универсальном протоколе защиты соединения* SSL (Secure Socket Layer).

SKIP-технологией называется стандарт защиты трафика IP-пакетов, позволяющий на сетевом уровне обеспечить защиту соединения и передаваемых по нему данных. Возможны два способа реализации SKIP-защиты трафика IP-пакетов: шифрование блока данных IP-пакета; инкапсуляция IP-пакета в SKIP-пакет.

В первом случае шифруются симметричной криптографией только данные IP-пакета, а заголовок, содержащий адреса отправителя и получателя, открыт и поэтому пакет маршрутизируется в соответствии с истинными адресами. Секретный (парный для двух узлов сети) ключ вычисляется по схеме Диффи-Хеллмана.

Во втором случае SKIP-пакет внешне похож на обычный IP-пакет, при этом в поле данных SKIP-пакета полностью размещается в зашифрованном виде исходный IP-пакет. В новом заголовке вместо истинных адресов могут быть помещены некоторые другие адреса, по которым и будет осуществляться адресация к любым хост-компьютерам в сети Internet, т. е. межсетевая адресация осуществляется по обычному IP-заголовку в SKIP-пакете. Конечный получатель SKIP-пакета по заранее определенному разработчиками алгоритму (данные о котором помещаются в поле SKIP-пакета перед криптограммой) расшифровывает криптограмму и формирует обычный TCP- (или UDP-) пакет, который и передает соответствующему (TCP или UDP) модулю ядра операционной системы.

Протокол защиты соединения SSL разработан компанией Netscape для сеансового уровня модели OSI, использует открытые ключи, является универсальным средством, динамически защищающим соединение при использовании любого прикладного протокола (FTP, TELNET, SMTP, DNS и т. п.) и поддерживается практически такими ведущими компаниями, как IBM, Microsoft Corporation, Motorola, Novell Inc., Sun Microsystems, Digital Equipment Corporation и др.

Атаки через Internet

Сетевая безопасность информации и Уголовный кодекс РФ о преступлениях в сфере компьютерной информации

Сетевая безопасность. Для рассмотрения вопросов защиты в Internet напомним с этой точки зрения основные понятия теории компьютерной безопасности. Обобщенно говоря, их всего три: *угрозы, уязвимости, атаки.* При этом если рассматривать атаку на компьютерную систему как действие, предпринимаемое злоумышленником с целью поиска и использования той или иной уязвимости, то *атака есть реализация угрозы.* Мы уже знаем, что выделяется три вида угроз – это угрозы *раскрытия, целостности* и *отказа в обслуживании.* Считается, что угрозе раскрытия («краже», «утечке») подвержены больше государственные структуры, угрозе целостности (модификация или даже удаление данных) – деловые и коммерческие структуры.

Угроза отказа в обслуживании возникает всякий раз, когда в результате определенных действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным, так что запрашиваемый ресурс никогда не будет получен, или блокирование может вызвать только задержку, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан. В локальных ВС наиболее частыми являются угрозы раскрытия и целостности, в глобальных сетях на первое место выходит угроза отказа в обслуживании.

Подчеркнем еще раз особенности безопасности компьютерных сетей. В сетевых системах, наряду с обычными *(локальными)* атаками, осуществляемыми в пределах одной корпоративной сети (КС), применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве – это так называемые, *сетевые* (или удаленные) атаки *(remove* или *net work attacks).* Под удаленной атакой обычно понимается информационное разрушающее воздействие на распределенную КС, программно осуществляемое по каналам связи. Это определение охватывает обе особенности сетевых систем: *распределенность компьютеров* и *распределенность информации.*

Поэтому рассматривают *два подвида удаленных атак:*

1) атаки на *инфраструктуру* и *протоколы сети* (на сложившуюся систему организации отношений между объектами сети и используемые в сети сервисные службы);
2) атаки на *телекоммуникационные службы* (операционные системы и приложения, т. е. все программное обеспечение, работающее на удаленном компьютере и обеспечивающее сетевое взаимодействие).

Несколько слов о реальной сетевой безопасности по отношению к удаленным атакам. Прежде всего, необходимо всегда уточнять, какие виды сетей имеются в виду. Серьезнейшие проблемы с безопасностью имеют только вычислительные сети общего назначения (СОН).

Там же, где требуется обработка критической информации (государственные правительственные структуры, министерство обороны, атомная энергетика и т. п.), используются специализированные защищенные вычислительные сети (ВС) стратегического назначения, они в основном изолированы от СОН (от Internet).

В отличие от сетей обработки критической информации банковские ВС более похожи на СОН, ибо банки из-за конкурентной борьбы между собой вынуждены для обеспечения удобства и быстроты работы с клиентами предоставлять им возможность удаленного доступа из СОН к своим банковским ВС. Однако, во-первых, мы уже знаем, что в этом случае используются защищенные криптопротоколы и разнообразные системы сетевой защиты (например, МЭ) и, во-вторых, предоставление клиенту возможности удаленного доступа вовсе не означает, что он получит непосредственно к внутренней банковской сети.

Тем не менее, работа через СОН имеет вероятность 99,9 % быть подвергнутой угрозе отказа в обслуживании. Кроме того, на практике все известные сегодня и рассмотренные выше МЭ не способны к отражению большинства из двух указанных подвидов удаленных атак.

Если смотреть на проблему безопасности со стороны кракера, то надо отметить, что в новых статьях Уголовного кодекса РФ (действующих с 1997 г.) появились, хотя и очень расплывчатые, формулировки о возможной уголовной ответственности за «преступления в сфере компьютерной безопасности» (глава 28 УК РФ). Для примера приведем полностью следующую статью.

Статья 272. *Неправомерный доступ к компьютерной информации*

1. Неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети – наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы, или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок до шести месяцев, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, систе-

ме или их сети, – наказывается штрафом в размере от 500 до 800 минимальных размеров оплаты труда или в размере заработной платы, или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Аналогичные ответственности предусмотрены еще в двух статьях УК РФ: в статье 273 *«Создание, использование и распространение вредоносных программ для ЭВМ»* и в статье 274 *«Нарушение правил эксплуатации ЭВМ или их сети».* Применение на практике статей УК чрезвычайно затруднено, во-первых, в связи со сложной доказуемостью подобных дел и, во-вторых, с естественным отсутствием здесь у следователей высокой квалификации.

Удаленные атаки на распределенные вычислительные сети (ВС)

Обобщенная классификация атак безопасности РВС. Итак, атака на инфраструктуру и протоколы сети используют следующие уязвимости:

1) в сетевых протоколах;
2) в сложившейся системе организации отношений между объектами сети;
3) в используемых сервисных службах сети.

Основными причинами возможной реализации данных атак являются следующие:

1) использование широковещательной среды передачи (например, Ethernet);
2) применение нестойких алгоритмов идентификации удаленных субъектов и объектов (РВС);
3) использование протоколов динамического изменения маршрутизации с нестойкими алгоритмами идентификации;
4) применение алгоритмов удаленного поиска с использованием широковещательных и направленных поисковых запросов;
5) возможность анонимного захвата одним субъектом РВС множества физических или логических каналов связи.

На основе этих причин в Санкт-Петербургском ГТУ на кафедре «Информационная безопасность КС» предложена наиболее обобщенная классификация атак безопасности РВС, сводящаяся к следующим *шести классам:*

1. *По характеру воздействия.*
   1.1. *Пассивные* (они не оказывают влияния на работу, но нарушают политику безопасности и их невозможно обнаружить – прослушивание канала связи).
   1.2. *Активные* (нарушают не только политику безопасности, но и непосредственно работу системы – изменение конфигурации РВС, нарушение работоспособности и т. п.).
2. *По цели воздействия.*
   2.1. *Нарушения конфиденциальности информации либо ресурсов* (пассивные атаки типа прослушивания канала).
   2.2. *Нарушение целостности информации* (осуществление полного контроля над информационным потоком или возможность передачи от имени другого объекта).
   2.3. *Нарушение работоспособности (доступности) системы* (вывод из строя операционной системы на атакованном объекте).
3. *По условию начала осуществления воздействия.*
   3.1. *Атака по запросу от атакуемого объекта* (наиболее характерный вид атак для РВС – например, в ОС Novell NetWare – это запрос SAP, в Internet – запросы DNS и ARP).
   3.2. *Атака по наступлению ожидаемого события на атакуемом объекте* (осуществление наблюдения за состоянием ОС объекта атаки и воздействие при возникновении в ней определенного события – например, прерывание сеанса работы пользователя с сервером в ОС Novell NetWare без выдачи команды *logout).*
   3.3. *Безусловная атака* (воздействие осуществляется немедленно, т. е. инициатор – атакующий).
4. *По наличию обратной связи с атакуемым объектом.*
   4.1. *Атака при наличии обратной связи взломщика и объекта атаки* (связь позволяет взломщику адекватно реагировать на изменение ситуации, что наиболее характерно для распределенных РВС).
   4.2. *Однонаправленная атака* (атака без реакции на какие-либо изменения ситуации).
5. *По расположению субъекта атаки относительно атакуемого объекта.* Этот класс определяет степень удаленности атаки.
   5.1. *Внутрисегментная атака* (субъект атаки – атакующая программа или оператор, непосредственно осуществляющий воздействие – и объект атаки находятся в одном сегменте – физическом соединении хостов).

5.2. *Межсегментная атака* (субъект и объект в разных сегментах – ее осуществить сложнее, но еще сложнее непосредственно обнаружить атакующего и адекватно отреагировать на атаку).

6) *По уровню модели* ISO/OSI*, на котором осуществляется атака.* Так как атака представляется сетевой программой, то здесь классификация атак делается в соответствии с уровнями модели ISO/OSI:
   6.1. На *физическом.*
   6.2. На *канальном.*
   6.3. На *сетевом.*
   6.4. На *транспортном.*
   6.5. На *представительном.*
   6.6. На *прикладном.*

Понятие типовой угрозы безопасности. Независимо от используемых сетевых протоколов, топологии и инфраструктуры распределенной РВС, механизмы реализации удаленных воздействий на нее инвариантны по отношению к особенностям конкретной системы. Это объясняется тем, что РВС проектируются на основе одних и тех же принципов, и следовательно, имеют практически одинаковые проблемы безопасности, и причины реализации угроз на них также одинаковы. Поэтому можно ввести понятие типовой угрозы безопасности РВС.

Типовая угроза безопасности – это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной ВС. Соответственно *типовая удаленная атака* – это реализация типовой угрозы безопасности РВС.

Такими типовыми удаленными атаками являются следующие:

1) анализ сетевого трафика;
2) подмена доверенного объекта РВС;
3) внедрение в РВС ложного объекта путем навязывания ножного маршрута;
4) внедрение в РВС ложного объекта путем использования недостатков алгоритма удаленного поиска;
5) отказ в обслуживании.

Рассмотрим их подробнее.

Анализ сетевого трафика (sniffing) позволяет изучить логику работы РВС, т. е. получить взаимно-однозначное соответствие *событий,* происходящих в системе, и *команд,* пересылаемых друг другу ее объектами в момент появления этих событий. Это достигается путем перехвата и анализа пакетов обмена на канальном уровне. Знание логики работы РВС позволяет на практике моделировать и осуществлять типовые

удаленные атаки, непосредственно перехватывающие поток данных, которыми обмениваются объекты РВС.

По характеру воздействия анализ сетевого трафика является пассивным (класс 1.1). Но осуществление данной атаки без обратной связи (класс 4.2) ведет к нарушению конфиденциальности информации (класс 2.1) внутри одного сегмента сети (класс 5.1) на канальном уровне OSI (класс 6.2).

Подмена доверенного объекта или субъекта РВС. Для осуществления однозначной идентификации сообщений между объектами и субъектами взаимодействия применяется «рукопожатие» (handshake). При этом для него иногда создается виртуальный канал между ними, а иногда нет (например, для служебных сообщений от маршрутизаторов используется передача одиночных сообщений, не требующих подтверждения).

Как известно, для адресации сообщений в РВС используется сетевой адрес, уникальный для каждого объекта системы (на канальном уровне – это аппаратный адрес сетевого адаптера, на сетевом уровне он определяется в зависимости от используемого протокола сетевого уровня, например адрес IP). Эти средства распознавания не должны быть единственными, так как в этом случае они довольно просто подделываются.

Если же в РВС применяются нестойкие алгоритмы идентификации удаленных объектов, то возможно удаленное воздействие, реализация которого заключается в передаче по каналам связи сообщений от имени любого объекта или субъекта РВС. При этом могут быть две разновидности такой атаки: при установленном виртуальном канале; без установленного виртуального канала.

Для первой разновидности атака заключается в передаче пакетов обмена с хоста кракера от имени доверенного субъекта взаимодействия (при этом переданные сообщения будут восприняты как корректные). На практике сегодня для осуществления такой атаки надо преодолеть систему идентификации и аутентификации сообщений, вырабатывающую контрольную сумму, вычисляемую с помощью двух 8-битных счетчиков – номера канала и номера пакета (в ОС Novell Net-Ware 3.12-4.1) или двух 32-битных счетчиков идентификации в протоколе TCP/IP.

При второй разновидности атака заключается в передаче служебных сообщений от имени сетевых управляющих устройств, например от имени маршрутизаторов. Очевидно, что для идентификации пакетов в этом случае могут использоваться только заранее определенные статические ключи, что довольно неудобно и требует сложной системы управления ключами. В противном случае идентификация пакетов обмена без установленного виртуального канала возможна лишь по сете-

вому адресу отправителя, который, как указывалось выше, легко подделать. Посылка же ложных управляющих сообщений может привести к серьезным нарушениям работы РВС, например к изменению ее конфигурации.

Подмена доверенного объекта РВС является активным воздействием (класс 1.2), совершаемым с целью нарушения конфиденциальности (класс 2.1) и целостности (класс 2.2) информации при наступлении на атакуемом объекте определенного события (класс 3.2). Такая удаленная атака может являться как внутрисегментной (класс 5.1), так и межсегментной (класс 5.2), иметь обратную связь с атакуемым объектом (класс 4.1) или не иметь ее (класс 4.2) и осуществляться на канальном (класс 6.2), сетевом (класс 6.3) или транспортном (класс 6.4) уровнях модели OSI.

Ложный объект РВС. Существуют две принципиально разные причины, обусловливающие появление типовой угрозы «ложный объект РВС»:

1. Если в РВС не решены проблемы идентификации сетевых управляющих устройств (например, маршрутизаторов), возникающие при взаимодействии этих устройств с объектами системы, то РВС может подвергнуться типовой удаленной атаке, связанной с изменением маршрутизации (навязыванием ложного маршрута) и внедрением в систему ложного объекта.
2. Внедрить ложный объект можно и в случае, если инфраструктурой РВС предусмотрена работа алгоритмов удаленного поиска, имеющих недостатки.

Внедрение в РВС *ложного объекта путем навязывания ложного маршрута.* Для обеспечения эффективной маршрутизации в РВС применяются специальные управляющие протоколы, играющие важнейшую роль и позволяющие маршрутизаторам:

1) обмениваться информацией друг с другом – RIP (Routing IP), OSPF (Open Shortest Path First);
2) уведомлять хосты о новом маршруте – ICMP (Internet Control Message Protocol);
3) удаленно управлять маршрутизаторами – SNMP (Simple Network Management Protocol).

Все эти протоколы позволяют удаленно изменять маршрутизацию в Internet, т. е. являются протоколами управления сетью.

Основная цель атаки, связанной с навязыванием ложного маршрута, – изменить исходную маршрутизацию между объектами РВС таким образом, чтобы новый маршрут проходил через ложный объект – хост атакующего. На первом этапе реализация этой атаки состоит в несанкционированном использовании протоколов управления сетью для изме-

нения исходных таблиц маршрутизации. При этом атакующий посылает по сети от имени сетевого маршрутизатора служебные сообщения (определенные данными протоколами), изменяет маршрут потока информации и в результате получает над ним полный контроль. На второй стадии атака заключается в приеме, анализе и передаче сообщений, получаемых от дезинформированных объектов РВС. Навязывание объекту РВС ложного маршрута – это активное воздействие (класс 1.2), совершаемое с любой из целей класса 2, представляет собой безусловную атаку (класс 3.3), может осуществляться как внутри одного сегмента (класс 5.1), так и межсегментно (класс 5.2); как с обратной связью (класс 4.1), так и без обратной связи с атакуемым объектом (класс 4.2) на канальном (класс 6.2), сетевом (класс 6.3) и транспортном (класс 6.4) уровнях модели OSI.

Внедрение в РВС *ложного объекта из-за недостатков алгоритмов поиска.* Обычно объекты РВС имеют не всю необходимую для адресации сообщений информацию. Для ее получения в РВС используются различные алгоритмы удаленного поиска, заключающиеся в передаче по сети специального вида поисковых запросов и в ожидании ответов на них. Полученных таким образом сведений об искомом объекте запросившему их субъекту РВС достаточно для последующей адресации к нему. Примером таких сообщений являются упоминавшиеся выше запрос SAP в ОС Novell NetWare и запросы DNS и ARP в Internet.

Реализация такой атаки состоит в *перехвате поискового запроса* (который может быть *широковещательным* (внутри одного сегмента на канальном уровне OSI) или *направленным* (при межсегментном поиске на сетевом уровне OSI); и передаче в ответ на него ложного сообщения, где указываются данные, использование которых приведет к адресации на атакующий ложный сервер. Далее весь поток информации между субъектом и объектом взаимодействия будет проходить через ложный объект РВС.

Другой вариант реализации этой же атаки состоит в *периодической передаче* на атакуемый объект заранее подготовленного ложного ответа без приема поискового запроса. Эти провокационные действия кракера характерны для глобальных сетей, когда атакующий и его цель находятся в разных сегментах и возможности перехватить поисковый запрос не существует.

Ложный объект РВС – активная атака (класс 1.2), совершаемая с целью нарушения конфиденциальности (класс 2.1) и целостности информации (класс 2.2), которая может являться атакой по запросу от атакуемого объекта (класс 3.1), а также безусловной атакой (класс 3.3); является как внутрисегментным (класс 5.1), так и межсегментным (класс 5.2),

имеет обратную связь с атакуемым объектом (класс 4.1) и осуществляется на канальном (класс 6.2), сетевом (класс 6.3) и транспортном (класс 6.4) уровнях модели OSI.

Использование ложного объекта для организации удаленной атаки на РВС. Получив контроль над проходящим информационным потоком, ложный объект РВС (являющийся целью многих удаленных атак и представляющий собой серьезную угрозу безопасности РВС) может применять различные методы воздействия на перехваченную информацию, к которым относятся: селекция потока информации и сохранение ее на ложном объекте РВС; модификация информации.

Первый метод воздействия определяется тем, что в перехватываемых пакетах обмена кроме полей данных существуют служебные поля, не представляющие интереса для атакующего. Поэтому, для того чтобы получить непосредственно передаваемый файл, необходимо проводить на ложном объекте динамическую семантическую селекцию потока информации.

Второй метод – позволяет программно модифицировать поток информации между объектами РВС с другого объекта, что качественно отличает атаку по схеме «ложный объект» от более эффективной атаки с помощью анализа сетевого трафика – она неспособна к модификации информации. Имеют место три вида модификации: модификация передаваемых данных; модификация передаваемого кода; подмена информации.

Первый вид заключается в том, что в результате селекции потока перехваченной информации «ложный объект» может распознавать тип передаваемых файлов (исполняемый или текстовый). В случае обнаружения текстового файла появляется возможность модифицировать данные, что представляет особую угрозу для сетей обработки конфиденциальной информации.

Второй вид модификации связан с проведением семантического анализа перехваченной информации и способностью «ложного объекта» выделять из потока исполняемый код (для этого ему необходимо использовать некоторые особенности, свойственные реализации сетевого обмена в конкретной РВС или присущие конкретным типам исполняемых файлов в данной локальной операционной системе).

Различают два различных по цели средства модификации исполняемого кода: внедрение разрушающих программных средств (РПС); изменение логики работы файла. В первом случае исполняемый код модифицируется по вирусной технологии, т. е. к нему одним из известных способов дописывается тело РПС, и точка входа изменяется таким образом, чтобы она указывала на начало кода внедренного воздействия.

Этот способ ничем не отличается от известных, за исключением того, что файл оказался зараженным вирусом (или РПС) в момент передачи его по сети, что возможно только при использовании системы воздействия, построенной по принципу «ложный объект». Во втором случае воздействие требует предварительного исследования работы исполняемого файла и может принести самые неожиданные результаты. Так, например, при запуске на сервере (в ОС Novell NetWare) программы идентификации пользователей распределенной базы данных ложный объект способен модифицировать код этой программы так, что появляется возможность беспарольного входа в базу данных с наивысшими привилегиями.

Третий вид модификации связан с ее полной подменой. Предположим, что ложный объект контролирует подключение пользователя к серверу. В этом случае взломщик ожидает запуска соответствующей программы входа в систему, которая находится на сервере и при ее запуске исполняемый файл передается на рабочую станцию. Следящий за событиями «ложный объект» передает вместо этого исполняемого файла код заранее написанной специальной программы – захватчика паролей, которая выполняет те же действия, что и настоящая программа входа в систему, например, запрашивает имя и пароль пользователя. После этого полученные сведения передаются на «ложный объект», а пользователю выводится сообщение об ошибке. При этом пользователь, предположив, что он неправильно ввел пароль (пароль обычно не отображается на экране), снова запустит программу подключения к системе, получит теперь настоящий исполняемый пароль и со второго раза доступ в систему. Результат атаки – имя и пароль пользователя, сохраненные на «ложном объекте».

Отказ в обслуживании. Существуют следующие две разновидности такой типовой атаки: направленный мини-шторм; направленный шторм запросов (flooding – наводнение).

Первая основана на проблеме, заключающейся в том, что при отсутствии статической ключевой информации в РВС идентификация запроса возможна только по адресу его отправителя. Если в РВС не предусмотрено средств аутентификации адреса отправителя, т. е. инфраструктура РВС позволяет с какого-либо объекта системы передавать на атакуемый объект бесконечное число анонимных запросов (для сетевой ОС на подключение) от имени других объектов (тем самым переполняя очередь запросов в ОС), числом, превышающим длину очереди запросов на подключение, то это и будет реализация типовой угрозы безопасности РВС «отказ в обслуживании».

Суть второй разновидности этой типовой атаки – передача с одного адреса стольких запросов на атакуемый объект, которые не обеспечит пропускная способность канала передачи. Результатами обоих разновидностей является нарушение работы системы от возможного переполнения очереди запросов и отказа одной из телекоммуникационных служб, вплоть до полной остановки компьютера из-за того, что система не может заниматься ничем другим, кроме обработки запросов.

Типовая удаленная атака «отказ в обслуживании» является активным воздействием (класс 1.2), осуществляемым с целью нарушения работоспособности системы (класс 2.3), безусловной атакой (класс 3.3), однонаправленной (класс 4.2), внутрисегментной (класс 5.1) или межсегментной (класс 5.2), осуществляемой на канальном, сетевом, транспортном и прикладном (соответственно классы 6.2, 6.3, 6.4, 6.7) уровнях модели OSI.

Контрольные вопросы и упражнения

8.1. Каковы особенности функционирования глобальных сетей в России?
8.2. Опишите структуру сети Интернет. Приведите положительные и отрицательные стороны.
8.3. Какие сети, в том числе и закрытые Вы знаете?
8.4. Обсудите, каким образом происходит обмен информацией по сети Интернет. Какие угрозы информации здесь существуют?
8.5. Каковы принципы построения протоколов обмена информацией? Отразите слабые места.
8.6. Какого вида соединения с Интернетом может быть соединение с пользователем? Опишите соответствующие угрозы в каждом случае отдельно.
8.7. Чем характеризуется сервер? Какие новые угрозы информации возникают в данной системе?
8.8. Охарактеризуйте различные виды серверов по выполняемым функциям? Выделите типовые нарушения информационной безопасности, которые могут возникнуть на сервере.
8.9. Какая атака называется DoS? Опишите распределенную атаку DoS.
8.10. Обоснуйте наличие авторизации и идентификации пользователя при доступе к глобальной сети.
8.11. Что такое «спам»? В чем его вред? Приведите типовые решения для защиты от спама.
8.12. Что такое path, service pack? Необходимо ли их устанавливать на сетевую операционную систему?

8.13. Опишите основные уязвимости следующих видов серверов:
   а) web-сервер;
   б) ftp-сервер;
   в) mail-сервер;
8.14. Что такое межсетевой экран? Каковы его основные функции и назначение? От какого вида атак он предназначен?
8.15. При выборе межсетевых экранов для своего сервера (на выбор) каким основным характеристикам Вы будете уделять большее внимание?
8.16. Что такое VPN (Virtual Private Network)? Приведите примеры архитектур построения виртуальных приватных сетей.
8.17. Рассмотрите распределенную виртуальную сеть, территориально расположенную:
   а) в одном здании с единственным выходом в Интернет;
   б) в одном здании с несколькими выходами в Интернет;
   в) в различных зданиях, доступ к различным сегментам сети осуществляется через сеть Интеренет;
   г) в различных городах, доступ к различным сегментам сети осуществляется через сеть Интернет;
   д) в различных зданиях города, доступ осуществляется по беспроводным сетям.

      Предложите типовые включения различных сегментов сети в единую сеть.
8.18. Что такое тунеллирование?
8.19. Перечислите протоколы защищенной передачи данных в виртуальных приватных сетях.
8.20. Рассмотрите возможность передачи конфиденциальных данных по сетям общего пользования.
8.21. Приведите основные требования к сетевой безопасности.
8.22. С помощью каких каналов возможен несанкционированный доступ к информации, расположенной на:
   а) компьютере пользователя;
   б) сервере;
8.23. Каковы особенности построения одноранговых сетей с выходом в Интернет?
8.24. При построении защищенной системы (с использованием глобальных компьютерных сетей) каким основным характеристикам Вы будете уделять наибольшее внимание?
8.25. Каковы особенности функционирования взаимодействия обмена информацией между различными глобальными сетями и подсетями различных стран?

8.26. Известно, что при настройке, как правило, начинающие администраторы пользуются настройками сервера «по умолчанию». Приведите аргументы в ошибочность такого подхода.

8.27. Приведите примеры сертифицированных программных средств (сервера, межсетевые экраны, криптографические средства), работающие в компьютерных сетях.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации. 2000 г. Утв. Президентом РФ от 9 сентября 2000 г. № Пр–1895 // Российская газета. – 2000. – 28 сентября (№ 187).
2. Об электронно-цифровой подписи. Федеральный закон РФ от 10 января 2001 г. № 1–ФЗ // Собрание законодательства РФ. – 2002. – № 2 – С. 127.
3. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий, 2003.
4. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники от несанкционированного доступа к информации. Москва, 1992.
5. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Москва, 1992.
6. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации. Москва, 1992.
7. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989.
8. ГОСТ 34.10–94. Информационная технология. Криптографическая защита информации. Система электронно-цифровой подписи на базе асимметричного криптографического алгоритма. – М.: Госстандарт России, 1994.
9. ГОСТ 34.10–01. Информационная технология. Криптографическая защита информации. Система электронно-цифровой подписи на базе асимметричного криптографического алгоритма. – М.: Госстандарт России, 2001.
10. ГОСТ 34.11–94. Информационная технология. Криптографическая защита информации. Функция хеширования. – М.: Госстандарт России, 1994.
11. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2000. – 384 с.
12. Гайкович В.Ю., Першин А. Ю. Безопасность электронных банковских систем. – М.: Единая Европа, 1994. – 365 с.
13. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 1994.

14. Герасименко В.А., Малюк А. А. Основы защиты информации. – М.: «Инкомбук», 1997. – 540 с.
15. Грушко А.А., Тимонина Е. Е. Теоретические основы защиты информации – М.: Изд-во агентства «Яхтсмен», 1996. – 192 с.
16. Зегжда Д.П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.
17. Касперский Е. Компьютерные вирусы: что это такое и как с ними бороться – М.: СК Пресс, 1998. – 288 с.
18. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 364 с.
19. Мещеряков Р.В., Шелупанов А.А. Специальные вопросы информационной безопасности. – Томск.: Изд-во ИОА ТНЦ СО РАН, 2003 – 250 с.
20. Мещеряков Р.В., Шелупанов А.А., Белов Е.Б., Лось В.П. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 540 с.
21. Партыка Т.Л., Попов И. И. Информационная безопасность. – М.: ФОРУМ: ИНФРА–М, 2002 – 368 с.
22. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учебное пособие для вузов / П.Ю. Белкин, О.О. Михальский, А.С. Першаков и др. – М.: Радио и связь, 2000. – 168 с.
23. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: учебное пособие для вузов / В.Г. Проскурин, С.В. Крутов, И.В. Мацкевич – М.: Радио и связь, 2000. – 168 с.
24. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защиты информации в компьютерных системах. – М.: Радио и связь, 2001. – 378 с.
25. Самосук М. Компьютерное пиратство / Защита программного обеспечения / под ред. Гроубера. – М.: Мир, 1992.
26. Семкин С.Н., Семкин А.Н. Основы информационной безопасности объектов обработки информации: научно-практическое пособие. – Орел: Труд, 2000. – 300 с.
27. Теоретические основы компьютерной безопасности: учебное пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков и др. – М.: Радио и связь, 2000. – 192 с.
28. Чижухин Г.Н. Основы защиты информации в вычислительных системах и сетях ЭВМ: учебное пособие. – Пенза.: Изд-во Пенз. гос. ун-та, 2001. – 164 с.
29. Хоффман Л.Дж. Современные методы защиты информации / пер. с англ. – М.: Советское радио, 1980. – 268 с.
30. Shneier B. Applied cryptography, 2nd Edition, John & Sons, 1996 / (Шнайдер Б. Прикладная криптография. – М.: Мир, 1999).
31. Trusted Computer System Evaluation Ctriteria. US Department of Defence 5200.28–STD, 1993.

Учебное издание

Мещеряков Роман Валерьевич

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Редактор	*С.П. Барей*
Верстка	*В.П. Аршинова*
Дизайн обложки	*О.Ю. Аршинова* *О.А. Дмитриев*

Подписано к печати 21.05.2008. Формат 60x84/16. «Снегурочка»
Печать XEROX. Усл. печ. л. 8.55. Уч.-изд. л. 7.73.
Заказ . Тираж 100 экз.

Томский политехнический университет
Система менеджмента качества
Томского политехнического университета сертифицирована
NATIONAL QUALITY ASSURANCE по стандарту ISO 9001:2000

ИЗДАТЕЛЬСТВО ТПУ. 634050, г. Томск, пр. Ленина, 30.