ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ВЫСШАЯ ШКОЛА ЭКОНОМИКИ

В.А.Сердюк

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

обнаружение и предотвращение информационных атак в автоматизированных системах предприятий

Учебное пособие

Издательский дом
Государственного университета — Высшей школы экономики

Москва, 2011

УДК 65.39(075)
ББК 004.056.5
С32

Р е ц е н з е н т
профессор кафедры корпоративных информационных систем
Государственного университета — Высшей школы экономики
О.Р. Козырев

ISBN 978-5-7598-0698-1

Содержание

Термины и определения

Автоматизированная система (АС) — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор безопасности АС — физическое или юридическое лицо, ответственное за реализацию политики обеспечения информационной безопасности АС.

Активная атака — преднамеренное несанкционированное изменение состояния системы. Примерами активных атак могут служить модификация сообщений, дублирование ранее переданных пакетов данных, вставка ложных сообщений.

Атака типа «отказ в обслуживании» (Denial of Service attack) — совокупность действий злоумышленника, направленная на нарушение доступности информационных ресурсов АС. Атаки данного типа могут быть направлены на нарушение работоспособности системы или на блокирование доступа к ней со стороны легальных пользователей.

Аудит информационной безопасности — периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения в организации установленных требований по обеспечению информационной безопасности.

Внутренние аудиты («аудиты первой стороной») проводятся самой организацией или от ее имени для анализа менеджмента или других внутренних целей и могут служить основанием для самодеклараций организации о соответствии требованиям по информационной безопасности. Внешние аудиты включают «аудиты второй стороной» и «аудиты третьей стороной». Аудиты второй стороной проводятся сторонами, заинтересованными в деятельности организации, например, потребителями или другими лицами от их имени. Аудиты третьей стороной проводятся внешними независимыми организациями.

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности.

Аутентификационные параметры — информация, используемая для установления подлинности субъекта доступа.

База данных — объективная форма представления и организации совокупности данных (статей, расчетов и т.д.), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной вычислительной машины.

Вредоносные программы типа «троянский конь» (Trojan Horses) — программы типа «троянский конь» относятся к вредоносному программному коду, однако в отличие от вирусов не имеют возможности самостоятельного распространения в АС. Программы данного типа маскируются под видом штатного программного обеспечения системы и позволяют нарушителю получить удаленный несанкционированный доступ к тем узлам, на которых они установлены.

Вредоносные программы типа «spyware» — вредоносное программное обесепечение типа «spyware» предназначено для сбора определенной информации о работе пользователя. Примером таких данных может служить список веб-сайтов, посещаемых пользователем, перечень программ, установленных на рабочей станции пользователя, содержимое сообщений электронной почты и др. Собранная информация перенаправляется программами «spyware» на заранее определенные адреса в сети Интернет. Вредоносное программное обеспечение данного типа может являться потенциальным каналом утечки конфиденциальной информации из АС.

Вредоносные программы типа «adware» — основная функциональная задача вредоносных программ класса «adware» заключается в отображении рекламной информации на рабочих станциях пользователей. Для этого, как правило, такие программы отображают на экране пользователя рекламные баннеры, содержащие информацию о тех или иных товарах и услугах. В большинстве случаев программы «adware» распространяются вместе с другим программным обеспечением, которое устанавливается на узлы АС. Несмотря на то что программы типа «adware» не представляют непосредственную угрозу для конфиденциальности или целостности информационных ресурсов АС, их работа может приводить к нарушению доступности вследствие несанкционированного использования вычислительных ресурсов рабочих станций.

Владелец информации — субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Внутренние атаки — атаки, источниками которых являются легальные пользователи АС. Примеры внутренних атак — кража конфиденциальной информации, запуск несанкционированного программного обеспечения и др.

Внешние атаки — атаки, источник которых находится за пределами АС, например в сети Интернет.

Датчики системы обнаружения атак — программные или программно-аппаратные модули, предназначенные для сбора информации, необходимой для выявления атак.

Доступ к информации — получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

Доступность информации — состояние информации, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Задание по безопасности — совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного продукта или системы.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защита информации — деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации от несанкционированного доступа или воздействия на информацию — деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию).

Идентификатор доступа — уникальный признак субъекта или объекта доступа.

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Интернет-портал — автоматизированная система, предназначенная для предоставления различных услуг и сервисов через сеть Интернет. Порталы могут применяться для решения самых разнообразных задач, таких, например, как реклама в сети Интернет характера деятельности компании, организация интернет-торговли или же обеспечение работы системы «клиент-банк».

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

Информационная атака (вторжение) — совокупность действий нарушителя, направленная на реализацию угрозы информационной безопасности АС.

Информационная безопасность — состояние информации, информационных ресурсов и информационных систем, при котором обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т.п.

Информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информационная технология — приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных.

Инцидент информационной безопасности — событие, вызывающее действительное, предпринимаемое или вероятное нарушение информационной безопасности организации. Нарушение может вызываться либо ошибкой людей, либо неправильным функционированием технических средств, либо природными факторами (например, пожар или наводнение), либо преднамеренными злоумышленными действиями, приводящими к нарушению конфиденциальности, целостности, доступности, учетности или неотказуемости.

Компьютерный вирус — специально созданный программный код, способный самостоятельно распространяться в компьютерной среде.

Контролируемая зона — это пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств. Границей контролируемой зоны могут являться: периметр охраняемой территории предприятия (учреждения); ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

Конфиденциальность информации — состояние защищенности информации, характеризуемое способностью АС обеспечи-

вать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

Корпоративная информационная система — информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Критерии фильтрации — параметры, атрибуты, характеристики, на основе которых осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных) в соответствии с заданными правилами разграничения доступа (правилами фильтрации).

Криптографическая защита — защита данных при помощи криптографического преобразования данных.

Ключ — последовательность символов, управляющая операциями шифрования и дешифрования.

Маскирование — стремление какого-либо логического объекта выглядеть в виде другого логического объекта.

Менеджмент риска — скоординированные действия по руководству и управлению в отношении риска с целью его минимизации.

Межсетевой экран (брандмауэр) — локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС. Межсетевой экран обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС.

Мониторинг информационной безопасности организации — постоянное наблюдение за событиями безопасности, сбор, анализ и обобщение результатов наблюдения.

Нарушитель (злоумышленник) — физическое или юридическое лицо, техническое устройство или программа, процесс или событие, субъект или пользователь АС, производящие несанкционированные или непреднамеренные действия, способные привести к реализации угрозы информационной безопасности АС.

Недекларированные возможности — функциональные возможности программного обеспечения, не описанные или не со-

ответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ к информации — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых АС.

Нормативный документ — документ, содержащий правила, общие принципы или характеристики, касающиеся различных видов деятельности или их результатов. Примечание: термин «нормативный документ» охватывает такие понятия, как стандарты, документы технических условий, своды правил и регламенты.

Носитель информации — физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Объект защиты информации — информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

Ошибка первого рода (false positive) — возникает в ситуации, при которой происходит ложное срабатывание, т.е. регистрируется факт проведения атаки, в то время как реальной атаки не происходит.

Ошибка второго рода (false negative) — появляется в ситуации, когда система не обнаруживает атаку, которая на самом деле проводится в АС.

Пароль — конфиденциальная информация аутентификации, состоящая из строки знаков.

Пассивная атака — угроза несанкционированного раскрытия информации без изменения состояния системы. К пассивным атакам относятся те, которые при их реализации не приводят к какой-либо модификации любой информации, содержащейся в системе (ах), и где работа и состояние системы не изменяются. Примером пассивной атаки является перехват конфиденциальной информации.

Пиринговые сети (P2P networks) — файлообменные сети, для подключения к которым должно использоваться специализиро-

ванное программное обеспечение. Примерами таких сетей являются «eDonkey», «DirectConnet», «BitTorrent» и «Kazaa».

Поведенческие методы выявления атак — базируются на моделях штатного процесса функционирования АС. Принцип использования поведенческих методов заключается в обнаружении несоответствия между текущим режимом функционирования АС и режимом штатной работы. Любое такое несоответствие в рамках поведенческого метода рассматривается в качестве информационной атаки.

Политика информационной безопасности АС — совокупность требований и правил по обеспечению информационной безопасности АС.

Пользователь сети — физические или юридические лица, имеющие доступ к ресурсам сети через терминал или другие средства связи, и процессы, выполняемые на различных ресурсах сети.

Пакет — блок данных, посланных по сети, состоящий из заголовка и поля данных.

Порт — числовой идентификатор сетевой службы, запущенной на хосте. Порт называется «открытым», если служба, которая с ним связана, может принимать входящие запросы от клиентов. В противном случае порт называется «закрытым».

Профиль защиты — независимая от реализации совокупность требований безопасности для некоторой категории систем, отвечающая специфическим запросам потребителя.

Распределенная атака типа «отказ в обслуживании» (Distributed denial of service attack) — атака типа «отказ в обслуживании», которая проводится одновременно из нескольких источников.

Расшифрование информации — процесс преобразования зашифрованных данных в открытые при помощи шифра.

Риск информационной безопасности — неопределенность, предполагающая возможность ущерба состояния защищенности интересов (целей) организации в условиях угроз в информационной сфере.

Сетевой адрес — адресные данные, идентифицирующие субъекты и объекты и используемые протоколом сетевого уровня модели взаимодействия открытых систем ISO.

Сигнатурные методы выявления атак — описывают каждую атаку в виде специальных сигнатур, примерами которых могут быть: строка символов, семантическое выражение на специаль-

ном языке, формальная математическая модель и др. Сущность алгоритма сигнатурных методов состоит в поиске сигнатур атак в исходных данных, присутствующих в журналах аудита, пакетах данных и др. В случае обнаружения искомой сигнатуры фиксируется факт информационной атаки. Основным преимуществом сигнатурных методов является высокая точность обнаружения известных типов атак. Недостаток же состоит в принципиальной невозможности обнаружения новых типов атак, сигнатуры которых не определены в параметрах модели.

Система обеспечения информационной безопасности — совокупность правовых норм, организационных и технических мероприятий, направленных на защиту от возможности реализации нарушителем угроз информационной безопасности.

Система обнаружения атак — совокупность программного и программно-аппаратного обеспечения, предназначенная для выявления информационных атак в АС.

Система анализа защищенности — совокупность программного и программно-аппаратного обеспечения, предназначенная для обнаружения уязвимостей АС.

Система контентного анализа — средство защиты, предназначенное для мониторинга сетевого трафика с целью выявления нарушений политики безопасности. В настоящее время можно выделить два основных вида средств контентного анализа — системы аудита почтовых сообщений и системы мониторинга интернет-трафика.

Система менеджмента информационной безопасности организации — часть общей системы менеджмента организации, основывающаяся на подходе бизнес-риска, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности организации. Система менеджмента включает структуру, политики, деятельности по планированию, обязанности, практики, процедуры, процессы и ресурсы организации.

Сканирование — процесс сбора информации об АС с целью выявления и последующего использования уязвимостей системы. Как правило, сканирование является начальной фазой реализации атаки злоумышленника.

Спам — незапрошенные почтовые сообщения рекламного характера.

Технологическая безопасность АС — защищенность АС от возможных информационных атак на этапе проектирования и разработки системы.

Угроза информационной безопасности АС — возможное последствие информационной атаки, необнаружение, непредотвращение и неликвидация последствий которого может привести к нарушению конфиденциальности, целостности и доступности информации АС.

Уязвимость АС — недостатки в системе мер защиты АС или же отсутствие таких мер, позволяющие нарушителю совершать действия, приводящие к успешной реализации угрозы информационной безопасности АС.

Уязвимость типа «buffer overflow» («переполнение буфера») — в основе уязвимости типа «переполнение буфера» лежит возможность переполнения стека атакуемой подпрограммы, в результате чего нарушитель получает возможность выполнить любые команды на стороне узла, где запущена эта подпрограмма.

Уязвимости типа «SQL Injection» («инъекция в SQL-запросы») — уязвимость даст возможность нарушителю выполнять несанкционированные операции над содержимым баз данных SQL-серверов путем вставки дополнительных команд в SQL-запросы.

Уязвимости типа «Directory traversal» («просмотр директорий») — уязвимость может позволить злоумышленнику получить несанкционированный доступ к файловым ресурсам сервера в обход установленных правил разграничения доступа.

Уязвимости типа «Cross Site Scripting» («межсайтовое выполнение сценариев») — уязвимость характерна для серверных вебприложений, не предусматривающих проверку синтаксиса входных данных, на основе которых формируются HTML-документы, отправляемые пользователям.

Уязвимости реализаций стека TCP/IP — связаны с ошибками, которые допускаются программистами на этапе реализации программных модулей, отвечающих за обработку входящих и исходящих пакетов данных. В подавляющем большинстве уязвимости данного типа обусловлены тем, что в программах не предусматривается возможность обработки пакетов данных, которые имеют некорректную структуру или поля которых содержат нестандартные значения. Как правило, атаки на основе данных уязвимостей приводят к нарушению работоспособности узлов АС.

Целостность информации — состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность информации при попытках несанкционированных или случайных воздействий на нее в процессе передачи, обработки или хранения.

Шифрование — криптографическое преобразование данных для получения шифротекста.

Эксплуатационная безопасность АС — защищенность АС от информационных атак в процессе ее эксплуатации.

Электронно-цифровая подпись — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронный документ — документ, в котором информация представлена в электронно-цифровой форме.

Введение

В настоящее время информационная безопасность является одним из наиболее динамично развивающихся направлений в области информационных технологий. В первую очередь это связано с тем, что количество информационных атак ежегодно увеличивается как в России, так и во всем мире. Так, например, согласно статистике Министерства внутренних дел РФ количество компьютерных преступлений, связанных с несанкционированным доступом к конфиденциальной информации, увеличилось с 600 инцидентов в 2000 г. до 7 тыс. в 2004 г. К основным причинам роста количества атак можно отнести следующие факторы:

- с каждым годом увеличивается количество пользователей общедоступных сетей связи, таких, например, как сеть Интернет. При этом в качестве новых пользователей выступают как отдельные клиентские рабочие станции, так и целые корпоративные сети;
- увеличивается количество уязвимостей, ежедневно обнаруживаемых в существующем общесистемном и прикладном программном обеспечении;
- возрастает число возможных объектов атаки. Если несколько лет назад в качестве основных объектов несанкционированного воздействия рассматривались исключительно серверы стандартных веб-служб, такие как HTTP, SMTP и FTP, то к настоящему моменту разработаны средства реализации атак на маршрутизаторы, коммутаторы, межсетевые экраны и др.;
- упрощение методов реализации информационных атак. В сети Интернет можно без труда найти программные реализации атак, направленных на активизацию различных уязвимостей. При этом использование этих средств сводится к вводу IP-адреса объекта атаки и нажатию соответствующей управляющей кнопки;
- увеличение числа внутренних атак со стороны пользователей АС. Примерами таких атак является кража конфиденциальной информации или запуск вредоносного ПО на рабочих станциях пользователей.

Вопрос защиты и безопасного взаимодействия компьютеров при подключении их к всемирной компьютерной сети Интернет, придерживающейся идеологии глобальности, открытости и свободной доступности, стал особенно острым. Поэтому для многих компаний важно не только защитить свои локальные сети и ин-

формационные ресурсы от вторжения извне, но и организовать надежные и безопасные системы взаимодействия с удаленными подразделениями через Интернет. Своего решения ждут также задачи, связанные с электронной коммерцией, так как ее широкомасштабное применение невозможно без принятия особых мер по обеспечению безопасности и конфиденциальности трансакций.

Создавшаяся ситуация заставила почти все ведущие страны мира резко повысить внимание к решению проблемы обеспечения информационной безопасности. Проведенный анализ доступных научно-технических источников показывает, что реализация задач по защите информации благодаря методам криптографии и существующим протоколам взаимодействия претерпела серьезную эволюцию. Однако решение многих важных вопросов в области информационной безопасности столкнулось с серьезными трудностями, обусловленными, в частности, и такой причиной, как наличие существенного разрыва между бурным развитием современных сетевых технологий и медленной проработкой теоретических положений и подходов к обеспечению информационной безопасности в открытой сетевой среде. Главным недостатком существующих средств и систем является то, что ими не учитываются ряд важных свойств динамики функционирования корпоративных в условиях нештатных и критических ситуаций и не обладают свойством адаптивности к постоянно меняющемуся уровню проявления угроз.

Необходимо также отметить, что уровень сложности информационных атак также постоянно растет. Данное утверждение можно проиллюстрировать на примере эволюции компьютерных вирусов. В момент своего первого появления в 1980-х гг. вирусы представляли собой достаточно простые программы, которые самостоятельно распространялись в автоматизированных системах (АС) и основной задачей которых было нарушение работоспособности системы. Сегодня же компьютерные вирусы представляют собой существенно более сложные программные средства, способные распространяться практически в любой среде передачи информации, а также маскироваться под работу штатного ПО. Кроме того, современные модификации компьютерных вирусов в основном используются для кражи конфиденциальной информации, а также для получения несанкционированного доступа к компьютерам пользователей. Аналогичная тенденция характерна

и для других видов угроз безопасности, для реализации которых постоянно придумываются более изощренные методы и средства проведения атак.

С учетом вышесказанного можно с уверенностью утверждать, что проблема защиты АС от информационных атак является одной из наиболее актуальных и значимых в области ИТ-индустрии. По всему миру ежегодно проводится большое количество исследований, направленных на разработку новых и более эффективных методов противодействия угрозам злоумышленников. С учетом актуальности вопросов, связанных с защитой от внешних и внутренних информационных атак, и было написано это учебное пособие, в основу которого заложен многолетний практический опыт проектирования, разработки и внедрения комплексных системы защиты от информационных атак. Особое внимание в пособии уделено средствам защиты, которые классифицируются как системы обнаружения атак — IDS (Intrusion Detection System) и системы предотвращения атак — IPS (Intrusion Prevention System).

Представленное на суд читателя учебное пособие включает лекционные материалы, охватывающие следующие основные темы в области информационной безопасности:

- основные виды уязвимостей, информационных атак и их возможных последствий;
- математические модели защиты автоматизированных систем от информационных атак;
- практические аспекты проведения аудита и оценки рисков информационной безопасности;
- существующие криптографические методы защиты информационных ресурсов;
- технологии идентификации, аутентификации и авторизации пользователей информационных систем;
- информационная безопасность территориально-распределенных сетей связи X.25, Frame Relay и ATM (Asynchronous Transfer Mode);
- системы обнаружения и предотвращения атак и особенности их практического применения;
- обучение и сертификация специалистов по информационной безопасности.

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Лекция 1 учебного пособия посвящена основным понятиям и определениям, на основе которых базируется область информационной безопасности. Одним из таких основополагающих понятий является информация, которая выступает объектом защиты от возможных угроз безопасности. Именно поэтому необходимо в первую очередь рассмотреть основные виды информационных ресурсов, определенные в соответствии с российским законодательством.

1.1. Информация как основной объект защиты

В соответствии с Федеральным законом «Об информации, информатизации и защите информации» информационные ресурсы могут быть:

- открытыми, т.е. общедоступными (публикации, сообщения в СМИ, выступления на конференциях и выставках, интервью и т.п.);
- ограниченного доступа, т.е. охраняемыми, требующими защиты.

В свою очередь, информационные ресурсы ограниченного доступа подразделяются на ресурсы, составляющие государственную тайну (секретные), и конфиденциальные (от лат. confidentia — доверие).

Информационные ресурсы, составляющие государственную тайну, регламентируются Законом РФ «О государственной тайне» от 21 июля 1993 г. № 5485-1. Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации. Правила отнесения сведений, составляющих государственную тайну, к раз-

личным степеням секретности утверждены постановлением Правительства РФ от 4 сентября 1995 г. № 870.

К конфиденциальной информации в соответствии с Указом Президента РФ от 6 марта 1997 г. № 188 относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, составляющие тайну следствия и судопроизводства;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами. Эти сведения составляют служебную тайну;
- сведения, которые связаны с профессиональной деятельностью и доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных сообщений и т.д.);
- сведения, которые связаны с коммерческой деятельностью и доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами. Эти сведения составляют коммерческую тайну;
- сведения о существе изобретения (идеи, конструкторской разработки или промышленного образца) до официальной публикации информации о нем.

Под служебной тайной следует понимать несекретные сведения ограниченного доступа, связанные с владением и распоряжением интеллектуальной собственностью на информационные ресурсы в сфере управленческих или производственных отношений в государственных учреждениях, неправомерное оглашение (разглашение, утечка или несанкционированный доступ) которых может нанести ущерб интересам конкретного ведомства или учреждения.

Классификация информации по степени конфиденциальности и нормативные правовые акты, закрепляющие требования к обработке служебной информации, представлены на рис. 1.1.

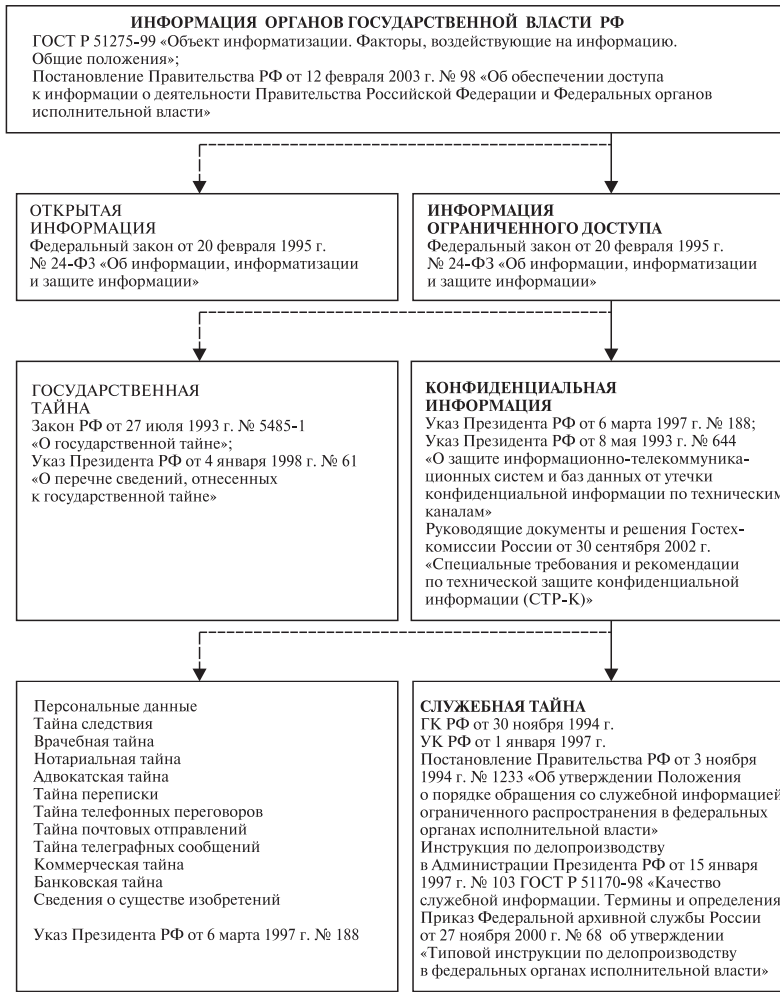

Рис. 1.1. Нормативно-правовые акты, закрепляющие требования к обработке служебной информации

Любой информационный ресурс хранится, обрабатывается или передается в рамках определенной автоматизированной системы, возможные характеристики которой будут рассмотрены ниже.

1.2. Автоматизированная система как среда для обработки, хранения и передачи информации

Автоматизированные системы представляют собой совокупность персонала и комплекса средств автоматизации его деятельности, реализующие информационную технологию выполнения установленных функций. Примерами АС могут являться локальные вычислительные сети, интернет-порталы, системы электронного документооборота и др. Основная задача АС заключается в поддержке бизнес-процессов организации посредством своевременного предоставления необходимых информационных ресурсов.

В общем случае АС можно представить в виде совокупности взаимодействующих узлов, таких как рабочие станции пользователей, серверы или коммуникационное оборудование. Каждый из них, в свою очередь, состоит из:

- аппаратного обеспечения, включающего технические средства узла, такие как сетевые адаптеры, процессоры, микросхемы плат и др.;
- общесистемного программного обеспечения, на котором функционирует операционная система узла и все ее составные модули;
- прикладного программного обеспечения, обеспечивающего решение прикладных задач, для которых предназначена АС.

На каждом из узлов АС могут храниться и обрабатываться информационные ресурсы, осуществить доступ к которым возможно через локальное или сетевое взаимодействие. В локальном варианте передача данных осуществляется при помощи элементов управления, непосредственно подключенных к узлам АС (например, консоли, клавиатуры, мыши и т.д.). При сетевом — обмен информацией производится по каналам связи. Сетевая передача данных может быть представлена в виде семиуровневой модели взаимодействия открытых систем (ВОС). Каждый уровень этой модели соответствует определенным функциям, реализация которых позволяет обеспечить эффективный обмен информацией (табл. 1.1).

Таблица 1.1

Функции семиуровневой модели взаимодействия открытых систем

Наименование уровня модели	Функции, которые реализуются на соответствующем уровне модели ВОС
Прикладной уровень	Реализуется программный интерфейс для доступа различных приложений к функциям передачи информации по каналам связи АС
Уровень представления	Определяется формат данных, которые будут передаваться между узлами АС по сети
Сеансовый уровень	Выполняются функции установления и закрытия логического соединения между узлами АС
Транспортный уровень	Реализуются функции управления сетевым соединением, по которому передаются данные между узлами АС
Сетевой уровень	Осуществляется управление сетевыми адресами узлов АС, а также обеспечивается фрагментация и сборка передаваемых пакетов данных
Канальный уровень	Обеспечивается преобразование данных в соответствующий формат физической среды передачи информации АС
Физический уровень	Обеспечивается передача информации через физическую среду передачи данных, в качестве которой могут выступать коаксиальные или оптоволоконные кабели, экранированные или неэкранированные витые пары, беспроводные каналы связи и др.

Хотелось бы заострить внимание на том, что при прохождении информации по каналам связи от одного узла к другому к ней последовательно применяются функции семи уровней модели ВОС, начиная с прикладного и заканчивая физическим. В процессе выполнения функций каждого уровня к информации добавляется служебный заголовок, содержащий информационные поля. Примерами таких полей могут служить адреса получателя и отправителя данных, объем передаваемых данных, тип режима передачи информации и др. При поступлении адресату информация также обрабатывается при помощи функций семи уровней модели ВОС, начиная с физического и заканчивая прикладным. При этом удаляются все служебные заголовки соответствующих

уровней, в результате чего она принимает первоначальный вид. Схематично процесс обработки информации при ее передаче от отправителя к получателю показан на рис. 1.2.

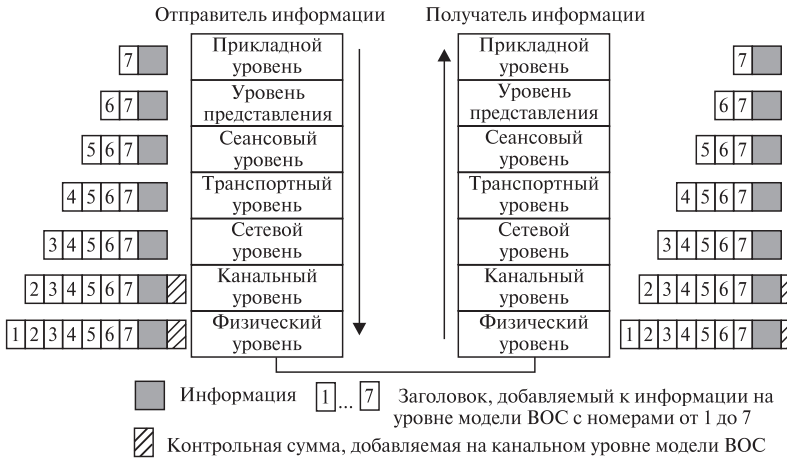

Рис. 1.2. Схема процесса преобразования информации при ее передаче по каналам связи

Необходимо отметить, что в настоящее время из всех известных вариантов сетевых протоколов, основанных на модели ВОС, наибольшее распространение получил стек TCP/IP, который используется более чем в 90% действующих локальных и территориально-распределенных сетях связи. Характерная особенность состоит в том, что он не использует ни функции уровня представления, ни сеансовый уровень модели ВОС. А поскольку в последующих лекциях учебного пособия речь будет идти только об АС, построенных на базе стека TCP/IP, эти два уровня модели ВОС в дальнейшем упоминаться не будут.

Существенным для функций модели ВОС является то, что реализованы они могут быть на уровне аппаратного, общесистемного или прикладного ПО АС. Причем для организации сетевого взаимодействия между узлами АС необязательно реализовывать функции всех уровней модели ВОС. Примеры того, какие функции тех или иных уровней модели ВОС используются узлами АС, отражены в табл. 1.2.

Таблица 1.2

Узлы АС, реализующие функции различных уровней модели ВОС

Тип узла	Физический уровень	Канальный уровень	Сетевой уровень	Транспортный уровень	Прикладной уровень
Повторитель	+	—	—	—	—
Коммутатор	+	+	—	—	—
Маршрутизатор	+	+	+	—	—
Автономная рабочая станция/сервер	—	—	—	—	—
Сетевая рабочая станция/сервер	+	+	+	+	+

Помимо уровней модели ВОС, уровней аппаратного, общесистемного и прикладного ПО, в АС присутствует также уровень информационных ресурсов, на котором хранятся, обрабатываются и передаются те или иные данные. Типы и формат информационных ресурсов этого уровня определяются составом и конфигурацией используемого аппаратного и программного обеспечения АС. Так, например, при использовании серверов СУБД в качестве информационных ресурсов могут выступать таблицы баз данных, а при использовании веб-серверов такими ресурсами могут быть гипертекстовые документы.

С учетом наличия модели ВОС и трехуровневой модели узлов концептуально АС представляется уже как множество узлов, способных взаимодействовать между собой по каналам связи. Этот тип концептуального ви́дения АС будет использован автором в последующих лекциях данного учебного пособия при описании информационных атак, а также средств защиты. Пример модели АС, состоящей из двух узлов, приведен на рис. 1.3.

Жизненный цикл любой АС включает, как правило, два этапа — технологический и эксплуатационный. На технологическом этапе осуществляются проектирование и разработка АС. На эксплуатационном выполняются настройка и штатное функционирование АС. На каждом из этапов жизненного цикла основным объектом защиты является информация, которая может передаваться по каналам связи или же находиться в состоянии хранения либо обработки в узлах АС.

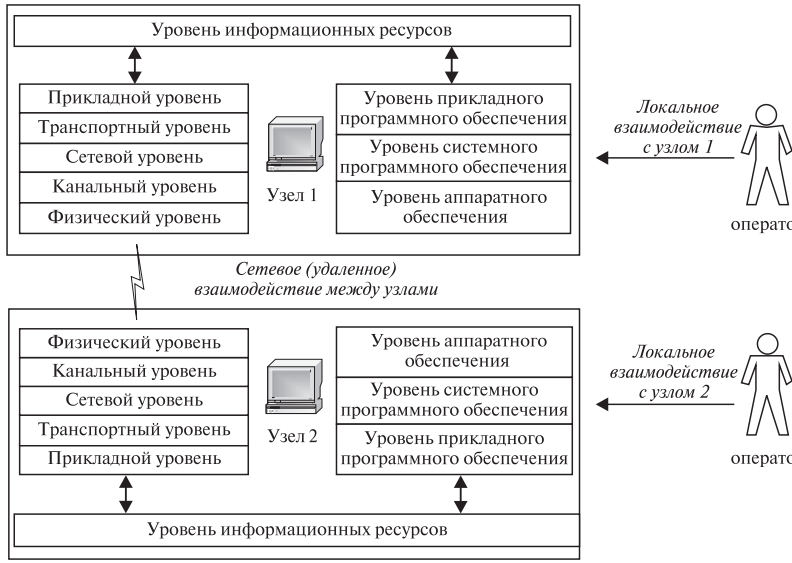

Рис. 1.3. Концептуальная модель АС, состоящей из двух узлов

По существу любая АС может быть подвергнута *информационной атаке*[1], или совокупному воздействию злоумышленника, направленному на нарушение одного из трех свойств информации — конфиденциальности, целостности или доступности. С учетом высокого уровня значимости рассмотрим их более подробно. Свойство *конфиденциальности* предполагает ограничение в праве на доступ к информации неполномочным лицам, логическим объектам или процессам. Характерным примером нарушения конфиденциальности информации является ее несанкционированное изъятие с целью дальнейшей перепродажи, использования ее во вред владельцу и т.п. *Целостность* информации подразумевает, что она не подвергалась изменению или уничтожению в результате несанкционированного доступа. В качестве примера нарушения этого свойства можно привести ситуацию, в которой злоумышленник преднамеренно искажает содержимое одного из электронных документов, хранящихся в системе. И наконец, свойство *доступ-*

[1] Иногда в литературе вместо понятия «информационная атака» используется синонимичный термин «вторжение» (от англ. intrusion).

ности информации говорит о том, что она может быть использована по запросу со стороны любого уполномоченного на это пользователя. Однако злоумышленник может нарушить доступность интернет-портала, в результате чего ни один из легальных пользователей уже не сможет воспользоваться его содержимым. Таким образом, в результате нарушения конфиденциальности, целостности или доступности информации злоумышленник может оказать отрицательное влияние на ход бизнес-процессов компании, базирующихся на информационных ресурсах, которые подверглись несанкционированному воздействию.

Однако стоит упомянуть о том, что для реализации информационной атаки нарушителю необходимо активизировать и использовать определенную *уязвимость* АС. Другими словами, ему необходимо найти то слабое место в АС, которое позволило бы успешно реализовать намеченную атаку. В перечень такого рода уязвимостей могут входить: некорректная конфигурация сетевых служб АС, наличие ПО без установленных модулей обновления, использование нестойких к угадыванию паролей, отсутствие необходимых средств защиты информации и др. Логическая взаимосвязь уязвимости, атаки и ее возможных последствий показана на рис. 1.4.

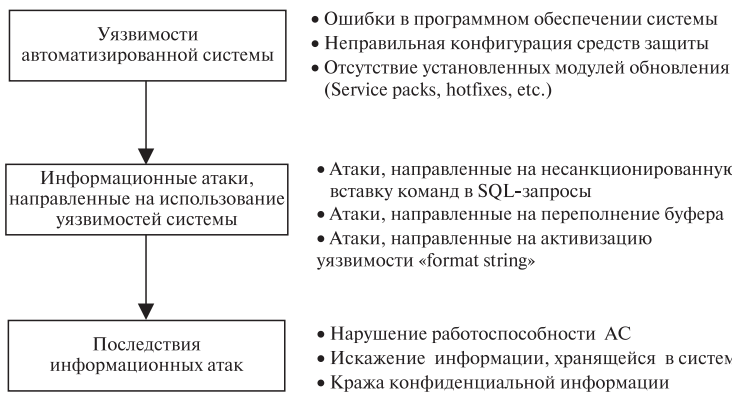

Рис. 1.4. Взаимосвязь уязвимости, атаки и ее возможных последствий

В последующих разделах лекции 1 приводится описание основных типов уязвимостей, информационных атак, а также их возможных последствий.

Сердюк, В. А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Текст] : учеб. пособие / В. А. Сердюк ; Гос. ун-т — Высшая школа экономики. — М. : Изд. дом Гос. ун-та — Высшей школы экономики, 2011. — 572, [4] с. — 1000 экз. — ISBN 978-5-7598-0698-1 (в пер.).

С32

Проблема защиты автоматизированных систем от информационных атак является одной из наиболее актуальных и значимых в ИТ-индустрии. В основу этого учебного пособия положен многолетний практический опыт проектирования, разработки и внедрения комплексных систем защиты от информационных атак. Особое внимание уделено средствам защиты, которые классифицируются как системы обнаружения атак и системы предотвращения атак. Учебное пособие включает лекционные материалы, охватывающие основные темы в области информационной безопасности: виды уязвимостей, информационных атак и их возможных последствий; математические модели защиты автоматизированных систем от информационных атак; практические аспекты проведения аудита и оценки рисков информационной безопасности; существующие криптографические методы защиты информационных ресурсов; технологии идентификации, аутентификации и авторизации пользователей информационных систем; информационная безопасность территориально-распределенных сетей связи X.25, Frame Relay и ATM; системы обнаружения и предотвращения атак и особенности их практического применения; обучение и сертификация специалистов по информационной безопасности.

Для студентов, изучающих курс «Организация и технологии защиты информации», а также всех интересующихся современными методами и средствами защиты от информационных атак.

УДК 65.39(075)
ББК 004.056.5

Учебное издание

Сердюк Виктор Александрович

Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий

Зав. редакцией *Е.А. Бережнова*
Редактор *З.А. Басырова*
Художественный редактор *А.М. Павлов*
Компьютерная верстка и графика: *О.А. Иванова*
Корректор *С.М. Хорошкина*

Подписано в печать 19.11.2010. Формат 60×88/16. Гарнитура Newton C
Печать офсетная. Усл.-печ. л. 34,9. Уч.-изд. л. 25,5
Тираж 1000 экз. Изд. № 1051

Государственный университет — Высшая школа экономики
125319, Москва, Кочновский проезд, д. 3
Тел./факс: (495) 772-95-71

ISBN 978-5-7598-0698-1