Министерство образования и науки Российской Федерации
Волгоградский государственный архитектурно-строительный университет

А. А. Платонов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Волгоград. ВолгГАСУ. 2016

УДК 004.056(075.8)
ББК 32.973-018.2я73
П374

Р е ц е н з е н т ы:
кандидат технических наук *А. В. Игнатьев*, доцент кафедры строительной механики Волгоградского государственного архитектурно-строительного университета;
директор ООО «ИТ-мастера» *А. Ю. Ромашев*

Утверждено редакционно-издательским советом университета в качестве учебного пособия

Платонов, А. А.

П374 Информационная безопасность [Электронный ресурс] : учебное пособие / А. А. Платонов ; М-во образования и науки Рос. Федерации, Волгогр. гос. архит.-строит. ун-т. — Электронные текстовые и графические данные (1,6 Мбайт). — Волгоград : ВолгГАСУ, 2016. — Электронное издание сетевого распространения. — Систем. требования: PC 486 DX-33; Microsoft Windows XP; Internet Explorer 6.0; Adobe Reader 6.0. — Официальный сайт Волгоградского государственного архитектурно-строительного университета. Режим доступа: http://www.vgasu.ru/publishing/on-line/ — Загл. с титул. экрана.

ISBN 978-5-98276-822-3

Написано в соответствии с программой дисциплины «Информационная безопасность». Содержит необходимый кратко изложенный теоретический материал и примеры решения типичных практических задач. Может быть использовано для самостоятельного изучения темы и является базой для подготовки к экзамену по данной дисциплине.

Для студентов направления подготовки «Информационные системы и технологии» (уровень «бакалавриат») очной формы обучения.

Для удобства работы с изданием рекомендуется пользоваться функцией Bookmarks (Закладки) в боковом меню программы Adobe Reader и системой ссылок.

УДК 004.056(075.8)
ББК 32.973-018.2я73

ISBN 978-5-98276-822-3

ОГЛАВЛЕНИЕ

1. АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С каждым годом растет количество преступлений в информационной сфере и увеличивается соответствующий ущерб от них. В связи с этим повышается интерес к проблеме защиты информации, в том числе и на уровне государства. Приняты закон об информации, информатизации и защите информации, закон о коммерческой тайне, закон об электронной цифровой подписи, закон о персональных данных.

Информация — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Основные факторы, способствующие повышению уязвимости информации:

1. Увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации.

2. Сосредоточение в единых базах данных информации различного назначения и различной принадлежности.

3. Расширение круга пользователей, имеющих непосредственный доступ к информационным ресурсам и находящимся в них массивам данных.

4. Усложнение режимов работы технических средств вычислительных систем.

5. Автоматизация межмашинного обмена информацией, в том числе на больших расстояниях.

Информационная безопасность — это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлимый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

К поддерживающей инфраструктуре относятся системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Понятие информационной безопасности шире, чем понятие компьютерной безопасности. В закрытых учреждениях имеется секретный документооборот и ведется учет без использования компьютеров.

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Информационная безопасность обеспечивает следующие свойства информации:

конфиденциальность — означает, что возможность ознакомиться с информацией имеют только лица, владеющие соответствующими полномочиями (пример — пароли, документы ограниченного доступа);

целостность — означает, что возможность внести изменения в информацию имеют только уполномоченные лица (пример нарушения целостности — подделка незашифрованного сообщения электронной почты);

доступность — возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий период времени (пример — защита от сбоев, потери данных).

Перечисленные три свойства информации нередко находятся в противоречии друг с другом, поэтому необходимо определять приоритеты в защите информации.

Вопросы для самоконтроля

1. Перечислите основные факторы, вызывающие повышение уязвимости информации с ростом информатизации. Дайте определения информации, информационной безопасности, защиты информации.

2. Какие три свойства информации обеспечивает информационная безопасность? Приведите примеры.

2. УГРОЗЫ ИНФОРМАЦИИ

Информацию можно разделить по степени ее важности. Важность информации устанавливается ее владельцами в виде дискретной шкалы категорий (рис. 1).

Рис. 1

Под **угрозами информации** будем понимать потенциальные или реально возможные действия по отношению к информационной сфере, приводящие к несанкционированным изменениям свойств информации (конфиденциальность, доступность, достоверность, целостность).

По конечному проявлению можно выделить следующие угрозы информации:

ознакомление;

модификация;

уничтожение;

блокирование.

Конкретные реализации угроз информации называются **сценариями угроз информации**.

Рассмотрим воздействие угроз на соответствующие свойства информации (рис. 2).

Ознакомление с конфиденциальной информацией может проходить различными путями и способами, при этом существенным является отсутствие изменений самой информации. Нарушение конфиденциальности или

секретности информации связано с ознакомлением с ней тех лиц, для которых она не предназначалась. Какая информация является конфиденциальной или секретной, решает собственник или владелец этой информации. Они же определяют круг лиц, имеющих доступ к ней. Нарушение конфиденциальности информации может произойти путем ознакомления с ней лицами, не имеющими на то права, и несанкционированной модификации грифа секретности (значимости).

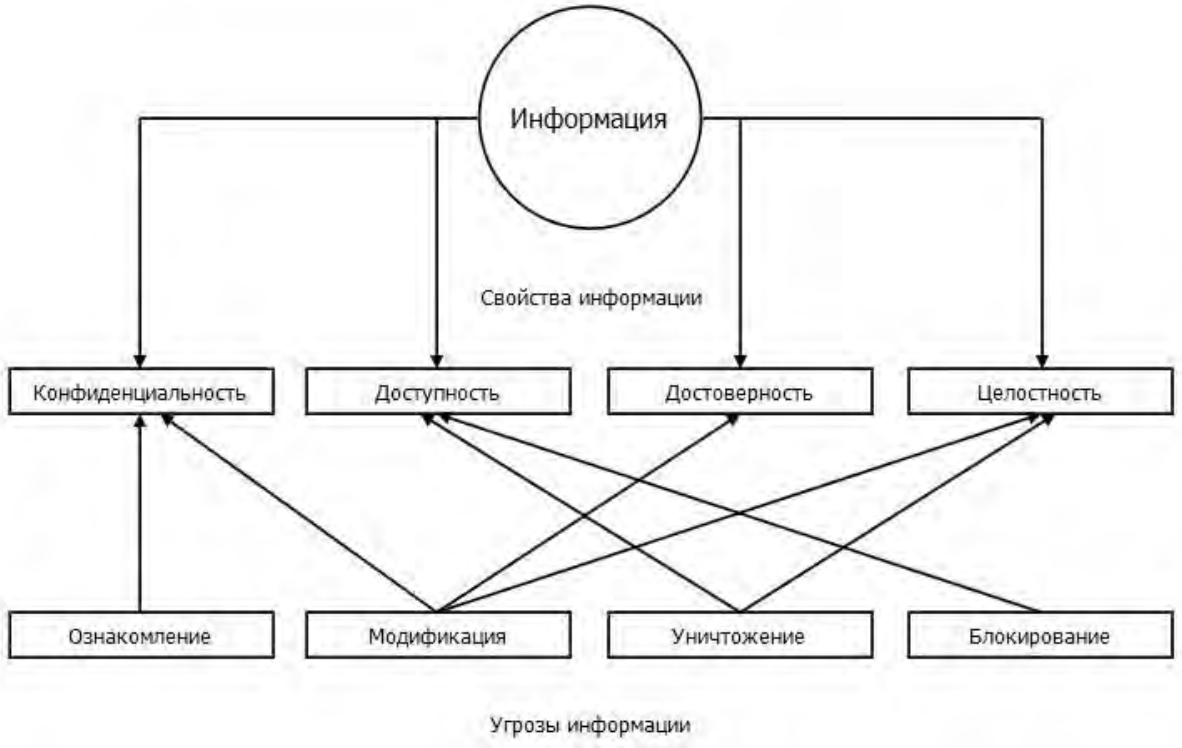

Рис. 2

Модификация информации направлена на изменение таких свойств, как конфиденциальность, достоверность, целостность, при этом подразумевается изменение состава и содержания сведений. Модификация информации не предполагает ее полное уничтожение.

Уничтожение информации приводит к ее полному разрушению. Нарушение целостности информации заключается в утере информации. При утере информации она пропадает безвозвратно и не может быть восстановлена никакими средствами. Утеря может произойти из-за разрушения или уничтожения носителя информации или его пропажи, из-за стирания информации на носителях с многократной записью, из-за отключения питания устройств с энергозависимой памятью. При уничтожении информации нарушается также свойство доступности информации.

Блокирование информации приводит к потере доступа к ней, т. е. к недоступности информации. Доступность заключается в том, что субъект, обладающий правом на ее использование, должен иметь возможность своевременного ее получения в удобном для него виде. При потере доступа

к информации она по-прежнему существует, но воспользоваться ею нельзя: субъект не может с ней ознакомиться, скопировать ее, передать другому субъекту или представить в виде, удобном для использования. Потеря доступа может быть связана с отсутствием или неисправностью некоторого оборудования автоматизированных систем (АС), отсутствием какого-либо специалиста или недостаточной его квалификацией, отсутствием или неработоспособностью какого-то программного средства, использованием ресурсов АС и др. Так как информация не утеряна, то доступ к ней может быть получен после устранения причин потери доступа.

Перечисленные угрозы информации могут проявляться в виде комплекса последовательных и параллельных реализаций. Реализация угроз информации, связанная с нарушением свойств информации, приводит к нарушению режима управления и в конечном итоге к моральным и (или) материальным потерям.

Указанные выше угрозы информации могут быть классифицированы по нескольким направлениям (рис. 3).

Рис. 3

Источники информационных угроз могут быть как внутренними, так и внешними. Чаще всего такое деление происходит по территориальному признаку и по признаку принадлежности к объекту информационной защиты (**рис. 4**).

Неправомерное овладение конфиденциальной информацией возможно вследствие ее разглашения источниками сведений, утечки информации через технические средства и несанкционированного доступа к охраняемым сведениям (**рис. 5**).

Рис. 4

Рис. 5

Разглашение — это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.

Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и других формах обмена и действий с конфиденциальной информацией. Реализуется разглашение по формальным и неформальным каналам распространения информации.

К формальным коммуникациям относятся деловые встречи, совещания, переговоры и тому подобные формы общения: обмен официальными деловыми и научными документами, средствами передачи официальной информации (почта, телефон, телеграф и др.). Неформальные коммуникации включают личное общение, выставки, семинары, конференции и другие массовые мероприятия, а также средства массовой информации. Как правило, причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты секретов и непонимание (или недопонимание) необходимости их тщательного соблюдения. Тут важно отметить, что субъектом в этом процессе выступает источник (владелец) охраняемых секретов.

Следует отметить информационные особенности разглашения. Это информация содержательная, осмысленная, упорядоченная, аргументированная, объемная, которая зачастую доводится в реальном масштабе времени. Часто имеется возможность диалога. Информация ориентирована по определенной тематической области и документирована. Для получения интересующей злоумышленника информации последний затрачивает практически минимальные усилия и использует простые легальные технические средства.

Утечка — это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она доверена, по техническим каналам утечки информации.

Утечка информации осуществляется по различным техническим каналам. Известно, что информация вообще переносится или передается либо энергией, либо веществом. По физической природе возможны следующие пути переноса информации: световые лучи, звуковые волны, электромагнитные волны, материалы и вещества. Соответственно этому каналы утечки информации классифицируются на визуально-оптические, акустические, электромагнитные и материально-вещественные. Под каналом утечки информации принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям. Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.

Несанкционированный доступ — это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам.

Для реализации этих действий злоумышленнику приходится проникать на объект защиты, используя различные технические средства. С развитием компьютерных технологий стал доступен дистанционный несанкционированный доступ к охраняемой информации или, иначе говоря, компьютерный взлом.

Вопросы для самоконтроля

1. Назовите основные грифы информации по степени конфиденциальности. Какой гриф обычно используется для информации, составляющей коммерческую тайну, и почему?
2. Что такое угрозы информации? Назовите основные четыре типа угроз. На какие свойства информации влияет каждый из них и почему?
3. Охарактеризуйте внутренние и внешние угрозы.
4. Что такое конфиденциальная информация? Что нужно сделать собственнику информации, для того чтобы она стала конфиденциальной?
5. Опишите три типа действий, приводящих к неправомерному овладению конфиденциальной информацией. В чем различия между утечкой и разглашением?

3. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Организационная защита

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

организацию охраны, режима, работу с кадрами, документами;

использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз безопасности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или по крайне мере сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

Организационные мероприятия — это мероприятия ограничительного характера, сводящиеся в основном к регламентации доступа и использования технических средств обработки информации. Они, как правило, проводятся силами самой организации путем использования простейших мер.

Организационные мероприятия выражаются в тех или иных ограничительных мерах. Можно выделить такие ограничительные меры, как территориальные, пространственные и временные.

Территориальные ограничения сводятся к умелому расположению источников на местности или в зданиях и помещениях, исключающему подслушивание переговоров или перехват сигналов радиоэлектронных средств.

Пространственные ограничения выражаются в выборе направлений излучения тех или иных сигналов в сторону наименьшей возможности их перехвата злоумышленниками.

Временные ограничения проявляются в сокращении до минимума времени работы технических средств, использовании скрытых методов связи, шифровании и других мерах защиты.

Одной из важнейших задач организационной деятельности является определение состояния технической безопасности объекта, его помещений, подготовка и выполнение организационных мер, исключающих возможность неправомерного овладения конфиденциальной информацией, воспрещение ее разглашения, утечки и несанкционированного доступа к охраняемым секретам.

3.2. Инженерно-техническая защита

Инженерно-техническая защита — это совокупность специальных органов технического надзора, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

По функциональному назначению средства инженерно-технической защиты классифицируются на следующие группы:

физические;

аппаратные;

программные;

криптографические.

Такое деление средств защиты информации достаточно условно, так как на практике очень часто они взаимодействуют и реализуются в комплексе в виде программно-аппаратных модулей с широким использованием алгоритмов закрытия информации.

Физические средства защиты — это разнообразные устройства, приспособления, конструкции, аппараты, изделия, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий.

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Эти средства применяются для решения следующих задач:

охрана территории предприятия и наблюдение за ней;

охрана зданий, внутренних помещений и контроль за ними;

охрана оборудования, продукции, финансов и информации;

осуществление контролируемого доступа в помещения.

Все физические средства защиты объектов можно разделить на три категории: средства предупреждения, средства обнаружения и системы ликвидации угроз.

Аппаратные средства защиты — это различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации.

Аппаратные средства защиты информации применяются для решения следующих задач:

проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;

выявление каналов утечки информации на разных объектах и в помещениях;

локализация каналов утечки информации;

поиск и обнаружение средств промышленного шпионажа;

противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

В особую группу выделяются аппаратные средства защиты ЭВМ и коммуникационных систем на их базе.

Программные средства защиты — это специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных.

Можно выделить следующие направления использования программ для обеспечения безопасности конфиденциальной информации:

защита информации от несанкционированного доступа;

защита информации и программ от копирования;

защита информации и программ от вирусов;

программная защита каналов связи.

Криптографические средства защиты — это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Преобразование математическими методами передаваемого по каналам связи секретного сообщения, телефонного разговора или компьютерных данных осуществляется таким образом, что они становятся совершенно непонятными для посторонних лиц.

3.3. Организационно-техническая защита

Организационно-технические мероприятия обеспечивают блокирование разглашения и утечки конфиденциальных сведений через технические средства обеспечения производственной и трудовой деятельности, а также противодействие техническим средствам промышленного шпионажа с помощью специальных технических средств.

Организационно-технические мероприятия по защите информации можно подразделить на пространственные, режимные и энергетические.

Пространственные меры выражаются в уменьшении ширины диаграммы направленности, ослаблении боковых и заднего лепестков диаграммы направленности излучения радиоэлектронных средств (РЭС).

Режимные меры сводятся к использованию скрытых методов передачи информации по средствам связи: шифрованию, использованию квазипеременных частот передачи и др.

Энергетические меры предполагают снижение интенсивности излучения и работу РЭС на пониженных мощностях.

3.4. Система защиты информации

Под **системой безопасности** будем понимать организационную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятий, государства от внутренних и внешних угроз (рис. 6).

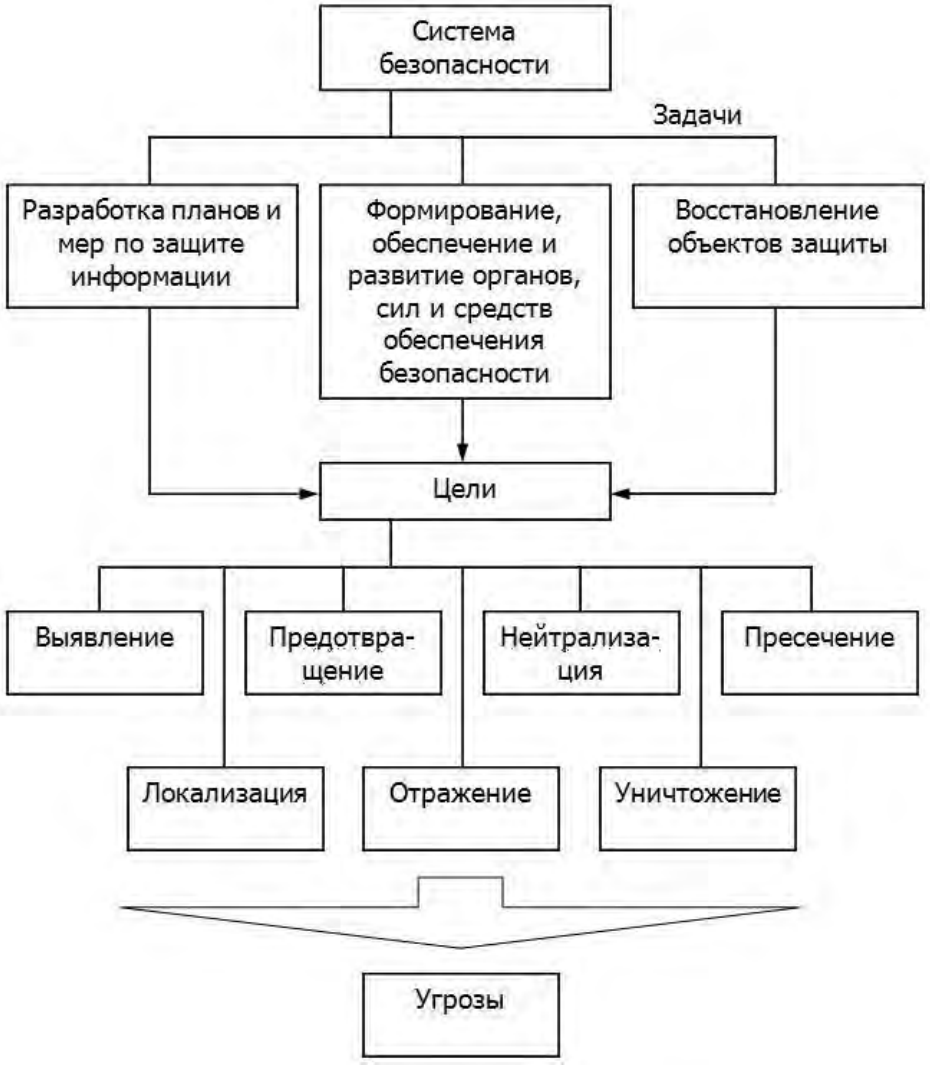

Рис. 6

Система защиты информации (СЗИ) — это организованная совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

С позиций системного подхода к защите информации предъявляются определенные требования. Так, защита информации должна быть:

1) непрерывной;

2) плановой (каждая служба разрабатывает план защиты информации в сфере своей компетенции);

3) целенаправленной (защищается то, что должно защищаться в интересах конкретной цели);

4) конкретной (защищаются конкретные данные, объективно подлежащие защите);

5) активной;

6) надежной;

7) универсальной (распространяется на любые каналы утечки информации);

8) комплексной (применяются все необходимые виды и формы защиты).

Обеспечение информационной безопасности достигается системой мер, направленных:

на предупреждение угроз, т. е. превентивные меры по обеспечению информационной безопасности в интересах упреждения;

выявление угроз, что выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;

обнаружение угроз, что имеет целью определение реальных угроз и конкретных преступных действий;

локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;

ликвидацию последствий угроз и преступных действий и восстановления статус-кво.

Предупреждение угроз может быть обеспечено самыми различными мерами и средствами, начиная от формирования осознанного отношения сотрудников к проблеме безопасности и защиты информации и заканчивая созданием эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Предупреждение угроз возможно и путем получения (добывания) информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний. Для этих целей необходима работа сотрудников службы безопасности с информаторами в интересах наблюдения и объективной оценки ситуации как внутри коллектива сотрудников, особенно главных участков ее фирмы, так и вне, среди конкурентов и преступных формирований.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

Выявление угроз имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции.

Обнаружение угроз — действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов.

Локализация угроз или *пресечение* предполагают устранение действующей угрозы и конкретных преступных действий. Это, например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий угроз направлена на восстановление состояния, предшествовавшего наступлению угрозы.

Каждому виду мер присущи его специфические способы, силы и средства.

Вопросы для самоконтроля

1. Какие три направления защиты информации вы знаете?
2. Что такое организационные мероприятия по защите информации? Какие ограничительные меры вы знаете? В чем они выражаются? Приведите примеры.
3. Что такое инженерно-техническая защита? Перечислите группы средств инженерно-технической защиты. Приведите краткие примеры.
4. Какие физические средства защиты информации вы знаете? Для каких задач они нужны?
5. Что такое аппаратные средства защиты информации? Перечислите их основные задачи. Приведите примеры.
6. Какие программные средства защиты вы знаете? Назовите основные направления защиты.
7. Что обеспечивают организационно-технические мероприятия по защите информации? Какие три вида мероприятий вы знаете?
8. Что такое система защиты информации (определение и ее основные качества)?
9. На что направлены меры по противодействию угрозам (предупреждение, выявление и т. д.)?

4. СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ (СПД)

4.1. Межсетевые экраны

4.1.1. Место межсетевых экранов в системе защиты СПД

Когда в качестве внешней сети используется открытая потенциально враждебная сеть, то возникают угрозы нарушения установленных правил межсетевого взаимодействия, а именно: угрозы неправомерного вторжения во внутреннюю сеть из внешней; угрозы НСД во внешнюю сеть из внутренней.

Неправомерное вторжение во внутреннюю сеть из внешней может выполняться как с целью несанкционированного использования ресурсов внутренней сети, так и с целью нарушения ее работоспособности. Без соответствующих средств защиты вероятность успешной реализации данных угроз является достаточно высокой.

Угрозы НСД во внешнюю сеть из внутренней сети актуальны в случае ограничения разрешенного доступа во внешнюю сеть правилами, установленными в организации. Такое ограничение, что особенно характерно для взаимодействия с открытыми сетями, может понадобиться в следующих случаях: для предотвращения утечки конфиденциальных данных; при запрете доступа, например в учебных заведениях, к информации нежелательной направленности; в случае запрета служебного доступа к развлекательным компьютерным ресурсам в рабочее время.

Проблема защиты от несанкционированных действий при взаимодействии с внешними сетями успешно может быть решена только с помощью специализированных программно-аппаратных комплексов, обеспечивающих целостную защиту компьютерной сети от враждебной внешней среды. Такие комплексы называют **межсетевыми экранами (МЭ)** или **брандмауэрами**. Межсетевой экран устанавливается на стыке между защищаемой внутренней и потенциально враждебными внешними сетями и выполняет функции противодействия несанкционированному межсетевому доступу. При этом все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Для него отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Межсетевой экран должен учитывать протоколы информационного обмена, положенные в основу функционирования внутренней и внешней сетей. Если эти протоколы отличаются, то экран должен поддерживать многопротокольный режим работы, обеспечивая протокольное преобразование

отличающихся по реализации уровней модели OSI для объединяемых сетей. Чаще всего возникает необходимость в совместной поддержке стеков протоколов SPX/IPX и TCP/IP.

4.1.2. Функции межсетевых экранов

В общем случае работа межсетевого экрана основана на динамическом выполнении двух групп функций:

фильтрации проходящих через него информационных потоков;

посредничества при реализации межсетевых взаимодействий.

В зависимости от типа экрана эти функции могут выполняться с различной полнотой. Простые межсетевые экраны ориентированы на выполнение только одной из данных функций. Комплексные экраны обеспечивают совместное выполнение указанных функций защиты.

Фильтрация трафика состоит в выборочном пропускании информационных потоков через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано.

Фильтрация осуществляется на основе набора правил, являющихся выражением сетевых аспектов принятой политики безопасности. Поэтому межсетевой экран удобно представлять как последовательность фильтров, обрабатывающих информационный поток. Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих стадий:

1) анализа информации по заданным критериям;

2) принятия одного из следующих решений: не пропустить данные; передать данные на следующий фильтр; пропустить данные.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например преобразование данных, регистрация событий и др.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;

непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;

внешние характеристики потока информации, например временные, частотные характеристики, объем данных и т. д.

Функции посредничества межсетевой экран выполняет с помощью специальных программ, называемых экранирующими агентами или просто программами-посредниками (NAT, proxy). Данные программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью.

При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере экрана.

Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять следующие защитные функции:

Идентификация и аутентификация пользователей на основе одноразовых паролей или цифровых сертификатов. Большинство программ-посредников разрабатывается таким образом, чтобы пользователь аутентифицировался только в начале сеанса работы с межсетевым экраном. После этого от него не требуется дополнительная аутентификация в течение времени, определяемого администратором.

Разграничение доступа к ресурсам внутренней или внешней сети. Способы разграничения к ресурсам внутренней сети ничем не отличаются от способов разграничения, поддерживаемых на уровне операционной системы. При разграничении доступа к ресурсам внешней сети чаще всего используется один из следующих подходов: разрешение доступа только по заданным адресам во внешней сети (белый и черный списки); фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам; накопление и обновление администратором санкционированных информационных ресурсов внешней сети в памяти брандмауэра и полный запрет доступа во внешнюю сеть.

Фильтрация и преобразование потока сообщений. Здесь следует различать два вида программ-посредников: экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например FTP, HTTP, Telnet; универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например агенты, ориентированные на поиск и обезвреживание компьютерных вирусов или прозрачное шифрование данных (организация защищенных виртуальных сетей). Программный посредник анализирует поступающие к нему пакеты данных, и если какой-либо объект не соответствует заданным критериям, то посредник либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например обезвреживание обнаруженных компьютерных вирусов. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файловые архивы.

Трансляция внутренних сетевых адресов для исходящих пакетов сообщений (NAT). Даная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов посредник выполняет автоматическое преобразование IP-адресов компьютеров-отправителей в один «надежный» IP-адрес, ассоциируемый с брандмауэром, из которого передаются все исходящие пакеты. В результате все исходящие из внутренней сети пакеты оказываются отправленными межсетевым экраном, что исключает прямой контакт между авторизованной

внутренней сетью и являющейся потенциально опасной внешней сетью. IP-адрес брандмауэра становится единственным активным IP-адресом, который попадает во внешнюю сеть. При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа.

Регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов. В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий является уведомление администратора, т. е. выдача предупредительных сигналов. Многие межсетевые экраны содержат мощную систему регистрации, сбора и анализа статистики. Учет может вестись по адресам клиента и сервера, идентификаторам пользователей, времени сеансов, времени соединений, количеству переданных/принятых данных, действиям администратора и пользователей. Системы учета позволяют провести анализ статистики и предоставляют администраторам подробные отчеты. Благодаря использованию специальных протоколов посредники могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

Кэширование данных, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска брандмауэра, называемого в этом случае proxy-сервером. Поэтому если при очередном запросе нужная информация окажется на proxy-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботится только о периодическом обновлении содержимого proxy-сервера. Функция кэширования успешно может использоваться для ограничения доступа к информационным ресурсам внешней сети. В этом случае все санкционированные информационные ресурсы внешней сети накапливаются и обновляются администратором на proxy-сервере. Пользователям внутренней сети разрешается доступ только к информационным ресурсам proxy-сервера, а непосредственный доступ к ресурсам внешней сети запрещается.

Экранирующие агенты намного надежнее обычных фильтров и обеспечивают большую степень защиты. Однако они снижают производительность обмена данными между внутренней и внешней сетями и не обладают той степенью прозрачности для приложений и конечных пользователей, которая характерна для простых фильтров.

4.1.3. Классификация межсетевых экранов

Межсетевые экраны поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Межсетевой экран может функционировать на сетевом, сеансовом, прикладном уровне эталонной модели. Соответственно, различают экранирующий маршрутизатор, экранирующий транспорт (шлюз сеансового

уровня) и экранирующий шлюз (шлюз прикладного уровня). Стоит отметить, что надежную защиту обеспечивают только комплексные межсетевые экраны, каждый из которых объединяет все типы экранов.

Экранирующий маршрутизатор, называемый также *пакетным фильтром*, предназначен для фильтрации пакетов сообщений и обеспечивает прозрачное взаимодействие между внутренней и внешней сетями. Он функционирует на сетевом уровне модели OSI, но для выполнения своих отдельных функций может охватывать и транспортный уровень эталонной модели. Решение о том, пропустить или отбраковать данные, принимается для каждого пакета независимо, на основе заданных правил фильтрации. Для принятия решения анализируются заголовки пакетов сетевого и транспортного уровней. В качестве анализируемых полей IP- и TCP- или UDP-заголовков каждого пакета выступают:

адрес отправителя;

адрес получателя;

тип пакета;

флаг фрагментации пакета;

номер порта источника;

номер порта получателя.

Первые четыре параметра относятся к IP-заголовку пакета, а следующие — к TCP- или UDP-заголовку.

Адреса отправителя и получателя являются IP-адресами. Поле типа пакета содержит код протокола ICMP, соответствующего сетевому уровню, либо код протокола транспортного уровня (TCP или UDP), к которому относится анализируемый IP-пакет. Флаг фрагментации пакета определяет наличие или отсутствие фрагментации IP-пакетов. Номера портов источника и получателя добавляются драйвером TCP или UDP к каждому отправляемому пакету сообщения и однозначно идентифицируют приложение-отправитель, а также приложение, для которого предназначен этот пакет.

При обработке каждого пакета экранирующий маршрутизатор последовательно просматривает заданную таблицу правил, пока не найдет правила, с которыми согласуется полная ассоциация пакета. Здесь под ассоциацией понимается совокупность параметров, указанных в заголовках данного пакета. Если экранирующий маршрутизатор получил пакет, не соответствующий ни одному из табличных правил, он применяет правило, заданное по умолчанию. Из соображений безопасности это правило обычно указывает на необходимость отбраковки всех пакетов, не удовлетворяющих ни одному из других правил.

В качестве пакетного фильтра может использоваться как обычный маршрутизатор, так и работающая на сервере программа, сконфигурированная таким образом, чтобы фильтровать входящие и исходящие пакеты.

К достоинствам экранирующих маршрутизаторов относятся:

простота самого экрана;

простота процедур конфигурирования и установки;

прозрачность для программ и приложений;

минимальное влияние на производительность сети;

низкая стоимость, обусловленная тем, что любой маршрутизатор в той или иной степени представляет возможность фильтрации пакетов.

Однако экранирующие маршрутизаторы не обеспечивают высокую степень безопасности, так как проверяют только заголовки пакетов и не поддерживают многие необходимые функции защиты, например аутентификацию конечных узлов, криптографическое закрытие пакетов сообщений, а также проверку их целостности и подлинности. Экранирующие маршрутизаторы уязвимы для таких распространенных сетевых атак, как подделка исходных адресов и несанкционированное изменение содержимого пакетов сообщений. «Обмануть» межсетевые экраны данного типа не составляет труда — достаточно сформировать заголовки пакетов, которые удовлетворяют разрешающим правилам фильтрации.

Экранирующий транспорт, называемый еще *шлюзом сеансового уровня*, предназначен для контроля виртуальных соединений и трансляции IP-адресов при взаимодействии с внешней сетью. Он функционирует на сеансовом уровне модели OSI, охватывая в процессе своей работы также транспортный и сетевой уровни эталонной модели. Защитные функции экранирующего транспорта относятся к функциям посредничества.

Контроль виртуальных соединений заключается в контроле квитирования связи, а также контроле передачи информации по установленным виртуальным каналам.

При контроле квитирования связи шлюз сеансового уровня следит за установлением виртуального соединения между рабочей станцией внутренней сети и компьютером внешней сети, определяя, является ли запрашиваемый сеанс допустимым. Такой контроль основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP. Однако если пакетный фильтр при анализе TCP-заголовков проверяет только номера портов источника и получателя, то экранирующий транспорт анализирует другие поля, относящиеся к процессу квитирования связи.

Чтобы определить, является ли запрос на сеанс связи допустимым, шлюз сеансового уровня выполняет следующие действия. Когда рабочая станция (клиент) запрашивает связь с внешней сетью, шлюз принимает этот запрос, проверяя, удовлетворяет ли он базовым критериям фильтрации. Затем, действуя от имени клиента, шлюз устанавливает соединение с компьютером внешней сети и следит за выполнением процедуры квитирования связи по протоколу TCP.

После того как шлюз определил, что рабочая станция внутренней сети и компьютер внешней сети являются авторизованными участниками сеанса TCP, и проверил допустимость данного сеанса, он устанавливает соединение. Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, контролируя передачу информации по установленному виртуальному каналу. Он поддерживает таблицу установленных соединений, пропуская

данные, относящиеся к одному из сеансов связи, которые зафиксированы в этой таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает цепь, использовавшуюся в данном сеансе.

В процессе контроля передачи информации по виртуальным каналам фильтрация пакетов экранирующим транспортом не осуществляется. Однако шлюз сеансового уровня способен отслеживать количество передаваемой информации и разрывать соединение после превышения определенного предела, тем самым препятствуя несанкционированному экспорту информации. Возможно также накопление регистрационной информации о виртуальных соединениях.

Для контроля виртуальных соединений в шлюзах сеансового уровня используются специальные программы, которые называют **канальными посредниками** (pipe proxies). Эти посредники устанавливают между внутренней и внешней сетями виртуальные каналы, а затем контролируют передачу по этим каналам пакетов, генерируемых приложениями TCP/IP.

Канальные посредники ориентированы на конкретные службы TCP/IP. Поэтому шлюзы сеансового уровня могут использоваться для расширения возможностей шлюзов прикладного уровня, работа которых основывается на программах-посредниках конкретных приложений.

На практике большинство шлюзов сеансового уровня не являются самостоятельными продуктами, а поставляются в комплекте со шлюзами прикладного уровня.

Шлюз сеансового уровня обеспечивает также ретрансляцию внутренних адресов сетевого уровня (IP-адресов) при взаимодействии с внешней сетью. Трансляция внутренних адресов выполняется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов IP-адреса компьютеров отправителей внутренней сети автоматически преобразуются в один IP-адрес, ассоциируемый с экранирующим транспортом. В результате все пакеты, исходящие из внутренней сети, оказываются отправленными межсетевым экраном, что исключает прямой контакт между внутренней и внешней сетью. IP-адрес шлюза сеансового уровня становится единственным активным IP-адресом, который попадает во внешнюю сеть.

Трансляция адресов, с одной стороны, вызвана необходимостью усиления защиты путем скрытия от внешних пользователей структуры защищаемой внутренней сети. При трансляции внутренних IP-адресов шлюз сеансового уровня экранирует, т. е. заслоняет, внутреннюю сеть от внешнего мира. В то же время субъектам внутренней сети кажется, что они напрямую общаются с компьютерами внешней сети. Кроме повышения безопасности, трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например в сети Интернет. Это эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней.

С другой стороны, трансляция адресов вызвана тем, что канальные посредники создают новое соединение каждый раз, когда они активизируются.

Посредник принимает запрос от рабочей станции внутренней сети и затем инициирует новый запрос к компьютеру внешней сети. Поэтому компьютер внешней сети воспринимает запрос как исходящий от посредника, а не от действительного клиента.

Недостатки у шлюза сеансового уровня те же, что и у экранирующего маршрутизатора: не обеспечивается контроль и защита содержимого пакетов сообщений, не поддерживается аутентификация пользователей и конечных узлов. Поэтому шлюз сеансового уровня применяют как дополнение к прикладному шлюзу.

Экранирующий шлюз, называемый также *прикладным шлюзом*, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает наиболее надежную защиту межсетевых взаимодействий. Защитные функции прикладного шлюза, как и экранирующего транспорта, относятся к функции посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять существенно большее количество функций защиты, к которым относятся следующие:

идентификация и аутентификация пользователей при попытке установления соединений через брандмауэр;

проверка подлинности информации, передаваемой через шлюз;

разграничение доступа к ресурсам внутренней и внешней сетей;

фильтрация и преобразование потока сообщений;

регистрация событий, реагирование на задаваемые события, анализ зарегистрированной информации и генерация отчетов;

кэширование данных, запрашиваемых из внешней сети.

Учитывая, что функции прикладного шлюза относятся к функциям посредничества, он представляет собой универсальный компьютер, на котором функционируют программные посредники (экранирующие агенты) — по одному для каждого обслуживаемого прикладного протокола (HTTP, SMTP, NNTP и др.).

Посредник каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе. Так же как и шлюз сеансового уровня, прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию через шлюз и функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью. Однако посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями (программными серверами), а во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели OSI.

Прикладные шлюзы используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб TCP/IP — серверы HTTP, FTP, SMTP, NNTP и др. Эти программные серверы функционируют на межсетевом экране в резидентном режиме и реализуют функции

защиты, относящиеся к соответствующим службам TCP/IP. Трафик UDP обслуживается специальным транслятором содержимого UDP-пакетов.

Как и в случае шлюза сеансового уровня, для связи между рабочей станцией внутренней сети и компьютером внешней сети соответствующий посредник прикладного шлюза образует два соединения: от рабочей станции до брандмауэра и от брандмауэра до места назначения. Но, в отличие от канальных посредников, посредники прикладного шлюза пропускают только пакеты, сгенерированные теми приложениями, которые им поручено обслуживать. Например, программа-посредник службы HTTP может обрабатывать лишь трафик, генерируемый этой службой. Если в сети работает прикладной шлюз, то входящие и исходящие пакеты могут передаваться лишь для тех служб, для которых имеются соответствующие посредники. Так, если прикладной шлюз использует только программы-посредники HTTP, FTP и Telnet, то он будет обрабатывать лишь пакеты, относящиеся к этим службам, блокируя при этом пакеты всех остальных служб.

Фильтрация потоков сообщений реализуется прикладными шлюзами на прикладном уровне модели OSI. В соответствии с этим посредники прикладного шлюза, в отличие от канальных посредников, обеспечивают проверку содержимого обрабатываемых пакетов. Они могут фильтровать отдельные виды команд или информации в сообщениях протоколов прикладного уровня, которые им поручено обслуживать. Например, для службы FTP возможно динамическое обезвреживание компьютерных вирусов в копируемых из внешней сети файлах. Кроме того, посредник данной службы может быть сконфигурирован таким образом, чтобы предотвращать использование клиентами команды PUT, предназначенной для записи файлов на FTP-сервер. Такое ограничение уменьшает риск случайного повреждения хранящейся на FTP сервере информации и снижает вероятность заполнения его гигабайтами ненужных данных.

При настройке прикладного шлюза и описания правил фильтрации сообщений используются такие параметры, как название сервиса, допустимый временной диапазон его использования, ограничения на содержимое сообщений, связанных с данным сервисом, компьютеры, с которых можно пользоваться сервисом, идентификаторы пользователей, схемы аутентификации и др.

Шлюз прикладного уровня обладает важными достоинствами:

за счет возможности выполнения подавляющего большинства функций посредничества обеспечивает наиболее высокий уровень защиты локальной сети;

защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, уменьшая тем самым вероятность проведения успешных атак, основанных на недостатках программного обеспечения;

при нарушении работоспособности прикладного шлюза блокируется сквозное прохождение пакетов между разделяемыми сетями, что не снижает безопасной защищаемой сети в случае возникновения отказов.

Не считая высокой стоимости, к недостаткам прикладного шлюза также относятся:

сложность самого брандмауэра;

сложность установки и конфигурирования;

высокие требования к производительности и ресурсоемкость;

отсутствие «прозрачности» для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий.

Последний недостаток рассмотрим более подробно.

Технология функционирования прикладного шлюза основана на использовании посредников, проверяющих подлинность обращающихся к ним клиентов, а также устанавливающих необходимые соединения и выполняющих другие функции защиты межсетевого взаимодействия. Посредники выступают в качестве промежуточного звена передачи пакетов между сервером и клиентом. Вначале устанавливается соединение с посредником, а уже затем посредник принимает решение о том, создавать соединение с адресатом или нет. Соответственно, прикладной шлюз в процессе своего функционирования дублирует любое разрешенное соединение. Следствием этого является отсутствие прозрачности для пользователей и дополнительные накладные расходы на обслуживание соединений.

4.2. Виртуальные частные сети

Технология построения виртуальных частных сетей (virtual private network, VPN, ВЧС) представляет собой совокупность методов обеспечения конфиденциальности и контроля целостности данных, передаваемых между пользователями, подключенными к сети общего пользования. Компания Check Point Software Technologies, которая не без основания считается «законодателем моды» в области VPN и МЭ, определяет VPN как технологию, которая объединяет доверенные сети, узлы и пользователей через открытые сети, которым нет доверия. Технология построения ВЧС реализуется при помощи криптошлюзов и центра управления ВЧС.

Криптошлюзы (VPN-шлюзы, шлюзы безопасности) выполняют функции обеспечения конфиденциальности данных пользователя путем их шифрования и функции контроля целостности сообщений пользователя на выходе из публичной сети при помощи аутентификаторов сообщений. Центр управления ВЧС выполняет функции мониторинга и управления работой криптошлюзов, а также отвечает за распределение криптографических ключей между ними.

В настоящее время существует четыре метода построения криптошлюзов:

на базе сетевых операционных систем со встроенными функциями организации ВЧС;

на базе маршрутизаторов/коммутаторов, программное обеспечение которых имеет функции построения ВЧС;

на базе МЭ, с интегрированным функционалом ВЧС;

на базе специализированного программно-аппаратного обеспечения, предназначенного только для построения ВЧС.

В рамках ВЧС все данные, как правило, передаются по так называемым туннелям (PPTP, L2TP), которые представляют собой виртуальное соединение между двумя криптошлюзами. Алгоритм передачи сообщений через туннель ВЧС выглядит следующим образом. Перед отправкой сообщений пользователя через туннель криптошлюз их зашифровывает, вычисляет для них аутентификатор (код аутентификации сообщения), после чего сообщения инкапсулируются (упаковываются) в новые сообщения, которые передаются по туннелю. При этом в поле заголовка «адрес получателя» сформированного сообщения указывается адрес криптошлюза, а не сетевой адрес пользователя, которому на самом деле предназначается сообщение, что позволяет скрыть истинные адреса субъектов соединения. После передачи сообщений на другом конце туннеля криптошлюз извлекает полученные данные, расшифровывает их, с помощью аутентификатора проверяет их целостность, после чего данные передаются адресатам. Такой способ передачи сообщений принято называть туннелированием.

Взаимодействие между криптошлюзами реазилуется при помощи протоколов специального типа, называемых криптопротоколами (защищенными протоколами). Криптопротоколы могут быть реализованы на различных уровнях модели OSI. В настоящее время наиболее часто для построения ВЧС используется протокол IPSec, спецификация которого является частью базового стандарта шестой версии протокола IP, посредством которого реализуются функции уровня межсетевого взаимодействия стека протоколов TCP/IP.

4.3. Системы анализа защищенности

Для обнаружения технологических и эксплуатационных уязвимостей программного обеспечения (ПО), используемого в СПД, применяются системы анализа защищенности (security assessment systems) или сканеры безопасности (security scanners).

Процесс выявления технологических уязвимостей ПО может осуществляться при помощи одного из следующих методов:

путем анализа исходных текстов ПО;

при помощи исполняемого кода ПО;

посредством имитации атаки на ПО.

Обнаружение технологических уязвимостей ПО путем анализа исходных текстов ПО, как правило, осуществляется при помощи составления алгоритма работы программы и последующей проверки его правильности. Алгоритм работы программы может быть составлен в виде блок-схем или формализован при помощи различных математических аппаратов. Недостатком данного метода обнаружения уязвимостей является высокая сложность его практической реализации, а также отсутствие четко определенной методики анализа исходных текстов, позволявшей бы гарантировать отсутствие уязвимостей в анализируемом коде ПО.

Существующие средства анализа защищенности, реализующие метод анализа исходных текстов ПО, не могут быть использованы для обнаружения технологических уязвимостей ПО узлов СПД и центра управления сетью (ЦУС), поскольку основная часть исходных текстов ПО узлов СПД и ЦУС является «закрытой», т. е. интеллектуальной собственностью производителей ПО, и не подлежит распространению вне рамок компании-разработчика. Процедура же дизассемблирования, которая может быть применена для получения исходного кода ПО узлов СПД из исполняемых модулей программ, не может однозначно гарантировать, что полученный в результате этой процедуры исходный код соответствует дизассемблированной программе. Это связано с тем, что в процессе дизассемблирования не всегда имеется возможность определить разницу между исполняемыми командами и данными программы.

Обнаружение технологических уязвимостей ПО при помощи анализа исполняемого кода ПО осуществляется путем запуска программы в рамках тестовой среды, которая проверяет правильность выполнения этой программы. В процессе выполнения программы для нее формируется ряд запросов, после чего анализируется реакция тестируемой программы, т. е. то, каким образом исполняемый код программы влияет на состояние тестовой среды. Если в результате сформированного запроса тестовая среда переходит в небезопасное состояние, приводящее, например, к нарушению работоспособности системы, то делается вывод о наличии ряда уязвимостей в тестируемой программе. Такой метод обнаружения уязвимостей позволяет выявить ряд ошибок, внесенных на технологическом этапе, например ошибки, приводящие к переполнению буфера, ошибки неправильного доступа к памяти, выход за границы массива данных и др. Основным недостатком рассмотренного метода является отсутствие гарантий обнаружения всех технологических уязвимостей ПО, поскольку смоделировать все возможные состояния среды, в рамках которой выполняется программа, не представляется возможным.

4.4. Шифрование и электронная цифровая подпись (ЭЦП)

4.4.1. Основные понятия и определения

Шифр — семейство обратимых преобразований множества открытых сообщений (текстов) в множество шифрованных сообщений (текстов) и обратно, каждое из которых определяется некоторым параметром, называемым ключом. Различают два класса шифров: симметричные (с единым ключом) и асимметричные (с двумя ключами).

Ключ — секретный параметр шифра, отвечающий за выбор конкретного варианта преобразования для зашифрования (расшифрования) из множества преобразований, составляющих шифр. Ключ является тем элементом, с помощью которого можно варьировать результат криптографического преобразования информации.

Шифрование данных — процесс преобразования открытых данных (исходного сообщения) в зашифрованные (зашифрование) и наоборот (расшифрование). Шифрование осуществляется по определенным правилам, содержащимся в шифре, и с использованием известного ключа.

Симметричное шифрование предполагает использование одного и того же ключа для зашифрования и расшифрования сообщения. Любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение. Тогда задача обеспечения конфиденциальности информации с помощью симметричного шифра сводится к задаче обеспечения конфиденциальности ключа шифрования (секретного ключа). Обычно ключ шифрования представляет собой файл или массив данных и хранится на персональном ключевом носителе, например дискете или смарт-карте. При использовании симметричного шифрования в компьютерных сетях требуется перед началом обмена зашифрованными данными обменяться секретными ключами со всеми адресатами. При этом передача секретного ключа не может быть осуществлена по общедоступным каналам связи: секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей. Это является основным недостатком симметричного шифрования.

В качестве типичных симметричных шифров можно указать шифр DES (data encryption standard) с длиной ключа 56 бит, долгое время являвшийся фактическим стандартом шифрования в США и мире, европейский стандарт шифрования IDEA (international data encryption algorithm) с длиной ключа 128 бит и российский стандарт шифрования ГОСТ 28147—89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» с длиной ключа 256 бит.

В асимметричном шифре используется два ключа — открытый ключ для зашифрования информации и закрытый ключ для расшифрования информации, зашифрованной с помощью парного ему открытого ключа.

Закрытый ключ необходимо надежно защищать от несанкционированного доступа (аналогично ключу шифрования в симметричных шифрах). Копия открытого ключа должна находиться у каждого абонента компьютерной сети, с которым обменивается информацией владелец закрытого ключа.

Самым известным из асимметричных шифров является шифр RSA, основанный на операциях с большими (100-значными и более) простыми числами и их произведениями. Надежность шифра RSA обеспечивается трудностью факторизации больших чисел и сложностью вычисления дискретных логарифмов в конечном поле. Шифр RSA всесторонне исследован и признан стойким при достаточной длине ключей. В настоящее время длина ключа 512 бит считается недостаточной для обеспечения стойкости, длина 1024 бит — приемлемый вариант.

Асимметричное шифрование, в отличие от симметричного, обладает определенным преимуществом: не нужна секретная доставка ключей. Однако по сравнению с симметричным шифрованием асимметричное существенно медленнее, поскольку при шифровании и расшифровке используются весьма

ресурсоемкие операции (в частности, в RSA это возведение одного большого числа в степень, являющуюся другим большим числом).

Существует эффективный метод комбинированного использования симметричного и асимметричного шифрования. Сообщение сначала зашифровывают с помощью симметричного шифра, затем секретный ключ симметричного шифра зашифровывают с помощью асимметричного шифра на открытом ключе получателя, после чего зашифрованные сообщение и ключ отправляются по сети.

4.4.2. Контроль целостности данных

В основе криптографического контроля целостности данных лежат два понятия: хэш-функция и электронная цифровая подпись (ЭЦП).

Хэш-функция (функция хэширования) — это труднообратимое преобразование данных (односторонняя функция), которое принимает в качестве аргумента данные M произвольной длины и возвращает хэш-значение (хэш) $H = h(M)$ фиксированной длины. Следует отметить, что значение хэш-функции $h(M)$ зависит сложным образом от M и не позволяет восстановить M, т. е. задача нахождения M по H является вычислительно неразрешимой.

Теоретически возможно, что два различных сообщения могут иметь один и тот же хэш (так называемая коллизия). Поэтому для обеспечения стойкости хэш-функции вероятность коллизий должна быть ничтожно мала. Таким образом, функция хэширования может использоваться для обнаружения изменений сообщения при передаче по каналу связи, т. е. она может служить для формирования криптографической контрольной суммы (также называемой кодом аутентификации сообщения). Обычно в этом случае используется хэш-функция $h_k(M)$ с параметром-ключом k. Для проверки целостности к сообщению M добавляется его хэш H, т. е. по каналу связи передается пара (M, H). Получатель сообщения, зная, какая хэш-функция была применена, заново вычисляет ее, используя сообщение M и известный ему параметр-ключ k. Если значения полученного и вычисленного хэшей совпадают, то, значит, содержимое сообщения M не было подвергнуто никаким изменениям.

Наиболее популярными хэш-функциями являются MD2, MD4, MD5, каждая из них вырабатывает 128-битовый хэш-код, а также SHA (secure hash algorithm) с 160-битовым хэш-кодом.

Хэш-функции также широко применяются в целях аутентификации пользователей сети и в процедурах формирования и проверки ЭЦП.

Функционально цифровая подпись аналогична обычной рукописной подписи и обладает ее основными свойствами: удостоверяет, что подписанный текст исходит от лица, поставившего подпись; не дает самому этому лицу возможность отказаться от обязательств, связанных с подписанным текстом; гарантирует целостность подписанного текста.

Электронная цифровая подпись — это уникальное число, зависящее от подписываемого документа и секретного ключа, известного только подписывающему субъекту. ЭЦП реализуется при помощи асимметричных

алгоритмов шифрования и хэш-функций. ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов делает невозможным подтверждение подлинности цифровой подписи.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый.

Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа.

Система ЭЦП включает две основные процедуры: процедуру формирования цифровой подписи и процедуру проверки цифровой подписи. В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи — открытый ключ отправителя. Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания. Поэтому необходимо защищать секретный ключ подписывания от несанкционированного доступа. Секретный ключ ЭЦП, аналогично секретному ключу симметричного шифрования, рекомендуется хранить на персональном ключевом носителе в защищенном виде.

Помещаемая в подписываемый файл (или в отдельный файл электронной подписи) ЭЦП обычно содержит дополнительную информацию, однозначно идентифицирующую автора подписанного документа. Эта информация добавляется к документу до вычисления ЭЦП, что обеспечивает и ее целостность.

ЭЦП содержит следующую информацию: дату подписи; срок окончания действия ключа данной подписи; информацию о лице, подписавшем файл (Ф.И.О., должность, организация); идентификатор подписавшего (имя открытого ключа); собственно цифровую подпись. Наиболее известными ЭЦП являются цифровая подпись Эль-Гамаля, американский стандарт-алгоритм цифровой подписи DSA (digital signature algorithm), два российских стандарта — ГОСТ Р34.10—94 и ГОСТ Р34.10—2001.

Вопросы для самоконтроля

1. Что такое межсетевой экран? Для чего он нужен? Что такое персональный межсетевой экран?
2. Опишите основные функции межсетевых экранов (фильтрация трафика, посредничество при сетевых взаимодействиях). Стадии фильтрации.
3. Что такое фильтрация трафика МСЭ? Перечислите основные функции фильтра.
4. Что такое программы-посредники? Опишите их основные функции. В чем их преимущество по сравнению с пакетными фильтрами?
5. Опишите типы МСЭ. Сравните их достоинства и недостатки.
6. Что такое виртуальная частная сеть (VPN)? Опишите принцип ее работы.

5. ТИПОВАЯ МОДЕЛЬ НАПАДЕНИЯ

5.1. Классификация атак

Локальной атакой будем называть случай, когда злоумышленник оказался непосредственно перед клавиатурой (дисководом, CD-ROM и т. п.) данного компьютера.

Удаленная атака — это вариант атаки, когда злоумышленник не видит (и, возможно, никогда не увидит) ту рабочую станцию (или сервер), с которой он работает. При этом сам атакуемый компьютер, возможно, не проявляет никакой сетевой активности.

Атака на поток данных — инцидент, когда атакуемый компьютер (компьютеры) активно отправляет/принимает данные или обменивается ими с другими компьютерами сети (локальной или глобальной), а местом приложения атакующего воздействия является сегмент сети или сетевой узел между этими системами.

Схематически три вида атак представлены на рис. 7.

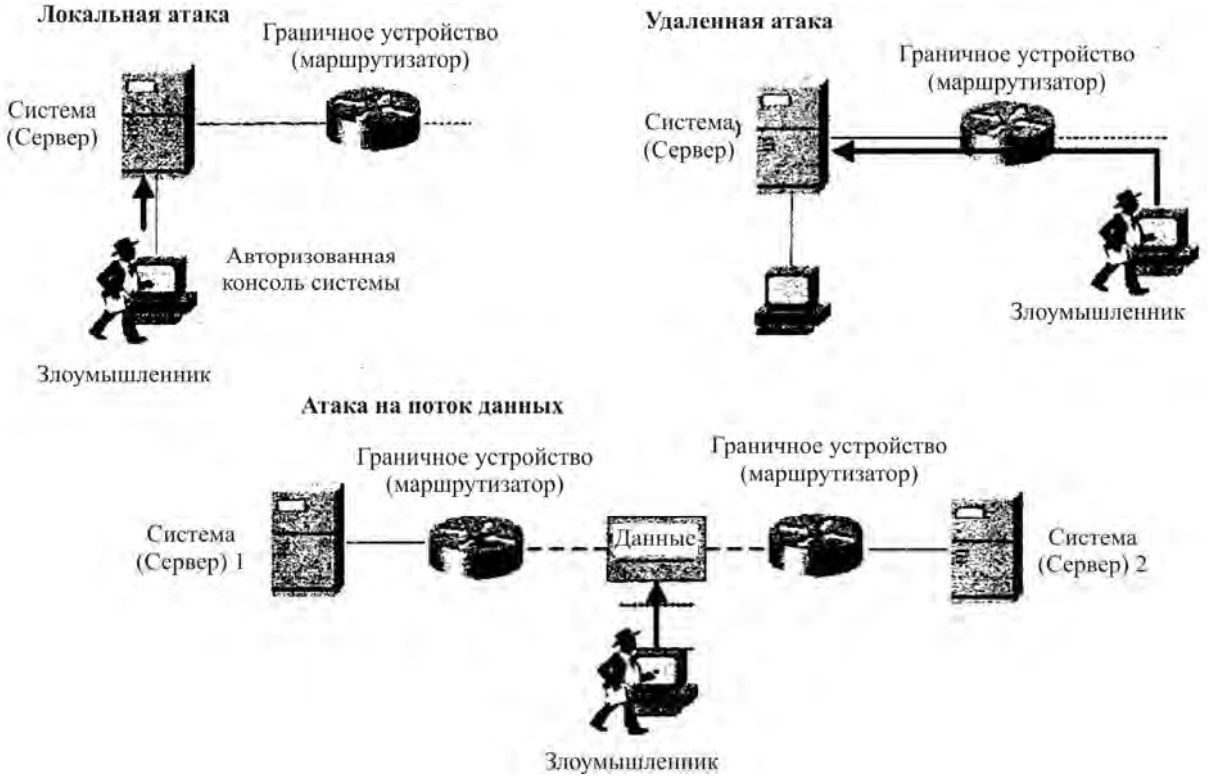

Рис. 7

5.2. Типовая атака на систему

Рассмотрим, как происходит типовая, абстрактная хакерская атака. Не будем пока говорить о серьезных профессиональных методах с внедрением шпионов в организацию, анализе содержания выброшенных документов компании или методах социальной инженерии.

Первое, о чем должен задуматься хакер, — это отсутствие обратной связи, т. е. о необходимости обеспечить себе условия, когда владелец атакуемой им системы (или тот, кто будет действовать в его интересах) не сможет узнать ни адреса, ни тем более личности того, кто произвел атаку. Простой периодической сменой IP-адреса тут не обойтись. Утилиты обратного отслеживания укажут путь как минимум до провайдера атакующего, после чего, используя регистрационные журналы сервиса, можно довольно быстро разыскать злоумышленника.

В связи с этим необходимы другие методы.

Первый метод — физический: надо периодически менять физическое место, откуда происходит атака. Например, переходить из одного интернет-кафе в другое, оставаясь анонимным клиентом. Но использовать этот метод целесообразно только для очень краткосрочной работы (несколько дней, а иногда и часов), так как довольно быстро можно определить страну и город хакера. Далее злоумышленник может быть задержан соответствующими структурами. Переезжать же постоянно из города в город довольно затратно.

Второй метод — логический. На просторах Интернета существуют сервера (так называемые прокси-службы или анонимайзеры), предоставляющие свои адреса для анонимной работы. Для работы с таким сервером достаточно знать его адрес и, атакуя удаленную систему, указать специальным образом ее адрес в сочетании с адресом прокси-сервиса. Анонимайзер скроет настоящий адрес хакера, поместив в соответствующее поле свой адрес. Таким образом, в атакуемой системе возможно будет увидеть только адрес прокси-службы, реально находящейся от хакера на произвольном удалении (сотни и тысячи километров). Используя в атакующем запросе последовательно несколько анонимайзеров, можно хорошо спрятать свой собственный адрес. Однако использование анонимайзеров возможно не для всех сетевых протоколов.

Кроме того, правоохранительные органы и государственные службы могут отслеживать использование сервисов в Интернете, в том числе и анонимайзеров. Дело в том, что топология Интернета представляет собой древовидную структуру относительно центральных узлов. Достаточно установить оборудование мониторинга на них, чтобы получить возможность исследовать подавляющий объем трафика сети.

Допустим, известно, что сайт компании «К» был взломан с адреса «А» с использованием средства «С». Если имеется доступ ко всему многообразию журналов мониторинга, можно сделать выборки: кто за последнее время интересовался сайтом «К», кто загружал или использовал средство «С» и кто использовал адрес «А». Сравнение результатов помогает существенно сузить область поиска.

Возможно, что злоумышленник достаточно смел, чтобы провести атаку. Что же нужно ему для начала? Адрес веб-сервера или шлюза организации? Да, но скорее всего там будут сконцентрированы наибольшие средства защиты. Поэтому будут использоваться и другие пути для атаки.

Если известен список телефонов организации (или диапазон номеров), можно попробовать узнать, не подключен ли кто-нибудь из них к модему. Используя программное обеспечение, которое методично обзвонит эти телефонные номера, например за ночь, хакер получит номера модемов организации. К сожалению, именно модемам служба безопасности часто уделяет недостаточно внимания, оставляя их включенными во внерабочее время, в режиме автоответа и т. д.

Можно обойтись и без сканирования коммутируемых каналов, если известен конкретный адрес, на котором обнаружена уязвимость. Второй подход — прямой перебор диапазона IP-адресов, третий — выяснение соответствия конкретных адресов конкретным организациям с использованием поисковых систем, а также распространенных сетевых служб и утилит (whois, nslookup).

Необходимым шагом любой неспонтанной атаки является выяснение топологии атакуемой сети. В этом злоумышленнику помогают утилиты трассировки сетевых маршрутов, а также программы генерации фальшивых пакетов. Первые смогут выявить расположение маршрутизаторов в сетях, не защищенных МЭ, и даже в сетях за МЭ, если в их настройках разрешен протокол ICMP. Вторые могут проходить через межсетевые экраны и даже NAT-узлы при неправильной их конфигурации.

Очень популярным средством удаленного изучения сетей является протокол SNMP. Многие администраторы, ответственные за настройку сетевого взаимодействия в системе, довольно легкомысленно относятся к его активности. Результатом этого становится огромный объем информации, собранный потенциальным злоумышленником о сети удаленно, без каких-либо усилий.

Следующим шагом исследований скорее всего станет сканирование портов. Обычно оно применимо к сетям, работающим на основе TCP/IP. Как известно, сокет (IP-адрес и номер порта) определяет службу, которая запущена на данном компьютере, т. е. наличие ответа на попытку TCP-соединения по данному порту означает функционирование сервиса, запущенного на атакуемом узле. Таким образом можно собрать данные о службах, запущенных на этом узле, и, возможно, об операционной системе и ее версии. Для сканирования портов применяется специальное программное обеспечение.

Когда злоумышленник знает, что и как работает в атакуемой системе, начинается наиболее интеллектуальная часть его работы. Многие сервисы и операционные системы имеют известные уязвимости, и, если администратор или специалист по безопасности атакуемой сети не позаботился об их устранении, они будут использованы.

Например, большинство операционных систем имеют установленные производителем административные учетные записи с большими привилегиями, с известными паролями по умолчанию. Если никто не удалил их или не отключил (не изменил пароль), ими можно воспользоваться.

Кроме того, известные уязвимости могут иметь прикладные программы. Примеров много, начиная от уязвимости программы sendmail, использованной еще червем Морриса, до применения спецсимволов в строке URL для некоторых Интернет-браузеров.

Если хакеру стало известно имя пользователя (логин), он может попробовать предпринять атаку перебором пароля. При отсутствии мер защиты от таких атак соответствующее программное обеспечение без участия человека произведет подбор пароля. Известны западные статистические исследования, которые утверждают, что в группе из 500 пользователей найдется минимум один, использующий в качестве пароля слова «suzi», «qwerty» или комбинацию символов «123».

Когда атакующий получил доступ на данный компьютер хотя бы с минимальными правами, он будет пытаться расширить свои права до максимальных. В некоторых случаях в системах или программах существует функционал запоминания пароля. Если администратор, работавший в такой системе, использовал эту возможность (например, когда устранял проблемы в работе пользователя) и не позаботился о том, чтобы удалить сохраненные данные о пароле, он окажется доступен злоумышленнику. Кроме того, может быть скопирована и база паролей пользователей сети (если она не защищена). Хотя пароли и хранятся в зашифрованном виде, тем не менее в некоторых системах с помощью специального программного обеспечения, времени и вычислительных мощностей можно восстановить пароли в исходном виде.

Получив необходимый доступ, хакер может не только скопировать интересующие его данные, но и перестроить существующую сеть по своему желанию. Например, отключить системы безопасности, создать дополнительные учетные записи пользователей с полными правами доступа, разместить троянскую программу и др., вплоть до полного разрушения данных программ. В тех случаях, когда захваченная машина является всего лишь шагом на пути к другой цели, очень высока вероятность установки злоумышленником программы-сниффера (sniffer). Выполненный с ее помощью результат перехвата трафика локальной сети — один из самых интересных для атакующего каналов сведений об атакуемой системе. И самое главное: злоумышленник с высокой степенью вероятности позаботится об уничтожении своих следов, т. е. удалит в регистрационных журналах записи о вторжении.

После такой деятельности администраторы сети вынуждены заново переустанавливать операционные системы не только основных серверов, но и всех пользовательских компьютеров, так как различные «шпионские» программы могут быть скрыты где угодно.

Таким образом, для предотвращения хакерских атак специалистам по безопасности необходимо принимать некоторые меры в «родной» сети:

производить анализ присутствия сканирования сетевых портов;

удалять или блокировать учетные записи по умолчанию;

устранять уязвимости систем и программ установкой актуальных обновлений и патчей;

внедрить парольную политику с требованиями к сложности пароля и ограничить число ввода неверных паролей;

наделять пользователей минимальными правами доступа (не более, чем им нужно для работы);

с осторожностью относится к использованию учетной записи с полными правами (администратора домена), вплоть до частой смены пароля;

защищать базу паролей пользователей от ее копирования рядовыми пользователями;

вести учет программного обеспечения (системного и прикладного) и его конфигураций на компьютерах пользователей;

постоянно и регулярно делать резервные копии данных, систем, инсталляционных файлов программ;

обеспечить сохранение регистрационных журналов в режиме, исключающем возможность их корректировки.

5.3. Дополнительные возможности атак изнутри

Рассмотренная типовая атака на предприятие была инициирована извне. Между тем большинство взломов происходит при участии самих сотрудников предприятия. Типовая атака в этом случае, скорее всего, сведется к попыткам раскрытия пароля пользователя, имеющего соответствующий доступ к интересующей системе.

Технические средства в виде программ подбора паролей или снифферов могут быть использованы и в этом случае. Однако атаки изнутри характеризуются одним очень серьезным фактором, который отсутствует в варианте удаленной атаки, а именно возможностью воздействия на самого пользователя. Атака, при которой злоумышленник сам активно воздействует на пользователя с целью узнать его пароль, использует методы социальной инженерии. В нашем случае интересен и, к сожалению, весьма распространен вариант, когда пользователь сам предлагает свой пароль, прямо или косвенно.

Косвенно — это когда пользователь скрывает свой пароль, но делает это довольно неумело, например записывает в блокнот (и оставляет его на столе), кладет листок с записанным паролем в ящик стола или под клавиатуру компьютера (подставку монитора) или консультируется с коллегами при выборе пароля («Можно я использую дату рождения?»).

Прямо — это когда пользователь сообщает свой пароль другому сотруднику по различным причинам. Например, в ситуации, когда сотрудник должен досрочно покинуть рабочее место и хочет, чтобы какую-либо операцию в системе сделали от его имени. Или он заболел, а его руководитель, звоня по телефону, требует пароль, чтобы срочно извлечь информацию, доступную только данному пользователю.

Поскольку в основе защиты на доступе по паролю лежит принцип самостоятельного сохранения пароля в секрете самим пользователем, то бороться с проявлением таких атак можно только обучением пользователей и постоянным разъяснением им важности сохранения пароля в тайне. В тех же случаях, когда удается установить факт передачи пароля одного пользователя другому, необходимо предпринимать административные меры с доведением информации об инциденте до остальных пользователей сети.

В реальной жизни, вероятнее всего, атаки (быть может, только за исключением атак на отказ в обслуживании) будут совмещать в себе оба описанных сценария: что-то удастся выяснить локально, что-то сделать удаленно.

Вопросы для самоконтроля

1. Что такое локальная, удаленная атака и атака на поток данных?
2. Опишите последовательность действий при типовой удаленной атаке.
3. Как атакующий скрывает свою личность при атаке?
4. Опишите основные методы противодействия удаленным атакам.

6. АТАКИ НА ПОТОК ДАННЫХ

Как было указано ранее, атака на поток данных — это ситуация, когда злоумышленник не применяет агрессивных воздействий на атакуемый хост или хосты, а, находясь вовне (например, в сети между двумя серверами, ведущими информационный обмен), пытается работать с данными, направляемыми от одного хоста к другому.

По своему характеру такие атаки могут быть пассивными, когда злоумышленник копирует себе данные для последующего анализа, и активными, когда злоумышленник вносит изменения в данные или полностью подменяет их. Случай, когда злоумышленник блокирует данные, не будет рассматриваться, так как в данной теме это означает просто разрыв связующего кабеля либо заполнение его зловредным трафиком. Такие атаки не интересны в силу своей примитивности (хотя при этом они не перестают быть действенными).

6.1. Пассивные атаки: прослушивание сетей

Другое название пассивных атак — **прослушивание сети** или **сниффинг** (sniffing). Различают два вида прослушивания — межсегментное (когда хосты, обменивающиеся данными, находятся в различных сегментах сети) и внутрисегментное (когда информационный поток идет между двумя хостами внутри одного сегмента).

В первом случае злоумышленник должен разместить устройство прослушивания в таком месте, где он сможет гарантированно иметь возможность копирования, — у выхода из первого сегмента (у шлюза), у входа во второй сегмент либо у одного из передающих промежуточных устройств (при условии, что сетевой трафик не имеет альтернативных каналов доставки). Поскольку в этом случае трафик не может миновать злоумышленника, его задача облегчается: он может анализировать на выбор любой из уровней сетевой модели (обычно от сетевого и выше).

Немного остановимся на рассуждениях о том, какой уровень сетевой модели наиболее интересен для злоумышленника. Больше всего значимой информации расположено на верхнем, прикладном уровне. Если злоумышленник, скажем, имеет возможность перехватывать пакеты незащищенных

Telnet-сессий, то, скорее всего, рано или поздно он получит аутентификационные данные (идентификатор и пароль) пользователя, работающего с Telnet-сервером. Анализ транспортных пакетов предоставит возможность узнать, какие службы функционируют на взаимодействующих хостах. Рассмотрение сетевого уровня может дать картину адресного пространства сегментов.

Поскольку основным средством защиты от прослушивания является шифрование, необходимо определиться, на каком уровне производить применение криптографических механизмов. Если исходящие из сегментного шлюза пакеты направлены только веб-серверу (возможно, еще DNS и почтовому серверу), а сам шлюз выполняет функцию сокрытия адресов, то применять шифрацию можно только на прикладном уровне. Если взаимодействие идет между управляющим и управляемым хостами (например, по протоколу SNMP), то защиту необходимо применять на сетевом уровне.

Во втором случае злоумышленнику не обязательно находиться на одном кабеле с хостом, он может использовать свойства работы протоколов канального уровня (например, Ethernet). В сетях подобной топологии сразу несколько (обычно около 10...20) сетевых карт подключено к одному и тому же носителю информации — сетевому кабелю. Каждый пакет, переданный в сети, поступает таким образом на вход каждой сетевой карты. Только после сравнения физического адреса карты получателя (так называемый MAC-адрес, от англ. media access controller — «контроллер доступа к среде передачи»), указанного в заголовке пакета, с собственным MAC-адресом сетевая карта принимает решение о том, ей ли предназначался этот пакет. Один из служебных регистров драйвера сетевой карты определяет, должна ли она передавать на более высокий уровень только пакеты, предназначенные ей (штатный режим), либо же все пакеты, прошедшие по сети (англ. promiscuous mode — дословно «неразборчивый режим»). Программы-снифферы переводят сетевую карту во второй режим и в результате получают все пакеты, проходящие по подключенному сетевому кабелю.

Казалось бы, в этом случае невозможно определить, установлен ли сниффер в данном сегменте сети или нет, т. е. ведется ли пассивная атака на хосты сегмента. Однако специалистами по безопасности было найдено довольно красивое решение — сниффер-детектор (sniffer-detector), о котором следует сказать как о примере направления развития мыслей специалистов по безопасности для обеспечения необходимой защиты сетевых ресурсов. Для того чтобы прийти к такому решению, необходимо соответствующее знание принципов работы сети и программы-сниффера, а также техническая сообразительность.

Как уже упоминалось, компьютер со сниффером отличается от других тем, что принимает к обработке все канальные кадры вне зависимости от указанного MAC-адреса. Идея заключается в том, чтобы сформировать набор кадров с некорректным MAC-адресом, который должен быть проигнорирован обычным сетевым узлом. Внутри кадры должны содержать сетевые

пакеты, на которые обязаны будут отреагировать служебные сервисы сетевого уровня (например, это может быть ping-пакет протокола ICMP). Таким образом, получение от какого-либо хоста ответа на подобный сетевой пакет означает, что он (кадры, его составляющие) был принят к обработке данным узлом и передан на сетевой уровень, который и ответил на служебный запрос. Следовательно, сетевая карта переведена в режим promiscuous mode и на данном хосте установлена программа-сниффер.

Другой, не столь красивый вариант решения, заключается в том, что сегмент должен быть заполнен большим количеством некорректных сетевых кадров, которые будут проигнорированы всеми узлами, кроме прослушивающего. Тогда наличие сниффера можно обнаружить по существенному замедлению работы данного хоста (например, в замедлении реакции на ту же команду ping).

Вследствие очень широкого распространения топологии сетей Ethernet, построенных на коммутаторах, необходимо немного рассказать и о прослушивании трафика в таких ситуациях. Технология построения сетей множественного доступа на активном оборудовании — концентраторах (hub) и коммутаторах (switch) — позволяет подключать каждую сетевую карту не к единому сетевому кабелю, а к этому оборудованию своим собственным кабелем. Оба типа устройств «прозрачны» на канальном уровне, т. е. прохождение через них кадра канального уровня никак не сказывается на его содержимом и не может быть обнаружено программами-снифферами.

Повторители выполняют единственную функцию копирования кадра, пришедшего по одному из подключенных к нему кабелей, во все остальные сетевые кабели. Коммутаторы выполняют роль «интеллектуального» перенаправления этого кадра. На каждом сетевом порту поддерживается список MAC-адресов, от которых в последнее время приходили пакеты с этого сетевого кабеля. Чаще всего на другой стороне кабеля находится единственный компьютер, в этом случае список для данного порта будет состоять из одного MAC-адреса. Но если к коммутатору подключается другой коммутатор или повторитель, количество адресов в списке возрастает.

Перенаправление кадра, пришедшего на коммутатор, производится по следующему алгоритму: если MAC-адрес получателя обнаружен в списке для какого-нибудь из портов коммутатора, пакет отправляется только по этому направлению, если же адрес не найден, то пакет копируется во все подключенные сетевые кабели, как в повторителе. Коммутаторы в несколько раз снижают нагрузку на сетевой носитель и, как следствие, очень ощутимо увеличивают быстродействие локальной сети в целом. Также они надежно защищают от прослушивания трафика: пакет не попадает на сетевые карты других абонентов, она идет только из кабеля отправителя в кабель получателя.

Но уязвимость все же была обнаружена. Оказалось, что у многих известных производителей сетевого оборудования логика работы коммутаторов такова, что, если на каком-либо из портов происходит переполнение списка

MAC-адресов, коммутатор начинает временно работать в режиме повторителя относительно всех своих портов, дабы не привести к полному разрыву сети относительно этих не поместившихся в список MAC-адресов, т. е. для превращения такого коммутатора в повторитель программе-генератору пакетов достаточно через определенный интервал времени устраивать в сети «шторм» из произвольных сетевых пакетов с различными произвольными MAC-адресами. Далее она будет получать все пакеты, идущие по сети через атакованный коммутатор.

Мерами защиты от подобной атаки являются:

постоянный мониторинг сети на предмет MAC-штормов;

анализ регистрационного журнала коммутатора, если таковой ведется данным устройством;

активация на всех портах, к которым подключены одиночные хосты, режима ограничения количества MAC-адресов или даже установка фиксированного разрешенного MAC-адреса, если какой-либо из этих режимов поддерживается коммутатором.

Еще одна возможность прослушивания коммутируемого Ethernet-трафика основана на специфике и ошибках протокола STP (spanning tree protocol). STP используется коммутаторами для обнаружения и блокирования петель в сегментах, состоящих из нескольких коммутаторов. В адрес подавляющего большинства современных реализаций этого протокола есть возможность отправить сфальсифицированный служебный STP-пакет, после которого коммутатор на несколько секунд перейдет в режим повторителя относительно всех своих портов.

До сих пор речь шла о прослушивании незащищенного, нешифрованного трафика. Однако, если пакеты криптографически защищены даже на сетевом уровне, то это не означает, что прослушивание такого информационного потока абсолютно бесполезно. Во-первых, шифрованный пакет — предмет для криптоанализа. Во-вторых, на основе знаний об объемах трафика и периодичности сетевой активности можно сделать определенные выводы о работе сети. В-третьих, это возможность проводить статистический и корреляционный анализ шифрованного трафика с нешифрованным (например, пакетами службы сервера имен), который также может позволить злоумышленнику завладеть полезной информацией.

6.2. Активные атаки

Проще всего активные атаки проводятся, если хост злоумышленника является узлом какого-либо уровня (коммутатором, маршрутизатором, прокси-сервером, почтовым сервером) на пути движения информации. Другими словами, устройство, управление над которым получил злоумышленник, должно иметь возможность фильтровать интересующий его трафик и направлять его на другой алгоритм обработки или даже по другому сетевому маршруту.

Если злоумышленник имеет сконфигурированный подобным образом хост-шлюз, он имеет и широкие возможности для работы с сетевым трафиком. Когда передаваемый трафик не имеет криптографической защиты ни на одном сетевом уровне, злоумышленник может полностью им манипулировать. Если же криптографическая защита применена, то тем не менее остаются некоторые возможности для ряда интересных атак. Оставим в стороне возможности криптоанализа, так как, если шифр успешно взломан, трафик становится для злоумышленника открытым, по крайней мере на время действия данного криптографического ключа.

Атака повтором. Атака повтором (replay attack) возможна только в том случае, когда в системе защиты пакетов отсутствуют или не включены механизмы обнаружения повторного приема одного и того же пакета. Сама атака заключается в том, что перехваченный и сохраненный злоумышленником пакет посылается повторно (возможно, несколько раз) в надежде на то, что он будет повторно принят к обработке системой получателя. В наиболее фантастическом варианте на банковский счет злоумышленника будет несколько раз зачислена одна и та же сумма. В менее фантастическом варианте, если система, например, в ответ на полученный пакет должна произвести серьезные вычислительные действия, повторное направление нескольких пакетов может привести к перегрузке и отказу в обслуживании. Механизмом защиты от таких атак является проверка в каждом пакете отметки времени его отправки (timestamp) или последовательного номера пакета. В качестве графического разъяснения атаки повтором приведем **рис. 8**.

Пример несколько утрирован, хотя бы потому что в системах межбанковских платежей существуют различные, в том числе не криптографические, способы защиты от подобных махинаций, например регулярный обмен между банками информацией по подтверждению переводов. Но для демонстрации атаки повтором такой схемы вполне достаточно.

1. Злоумышленник открывает счет в Банке 2, а из Банка 1 переводит на этот счет некоторую сумму $. Банк 1 готовит электронный документ — поручение Банку 2 о зачислении на счет С1 указанной суммы, применяет к документу методы криптозащиты и отсылает в Банк 2.

2. Далее злоумышленник перехватывает (копирует) шифрованное сообщение о переводе.

3. Банк 2, получив документ и проверив его корректность с точки зрения криптозащиты, исполняет поручение.

4. Злоумышленник, пусть даже не имея возможности обойти средства криптозащиты, просто повторно направляет перехваченный документ (возможно, через несколько дней) в адрес Банка 2.

5. Поскольку в документ не было внесено изменений, Банк 2 воспринимает его как корректный и повторно выполняет поручение на зачисление средств.

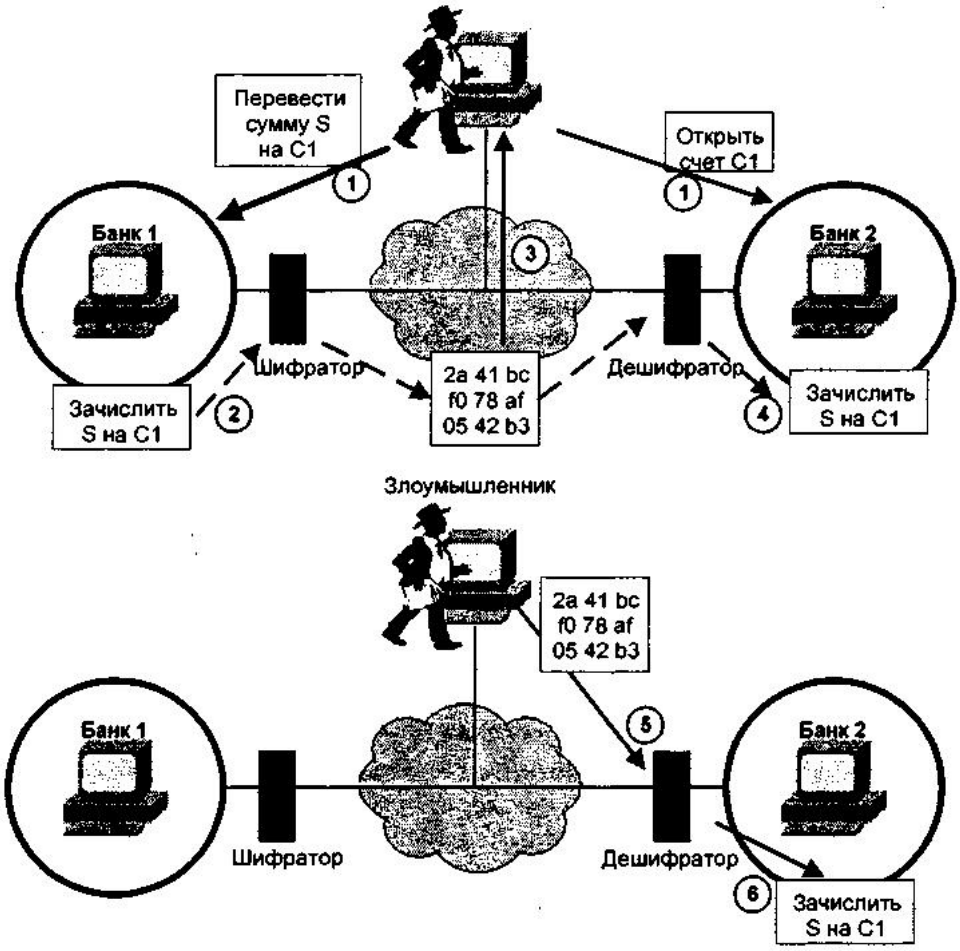

Рис. 8

Атака «злоумышленник-посредник». Данный вид атак (man-in-the-middle) породил целое новое направление в электронном бизнесе, а именно создание центров сертификации (CA — certification authority). Для понимания сущности атаки необходимо представление о функционировании криптографической системы с открытыми ключами.

Для успешного защищенного взаимодействия пары пользователей А и Б каждый из них должен сгенерировать пару криптографических ключей — открытый и закрытый, одним из которых можно только шифровать, другим — только дешифровать. Открытый ключ, в отличие от закрытого, не требует сохранения в конфиденциальности и отсылается удаленному адресату, т. е. А посылает свой открытый ключ (ОА) Б, а Б посылает свой открытый ключ (ОБ) А. Теперь, если А хочет отправить Б зашифрованное сообщение, он шифрует его открытым ключом ОБ. Зашифровать такое сообщение может кто угодно, поскольку открытый ключ известен всем желающим. Но дешифровать сообщение сможет только обладатель закрытого ключа (ЗБ), т. е. сам Б. Идентификацию отправителя, зашифровавшего сообщение, можно производить по второй паре ключей, т. е. А может вставить в сообщение для Б некий элемент, зашифрованный закрытым ключом А (ЗА). Так как у Б есть открытый ключ А, он сможет дешифровать этот элемент

и проверить, что он был действительно зашифрован обладателем секретного ключа А, т. е. самим А (на этом принципе основывается механизм ЭЦП).

Данный защищенный механизм работает на основе убеждения, что открытый и закрытый ключи (ОА и ЗА) принадлежит именно А, а открытый и закрытый ключи (ОБ и ЗБ) принадлежит именно Б. Однако иногда абоненты защищенной связи могут быть введены в заблуждение. Уже было отмечено, что открытые ключи не требуют сохранения их в конфиденциальности, и это действительно так. Однако отправление открытых ключей адресатам без доверенного контроля пути следования как раз и приводит к возможности реализации описываемой атаки.

Предположим, что между А и Б имеется шлюз, управляемый злоумышленником, — З. Тогда при подготовке к общению в защищенном режиме (или при очередной смене ключей), когда А направляет Б свой открытый ключ, З перехватывает его и сохраняет у себя. Далее вместо этого ключа он отправляет Б открытый ключ из пары, сгенерированной им самим, т. е. открытый ключ ОА`. Когда Б направляет А свой открытый ключ, З также перехватывает его и сохраняет у себя. Вместо этого он отправляет А открытый ключ из другой пары, сгенерированной им самим, т. е. открытый ключ ОБ`. В общем случае пары и ключи ОА` и ОБ` могут совпадать, это не принципиально. Важно то, что теперь злоумышленник выступает прозрачным посредником в защищенном обмене информацией между А и Б, которые общаются друг с другом, не подозревая, что на самом деле их обмен данными контролируется (**рис. 9**).

Для предотвращения атак подобного класса необходимо обеспечение доверенной доставки открытых ключей абонентам. Если А и Б находятся в личном контакте или имеют альтернативный доверенный канал обмена информацией, то задача решается достаточно просто. Но если они находятся в разных концах света и общаются только с помощью Интернета, задача доверенной доставки становится нетривиальной.

Организации, занимающиеся сертификацией открытых ключей, — СА — обеспечивают установку своей цифровой подписи на набор параметров пользователя сети, включающих его идентификационные данные и открытый ключ — так называемый цифровой сертификат. После этого сертификат с открытым ключом может быть свободно распространен без опасности подмены. Вопрос об удостоверении полномочий данного абонента в получении сертификата решается, например, таким образом: пользователь устанавливает защищенную сессию связи с веб-сервером СА, на сервере генерируется пара ключей, причем на сервере сохраняется только копия открытого ключа, а секретный ключ сохраняется только клиентом. После этого СА дополнительно альтернативными методами (факсом, обычной почтой и т. д.) получает подтверждение пользователя, сгенерировавшего ключи, формирует для него сертификат, отсылает пользователю и сохраняет копию сертификата у себя для дальнейшего использования. Иногда СА сохраняет у себя и секретный ключ пользователя на случай его утери, но это уже предмет договорных отношений между самим пользователем и СА.

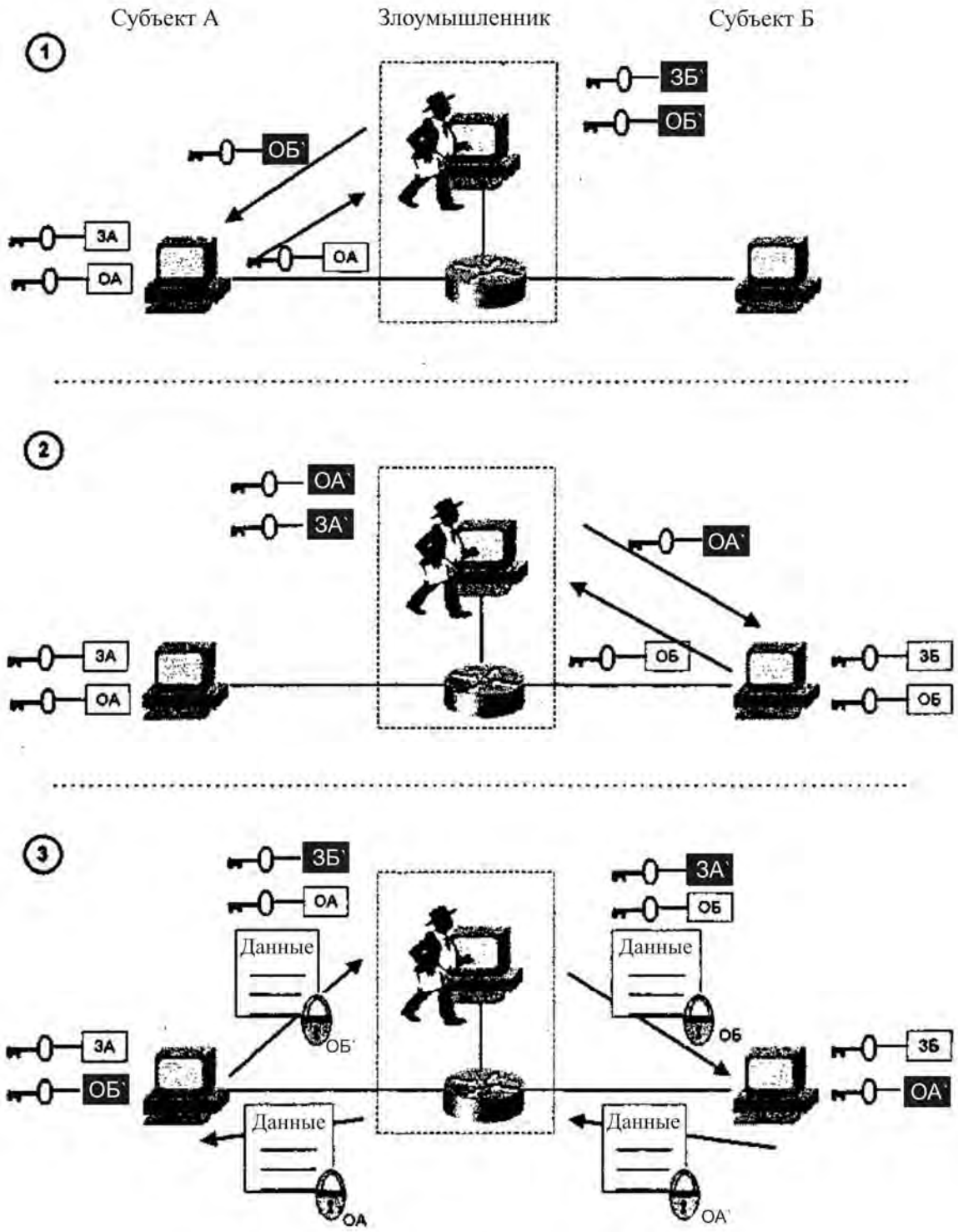

Рис. 9

Атаки на основе сетевой маршрутизации. Возможность смены штатного маршрута движения информации может оказаться чрезвычайно необходимой злоумышленнику как при пассивных, так и при активных атаках. Достижимо это в сетях с динамической маршрутизацией пакетов (т. е. направление дальнейшего следования для каждого очередного пришедшего пакета маршрутизатор выбирает исходя не из своих настроек, а из сетевой обстановки). В тех случаях, когда злоумышленник может формировать

фальшивые служебные пакеты протоколов динамической маршрутизации и эти пакеты затем принимаются маршрутизаторами как корректные, у него появляется возможность манипулировать сетевым трафиком в самой произвольной форме (рис. 10).

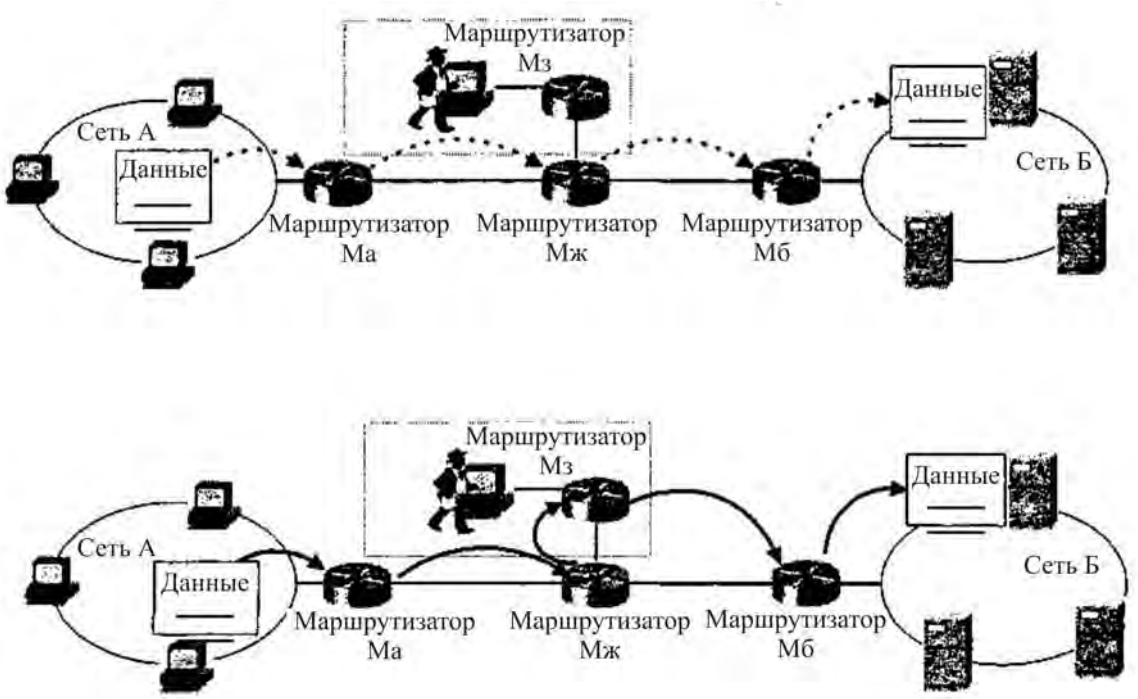

Рис. 10

В некоторых протоколах динамической маршрутизации для перестраивания логики отправки пакетов достаточно отправить всего один служебный пакет с определенным образом сформированной фальшивой информацией о сетевой обстановке. В других протоколах для перенаправления трафика в сторону другого узла необходим постоянный поток фальшивых сетевых пакетов. При этом совсем необязательно, чтобы через хост злоумышленника проходил альтернативный путь следования трафика: он может находиться и в сетевом тупике — специальное (хотя и довольно сложное) программное обеспечение превратит его машину в транзитный узел.

Последовательность атаки на маршрутизатор:

1. Нормальное прохождение маршрута от сети А через маршрутизатор Ма, находящийся под управлением администратора сети А, далее через маршрутизатор Мж — жертву атаки — на маршрутизатор Мб, находящийся под управлением администратора сети Б, и в сеть Б. При этом злоумышленник — администрирующий маршрутизатор Мз — пока не вмешивается.

2. Результат после успешной атаки на маршрутизатор-жертву Мж. Поток данных перенаправляется на маршрутизатор злоумышленника Мз.

Данный класс атак невозможен:

в сетях со статической маршрутизацией;

в протоколах динамической маршрутизации, авторизующих свои служебные пакеты с помощью криптографических механизмов;

извне в сетях, где маршрутизатор сам выполняет функции межсетевого экрана и при этом правильно настроен (служебный трафик протоколов динамической маршрутизации не должен поступать в систему, если он ей не нужен);

изнутри в сетях с правильно настроенными межсегментными сетевыми экранами (в этом случае при атаке подобного рода информационный поток просто прервется, но не будет доставлен злоумышленнику и, следовательно, сохранит конфиденциальность и целостность информации).

Кроме того, необходимо отметить, что атака на смену сетевых маршрутов трудно реализуема в сетях со стыками различных протоколов динамической маршрутизации.

Перехват сессии. После того как злоумышленник научился обходить аутентификацию, основанную на сетевом адресе (путем подмены этого адреса в пакетах), вопрос обеспечения доверия к сеансу работы хоста с хостом перешел на более высокий уровень. Хост-сервер, например, может производить предварительную идентификацию и аутентификацию хоста-клиента, устанавливающего сеанс работы, и далее учитывать установленную сессию как доверенную.

В стандартном наборе протоколов TCP/IP функцию сессионного протокола выполняет TCP, обеспечивая контроль (идентификацию) сессии путем последовательной нумерации каждого нового пакета уникальными номерами (sequence number и acknowledge number), увеличивающимися на длину переданной информации от пакета к пакету, при этом начальное значение каждого из этих двух номеров генерируется случайно на этапе установления соединения. Если сервер не предпринимает дополнительные меры по идентификации пакетов, то злоумышленнику достаточно знания о текущих номерах сессии, чтобы сформировать свой пакет, в котором адрес отправителя будет адресом клиента, а оба номера пакета будут соответствовать тем, которые он узнал. Доверенному клиенту будет послан пакет разрыва сессии, и таким образом злоумышленник сможет продолжать работу в сессии от имени доверенного хоста (перехватить сессию).

Если злоумышленник имеет возможность установить свой хост или свое программное обеспечение на компьютере, расположенном в том же сегменте, что и клиент или сервер, либо на канале передачи данных между ними, то, используя средства пассивного прослушивания сети (сниффер), он может получить информацию о номерах из перехваченных пакетов. Если же такой возможности у него нет, то он может попытаться предугадать эти номера. Дело в том, что ряд реализаций сервисов TCP в операционных системах имеет такие алгоритмы генерации начального случайного числа, что оно может быть предсказано на основе предварительных знаний об уже сформированных пакетах других сессий (которые обычно инициируются самим злоумышленником с этой единственной целью).

Данный пример обычно приводится в литературе по отношению к ситуации, когда злоумышленник не имеет возможность непосредственно

перехватывать поток сообщений между хостами А и Б. В этом случае он инициирует соединение от имени хоста А, выполняет атаку «отказ в обслуживании» на хост А (чтобы тот не смог оповестить хост Б, что на адрес А пришли пакеты о начале сессии) и, предугадывая порядковые номера пакетов, продолжает соединение (точнее, односторонний поток, так как ответные пакеты от Б не вернутся к злоумышленнику) с хостом Б. В нашем случае схема упрощена (злоумышленник может перехватывать пакеты сессии А—Б), но интересна тем, что атака может начаться после того, как пользователь хоста А был аутентифицирован и авторизован на хосте Б, т. е. получил некие расширенные права (рис. 11).

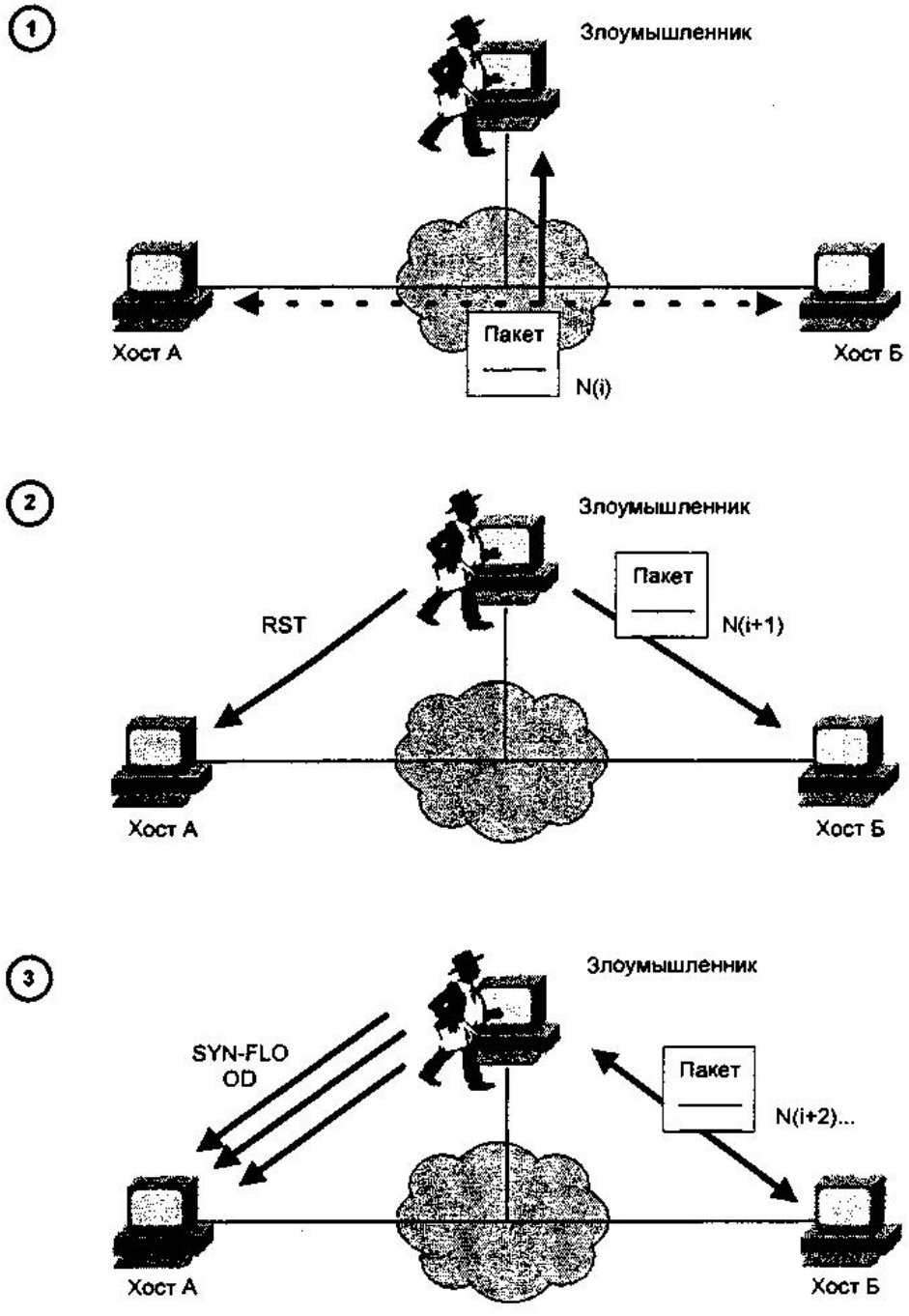

Рис. 11

1. Злоумышленник «слушает» трафик А—Б, ожидая авторизации пользователя А на хосте Б.

2. Злоумышленник посылает на хост Б следующий по очереди пакет как продолжение нормальной сессии А—Б. На хост А он посылает сигнал о разрыве соединения, хотя это больше формальность, поскольку хост А далее выводится из работы любой из доступных атак класса deny of service («отказ в обслуживании»), например атакой SYN-FLOOD.

3. Продолжая сессию от имени А, злоумышленник обычно поддерживает хост А в состоянии отказа от обслуживания.

Учитывая то, что даже некоторые межсетевые экраны (из тех, которые вполне могут находиться на службе), уделяя внимание аутентификации клиента при установлении соединения, не контролируют далее аутентичность пакетов, описанная атака — перехват авторизованной сессии — вполне может быть использована.

Злонамеренные действия могут быть применены на любом участке информационного потока, и ко всем им следует быть готовым.

Вопросы для самоконтроля

1. Что такое атака на поток данных? Какие способы противодействия ей вы знаете?
2. Дайте определение пассивной атаки на поток данных. Что такое сниффинг? Какие условия для него необходимы?
3. Как осуществляется атака на коммутатор (свитч)? Зачем она нужна?
4. Дайте определение активной атаки на поток данных. Каковы условия ее осуществления?
5. Опишите атаку повтором.
6. Опишите атаку на ключи «злоумышленник-посредник». Какие способы противодействия ей существуют?
7. Опишите атаку на маршрутизацию и перехват сессии.

7. ВОССТАНОВЛЕНИЕ ПОСЛЕ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Подготовка к созданию аварийного плана

Авария — это нештатная ситуация, которая требует действий, отличных от рутинных, определенных регулярными процедурами, т. е. ввод в действие того или иного элемента плана.

При этом необходимо выбрать такую классификацию событий, которая бы наиболее эффективно работала при реализации плана. Возможно, не стоит разделять в классификации пожар, наводнение и землетрясение, если все эти катастрофы потребуют с точки зрения плана одинаковых действий. В таком случае следует принять иную классификацию. Например, разделить их на события природные и зависящие от человеческого фактора (такая классификация различает способы предварительной подготовки), на требующие эвакуацию персонала и не требующие (здесь существенно разнятся действия, происходящие во время самого события), и т. д.

Большинство природных катастроф можно классифицировать как временную или постоянную недоступность некоторого информационного обеспечения (оборудования, программ, данных), а внутри этого класса подклассифицировать на недоступность в рамках участка или части одного подразделения или здания (кража или разрушение оборудования), затрагивающую все здание (пожар), затрагивающую все учреждения предприятия в данной местности (землетрясение, война). Можно производить классификацию и с точки зрения угроз информационной безопасности, однако при этом следует учесть, что на первое место всегда выходит угроза жизни и здоровью людей, а лишь затем — угрозы всему остальному (возможно, для ряда организаций на втором месте будут не информационные угрозы, а угрозы материальным ресурсам — зданиям, ценностям и т. д.).

Следующим шагом будет определение приоритетов восстановления систем и объектов. В этом случае для упрощения процесса следует идти от верхнего уровня.

Когда речь идет об информационных системах, необходимо учитывать, что после катастрофы, при переходе к восстановлению бизнеса, не все системы потребуются незамедлительно, поэтому следует классифицировать информационные системы с точки зрения аварийного плана.

Так, системы могут быть:

критически важными (без них невозможно продолжение бизнеса), с подразделением на постоянно и периодически требующиеся;

для вторичных и вспомогательных бизнес-задач;

для рутинной работы, в которых потребность возникнет, но не в первые часы/дни после катастрофы;

необходимыми для перспектив развития предприятия.

7.2. Структура аварийного плана

Структурированный аварийный план должен состоять из нескольких частей, возможно, это будут отдельные документы, тем не менее приведенные элементы должны присутствовать в нем обязательно.

Определения аварийных ситуаций и расстановка приоритетов по объектам и системам. Работа по определению и расстановке приоритетов должна быть проделана до начала составления плана. Результаты этой работы необходимо формально закрепить в утвержденном руководством предприятия плане, с тем чтобы при наступлении аварийной ситуации не возникали дополнительные споры о том, какие мероприятия проводить и какие системы в какой очередности восстанавливать.

Предварительные меры. Предварительные меры содержат описание мероприятий и процедур, которые должны быть произведены или регулярно проводиться для того, чтобы при возникновении аварийного события устранить или существенно снизить размер ущерба для предприятия. Поскольку речь идет об информационной безопасности, далее будут проанализированы в основном мероприятия, связанные именно с информационными объектами и системами. Также будем предполагать, что аварийный план составляется для аварийных событий, максимальным из которых будет полное уничтожение информационного пространства предприятия.

Основой восстановления должно быть создание нового места работы — существования восстановленного информационного пространства. Эту задачу можно не рассматривать только в том случае, если уничтожение текущего места размещения означает прекращение деятельности предприятия. В остальных случаях организации необходимо здание с имеющейся информационной и вспомогательной (электропитание, водоснабжение, телефонная связь и т. д.) инфраструктурой. Возможные варианты для этого случая зависят от финансовых возможностей компании.

Содержание отдельного запасного здания, принадлежащего предприятию. Возможны различные конфигурации готовности резерва:

«горячий» — место полностью копирует рабочую обстановку (возможно, в несколько усеченном виде), пользователям осталось только разместиться на своих новых местах и включить рабочие станции (серверы уже могут работать);

степени «постепенного охлаждения» — например, локальная сеть присутствует только в виде кабелей и пассивного оборудования, требуется

установка дополнительного (активного) оборудования, электропитание подведено, но не подключено и т. д.;

«холодный» — готово только само здание и инфраструктура электропитания и санитарно-технического оборудования.

Содержание выделенного здания совместно с другой организацией (организациями) с условием одновременного или поочередного использования при катастрофе.

Содержание выделенного здания с возможным частичным его использованием в обычной жизни, например как склад или место расположения зеркального рабочего сервера и т. д.

Переезд в случае катастрофы в здание одного из подведомственных учреждений (отделение, филиал) или к организации-партнеру.

При наличии альтернативного запасного здания необходимо обеспечить его охрану и регулярно проверять его готовность к принятию рабочей нагрузки.

Если предположить, что у организации нет «горячего» резерва компьютерного оборудования, стоящего «наготове» в ожидании аварии, значит, надо обеспечить запас такого оборудования на складе предприятия (желательно сделать запас распределенным по различным складам, с тем чтобы запасное оборудование не погибло вместе с основным в случае масштабной катастрофы) либо обеспечить получение оборудования в кратчайшее время после катастрофы. Второй вариант предполагает предварительные договоренности с поставщиками или организацией-партнером, которые предоставят некий лимит оборудования во временное пользование. Это предполагает, что к аварийному плану прилагается предварительно согласованный договор на поставку оборудования. То же самое должно относиться и к другим объектам, в которых организация зависима от внешних поставщиков (электропитание, линии связи и т. д.).

Следующим важным элементом является сохранение инсталляционных комплектов (дистрибутивов) информационных систем — системного и прикладного программного обеспечения. Необходимо учитывать, что восстанавливать, т. е. заново инсталлировать, придется, возможно, в спешке и совсем не тем специалистам, которые проводили установку систем на обычном месте работы. Это не означает, что в аварийный план необходимо переписать руководства по инсталляции всех систем, однако, если при установке существуют специфические детали, требующие особого внимания, о них нужно обязательно упомянуть. Особое внимание следует уделить специфическим настройкам: какие дополнительные сервисы должны быть включены и как настроены, порядок взаимодействия между ними и т. д.

Восстанавливая информационное пространство, нельзя забывать и об обеспечении его защиты, поэтому следует внести в аварийный план пункт о восстановлении систем безопасности с заранее заданным приоритетом. Если данная информационная система позволяет сохранять свои настройки в отдельных конфигурационных файлах, значит, следует сохранять копии актуальных из них наряду с резервными копиями данных.

В зависимости от специфики работы предприятия данные могут иметь существенную или даже основную значимость для организации. Иначе говоря, эти данные и могут представлять из себя организацию, а их отсутствие означает закрытие предприятия как такового. Следовательно, вопросам сохранности данных следует уделять особое внимание.

Данные должны быть проклассифицированы с точки зрения аварийного плана (в этом поможет классификация информационных активов по разделу «доступность») на категории. В литературе, посвященной этому вопросу, можно встретить термин «управление структурированным хранением» (hierarchical store management — HSM), которое подразумевает следующее разделение данных:

первичные (оперативные) — те данные, которые должны быть постоянно доступны;

вторичные (полуоперативные) — те данные, которые могут стать доступными автоматически, при возникновении необходимости;

третичные (автономные) — те данные, которые станут доступными после выполнения ряда ручных операций.

Учитывая эту классификацию, становится понятным, почему резервное копирование данных, оставаясь важной составляющей, тем не менее не является единственным средством. Например, для организации, предоставляющей онлайн-услуги, крах сервера с данными, требующими восстановление с резервных копий в течение нескольких часов, может означать очень серьезные потери, превышающие расходы на приобретение дублирующего (зеркального) сервера.

Вопросам обеспечения бесперебойной работы дисков и дисковых массивов можно также посвятить отдельное издание. Рекомендуем обратиться к документам, в которых обсуждаются на соответствующем техническом уровне технологии RAID (redundant arrays of independent disks) — зеркалирования, дуплексирования и т. д. Кроме того, отметим, что среди современных технологий есть возможности использования территориально разнесенных дублирующих узлов (географически разнесенный кластер), а также возможность аренды дискового, процессорного и других ресурсов у стороннего провайдера.

На предварительном этапе также необходимо определить уполномоченных лиц — комитет, рабочую группу или иное объединение, которые будут осуществлять управление действиями сотрудников во время наступления аварии и при восстановлении. Возможно, оперативной и восстановительной деятельностью будут заниматься различные лица.

Рассматривая возможность удаленного внешнего сохранения резервных копий, следует учесть, что они также должны быть предметом для применения мер безопасности. Одна из существующих распространенных ошибок — отсутствие защиты резервных копий, а между тем в них может присутствовать сверхкритическая информация, такая как база паролей пользователей и администраторов. Нормальным способом сохранения данных на внешних

носителях вне защищенного и контролируемого размещения в центре является применение сильных криптографических механизмов защиты данных.

Заканчивая разговор о предварительных мероприятиях, необходимо сказать, что обсуждаемые процедуры и механизмы безопасности также относятся к предварительным мероприятиям аварийного плана, просто они носят характер защиты не от катастроф глобального или природного характера, а от катастроф, спровоцированных злоумышленниками, ошибками персонала и т. д.

7.3. Мероприятия во время катастрофы

Рассмотрим активность, которая наступает во время аварийного события и сразу же после аварии до того момента, когда предприятие начинает продолжение производственного процесса.

Несмотря на то что при описании аварийного плана мы ориентируемся на аспект информационных систем, в первую очередь необходимо обеспечить отсутствие угрозы жизни и здоровью людей либо, если ущерб людям уже нанесен, постараться максимально сократить негативные последствия и обеспечить пострадавших соответствующей помощью (медицинской, транспортной и т. д.). Этот пункт также подразумевает необходимые меры для оперативного информирования работников организации, клиентов и других лиц, находящихся в сфере действия мероприятий, о наступающем или наступившем аварийном событии, мерах по эвакуации людей в безопасное место, обеспечению порядка и предотвращению паники и др.

Если нет угрозы жизни людей, необходимо сразу же позаботиться о сохранности информационных ресурсов. Для начала следует проанализировать, какие действия потребуются в определенных случаях для тех или иных систем. Возможно, если требуется эвакуация персонала при отсутствии непосредственной немедленной угрозы жизни и здоровью, целесообразно произвести корректное выключение рабочих станций. Может быть, потребуется перевод серверов в сокращенный режим работы (при наступлении аварии типа «распределенная атака на отказ в обслуживании» — DDoS — одним из стандартных требований является отключение на маршрутизаторах и межсетевых экранах поддержки обработки трафика второстепенных сервисов).

Таким образом, необходимо:

на этапе подготовки определить и формализовать действия, требуемые для выполнения в момент аварии;

при наступлении аварийного события идентифицировать, к какому виду событий оно относится с точки зрения необходимых мероприятий;

проинформировать работников, которые будут задействованы в мероприятии, о наступлении данного вида события;

обеспечить информированность работников о необходимых действиях и проверить готовность к их выполнению.

Последний пункт следует рассмотреть подробнее. Его особенность заключается в необходимости учитывать то, что описываемые мероприятия будут производиться в момент аварии или катастрофы, в условиях нервозности, стресса или даже шока, когда действия, кажущиеся простыми и понятными в обычных условиях, могут оказаться затруднительными к выполнению.

Для обеспечения эффективной работы сотрудник должен иметь под рукой подробную инструкцию:

- о том, кому из ответственных сотрудников предприятия позвонить для сообщения о возникновении аварийного события, для вызова на место происшествия и консультаций, со всеми возможными номерами телефонов (рабочий, домашний, мобильный) и других средств связи;
- что конкретно делать для данной информационной системы — запуск исполняемых модулей или скриптов, дополнительное аварийное копирование, внесение изменений в конфигурацию и т. д.;
- где находятся дополнительные средства, необходимые для выполнения мероприятий, — средства резервного копирования, дополнительные инструкции, огнетушители и т. п.

Подобные инструкции должны быть написаны простыми доступными словами, без использования сложных технических терминов, с «разжевыванием» всего, что, казалось бы, и так всем известно. Примерами таких инструкций могут быть следующие:

> Открыть большой серый шкаф справа от входа в помещение, если стоять лицом к двери. На второй полке сверху взять синюю коробку и вынуть из нее компакт-диск с надписью «Экстренная резервная копия».
>
> В главном меню системы выбрать раздел Options, затем подраздел Services. В открывшемся окне выбрать закладку Emergency и на появившейся странице установить флажки 1 и 2 в положение «включено», щелкнув по ним левой кнопкой мыши до появления в ячейке символа X.

После выполнения всех требуемых действий уполномоченные лица должны проанализировать сложившуюся ситуацию. Возможно, при каких-либо нестандартных условиях потребуются дополнительные работы, о которых не было известно на этапе составления и тестирования плана.

После того как все возможные действия, направленные на сокращение ущерба, выполнены, необходимо произвести оценку понесенного ущерба; не исключено, что для этого потребуется привлечение сторонних арбитражных организаций. Материал, полученный на этом этапе, будет нужен при обращении в страховые компании, для предъявления исков и т. п.

7.4. Возвращение к бизнесу

Как только воздействие аварии или катастрофы закончено, а иногда, возможно, и во время продолжения воздействия, организация принимает решение о возврате или продолжении своего бизнес-процесса. В зависимости от результатов аварии и составленного плана это может быть бизнес-процесс в полном объеме, такой же, каким он был до наступления аварии, либо в сокращенном объеме на определенный период времени.

В зависимости от созданного на подготовительном этапе плана необходимо начать восстановление функционирования систем по предопределенным приоритетам от критических к менее важным. Уже были рассмотрены степени возможного поражения предприятия и степени готовности к подобным случаям, поэтому лишь напомним, что это может быть перемещение в новое здание, получение или приобретение нового оборудования, переустановка системного и прикладного программного обеспечения, восстановление данных с резервных копий. Таким образом, часть плана должна включать следующие данные:

- Адрес нового месторасположения предприятия и систему доступа на новое место (документы, пропуски, идентификаторы), схемы подходов и подъездов, график движения транспорта и т. д.
- Способы получения оборудования — адреса и телефоны поставщиков, гарантийных и ремонтных центров, копии или ссылки на договоры поставок и поддержки, предварительно согласованные договоры на поставку нового оборудования и т. д.
- Адреса и телефоны своих и привлеченных специалистов, которые будут заниматься установкой и приведением систем в рабочее состояние.
- Место хранения инсталляционных копий программного обеспечения, копии конфигураций систем, специфических для данного предприятия. Для формирования последних еще на предварительной фазе особенно актуально зафиксировать все изменения настроек, проводимые для работы (это бывает затруднительно, так как в отличие от резервного копирования данных может происходить нерегулярно).
- Место хранения резервных копий данных и порядок их получения.
- Правила восстановления данных из резервных копий. Они должны быть не менее простыми и понятными, чем инструкции по действиям во время самой аварии, поскольку восстановление работоспособности может происходить в экстремальных условиях, в сжатые сроки, при постоянном появлении дополнительных задач и т. д.
- Возможно, процедуры по дополнительному обучению или тренировкам пользователей для работы в новых условиях.

Если работа первоначально восстанавливается в сокращенном объеме, значит, план должен предусматривать переход к полнообъемному функционированию с указанием этапов (контрольных точек), после которых выполняется следующая фаза перехода.

7.5. Методология работы с аварийным планом

Извлечение уроков. Когда высвобождаются ресурсы, направленные на возвращение бизнеса в обычный режим, а для ряда организаций или видов аварий одновременно с этим или даже предшествуя нормализации бизнеса, должно быть произведено расследование.

Не следует думать, что расследование необходимо производить только в случае подозрения на злой умысел как на источник аварии. К сожалению, и при природных катаклизмах, когда большинство сотрудников предприятия будет занято сокращением ущерба и восстановлением бизнеса, могут найтись люди, которые постараются использовать нестандартную ситуацию в собственных интересах. Если служба безопасности не может сразу обеспечить полный контроль всех действий сотрудников в момент наступления аварии и при восстановлении бизнеса, то сразу же при появлении возможности, высвобождении ресурсов должна быть произведена своего рода инвентаризация использования корпоративных ресурсов за критический период, с возможным охватом стадии до начала аварии и после восстановления бизнеса.

Дополнительно к этому действия персонала предприятия в период реализации аварийного плана являются приобретением опыта, в том числе, возможно, и негативного. Следовательно, он становится источником для анализа уполномоченными специалистами с целью последующего улучшения плана. Таким образом, само наступление аварии можно рассматривать с определенными «натяжками» как вариант тестирования аварийного плана.

Тестирование плана. Тестирование — один из самых существенных вариантов проверки правильности подготовки аварийного плана. Проблема заключается только в практической невозможности полного его тестирования, ведь для этого пришлось бы создать аварийную ситуацию со всеми вытекающими последствиями. Поэтому предлагается тестировать:

аварийный план по составляющим, отдельным системам в выделенной тестовой среде (на тестовом оборудовании, в тестовом сегменте сети, с тестовыми данными) в режиме, максимально приближенном к реальной аварии;

реальные отдельные системы — в щадящем режиме с минимальным влиянием на производительность и работу;

весь комплекс составляющих, объектов и систем — по предопределенным сценариям, обычно при временном прекращении или приостановлении рабочей деятельности.

Возможно также последовательно пройти по всем вариантам, на каждом этапе внося в аварийный план необходимые изменения и дополнения. Следует только учесть, что если в первом варианте организация тестирования возможна в рабочем порядке, то уже во втором потребуется содействие администраторов и пользователей систем, а третий вариант возможен только при привлечении руководства предприятия. Очевидно, что такие полномасштабные тестирования не могут проводиться часто, чтобы не оказать негативного влияния на работу организации. Компетентные специалисты по безопасности называют сроки, в зависимости от размеров предприятия, от одного раза в полгода до одного раза в два года. Более редкое тестирование нецелесообразно, так как непротестированный план будет уже неактуальным, и перед очередным тестированием его придется предварительно перерабатывать.

В западных источниках можно встретить следующие рекомендуемые стадии тестирования аварийного плана (в данном случае disaster recovery plan — плана восстановления после несчастного случая):

1. Контрольная проверка (checklist). Копии плана распределяются между различными подразделениями, которым предлагается просмотреть его и убедиться, что в плане отражено все, что необходимо.

2. Структурированный обзор (structured walk-through). Руководители подразделений собираются вместе, чтобы в ходе совещания обсудить каждый из пунктов. Требуется убедиться, что разработанные мероприятия позволят эффективно противостоять аварии.

3. Симуляция (simulation). Весь выделенный операционный и поддерживающий персонал выполняет тренировочные мероприятия по предопределенному сценарию, в том числе перемещение на альтернативное место работы, используя только средства, предназначенные для аварийного использования. При этом, однако, не выполняются собственно процедуры восстановления или альтернативной работы.

4. Параллельная проверка (parallel). Весь персонал выполняет полное тестирование аварийного плана. Единственное отличие от реального аварийного события заключается в том, что не производится остановка основного производственного процесса (в нем задействуется минимум требуемого персонала). При этом сравнивается эффективность производительности продолжающейся реальной деятельности и тестовой деятельности, выполненной на альтернативном месте расположения.

5. Полное прекращение деятельности (full-interruption). Все происходит как при реальном наступлении аварии с остановкой основного производственного процесса. Вся деятельность переносится на альтернативное место работы. При этом важно отметить необходимость кооперации предприятия с внешними органами управления (полицией, пожарной службой, транспортом и т. д.).

Обновление плана. Поскольку и в промежутках между этапами тестирования как основными источниками внесения изменений и дополнений жизнь не стоит на месте, план придется дорабатывать и изменять. Наиболее существенной причиной изменения будет внедрение новой информационной системы — в аварийном плане появится целый новый раздел, посвященный обеспечению работы этой системы, а также изменения в тех частях плана, где новая система сопрягается с другими объектами и системами.

Другим минимальным примером изменения плана может служить увольнение с предприятия одного ключевого работника и замена его другим. Поскольку в плане присутствуют персональные контактные данные, они должны быть обновлены со сменой в должности конкретного лица. Кроме того, возможно, новый человек не будет обладать достаточной квалификацией, и часть его обязанностей в рамках плана придется перераспределить между другими участниками, либо, наоборот, из-за высокой квалификации на него можно будет возложить дополнительные обязанности.

В любом случае необходимо, чтобы уполномоченный человек или группа контролировали изменения в информационном пространстве предприятия, затрагивающие аварийный план, и инициировали обновление плана при возникновении соответствующих условий. Особенно это может быть важно при переконфигурировании систем. Восстановление систем после сбоя подразумевает и тонкую настройку системы для данного конкретного предприятия. Если настройки, произведенные в системе, не были закреплены в одном из документов или приложений аварийного плана, то при восстановлении система может оказаться в конфигурации, предшествующей последним изменениям, и не отвечать текущим условиям работы.

Заканчивая разговор об аварийном плане, следует напомнить, что, кроме качества составления плана (подробности, ясности изложения и т. д.), он должен быть доступен соответствующему персоналу в критический момент. Это означает, что копии плана требуется подготовить не только в электронном, но и в печатном виде.

Сохранение данных. Следует различать два способа сохранения данных.

Архивирование — сохранение копий данных, которые не требуются в постоянном оперативном использовании. Чаще всего это данные приложений за истекший период времени, которые могут потребоваться при необходимости исторической справки.

Резервное копирование — сохранение избыточных копий данных, используемых оперативно либо за ближайший период. Основное их предназначение — восстановление данных в случае утери или повреждения текущей копии, используемой системой.

Архивирование — это вопрос бизнес-процесса и безопасности, касается в основном обеспечения защиты архивных копий и разграничения доступа к ним. С точки зрения аварийного плана более важно резервное копирование, поэтому остановимся на нем подробнее.

Следует помнить, что при планировании резервного копирования необходимо найти оптимальный баланс между актуальностью данных и загруженностью системы. С одной стороны, данные, сохраненные в резервной копии, должны быть по времени максимально приближены к текущим данным, используемым системой (возможны случаи, когда наличие данных недельной давности равнозначно полному их отсутствию). С другой стороны, ежечасный запуск процедуры резервного копирования может послужить серьезной помехой работоспособности системы.

Процедуры регулярного резервного копирования по видам разделяются следующим образом:

Полное копирование, когда заданный набор данных (файлы, каталоги и т. д.) регулярно полностью переносится в альтернативное место сохранения. Резервная копия занимает большой объем, и процесс растянут по времени, однако этот метод наиболее надежен (никакие данные не пропущены) и прост в аварийной ситуации — восстанавливается все сразу.

Наращиваемое, или *инкрементальное, копирование*. После первой полной копии данных в каждую последующую помещаются только те данные, которые были модифицированы со времени выполнения предыдущей копии. Периодически, по завершении выбранного цикла, снова выполняется полное копирование, и наращивание начинается заново. Резервная копия занимает мало места, процесс копирования проходит быстро, однако восстановление растянуто во времени: сначала восстанавливается первая полная копия, затем последовательно все остальные. Кроме того, при неверно выбранном критерии модифицированности данных возможен пропуск части данных (которые были изменены, но по каким-либо причинам не попали в разряд модифицированных).

Метод различий, или *дифференциальное копирование*. После первой полной копии данных в каждую последующую помещаются только те данные, которые были модифицированы со времени выполнения первой полной копии. По своим характеристикам этот способ является промежуточным между первыми двумя. Время копирования и объем архива меньше, чем у полной копии, но больше, чем у наращиваемой. Однако для восстановления требуются только первая и последняя копии.

Резервное копирование имеет ряд тонкостей, на которые следует обратить внимание. Но перед рассмотрением этих вопросов и проблем необходимо провести еще одно разделение способов резервного копирования — на ручное и автоматическое. Для небольшого предприятия, где все данные сохраняются на одном сервере, возможно поручить процедуру резервного копирования системному администратору, оставив на его усмотрение способ, время, критерии и т. д. Но для предприятия с несколькими десятками серверов, возможно, географически разнесенных, с сотнями гигабайт или терабайтами постоянно изменяющихся данных, открытых для использования 24 часа в сутки, необходима отдельная система резервного копирования.

Для выбора и настройки системы резервного копирования данных требуется учитывать ряд особенностей ее функционирования:

- Выбор критериев того, была ли конкретная часть набора данных изменена со времени последней копии. По каким параметрам система будет это определять (размер, дата модификации, специальные флаги, совокупность различных параметров)?
- Какие действия необходимо предпринять, если в момент резервного копирования данный файл, подлежащий копированию, находится в процессе модификации? Подождать, пропустить, вернуться к попытке через некоторое время?
- Должна ли система при восстановлении перезаписывать те данные, которые уже имеются на месте восстановления? Возможно, эти данные более актуальны, чем восстанавливаемые? Если не перезаписать, то не возникнет ли рассогласование между актуальными данными и восстановленными? Восстанавливать ли данные, которые были санкционировано удалены в ходе бизнес-процесса?

- Если данные распределены между различными операционными или файловыми системами, система резервного копирования должна быть одной для всех или для каждого отдельной? Сохранять все резервные копии единообразно (например, все на стриммерные ленты) или для различных видов данных различно (что-то на жесткий диск, что-то на ленту, что-то на магнитооптику)?
- Нужно ли одновременно с копированием шифровать данные?

Кроме перечисленных вопросов, касающихся собственно системы копирования, возникнут еще и вопросы о сохранении самих резервных копий. Если хранить их рядом с текущими данными, то серьезная катастрофа может уничтожить и основные данные, и резервные копии. Географическое разнесение копий возможно для многофилиального предприятия, но что делать, если все учреждения организации сконцентрированы в одном районе? Может быть, необходимо передать копии (естественно, позаботившись об их защищенности с точки зрения информационной безопасности) организации-партнеру или отдельной компании, предоставляющей услуги хранения, например в банковский депозитный ящик?

Вопросы для самоконтроля

1. Что такое авария, аварийный план?
2. Какие типы систем по уровню критичности вы знаете?
3. Какие виды резервных систем существуют?
4. Опишите основные разделы аварийного плана.
5. Как поддерживается актуальность аварийного плана?

8. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Понятие об аудите безопасности

На сегодняшний день АС играют ключевую роль в обеспечении эффективного выполнения бизнес-процессов как коммерческих, так и государственных предприятий. Вместе с тем повсеместное использование АС для хранения, обработки и передачи информации приводит к повышению актуальности проблем их защиты. Подтверждением служит тот факт, что за последние несколько лет, как в России, так и в ведущих зарубежных странах, имеет место тенденция увеличения числа информационных атак, приводящих к значительным финансовым и материальным потерям. Для того чтобы гарантировать эффективную защиту от информационных атак злоумышленников, компаниям необходимо иметь объективную оценку текущего уровня безопасности АС. Именно для этих целей и применяется аудит безопасности.

Несмотря на то что в настоящее время еще не сформировалось устоявшееся определение аудита безопасности, в общем случае его можно представить в виде процесса сбора и анализа информации об АС, необходимой для последующего проведения качественной или количественной оценки уровня защиты от атак злоумышленников.

Существует множество случаев, в которых целесообразно проводить аудит безопасности. Вот лишь некоторые из них:

аудит АС с целью подготовки технического задания на проектирование и разработку системы защиты информации;

аудит АС после внедрения системы безопасности для оценки уровня ее эффективности;

аудит, направленный на приведение действующей системы безопасности в соответствие требованиям российского или международного законодательства;

аудит, предназначенный для систематизации и упорядочивания существующих мер защиты информации;

аудит в целях расследования произошедшего инцидента, связанного с нарушением информационной безопасности.

Как правило, для проведения аудита привлекаются внешние компании, которые предоставляют консалтинговые услуги в области информационной безопасности. Инициатором процедуры аудита может являться руководство предприятия, служба автоматизации или служба информационной безопасности. В ряде случаев аудит также может проводиться по требованию

страховых компаний или регулирующих органов. Аудит безопасности проводится группой экспертов, численность и состав которой зависит от целей и задач обследования, а также сложности объекта оценки.

8.2. Виды аудита безопасности

В настоящее время можно выделить следующие основные виды аудита информационной безопасности:

экспертный аудит безопасности, в процессе которого выявляются недостатки в системе мер защиты информации на основе имеющегося опыта экспертов, участвующих в процедуре обследования;

оценка соответствия рекомендациям, содержащимся в международном стандарте ISO 17799, а также требованиям руководящих документов ФСТЭК (Гостехкомиссии);

инструментальный анализ защищенности АС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы;

комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования.

Каждый вид аудита может проводиться по отдельности или в комплексе, в зависимости от тех задач, которые необходимо решить предприятию. В качестве объекта аудита может выступать как АС компании в целом, так и ее отдельные сегменты, в которых проводится обработка информации, подлежащей защите.

8.3. Состав работ по проведению аудита безопасности

В общем случае аудит безопасности, вне зависимости от формы его проведения, состоит из четырех основных этапов, каждый из которых предусматривает выполнение определенного круга задач (рис. 12).

Рис. 12

На первом этапе совместно с заказчиком разрабатывается регламент, устанавливающий состав и порядок проведения работ. Основная задача регламента заключается в определении границ, в рамках которых будет проведено обследование. Регламент является тем документом, который позволяет избежать взаимных претензий по завершению аудита, поскольку четко

определяет обязанности сторон. Как правило, регламент содержит следующую основную информацию:

состав рабочих групп от исполнителя и заказчика, участвующих в процессе проведения аудита;

перечень информации, которая будет предоставлена исполнителю для проведения аудита;

список и местоположение объектов заказчика, подлежащих аудиту;

перечень ресурсов, которые рассматриваются в качестве объектов защиты (информационные, программные, физические и т. д.);

модель угроз информационной безопасности, на основе которой проводится аудит;

категории пользователей, которые рассматриваются в качестве потенциальных нарушителей;

порядок и время проведения инструментального обследования автоматизированной системы заказчика.

На втором этапе, в соответствии с согласованным регламентом, осуществляется сбор исходной информации. Методы сбора информации включают интервьюирование сотрудников заказчика, заполнение опросных листов, анализ предоставленной организационно-распорядительной и технической документации, использование специализированных инструментальных средств.

Третий этап работ предполагает проведение анализа собранной информации с целью оценки текущего уровня защищенности АС. По результатам проведенного анализа на четвертом этапе проводится разработка рекомендаций по повышению уровня защищенности АС от угроз информационной безопасности.

8.4. Сбор исходных данных для проведения аудита безопасности

Качество проводимого аудита безопасности во многом зависит от полноты и точности информации, которая была получена в процессе сбора исходных данных. Поэтому информация должна включать в себя: существующую организационно-распорядительную документацию, касающуюся вопросов информационной безопасности, сведения о программно-аппаратном обеспечении АС, информацию о средствах защиты, установленных в АС, и т. д. (**табл.**).

Как уже отмечалось, сбор исходных данных может осуществляться с использованием следующих методов:

Интервьюирование сотрудников заказчика, обладающих необходимой информацией. При этом интервью, как правило, проводится как с техническими специалистами, так и с представителями руководящего звена компании. Перечень вопросов, которые планируется обсудить в процессе интервью, согласовывается заранее.

Предоставление опросных листов по определенной тематике, самостоятельно заполняемых сотрудниками заказчика. В тех случаях, когда представленные материалы не полностью дают ответы на необходимые вопросы, проводится дополнительное интервьюирование.

Анализ существующей организационно-технической документации, используемой заказчиком.

Использование специализированных программных средств, которые позволяют получить необходимую информацию о составе и настройках программно-аппаратного обеспечения автоматизированной системы заказчика. Так, например, в процессе аудита могут использоваться системы анализа защищенности (security scanners), которые позволяют провести инвентаризацию имеющихся сетевых ресурсов и выявить в них уязвимости.

Перечень исходных данных, необходимых для проведения аудита безопасности

Тип информации	Описание состава исходных данных
Организационно-распорядительная документация по вопросам информационной безопасности	Политика информационной безопасности АС. Руководящие документы (приказы, распоряжения, инструкции) по вопросам хранения, порядка доступа и передачи информации. Регламенты работы пользователей с информационными ресурсами АС
Информация об аппаратном обеспечении хостов	Перечень серверов, рабочих станций и коммуникационного оборудования, установленного в АС. Информация об аппаратной конфигурации серверов и рабочих станций. Информация о периферийном оборудовании, установленном в АС
Информация об общесистемном ПО	Информация об операционных системах, установленных на рабочих станциях и серверах АС. Данные о системах управления базами данных, установленных в АС
Информация о прикладном ПО	Перечень прикладного ПО общего и специального назначения, установленного в АС. Описание функциональных задач, решаемых с помощью прикладного ПО, установленного в АС
Информация о средствах защиты, установленных в АС	Информация о производителе средства защиты. Конфигурационные настройки средства защиты. Схема установки средства защиты
Информация о топологии АС	Карта локальной вычислительной сети, включающей схему распределения серверов и рабочих станций по сегментам сети. Информация о типах каналов связи, используемых в АС. Информация об используемых в АС сетевых протоколах. Схема информационных потоков АС

8.5. Оценка уровня безопасности автоматизированных систем

После сбора необходимой информации проводится ее анализ с целью оценки текущего уровня защищенности системы. В процессе проведения аудита безопасности могут использоваться специализированные программные комплексы, позволяющие автоматизировать процесс анализа исходных данных и расчета значений рисков.

Результаты аудита безопасности. На последнем этапе проведения аудита информационной безопасности разрабатываются рекомендации по совершенствованию организационно-технического обеспечения предприятия. Такие рекомендации могут включать в себя следующие типы действий, направленных на минимизацию выявленных рисков:

- Уменьшение риска за счет использования дополнительных организационных и технических средств защиты, позволяющих снизить вероятность проведения атаки или уменьшить возможный ущерб от нее. Так, например, установка межсетевых экранов в точке подключения АС к Интернету позволяет существенно снизить вероятность проведения успешной атаки на общедоступные информационные ресурсы АС, такие как web-серверы, почтовые серверы и т. д.
- Уклонение от риска путем изменения архитектуры или схемы информационных потоков АС, что позволяет исключить возможность проведения той или иной атаки. Так, например, физическое отключение от Интернета сегмента АС, в котором обрабатывается конфиденциальная информация, позволяет исключить атаки на конфиденциальную информацию из этой сети.
- Изменение характера риска в результате принятия мер по страхованию. В качестве примеров такого изменения характера риска можно привести страхование оборудования АС от пожара или страхование информационных ресурсов от возможного нарушения их конфиденциальности, целостности или доступности. В настоящее время российские компании уже предлагают услуги по страхованию информационных рисков.
- Принятие риска в том случае, если он уменьшен до того уровня, на котором он не представляет опасности для АС.

Как правило, разработанные рекомендации направлены не на полное устранение всех выявленных рисков, а лишь на их уменьшение до приемлемого остаточного уровня. При выборе мер по повышению уровня защиты АС учитывается одно принципиальное ограничение — стоимость их реализации не должна превышать стоимость защищаемых информационных ресурсов.

В завершении процедуры аудита его результаты оформляются в виде отчетного документа, который предоставляется заказчику. В общем случае этот документ состоит из следующих основных разделов:

описание границ, в рамках которых был проведен аудит безопасности;

описание структуры АС заказчика;

методы и средства, которые использовались в процессе проведения аудита;

описание выявленных уязвимостей и недостатков, включая уровень их риска;

рекомендации по совершенствованию комплексной системы обеспечения информационной безопасности;

предложения по плану реализации первоочередных мер, направленных на минимизацию выявленных рисков.

Аудит информационной безопасности является сегодня одним из наиболее эффективных инструментов для получения независимой и объективной оценки текущего уровня защищенности предприятия от угроз информационной безопасности. Кроме того, результаты аудита являются основой для формирования стратегии развития системы обеспечения информационной безопасности организации. Однако необходимо понимать, что аудит безопасности не является однократной процедурой, а должен проводиться на регулярной основе. Только в этом случае аудит будет приносить реальную отдачу и способствовать повышению уровня информационной безопасности компании.

Вопросы для самоконтроля

1. Что такое аудит информационной безопасности и когда его следует проводить?
2. Назовите виды работ при аудите информационной безопасности.
3. Каковы исходные данные и результаты аудита?

Список рекомендуемой литературы

1. *Громов, Ю. Ю.* Информационная безопасность и защита информации : учеб. пособие для вузов / Ю. Ю. Громов и др. — Старый Оскол : ТНТ, 2010. — 384 с.

2. *Цирлов, В. Л.* Основы информационной безопасности. Краткий курс / В. Л. Цирлов. — Ростов н/Д. : Феникс, 2008. — 256 с.

3. *Конеев, И. Р.* Информационная безопасность предприятия / И. Р. Конеев, А. В Беляев. — СПб. : БХВ-Петербург, 2003. — 752 с.

4. *Галатенко, В. А.* Стандарты информационной безопасности / В. А. Галатенко. — М. : Интернет-университет информационных технологий, 2004. — 208 с.

Учебное электронное издание

Платонов Андрей Анатольевич

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Начальник РИО *М. Л. Песчаная*
Редактор *Н. Э. Фотина*
Компьютерная правка и верстка *А. Г. Сиволобова*

Минимальные систем. требования:
PC 486 DX-33; Microsoft Windows XP; Internet Explorer 6.0; Adobe Reader 6.0.

Подписано в свет 27.05.2016.
Гарнитура «Таймс». Уч.-изд. л. 5,0. Объем данных 1,6 Мбайт.

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Волгоградский государственный архитектурно-строительный университет»
Редакционно-издательский отдел
400074, Волгоград, ул. Академическая, 1
http://www.vgasu.ru, info@vgasu.ru