Московский государственный технический университет
имени Н.Э. Баумана

В.В. Бондарев

Введение в информационную безопасность автоматизированных систем

Учебное пособие

BAUMANPRESS
Москва
ИЗДАТЕЛЬСТВО
МГТУ им. Н. Э. Баумана
2016

УДК 681.326
ББК 67.408
Б81

Издание доступно в электронном виде на портале *ebooks.bmstu.ru*
по адресу: http://ebooks.bmstu.ru/catalog/117/book1425.html

Факультет «Информатика и системы управления»
Кафедра «Информационная безопасность»

Рекомендовано
Редакционно-издательским советом
МГТУ им. Н.Э. Баумана в качестве учебного пособия

Рецензент
канд. юрид. наук, доцент *Б.Н. Коробец*

Бондарев, В. В.

Б81 Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — Москва : Издательство МГТУ им. Н. Э. Баумана, 2016. — 250, [2] с. : ил.

ISBN 978-5-7038-4414-4

Рассмотрена законодательная база информационной безопасности, приведен перечень возможных угроз, отражены основные подходы к созданию систем защиты информации, представлена классификация предупредительных мер, изучены вопросы, связанные с программно-аппаратными механизмами обеспечения информационной безопасности.

Для студентов, обучающихся по направлению подготовки «Информационная безопасность», по специальности «Информационная безопасность автоматизированных систем» и слушателей факультета повышения квалификации. Может быть полезно студентам и аспирантам других специальностей, интересующимся современными средствами и методами обеспечения информационной безопасности.

УДК 681.326
ББК 67.408

ISBN 978-5-7038-4414-4

ПРЕДИСЛОВИЕ

Цель учебного пособия — ознакомление студентов с основами комплексного подхода к обеспечению информационной безопасности (ИБ) автоматизированных систем (АС), проблемами защиты информации и подходами к их решению.

В пособии рассмотрены:

- теоретические и правовые вопросы защиты информации и обеспечения безопасности АС;
- принципы построения комплексных систем защиты АС;
- основные направления деятельности служб технической защиты информации (подразделений обеспечения безопасности АС);
- современная технология обеспечения безопасности АС, предусматривающая рациональное распределение функций и организацию эффективного взаимодействия по вопросам защиты информации сотрудников всех подразделений, которые используют АС в процессе работы и гарантируют ее функционирование;
- вопросы разработки нормативно-методических и организационно-распорядительных документов, необходимых для реализации технологии обеспечения безопасности АС;
- разработка защищенных АС;
- проектирование системы управления информационной безопасностью АС;
- разработка модели угроз и модели нарушителя информационной безопасности АС;
- организация эксплуатации АС с учетом требований информационной безопасности;
- восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций.

Для лучшего усвоения материала студентам необходимо иметь представление о современных информационных технологиях и автоматизированных системах управления, о правовых, организационных и технических аспектах проблемы обеспечения информационной безопасности.

После изучения данного пособия студент должен

➤ *знать:*

- основные угрозы безопасности информации и модели нарушителя в АС;
- АС как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;

• содержание и порядок деятельности персонала по эксплуатации защищенных АС;

• законодательные акты в области защиты информации;

• основные задачи подразделения защиты информации;

• основные меры по защите информации в АС (организационные, правовые, программно-аппаратные, физические, технологические);

• основные защитные механизмы, применяемые в АС;

➤ *уметь:*

• разрабатывать модели угроз и нарушителей в АС;

• анализировать и оценивать риски информационной безопасности;

• разрабатывать структуру системы обеспечения безопасности АС;

• классифицировать уязвимости АС;

• правильно выбирать средства защиты АС;

➤ *иметь навыки:*

• использования основных защитных механизмов подсистем безопасности АС;

• разработки системы организационно-распорядительных и нормативно-методических документов по защите информации;

• определения требований к защите и категорирования ресурсов АС;

• применения штатных и дополнительных средств защиты информации от несанкционированного доступа (НСД);

• построения инфраструктуры управления событиями.

РАЗДЕЛ I

ОСНОВЫ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Глава 1. АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Автоматизированные системы, в состав которых входят информационные технологии (ИТ), основанные на новейших разработках в области средств вычислительной техники (СВТ) и связи, находят все более широкое применение практически во всех сферах жизни и деятельности (в отличие от индустриальных технологий, где основным объектом переработки являются сырье и материалы, информационные технологии «потребляют» и «перерабатывают» информацию). С развитием ИТ объемы обрабатываемой и передаваемой информации, как в абсолютных значениях, так и по отношению к объемам переработки сырья и материалов в индустриальных технологиях, непрерывно возрастают.

1.1. Место и роль автоматизированных систем в управлении бизнес-процессами

Почему же современные компьютеры и средства телекоммуникации так широко востребованы? Что они умеют делать, что становятся необходимыми практически везде? В ответ на эти вопросы, как правило, можно услышать: «Компьютеры позволяют автоматизировать умственный труд». Но разве физический труд они не автоматизируют и как объяснить понятие «умственный труд»?

Ответим на поставленные вопросы. Компьютерные технологии дают возможность автоматизировать процессы управления (умственный труд по управлению — по принятию решений в конкретных ситуациях на основе имеющейся информации). А поскольку управление необходимо везде, всегда и всем, то и средства автоматизации управления применяются повсеместно. Автоматизация на основе современных ИТ позволяет принимать решения более оперативно и

обоснованно, учитывая при этом большой объем сведений, повышая качество и эффективность управления — управления чем бы то ни было — от отдельных узлов и агрегатов (например, в автомобилях), деятельностью отдельных людей до технологических процессов на производстве, бизнес-процессов компаний, экономических и социально-политических процессов в обществе.

Широкое внедрение АС во все сферы жизни общества требует повышенного внимания к защите применяемых для автоматизации управления информационных технологий и непосредственно информации. Любые нарушения и неполадки в работе автоматизированных/информационных систем (ИС), систем обработки и передачи информации приводят к снижению качества или полной потере управления критичными процессами и, соответственно, к убыткам.

Следует отметить, что любая информационная система всегда является частью соответствующей системы управления, а любая автоматизированная информационная система (АИС) — частью автоматизированной системы управления (АСУ).

Практически каждое фундаментальное техническое или технологическое новшество, предоставляя возможности для решения каких-либо социальных проблем и открывая широкие перспективы для развития личности и общества, вызывает обострение существующих или порождает новые, ранее неизвестные, проблемы, становится источником новых потенциальных опасностей.

Без должного внимания к вопросам обеспечения безопасности последствия перехода общества к новым технологиям могут быть катастрофическими как для отдельных граждан, так и общества в целом. Именно так обстоит дело в области атомных, химических и других экологически опасных технологиях, в сфере транспорта.

Аналогичная ситуация и с информатизацией общества. Искажение или фальсификация, уничтожение или разглашение определенной части информации, а также дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах автоматизированного информационного взаимодействия.

Жизненно важные интересы этих субъектов, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их экономических, политических и других сфер деятельности, конфиденциальная коммерческая и персональная информация была бы легко доступна для пользователя и в то же время надежно защищена.

1.2. Обострение проблемы обеспечения безопасности автоматизированных систем на современном этапе

Актуальность проблемы защиты АС в современных условиях определяется следующими основными факторами:

• обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными (недостаточными) ограничениями на ее распространение и использование;

• расширением сферы применения электронно-вычислительных машин (ЭВМ), многообразием и повсеместным распространением информационно-управляющих систем, высокими темпами увеличения парка средств вычислительной техники и связи;

• повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности;

• вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса;

• концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях;

• количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;

• отношением к информации как к товару, переходом к рыночным отношениям в области предоставления информационных услуг;

• многообразием видов угроз и возникновением новых каналов несанкционированного доступа к информации;

• увеличением числа квалифицированных пользователей средствами вычислительной техники и возможностей по созданию ими нежелательных программно-математических воздействий на системы обработки информации;

• возрастанием уязвимости субъектов вследствие увеличения потерь от уничтожения, фальсификации, разглашения или незаконного тиражирования информации;

• развитием рыночных отношений в сфере ИТ (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты).

Проблема обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более обостряется по следующим объективным п р и ч и н а м:

• *расширение сферы применения СВТ и возросший уровень доверия к автоматизированным системам управления и обработки информации.* С помощью компьютерных систем выполняют самую ответственную работу, от которой зависит жизнь и благосостояние многих людей. Автоматизированные системы позволяют управлять технологическими процессами на предприятиях и атомных электростанциях (АЭС), движением самолетов и поездов, выполнять финансовые операции, обрабатывать секретную и конфиденциальную информацию;

• *изменение подхода к самому понятию «информация»*. Данный термин все чаще используется для обозначения особого товара, стоимость которого нередко превышает стоимость автоматизированной системы, в рамках которой он существует;

• *переход к рыночным отношениям* в области создания и предоставления информационных услуг с присущей этим отношениям *конкуренцией и промышленным шпионажем*;

• *развитие и распространение информационно-телекоммуникационных сетей, территориально распределенных систем и систем с удаленным доступом* как совместно используемых ресурсов;

• *распространение компьютерной грамотности* в широких слоях населения из-за доступности СВТ и прежде всего персональных компьютеров (ПК), что вызвало увеличение числа попыток неправомерного вмешательства в работу государственных и коммерческих АСУ как случайных, так и умышленных;

• *отсутствие стройной и непротиворечивой системы законодательно-правового регулирования отношений* в сфере накопления, использования и защиты информации создает условия для возникновения и широкого распространения «компьютерного хулиганства» и «компьютерной преступности»;

• *бурное развитие и широкое распространение компьютерных вирусов*, способных скрытно существовать в системе и совершать любые несанкционированные действия;

• *наличие злоумышленников — специалистов-профессионалов в области вычислительной техники и программирования*, досконально знающих все достоинства и слабые места АС и занимающихся анализом и взломом механизмов защиты.

Исследование в области информационной безопасности, проведенное английской консалтинговой компанией «Ernst & Young» в России и странах СНГ, показало, что более 65 % российских компаний сталкивались с нарушениями информационной безопасности, при этом в 50 % случаев данные нарушения были вызваны хакерскими атаками, в том числе с проникновением в информационную систему извне, несанкционированным доступом непосредственно в компании, атаками, имеющими целью вызвать отказ в обслуживании, саботажем, финансовым мошенничеством и хищением коммерческой информации.

Проблема обеспечения безопасности АС относится к числу трудноразрешимых, что связано со следующими объективными обстоятельствами:

• недостаточным (неадекватным реалиям) пониманием необходимости защиты используемых АС;

• высокой степенью неопределенности рисков при применении новейших АС;

• сложностью АС как объектов защиты;

• необходимостью комплексного подхода к защите АС с учетом их значительной зависимости от человеческого фактора;

• сложностью разрешения конфликтов интересов между различными категориями субъектов (операторами информационных систем, системными и сетевыми администраторами, администраторами безопасности, пользователями, обслуживающим персоналом систем и менеджерами различных уровней);

• отставанием методов и средств защиты от развития информационных технологий, а также методов и средств нападения;

• недостатком квалифицированных специалистов в сфере компьютерной безопасности и низким уровнем компьютерной культуры пользователей (слабой осведомленностью в вопросах безопасности ИТ).

1.3. Защита автоматизированных систем как процесс управления рисками

Создание абсолютно непреодолимой системы защиты принципиально невозможно. До тех пор пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить полностью. При достаточном количестве времени и средств можно преодолеть любую защиту, поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности, соответствующий реально существующим угрозам (рискам).

Под *угрозой* обычно понимают потенциально возможное событие, вызванное действием, процессом или явлением, которое может (воздействуя на что-либо) привести к нанесению ущерба чьим-либо интересам.

Риск — это оценка опасности определенной угрозы.

Риск выражает вероятностно-стоимостную оценку возможных потерь (ущерба) и характеризуется:

• вероятностью успешной реализации угрозы;

• стоимостью потерь (ущерба) в случае реализации угрозы.

Стоимостную составляющую информационной безопасности хорошо иллюстрирует упрощенная формула оценки издержек, связывающая количественные характеристики рисков, стоимость реализации мер защиты и суммарные издержки:

$$R = \sum_{i=1}^{n} (A_i B_i + C_i) < R_{\max},$$

где n — количество рисков (угроз); A — вероятностная оценка риска (0-1); B — стоимостная оценка риска; C — стоимость реализации мер защиты; $R_{\max}$ — допустимые издержки.

Анализ рисков заключается в выявлении существующих угроз и оценке их опасности. На этапе анализа рисков выявляют все значимые угрозы, т. е. угрозы, характеризующиеся большой частотой (вероятностью) реализации и/или приводящие к существенным (ощутимым) потерям.

Суть защиты ресурсов АС — управление рисками, связанными с использованием этих АС.

Известно два основных подхода к анализу рисков — качественный и количественный. Наиболее привлекательным, на первый взгляд, является количественный подход, позволяющий сравнивать защищенность различных систем, но его внедрение осложнено следующими причинами:

- отсутствием достоверной статистики в быстро меняющемся мире ИТ;
- трудностью оценки ущерба по нематериальным активам (репутация, конфиденциальность сведений, идеи, бизнес-планы, здоровье персонала);
- сложностью оценки косвенных потерь от реализации угроз;
- обесцениванием результатов длительной количественной оценки рисков из-за постоянной модификации и реконфигурации АС.

В связи с этим для анализа рисков в настоящее время используется качественный подход, предусматривающий простое ранжирование угроз и связанных с ними рисков по степени их опасности.

Управление рисками предполагает принятие мер защиты (контрмер), направленных на снижение частоты успешной реализации угроз и/или ущерба в случае их реализации. Защитные меры выбирают на основе принципа разумной достаточности (экономической целесообразности, сопоставимости возможного ущерба и затрат на защиту), исходя из минимизации общих издержек — затрат на защиту и остаточных потерь от угроз.

Существует несколько вариантов противодействия выявленным рискам (угрозам):

1) признание допустимости риска от конкретной угрозы (например, если вероятность реализации угрозы ничтожна мала или затраты на защиту от нее катастрофически велики);

2) частичная передача ответственности за инциденты в сфере безопасности ИТ сторонней организации (например, страховой компании);

3) проведение комплекса мероприятий (мер противодействия), позволяющих уменьшить или полностью исключить риск.

Основные этапы анализа рисков и управления ими:

- определение границ системы и методологии оценки рисков;
- идентификация и оценка информационных ресурсов системы (ценностей);
- идентификация угроз и оценка вероятностей их реализации;
- определение риска и выбор средств защиты;
- внедрение средств защиты и оценка остаточного риска.

1.4. Методы оценки целесообразности затрат на обеспечение безопасности

К методу оценки целесообразности затрат на обеспечение безопасности АС предъявляются определенные требования:

- метод должен обеспечивать количественную оценку затрат на безопасность АС, используя качественные показатели оценки вероятностей событий и их последствий;

• быть прозрачным с точки зрения пользователя и давать возможность вводить собственные эмпирические данные;

• быть универсальным, т. е. одинаково применимым к оценке затрат на приобретение аппаратных средств, специализированного и универсального программного обеспечения, затрат на услуги, перемещение персонала, обучение конечных пользователей и т. д.;

• позволять моделировать ситуацию, при которой существует несколько контрмер, направленных на предотвращение определенных угроз, в разной степени влияющих на сокращение вероятности происшествия.

Перечислим категории затрат, связанных с безопасностью АС.

Организационные затраты на формирование и поддержание звена управления системой защиты информации включают следующие статьи расходов:

• формирование политики безопасности АС;

• приобретение и ввод в эксплуатацию программно-технических средств (серверов, компьютеров конечных пользователей — настольных и переносных), периферийных устройств и сетевых компонентов;

• приобретение и настройку средств защиты информации;

• содержание персонала (стоимость работ и аутсорсинг).

Затраты на контроль — определение и подтверждение достигнутого уровня защищенности ресурсов АС — состоят из следующих позиций:

• контроль реализации функций, обеспечивающих управление безопасностью АС;

• организация взаимодействия между подразделениями для решения конкретных задач по обеспечению безопасности АС;

• проведение аудита безопасности по каждой части АС;

• материально-техническое обеспечение системы контроля доступа к объектам и ресурсам;

• плановые проверки и испытания средств защиты информации;

• проверка навыков эксплуатации средств защиты персоналом;

• создание условий для нормальной работы лицам, ответственным за реализацию конкретных процедур безопасности по подразделениям;

• контроль правильности ввода данных в прикладных системах;

• оплата труда инспекторов по контролю выполнения требований, предъявляемых к средствам защиты при разработке систем (контроль на стадии проектирования и спецификации требований);

• внеплановые проверки и испытания (оплата труда испытательного персонала специализированных организаций; обеспечение испытательного персонала материально-техническими средствами);

• контрольно-проверочные мероприятия, связанные с лицензионно-разрешительной деятельностью в сфере безопасности АС.

Внутренние затраты на ликвидацию последствий нарушений политики безопасности АС, т. е. пересмотр политики безопасности АС (проводится периодически):

• идентификация угроз безопасности АС;

• поиск уязвимостей системы безопасности АС;

• оплата труда специалистов, выполняющих работы по определению возможного ущерба и переоценке степени риска;

• ликвидация последствий нарушения режима безопасности;

• восстановление системы безопасности АС до соответствия требованиям политики безопасности;

• установка патчей или приобретение последних версий программных средств защиты информации;

• приобретение новых технических средств взамен пришедших в негодность;

• проведение дополнительных испытаний и проверок технологических информационных систем;

• утилизация скомпрометированных ресурсов;

• восстановление информационных ресурсов — баз данных и прочих информационных массивов;

• проведение мероприятий по контролю достоверности данных, подвергшихся атаке на целостность;

• выявление причин нарушения политики безопасности — проведение расследований нарушений политики безопасности АС (сбор данных о способах совершения неправомерного деяния, поиск предметов посягательства, выявление мотивов неправомерных действий и т. д.);

• обновление планов обеспечения непрерывности деятельности службы безопасности;

• переделки — внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности АС;

• повторные проверки и испытания системы безопасности АС.

Внешние затраты на ликвидацию последствий нарушения политики безопасности АС объединяют следующие позиции:

• невыполнение обязательств перед государством и партнерами;

• юридическое сопровождение и выплата компенсаций;

• проведение дополнительных исследований и разработка новой рыночной стратегии;

• отказ от организационных, научно-технических или коммерческих решений, ставших неэффективными в результате утечки сведений, разработка новых средств ведения конкурентной борьбы;

• потери от снижения приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения;

• заработная плата служащих, организационные и прочие расходы, непосредственно связанные с предупредительными мероприятиями;

• другие виды возможного ущерба, в том числе невозможность выполнения функциональных задач.

Затраты на техническое обслуживание системы безопасности ИТ, т. е. на мероприятия по предотвращению нарушений политики безопасности ИТ (предупредительные мероприятия) включают следующие статьи:

• управление системой безопасности ИТ;

• планирование системы безопасности ИТ;

• изучение возможностей инфраструктуры по обеспечению безопасности ИТ;

• техническая поддержка персонала при внедрении средств защиты информации и процедур, а также планов по безопасности ИТ;

• проверка сотрудников на лояльность, выявление угроз безопасности ИТ;

• организация системы допуска исполнителей и сотрудников к защищаемым ресурсам;

• регламентное обслуживание средств защиты информации;

• обслуживание и настройка программно-технических средств защиты информации, операционных систем (ОС) и сетевого оборудования;

• организация сетевого взаимодействия и безопасного использования ИС;

• поддержание системы резервного копирования и ведения архива данных;

• проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, СВТ и т. п.;

• аудит системы безопасности ИТ — контроль изменений состояния информационной среды и действий исполнителей;

• обеспечение соответствия используемых ИТ заданным требованиям по безопасности, совместимости и надежности, в том числе анализ возможных негативных аспектов ИТ, влияющих на целостность и доступность;

• доставка (обмен) конфиденциальной информации;

• удовлетворение субъективных требований пользователей (стиль, удобство интерфейса и др.);

• обеспечение соответствия требованиям стандартов;

• повышение квалификации сотрудников по вопросам использования имеющихся средств защиты, выявления и предотвращения угроз безопасности ИТ;

• развитие нормативной базы и технической оснащенности подразделения безопасности.

Приведенный перечень затрат на обеспечение высокоэффективной системы защиты информации указывает на высокую стоимость компьютерной безопасности. Излишние меры безопасности, помимо экономической неэффективности, приводят к созданию дополнительных неудобств и недовольству персонала. Важно правильно выбрать тот необходимый и достаточный уровень защиты, при котором соотношение затрат на контрмеры и размер возможного ущерба были бы приемлемыми.

1.5. Особенности современных автоматизированных систем как объектов защиты

Большинство современных автоматизированных систем обработки информации представляют собой территориально распределенные системы интенсивно взаимодействующих (синхронизирующихся) между собой по данным (ресурсам) и управлению (событиям) локальных вычислительных сетей (ЛВС) и отдельных ЭВМ.

В распределенных АС возможны все «традиционные» для локально расположенных (централизованных) вычислительных систем способы несанкционированного вмешательства в их работу и доступа к информации, а также

характерные только для них специфические каналы проникновения в систему, что объясняется целым рядом их о с о б е н н о с т е й , среди которых:

• территориальная разнесенность компонентов АС и наличие интенсивного обмена информацией между ними;

• широкий спектр способов представления, хранения и передачи информации;

• интеграция данных, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в удаленных узлах сети;

• абстрагирование владельцев данных от физических структур и места размещения данных;

• использование режимов распределенной обработки данных;

• участие в процессе автоматизированной обработки информации большого количества пользователей и персонала;

• непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей;

• разнородность средств вычислительной техники и связи, а также их программного обеспечения;

• отсутствие специальных средств защиты в большинстве типов технических средств, широко используемых в АС.

* * *

Трудности решения практических задач обеспечения безопасности конкретных АС связаны с отсутствием развитой стройной теории и необходимых научно-технических и методических основ обеспечения защиты информации в современных условиях.

Применяемые в настоящее время большинством организаций меры не обеспечивают необходимого уровня безопасности субъектов, участвующих в процессе информационного взаимодействия, и не способны в необходимой степени противостоять разного рода воздействиям в целях доступа к критичной информации и дезорганизации работы автоматизированных систем.

Контрольные вопросы

1. Охарактеризуйте место и роль автоматизированных систем в управлении бизнес-процессами.

2. Какие факторы определяют актуальность проблемы защиты АС в современных условиях?

3. Перечислите особенности современных автоматизированных систем как объектов защиты.

4. Назовите причины обострения проблемы обеспечения информационной безопасности.

5. Почему проблема обеспечения безопасности АС относится к числу трудноразрешимых?

6. Что понимается под риском информационной безопасности? Каковы составляющие риска?

7. В чем заключается анализ рисков и управление ими? Перечислите этапы анализа и управления.

8. Каковы требования к методам оценки целесообразности затрат на обеспечение безопасности АС?

9. Назовите категории затрат, связанных с безопасностью АС; кратко охарактеризуйте каждую категорию и перечислите статьи расходов для каждой из них.

ГЛАВА 2. ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Прежде всего, необходимо понять, что же такое безопасность АС и определить *что (кого), от чего (от кого), почему (зачем), как (в какой степени и какими средствами) надо защищать*. Получив четкие ответы на данные вопросы, можно правильно сформулировать общие требования к системе обеспечения безопасности АС и перейти к обсуждению проблем построения соответствующих систем защиты. Основные понятия безопасности и их взаимосвязь приведены в ГОСТ Р ИСО/МЭК15408-1–2012 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий».

2.1. Определение безопасности автоматизированных систем

Что же такое безопасность вообще и безопасность АС в частности? Нередко можно слышать, что безопасность — это отсутствие опасностей. Данное определение не совсем верно, поскольку полностью устранить все возможные опасности нельзя.

Безопасность — это защищенность от опасностей, более точно, защищенность от возможного ущерба, наносимого при реализации этих опасностей (угроз).

Различают материальный, моральный и физический ущерб. Ущерб может быть причинен как напрямую, так и косвенно. *Субъектами нанесения ущерба, в конечном счете, всегда являются люди*. Даже если пострадают материальные объекты или информационные ресурсы, косвенный ущерб, проблемы возникнут у пользователей, каким-либо образом связанных с этими объектами или заинтересованных в их сохранности и целостности. И чем с бóльшим числом объектов человека что-то связывает, тем в большей опасности для косвенного нанесения ущерба он находится.

Косвенный ущерб интересам пользователя может быть нанесен либо путем сбоя нормального функционирования автоматизированной системы, либо за счет нарушения необходимых свойств отдельных компонентов и ресурсов АС, среди которых не только непосредственно информация, но и ее носители (устройства хранения, обработки, передачи данных), а также процессы обработки и передачи информации.

Под *автоматизированной системой обработки информации* будем понимать организационно-техническую систему, представляющую собой совокупность следующих взаимосвязанных компонентов (рис. 2.1), объединенных по организационно-структурному, тематическому, технологическому или иным основаниям для выполнения автоматизированной обработки информации (данных) в целях удовлетворения информационных потребностей субъектов информационных отношений:

- технических средств обработки и передачи данных (средств вычислительной техники и связи);
- методов и алгоритмов обработки данных в виде программного обеспечения;
- информации (массивов, наборов, баз данных) на различных носителях;
- обслуживающего персонала и пользователей системы.

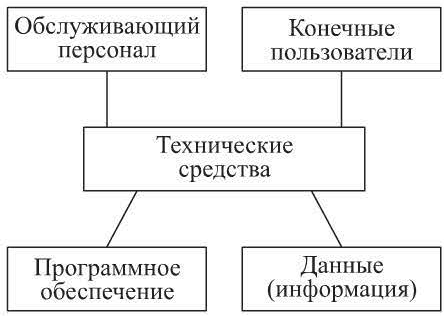

Рис. 2.1. Основные компоненты АС

Под *обработкой информации* в АС будем понимать любую из операций (прием, накопление, хранение, преобразование, отображение, передача и т. п.), осуществляемых над информацией (сведениями, данными) с использованием средств АС.

Безопасность автоматизированной системы (системы обработки информации, компьютерной системы) — защищенность всех ее компонентов (технических средств, программного обеспечения, данных, пользователей и персонала) от разного рода нежелательных для соответствующих субъектов воздействий. Отметим, что пользователи и персонал системы также являются заинтересованными в обеспечении безопасности субъектами (внутренними).

Необходимо различать понятия «информационная безопасность» и «безопасность информации», которые до недавнего времени воспринимались как синонимы.

Под *информационной безопасностью* понимается защищенность общества и личности от деструктивного информационного воздействия (пропаганды, агрессивной рекламы, низкопробных видов искусства и т. п.), а под *безопасностью информации* — состояние защищенности информации от угроз.

2.2. Информация и информационные ресурсы

Информация — это сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах, характеристиках) в некоторой предметной

области, необходимые для оптимизации принимаемых решений в процессе управления этими объектами.

Приведем наиболее важные с в о й с т в а и н ф о р м а ц и и:

• *существование в виде данных* (в кодированном виде) — информация может быть представлена в разных формах в виде совокупностей некоторых кодовых знаков (символов, знаков, сигналов и т. п.) на носителях различных типов. Информация — это смысл (семантика), а данные — код, носитель смысла (синтаксис);

• *неисчерпаемость* ресурса — при копировании информации ничего не убывает;

• потенциальная *полезность* при монопольном владении, позволяющая получить определенную выгоду в экономической, политической, военной или иной области (отсюда и смысл введения ограничений на распространение данной информации, т. е. тайны);

• *доступность* — свойство системы (средств и технологий обработки, инфраструктуры, в которой циркулирует информация), характеризующее способность обеспечивать своевременный доступ субъектов к интересующей их информации и соответствующим автоматизированным службам всегда, когда в этом возникает необходимость (готовность к обслуживанию поступающих от субъектов запросов);

• *целостность* — существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);

• *конфиденциальность* — субъективно определяемая (приписываемая собственником) характеристика информации, которая указывает на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемую способностью системы (инфраструктуры) сохранять указанную информацию в тайне от субъектов, не имеющих прав на доступ к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

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

2.3. Субъекты информационных отношений, их безопасность

В процессе деятельности субъекты могут находиться друг с другом в разного рода отношениях, в том числе касающихся вопросов получения, хранения, обработки, распространения и использования определенной информации. Такие отношения между субъектами называют *информационными отношениями*, а самих участвующих в них субъектов — *субъектами информационных отношений*.

К субъектам информационных отношений относят:

• государство в целом или отдельные его ведомства, органы и организации;

• общественные или коммерческие организации (объединения) и предприятия (юридические лица);

• граждан (физических лиц).

Различные субъекты по отношению к определенной информации могут (возможно, одновременно) выступать в р о л и :

• источников (поставщиков) информации;

• потребителей (пользователей) информации;

• собственников, владельцев, обладателей, распорядителей информации и систем ее обработки;

• физических и юридических лиц, о которых собирается информация;

• участников процессов обработки и передачи информации и т. д.

Для успешной деятельности по управлению объектами некоторой предметной области субъекты информационных отношений заинтересованы в обеспечении следующих в о з м о ж н о с т е й :

• *своевременный доступ* (за приемлемое для них время) к необходимой информации и определенным автоматизированным службам (услугам);

• *конфиденциальность* (сохранение в тайне) определенной части информации;

• *достоверность* (полнота, точность, адекватность, целостность) информации и защита от навязывания ложной (недостоверной, искаженной) информации, т. е. от дезинформации;

• *защита от незаконного тиражирования* (защита авторских прав, прав интеллектуальной собственности, прав собственника информации);

• *разграничение ответственности* за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

• *возможность* осуществления *непрерывного контроля и управления* процессами обработки и передачи информации и т. д.

В процессе осуществления перечисленных возможностей субъект информационных отношений становится уязвимым, т. е. потенциально подверженным нанесению ему ущерба (прямого или косвенного, морального или материального) посредством либо воздействия на критичную для него информацию, ее носители и процессы обработки либо посредством неправомерного использования такой информации.

В связи с этим все субъекты информационных отношений в той или иной степени (в зависимости от размеров ущерба, который им может быть нанесен) заинтересованы в обеспечении своей информационной безопасности.

Поскольку в плане информационной безопасности ущерб субъектам информационных отношений может быть нанесен только опосредованно, через определенную информацию и ее носители, закономерно возникает и интерес к защите носителей, процессов и систем обработки информации.

Отсюда следует, что в качестве *объектов, подлежащих защите* в целях обеспечения безопасности субъектов информационных отношений, должны рассматриваться: информация, любые ее носители (отдельные компоненты и АС в целом) и процессы ее обработки (передачи).

Вместе с тем, говоря о защите АС, всегда следует помнить, что уязвимыми, в конечном счете, являются именно заинтересованные в обеспечении определенных свойств информации и систем ее обработки субъекты (информация, равно как и средства ее обработки, не имеет своих интересов, которые можно было бы ущемить). Поэтому под *безопасностью АС* или циркулирующей в ней информации понимают косвенное обеспечение безопасности соответствующих субъектов, участвующих в процессах автоматизированного информационного взаимодействия.

Поскольку субъектам информационных отношений ущерб может быть нанесен также посредством воздействия на процессы и средства обработки критичной для них информации, становится очевидной необходимость обеспечения защиты системы обработки и передачи данной информации от несанкционированного вмешательства в процесс ее функционирования, а также от попыток хищения, незаконной модификации и/или разрушения любых компонентов данной системы.

Для защиты субъектов от пиратства и разграничения их ответственности необходимо обеспечивать следующие с в о й с т в а информационной инфраструктуры:

- *неотказуемость* субъектов от выполненных критичных действий;
- *защиту от неправомерного тиражирования* открытой информации.

2.4. Цель защиты автоматизированной системы и циркулирующей в ней информации

При рассмотрении проблемы обеспечения компьютерной, информационной безопасности следует всегда исходить из того, что защита информации и системы ее обработки не является самоцелью.

Цель обеспечения безопасности АС — защита внешних и внутренних субъектов, которые участвуют в процессах информационного взаимодействия, от нанесения им материального, морального или иного ущерба в результате случайных или преднамеренных нежелательных воздействий на информацию и системы ее обработки и передачи.

Цель защиты циркулирующей в АС информации — предотвращение утечки, искажения, утраты, блокирования или незаконного тиражирования информации.

Для выполнения перечисленных целей создают препятствия для любого несанкционированного вмешательства в процесс функционирования АС, попыток хищения, модификации, выведения из строя или разрушения ее компонентов, т. е. защиту всех компонентов АС (оборудования, программного обеспечения, данных и персонала).

В этом смысле защита информации от несанкционированного доступа — только часть общей проблемы обеспечения безопасности компьютерных систем и защиты законных интересов субъектов информационных отношений, а сам термин НСД точнее было бы трактовать не как «несанкционированный доступ» (к информации), а шире, — как «несанкционированные (неправомерные) действия», наносящие ущерб субъектам информационных отношений.

* * *

С развитием возможностей новых информационных технологий компьютерным системам поручается решение все более объемных, сложных, важных и ответственных задач, поэтому актуальность проблемы обеспечения безопасности применяемых информационных технологий в дальнейшем будет только возрастать.

Контрольные вопросы

1. Что понимается под безопасностью вообще и безопасностью АС в частности?
2. Дайте определение АС и безопасности АС.
3. Приведите определения информации и информационных ресурсов.
4. Перечислите категории субъектов информационных отношений.
5. Охарактеризуйте три свойства информации — конфиденциальность, целостность и доступность.
6. Сформулируйте цели защиты АС и циркулирующей в ней информации.

Глава 3. УГРОЗЫ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Один из важнейших аспектов проблемы обеспечения безопасности АС — определение, анализ и классификация возможных угроз безопасности АС. Перечень значимых угроз, оценка вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа рисков и формулирования требований к системе защиты АС.

3.1. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем

Автоматизированная система состоит из следующих основных структурно-функциональных э л е м е н т о в :

• *рабочих станций* — отдельных ЭВМ (персональных ЭВМ — ПЭВМ) или терминалов сети, на которых реализуются автоматизированные рабочие места (АРМ) пользователей (абонентов, операторов);

• *серверов* или *host-машин* (служб файлов, печати, баз данных и т. п.) не выделенных (или выделенных, т. е. не совмещенных с рабочими станциями)

высокопроизводительных ЭВМ, предназначенных для реализации функций хранения, печати данных, обслуживания рабочих станций сети и других действий;

• *сетевых устройств* (маршрутизаторов, коммутаторов, шлюзов, центров коммутации пакетов, коммуникационных ЭВМ) — элементов, обеспечивающих соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, возможно имеющих различные протоколы взаимодействия;

• *каналов связи* (локальных, телефонных, с узлами коммутации и т. д.).

Рабочие станции — наиболее доступный компонент сетей, поэтому именно с них могут быть предприняты попытки совершения несанкционированных действий. С рабочих станций осуществляется ввод имен и паролей пользователями, управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На мониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Поэтому рабочие станции должны иметь средства защиты от доступа посторонних лиц, нарушения нормальной настройки (конфигурации) рабочих станций и режимов их функционирования, вызванные неумышленным вмешательством неопытных (невнимательных) пользователей, а также средства разграничения доступа законных пользователей, имеющих разные полномочия.

Особой защиты требуют серверы (host-машины) и сетевые устройства: первые — как концентраторы больших объемов информации, вторые — как элементы, в которых осуществляется преобразование (возможно через открытую, незашифрованную форму представления) данных при согласовании протоколов обмена в различных участках сети. Благоприятным для повышения безопасности серверов и мостов обстоятельством является возможность их надежной защиты физическими средствами и организационными мерами в силу их выделенности, позволяющей сократить до минимума число лиц из персонала, имеющих к ним непосредственный доступ. Все более распространенными становятся массированные атаки на работу различных подсистем рабочих станций, серверов и мостов с применением средств удаленного доступа, которые используют недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам и системным таблицам. Применяться могут все возможности и средства — от стандартных (без модификации компонентов) до подключения специальных аппаратных средств (каналы, как правило, слабо защищены от подключения) и применения специальных программ для преодоления системы защиты.

Возможно и непосредственное внедрение аппаратных и программных закладок в мосты и серверы, открывающее широкие дополнительные возможности по несанкционированному удаленному доступу. Закладки могут быть внедрены как с удаленных станций (посредством вирусов или иным способом),

так и непосредственно в аппаратуру и программы серверов при их ремонте, обслуживании, модернизации, переходе на новые версии программного обеспечения, смене оборудования.

Каналы и средства связи также нуждаются в защите. В силу большой пространственной протяженности линий связи (через неконтролируемую или слабо контролируемую территорию) практически всегда существует возможность подключения к ним, либо вмешательства в процесс передачи данных.

3.2. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений

Определение основных терминов, связанных с обеспечением безопасности АС, приведены в ГОСТ Р 50922–2006.

Угроза интересам субъектов информационных отношений — потенциально возможное событие, вызванное действием, процессом или явлением, которое посредством воздействия на информацию, ее носители и процессы обработки может привести к ущемлению интересов определенных субъектов.

Нарушением безопасности (нарушением, атакой) называют реализацию угрозы безопасности (наступление соответствующего события).

В силу особенностей современных АС существует значительное число различных видов угроз безопасности субъектов информационных отношений.

Различают два типа угроз безопасности:

1) несанкционированное распространение сведений — *утечка информации* (разглашение, разведка, несанкционированный доступ к информации);

2) несанкционированное воздействие на информацию и ее носители — *воздействие на информацию* с нарушением установленных прав и/или правил на изменение информации. Несанкционированное воздействие бывает *целенаправленным* (искажение, уничтожение, копирование, блокирование, утрата, сбой функционирования носителя информации) и *непреднамеренным* (ошибки пользователей и персонала, сбои и отказы техники, природные явления, другие случайные воздействия).

Разглашение информации — действие, в результате которого информация становится известной неконтролируемому числу лиц.

Разведка — целенаправленная деятельность по добыванию сведений в интересах информационного обеспечения военно-политического руководства другого государства либо конкурирующей организации.

Разведка может быть агентурной и технической. *Агентурная разведка* ведется оперативниками (лица, состоящие в штате оперативного подразделения государственного органа или негосударственной структуры) с привлечением агентов (лица, конфиденциально сотрудничающие с разведывательной структурой) и специалистов (лица, обладающие специальными знаниями, умениями и навыками, привлекаемые в целях оказания содействия в сборе, исследовании, оценке и использовании фактической информации). Среди

оперативников различают агентуристов, сотрудников, добывающих сведения лично, сотрудников подразделений наружного наблюдения, сотрудников оперативно-технических подразделений, оперативников-аналитиков.

Под *технической разведкой* понимается целенаправленная деятельность по добыванию с помощью технических систем, средств и аппаратуры сведений в интересах информационного обеспечения военно-политического руководства другого государства или конкурирующей организации, подготовки и ведения информационной борьбы. Источником данной угрозы является деятельность иностранных разведывательных и специальных служб (органов), иностранных общественных организаций (в том числе коммерческих), а также деятельность отечественных преступных группировок и отдельных лиц.

Руководящими документами ФСТЭК России предусматривается многоуровневая классификация технических разведок. Наиболее часто на практике применяют два классификационных признака: 1) физический принцип построения аппаратуры разведки; 2) местонахождение носителей разведывательной аппаратуры.

Главные отличия разведки от разглашения заключаются в том, что информацией, добытой с помощью разведки, владеет ограниченный круг лиц. Разведка, как правило, ведется с враждебными целями, тогда как разглашение может таких целей и не преследовать. Разведка всегда ведется умышленно, а разглашение нередко бывает следствием неосмотрительности лица-носителя информации.

Под *несанкционированным доступом к информации* понимают действие, в результате которого нарушены правила разграничения доступа, и информацией завладело лицо, не имеющее соответствующего права. Результатом НСД не обязательно становится утечка информации, несанкционированный доступ может совершаться в целях активного воздействия на информацию, получения незаконных привилегий, удовлетворения амбиций и т. п. НСД может быть следствием как умышленных, так и неумышленных (ошибки в организации защиты информации, недостаточная квалификация персонала и т. д.) действий. Очевидно, что элементы НСД присутствуют и при ведении разведки, и при несанкционированном воздействии на информацию. В то же время разведка (например, путем сбора открытых сведений) и несанкционированное воздействие могут осуществляться без НСД к информации или ее носителю.

Несанкционированное воздействие на информацию и ее носитель можно классифицировать следующим образом:

• *модификация информации* — осуществляется, как правило, без предварительного ознакомления, иначе будет иметь место утечка. Возможна модификация как следующий шаг после организации утечки. Различают следующие виды модификации информации:

– *уничтожение* — наблюдается при хакерском проникновении в вычислительные системы, при стихийных бедствиях и т. д.;

— *искажение* — если злоумышленник получил доступ к каналу передачи информации, но не может ознакомиться с самой информацией, например

вследствие ее зашифрованности, то он может попытаться внести в нее ложные данные в целях нанесения ущерба владельцу. Искажение также может возникать непреднамеренно как следствие помех в канале передачи;

— *подделка* — широко используется при фальсификации банковских операций, осуществляемых в электронном виде;

• *блокирование доступа к информации* — встречается в том случае, когда злоумышленник не может сам воспользоваться информацией, но имеет доступ к средствам ее обработки и своими (в том числе, несознательными) действиями препятствует, в том числе временно, законному владельцу обрабатывать эту информацию. Например, спамминг — рассылка «почтовых бомб» по электронной почте. Почтовый ящик владельца оказывается забит информационным мусором, из-за которого тот не может принять полезные сообщения;

• *хищение носителя* (даже если это не привело к утечке информации, например, вследствие ее зашифрованности, само по себе хищение способно лишить законного владельца возможности обрабатывать информацию);

• *утрата носителя* — отличается от хищения непредумышленным характером действия.

Появление новых научно-технических разработок может привести к возникновению принципиально новых видов угроз и способов преодоления систем безопасности, НСД к данным и дезорганизации работы АС.

3.3. Классификация угроз безопасности

Основными источниками угроз безопасности АС и информации (угроз интересам субъектов информационных отношений) являются:

• *стихийные бедствия* (наводнение, ураган, землетрясение, пожар и т. п.);

• *аварии, сбои и отказы оборудования* (технических средств) АС;

• *ошибки проектирования и разработки компонентов АС* (аппаратных средств, технологии обработки информации, программ, структур данных и т. п.);

• *ошибки эксплуатации* (пользователей, операторов и другого персонала);

• *преднамеренные действия нарушителей и злоумышленников* (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т. п.).

Источники угроз безопасности по отношению к АС могут быть как внешними, так и внутренними (например, компоненты самой АС — аппаратура, программы, персонал, конечные пользователи).

Потенциальные угрозы по источнику возникновения подразделяют на естественные (объективные) и искусственные (субъективные).

Естественные угрозы — вызваны воздействиями на АС и ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека; *искусственные угрозы* — связаны с деятельностью человека.

Различают *непреднамеренные (неумышленные, случайные)* угрозы и *преднамеренные (умышленные)* искусственные угрозы.

Непреднамеренные искусственные угрозы. Случайные угрозы возможны из-за ошибок в проектировании АС и ее элементов, ошибок в программном обеспечении, в действиях персонала и т. п.

К основным непреднамеренным искусственным угрозам АС (действиям, совершаемым людьми случайно — по незнанию, невнимательности или халатности, из любопытства, но без злого умысла) относят:

- частичный или полный отказ системы или разрушение аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т. п.);
- неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависание или зацикливание) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т. п.);
- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др.), не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей, с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- заражение компьютера вирусами;
- неосторожные действия, приводящие к разглашению конфиденциальной информации;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. п.);
- проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и информации;
- игнорирование установленных правил при работе в системе;
- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т. п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

Преднамеренные искусственные угрозы. Умышленные угрозы связаны с корыстными, идейными или иными устремлениями людей (злоумышленников).

Возможны следующие способы умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

• физическое разрушение системы (взрыв, поджог и т. п.) или вывод из строя отдельных наиболее важных компонентов системы (устройств, носителей важной системной информации и т. п.);

• отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т. п.);

• дезорганизация функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т. п.);

• внедрение агентов в число персонала системы (в том числе, в административную группу, отвечающую за безопасность);

• вербовка (путем подкупа, шантажа и т. п.) персонала или отдельных пользователей, имеющих определенные полномочия;

• применение подслушивающих устройств, дистанционной фото- и видеосъемки и т. п.;

• перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, системы пожарно-охранной сигнализации, видеонаблюдения и т. п.) и инженерные коммуникации (системы отопления, кондиционирования, заземления и т. п.);

• перехват данных, передаваемых по каналам связи, и их анализ в целях выяснения протоколов обмена, правил вхождения в сеть и авторизации пользователей и последующих попыток их имитации для проникновения в систему;

• хищение носителей информации (дисков, флеш-карт и т. п.);

• несанкционированное копирование носителей информации;

• хищение производственных отходов (распечаток, записей и т. п.);

• чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств или из областей оперативной памяти операционной системой в асинхронном режиме, используя недостатки мультизадачных ОС и систем программирования;

• незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, по халатности пользователей, подбором, имитацией интерфейса системы и т. д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);

• несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т. п.;

• вскрытие шифров криптозащиты информации;

• внедрение аппаратных «спецвложений», программных закладок и вирусов («троянских коней» и «жучков»), т. е. таких участков программ, которые позволяют преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам в целях регистрации и передачи критичной информации или дезорганизации функционирования системы;

• незаконное подключение к линиям связи для работы «между строк» с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений, или в целях прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Заметим, что обычно для достижения поставленной цели злоумышленник использует не один, а несколько из перечисленных способов дезорганизации работы.

3.4. Классификация каналов проникновения в автоматизированную систему и утечки информации

По способу проникновения в систему различают прямые и косвенные каналы. Использование *косвенных* каналов не требует проникновения в помещения, где расположены компоненты системы. Для *прямых* каналов такое проникновение необходимо (при этом возможно два варианта: без внесения изменений в компоненты системы или с изменениями компонентов).

По типу основного средства реализации угрозы каналы условно разделяют на три группы (в зависимости от объекта воздействия: программа, оборудование, персонал).

Классификация видов нарушений работоспособности систем и несанкционированного доступа к информации по объектам воздействия и способам нанесения ущерба безопасности приведена в табл. 3.1.

По способу получения информации потенциальные каналы подразделяют следующим образом:

• *физический*;

• *электромагнитный* (перехват излучений);

• *информационный* (программно-математический).

По способу осуществления воздействия различают контактный и бесконтактный НСД.

Контактный НСД (физический, программно-математический) предусматривает реализацию угроз путем доступа к элементам АС, носителям информации, самой вводимой и выводимой информации (и результатам), программному обеспечению (в том числе к операционным системам), а также подключением к линиям связи.

При бесконтактном НСД (например, по электромагнитному каналу) возможные угрозы информации реализуются перехватом излучений аппаратуры АС, в том числе наводимых в токопроводящих коммуникациях и цепях питания, перехватом информации в линиях связи, вводом в линии связи ложной информации, визуальным наблюдением (фотографированием) устройств отображения информации, прослушиванием переговоров персонала АС и пользователей.

Таблица 3.1

Классификация нарушений работоспособности АС по объектам воздействия и способам нанесения ущерба

Способ нанесения ущерба	Объект воздействий			
	Оборудование	Программа	Данные	Персонал
Утечка информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкционированное копирование, перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, «спецвложения», изменение режимов работы, несанкционированное использование ресурсов	Внедрение «троянских коней» и «жучков»	Искажение, модификация	Вербовка персонала, «маскарад»
Нарушение работоспособности автоматизированной системы	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование информации	Изготовление аналогов без лицензий	Использование незаконных копий	Публикация без ведома авторов	—

3.5. Неформальная модель нарушителя

Нарушения и преступления, в том числе компьютерные, совершаются людьми. Следуя известному выражению: «Бывают «виртуальные преступления», но «виртуальных преступников» не бывает», можно утверждать, что

вопросы безопасности автоматизированных систем во многом по своей сути являются вопросами человеческих отношений и человеческого поведения.

Современные исследования проблемы обеспечения безопасности компьютерных систем направлены на изучение природы фактов нарушения целостности и конфиденциальности информации, дезорганизации работы компьютерных систем. В процессе анализа статистики нарушений, а также вызывающих их причин, сути применяемых нарушителями приемов и средств, которые используют недостатки систем и средств их защиты, и ряда других вопросов можно построить *модель потенциального нарушителя*.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т. п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Зная причины нарушений, можно либо повлиять на сами эти причины (конечно, если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

Нарушитель — это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, в целях самоутверждения и т. п.) и использующее для этого различные возможности, методы и средства.

Заметим, что при отсутствии правил (запретов и ограничений) не существует и нарушителей (если нет правил, значит, нечего нарушать), поэтому борьбу с нарушениями следует начинать с установления четких правил (ограничений, политики безопасности).

Злоумышленник — это нарушитель, намеренно (умышленно, со злым умыслом) идущий на нарушение.

При построении модели нарушителя обычно формулируются предположения:

- о *категориях* лиц, к которым может принадлежать нарушитель;
- *мотивах* действий нарушителя и преследуемых им целях;
- *квалификации* нарушителя и его технической оснащенности (используемые для совершения нарушения методы и средства);
- характере возможных действий нарушителей.

По отношению к АС нарушители могут быть внутренними (из числа обслуживающего персонала и пользователей системы) или внешними (посторонними лицами).

Внутренним нарушителем может быть лицо из следующих категорий сотрудников:

- конечные пользователи (операторы) системы;
- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения ПО (прикладные и системные программисты);
- сотрудники службы безопасности АС;
- руководители различных уровней.

Внешние нарушители могут быть из числа категорий:

• технического персонала сторонних организаций, обслуживающих здания и СВТ (уборщики, электрики, сантехники, ремонтники и другие сотрудники, имеющие доступ в здания и помещения, где расположены компоненты АС);

• клиентов (представители сторонних организаций и отдельные граждане);

• посетителей (приглашенные по какому-либо поводу);

• представителей организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т. п.);

• представителей конкурирующих организаций, в том числе иностранных спецслужб или лиц, действующих по их заданию;

• лиц, случайно или умышлено нарушивших пропускной режим (без цели нарушить безопасность АС);

• любых лиц за пределами контролируемой территории.

Среди основных м о т и в о в совершения нарушений выделяют: безответственность, вандализм, месть, идейные соображения и др.

При нарушениях, вызванных халатностью, пользователь производит какие-либо разрушающие действия, не связанные со злым умыслом, обычно это следствие некомпетентности или небрежности.

Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, затевая своего рода игру «пользователь против системы» либо ради утверждения в собственных глазах, либо в глазах коллег.

Нарушение безопасности АС может быть связано с принуждением (шантаж, угроза), местью, идейными соображениями или корыстными интересами пользователя системы. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой информации и другим ресурсам АС.

По уровню знаний об АС нарушителей классифицируют следующим образом:

• знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;

• обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;

• обладает высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;

• знает структуру, функции и механизм действия средств защиты, их «сильные» и «слабые» стороны.

По уровню возможностей применения средств и методов различают нарушителей:

• использующих только агентурные методы получения сведений;

• пассивные средства (технические средства перехвата без модификации компонентов системы);

• штатные средства и недостатки системы защиты для ее преодоления (несанкционированные действия с помощью разрешенных средств), а также ком-

пактные магнитные носители информации, которые можно скрытно пронести через пост охраны;

• методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и специальных инструментальных и технологических программ).

Существует также классификация нарушителей в зависимости от времени (в процессе функционирования АС или в период неактивности компонентов системы) и места действия (как без доступа на территорию организации или в здания и сооружения, так и с доступом либо на территорию, либо в здание, в зону хранилищ данных (серверов баз данных, архивов и т. п.), либо в зону управления средствами обеспечения безопасности АС).

При анализе возможных действий нарушителей учитывают также дополнительные ограничения, связанные с работой по подбору кадров и проведением специальных мероприятий, затрудняющих создание коалиций нарушителей, т. е. объединения (сговора) двух и более лиц.

Определение точных характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенную с учетом особенностей конкретной предметной области и технологии обработки информации, можно представить перечислением нескольких критериев, для каждого из которых оценив количество сотрудников организации, попадающих в данную категорию.

Пользователи системы и обслуживающий ее персонал, с одной стороны, являются составной частью, необходимым элементом АС, а с другой — основным источником угроз и движущей силой нарушений и преступлений.

На круговой диаграмме (рис. 3.1) приведены результаты анализа нарушений и проблем с ИТ, проведенного Институтом компьютерной безопасности (США), из которых видно, что более половины (55 %) проблем возникает из-за ошибок пользователей и обслуживающего персонала системы. К этому следует добавить нарушения со стороны обиженных (9 %) и нечестных (10 %) сотрудников организаций. На вирусы приходится 4 % и всего лишь 2 % — на внешние нападения; отказы и сбои в работе системы, включая проблемы электропитания, составляют 20 %.

Согласно одному из обзоров журнала The Economist (Великобритания), информационная безопасность — одна из самых приоритетных проблем для 78 %

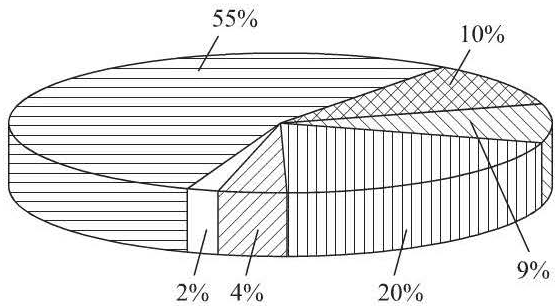

Рис. 3.1. Анализ нарушений и проблем с ИТ

из 254 опрошенных по всему миру первых лиц компаний, причем бóльшую часть проблем (83 %) создают сами сотрудники корпораций.

Сотрудники компании являются самой массовой категорией нарушителей в силу их многочисленности, наличия у них санкционированного доступа на территорию, в помещения и к ресурсам системы, разнообразия мотивов совершения разного рода небезопасных действий. Причем подавляющее большинство нарушений со стороны сотрудников неумышленного характера. Однако, ущерб, который они при этом наносят компании, весьма значителен. Именно поэтому борьба с ошибками пользователей и обслуживающего персонала АС — одно из основных направлений работы по обеспечению безопасности.

* * *

Итак, цель защиты ИТ — минимизация рисков для субъектов. Защита (обеспечение безопасности) ИТ — это непрерывный процесс управления рисками, связанный с выявлением информационных активов (ценностей), подлежащих защите, определением стоимости этих активов, размеров ущерба и риска, разработкой плана действий по защите и выбором технологий, реализующих этот план.

На практике это означает сведение всех значимых для субъектов угроз к допустимому (приемлемому) уровню остаточного риска и защиту наиболее важных (критичных) информационных ресурсов, исходя из существующих возможностей и предоставленных финансовых средств.

Уязвимыми являются буквально все основные структурно-функциональные элементы современных АС. Защищать компоненты АС необходимо от всех видов воздействий: стихийных бедствий и аварий, сбоев и отказов технических средств, ошибок персонала и пользователей, ошибок в программах и от преднамеренных действий злоумышленников.

Имеется широчайший спектр вариантов преднамеренного или случайного несанкционированного доступа к данным и вмешательства в процессы обработки и обмена информацией (в том числе, управляющей согласованным функционированием различных компонентов сети).

Правильно построенная модель нарушителя, в которой отражаются его практические и теоретические возможности, время, место действия и другие характеристики — важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

Контрольные вопросы

1. Дайте определение понятий «угроза», «уязвимость» и «атака».
2. Какие классификационные схемы угроз ИБ вам известны?
3. Перечислите источники угроз ИБ.
4. Назовите каналы проникновения в автоматизированную систему и утечки информации.
5. Какие факторы лежат в основе формирования модели нарушителя?
6. Каковы цели разработки моделей угроз и нарушителей?
7. В чем разница между нарушителем и злоумышленником?

Глава 4. МЕРЫ И ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

В данной главе рассмотрены меры противодействия угрозам безопасности АС (контрмеры), а также основные принципы построения систем защиты информации. Здесь будет дан ответ на вопрос: «Как защищать ресурсы АС?»

4.1. Виды мер противодействия угрозам безопасности

По способам осуществления меры защиты информации, а также ее носителей и систем обработки подразделяют на следующие виды:

- законодательные;
- морально-этические;
- организационные;
- физические;
- технические (аппаратные и программные).

Законодательные меры включают в себя указы, постановления, законы, руководящие документы и другие нормативно-правовые акты, которые определяют нормы обращения с информацией, права и обязанности участников информационных отношений и устанавливают ответственность за несоблюдение данных норм.

Морально-этические меры предполагают соблюдение норм поведения, которые традиционно сложились в обществе или формируются по мере распространения информационных технологий. Данные нормы не обязательны к применению, как требования нормативных актов, однако, их несоблюдение может нередко привести к снижению престижа компании.

Организационные меры — меры административного характера, которые устанавливают правила функционирования системы обработки данных и деятельности обслуживающего персонала, а также порядок их взаимодействия для снижения вероятности осуществления угроз безопасности или потерь в случае их реализации. К организационным мерам относят надлежащую охрану территории объекта, соблюдение требований разграничения доступа, формирование дисциплины и ответственности сотрудников и др.

Технологические меры предусматривают такие технологические решения и приемы, которые основаны на принципе избыточности (структурной, функциональной, информационной, временно́й и т. п.) и направлены на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках мандатного доступа (например, двойной ввод ответственной информации, инициализация ответственных операций только при наличии разрешений от нескольких должностных лиц, процедура проверки соответствия реквизитов исходящих и входящих сообщений в системах коммутации сообщений, периодическое подведение общего баланса всех банковских счетов и т. п.).

Меры физической защиты на основе механических, электромеханических и электронно-механических устройств позволяют создавать физические препят-

ствия на возможных путях проникновения потенциальных нарушителей к компонентам системы. К данному виду относят установку средств визуального наблюдения охранной сигнализации и контроля физической целостности компонентов АС (наличие пломб, наклеек и т. п.), проверку поступающего оборудования, установку средств защиты от перебоев в электроснабжении и помех в линиях связи.

Технические меры защиты предполагают использование электронных устройств и программ для осуществления функции идентификации пользователей, разграничения доступа к информации, блокирования системы при НСД и др.

Взаимосвязь рассмотренных видов мер обеспечения безопасности приведена на рис. 4.1, а их достоинства и недостатки — в табл. 4.1.

Таблица 4.1

Достоинства и недостатки различных видов мер защиты

Меры	Достоинства	Недостатки
Законодательные и морально-этнические	• Определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение. • Универсальны — применимы для всех каналов НСД. • Единственно применимы: — при защите открытой информации от незаконного тиражирования; — при защите от злоупотребления служебным положением при работе с информацией	Требуют проведения постоянной разъяснительной работы с пользователями и обслуживающим персоналом АС
Организационные	• Играют значительную роль в обеспечении безопасности компьютерных систем. • Единственно применимы, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. • Необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей	• Низкая надежность без соответствующей поддержки физическими, техническими и программными средствами. • Большой объем рутинной деятельности. • Необходимо поддерживать более надежными физическими и техническими мерами
Физические и технические	• Устраняют недостатки организационных мер. • Поставят прочные барьеры на пути злоумышленников. • В максимальной степени исключают возможность неумышленных (по ошибке или халатности) нарушений регламента со стороны персонала и пользователей АС	Сложность осуществления (электронные и магнитные карты с личными данными можно потерять, пароли вычислить, электронную цифровую подпись подделать)

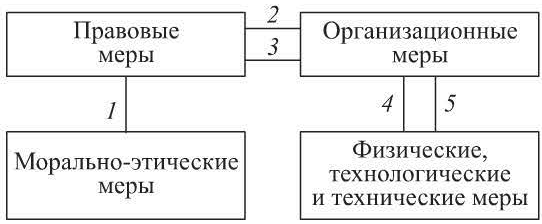

Рис. 4.1. Взаимосвязь мер обеспечения информационной безопасности:

1 — нормативные и организационно-распорядительные документы составляются на основе норм морали и этики, существующих в обществе; *2* — организационные меры обеспечивают исполнение нормативных актов с учетом правил поведения, принятых в стране и/или организации; *3* — организационные меры требуют разработки нормативных и организационно-распорядительных документов, не противоречащих нормам правовых мер; *4* — для эффективного применения организационные меры должны быть поддержаны физическими и техническими средствами; *5* — применение технических мер требует проведения соответствующих организационных мер

Рассмотрим известное утверждение о том, что создание абсолютно надежной системы защиты принципиально невозможно.

Если допустить возможность создания идеально надежных физических и технических средств защиты, перекрывающих все уязвимые каналы, то всегда остается возможность воздействия на персонал системы, осуществляющий необходимые действия по обеспечению корректного функционирования этих средств — администратора АС, администратора безопасности и т. п. Вместе с самими средствами защиты эти люди образуют так называемое «ядро безопасности». В этом случае стойкость системы безопасности будет определяться стойкостью персонала из «ядра безопасности» системы, и повышать ее можно только за счет организационных (кадровых) мероприятий, законодательных и морально-этических мер.

Но даже совершенные законы и оптимальная кадровая политика не могут до конца решить проблему защиты, поскольку, во-первых, сложно найти персонал, в котором можно быть абсолютно уверенным и в отношении которого невозможно было бы предпринять действия, вынуждающие его нарушить запреты; а во-вторых, даже абсолютно надежный человек может допустить случайное, неумышленное нарушение.

4.2. Принципы построения системы обеспечения безопасности информации в автоматизированной системе

Построение системы обеспечения безопасности информации в АС и ее функционирование осуществляют в соответствии со следующими п р и н ц и п а м и :

- законность;
- системность;
- комплексность;
- своевременность;
- непрерывность;

- преемственность и непрерывное совершенствование;
- разделение функций;
- разумная достаточность;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- взаимодействие и координация;
- обязательность контроля.

Рассмотрим перечисленные принципы более подробно.

Законность предполагает проведение защитных мероприятий и разработку системы безопасности информации в организации в соответствии с действующим законодательством в области информации, информационных технологий и защиты информации, других нормативно-правовых актов, руководящих и нормативно-методических документов по безопасности информации, утвержденных органами государственной власти в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.

Системность заключается в учете всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, которые имеют существенное значение для решения проблемы обеспечения безопасности информации в организации.

В соответствии с данным принципом при создании системы защиты учитывают все наиболее уязвимые места АС, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и НСД к информации. При этом учитываются не только известные каналы проникновения и несанкционированного доступа к информации, но и возможности появления принципиально новых путей реализации угроз безопасности.

Комплексность использования методов и средств защиты компьютерных систем состоит в согласованном применении разнообразных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей «слабых» мест на стыках ее отдельных частей.

Внешняя защита обеспечивается физическими, организационными, технологическими и правовыми мерами.

Внутренняя защита, учитывающая особенности предметной области, реализуется на уровне операционных систем СВТ в силу того, что ОС — это та часть компьютерной системы, которая управляет всеми ее ресурсами.

Своевременность предполагает применение мер обеспечения безопасности информации упреждающего характера, т. е. параллельно с разработкой и

развитием самой защищаемой системы. Это позволяет учитывать требования безопасности при проектировании архитектуры и создавать более защищенные системы.

Непрерывность защиты информации заключается в регулярном проведении мероприятий по обеспечению защиты системы и принятии необходимых мер по противодействию угрозам безопасности на всех этапах жизненного цикла АС, начиная со стадии проектирования.

Поскольку большинство физических и технических средств защиты для эффективного выполнения своих функций нуждается в постоянной организационной (административной) поддержке (своевременной смене и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределении полномочий и т. п.), перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов защиты, внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

Преемственность и совершенствование — это улучшение организационных и технических решений средств защиты информации на основе анализа функционирования АС и ее системы защиты с учетом последних изменений методов и средств воздействия на компоненты АС, нормативных требований по защите, современного отечественного и зарубежного опыта в этой области.

Разделение функций предполагает мандатный доступ к информации, в соответствии с которым ни один сотрудник организации не имеет полномочий, позволяющих ему единолично проводить критичные операции. Все такие операции должны выполняться по частям различными сотрудниками. Кроме того, предпринимаются дополнительные меры по недопущению сговора и разграничению ответственности между этими сотрудниками.

Разумная достаточность (экономическая целесообразность, сопоставимость возможного ущерба и затрат) состоит в соответствии уровня затрат на обеспечение безопасности информации возможному ущербу от ее разглашения или уничтожения.

Высокоэффективная система защиты требует больших затрат, использует при работе существенную часть ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям, поэтому важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были соразмерными (задача анализа риска).

Персональная ответственность предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий.

В соответствии с этим принципом распределение прав и обязанностей сотрудников устроено таким образом, чтобы в случае нарушения круг виновных был четко очерчен или сведен к минимуму.

Минимизация полномочий означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью,

т. е. в объеме, необходимом сотруднику для выполнения его должностных обязанностей.

Взаимодействие и сотрудничество заключается в создании благоприятной атмосферы в коллективе, чтобы сотрудники осознанно соблюдали установленные правила и оказывали содействие в деятельности подразделений обеспечения безопасности информации.

Гибкость системы защиты предполагает варьирование уровней защищенности, поскольку принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты.

Данный принцип особенно актуален в случаях, когда средства защиты устанавливают на функционирующую систему и при этом требуется сохранять процесс ее нормальной работы. Кроме того, внешние условия и требования с течением времени изменяются.

Открытость алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Но знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это не означает, что информация о конкретной системе защиты должна быть общедоступна.

Простота применения средств защиты подразумевает, что их использование не должно быть связано со знанием специальных языков или выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей.

Научная обоснованность и техническая реализуемость заключается в том, что средства защиты должны отвечать современному уровню развития науки и техники.

Специализация и профессионализм предполагают привлечение к разработке и реализации средств защиты специализированных организаций, имеющих опыт работы и государственные лицензии на право оказания услуг в области обеспечения безопасности ИТ. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионалами (специалистами подразделений обеспечения безопасности информации).

Взаимодействие и координация состоят в слаженной работе всех подразделений организации, а также сторонних структур, имеющих авторизованный доступ к АС и специализирующихся в области защиты информации.

Обязательность контроля заключается в своевременном выявлении и пресечении попыток нарушения установленных правил обеспечения безопасности информации с использованием систем и средств защиты информации при непрерывном совершенствовании критериев и методов оценки их эффективности.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты осуществляется на основе применения средств оперативного контроля и регистрации и охватывает как несанкционированные, так и санкционированные действия пользователей.

* * *

Таким образом, специалисты по информационной безопасности располагают широким спектром защитных мер: законодательных, морально-этических, административных (организационных), физических и технических. Предпринимаемые меры имеют как достоинства, так и недостатки, которые необходимо знать и правильно учитывать при создании систем защиты.

Все известные каналы проникновения и утечки информации должны быть перекрыты с учетом анализа риска, вероятностей реализации угроз безопасности в конкретной прикладной системе и обоснованного рационального уровня затрат на защиту.

Наилучшие результаты достигаются при системном подходе к вопросам безопасности компьютерных систем и комплексном использовании различных мер защиты на всех этапах жизненного цикла системы, начиная с самых ранних стадий ее проектирования.

Контрольные вопросы

1. Перечислите основные виды мер противодействия угрозам безопасности АС (контрмер).
2. Охарактеризуйте каждую меру противодействия.
3. Какая мера противодействия является, на ваш взгляд, наиболее важной, а какая — второстепенной?
4. Перечислите достоинства и недостатки различных мер защиты.
5. Возможно ли создание идеально надежной системы защиты?
6. Перечислите основные принципы построения систем защиты информации. Какие из них, по вашему мнению, являются важнейшими? Кратко охарактеризуйте каждый принцип.

Глава 5. ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Современный этап развития системы обеспечения информационной безопасности государства и общества характеризуется переходом от тотального сокрытия большого объема сведений к гарантированной защищенности принципиально важных данных, обеспечивающей:

- конституционные права и свободы граждан, предприятий и организаций в сфере информатизации;
- необходимый уровень безопасности информации, подлежащей защите;
- защищенность систем формирования и использования информационных ресурсов (технологий, систем обработки и передачи данных).

В *Стратегии развития информационного общества в Российской Федерации*, утвержденной Указом Президента РФ от 07.02.2008 № 212 одной из основных задач, требующих решения для формирования и развития инфор-

мационного общества в России, значится противодействие использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам России при реализации следующих мер:

• создание единой системы информационно-телекоммуникационного обеспечения нужд государственного управления, обороны страны, национальной безопасности и правопорядка;

• совершенствование правоприменительной практики в области противодействия угрозам использования информационно-телекоммуникационных технологий во враждебных целях;

• обеспечение неприкосновенности частной жизни, личной и семейной тайны, соблюдение требований по обеспечению безопасности информации ограниченного доступа;

• противодействие распространению идеологии терроризма и экстремизма, пропаганде насилия.

В *Стратегии национальной безопасности Российской Федерации до 2020 года*, утвержденной Указом Президента Российской Федерации от 12.05.2009 № 537, отмечено, что государственная политика Российской Федерации в области национальной безопасности обеспечивается согласованными действиями всех элементов системы обеспечения национальной безопасности при координирующей роли Совета Безопасности Российской Федерации за счет реализации комплекса мер организационного, нормативно-правового и информационного характера (помимо указанных в Стратегии развития):

• совершенствования безопасности функционирования информационно-телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации;

• повышения уровня защищенности корпоративных и индивидуальных информационных систем;

• создания единой системы информационно-телекоммуникационной поддержки нужд системы обеспечения национальной безопасности.

Меры нормативно-правовой поддержки регулирования вопросов информатизации и защиты информации в Российской Федерации определяются на основании:

• Конституции Российской Федерации;

• международных договоров и соглашений;

• законов Российской Федерации;

• указов и распоряжений Президента Российской Федерации;

• постановлений и распоряжений Правительства Российской Федерации;

• технических регламентов;

• национальных (государственных) стандартов и стандартов организаций;

• нормативно-правовых актов (положения, порядки, руководства, концепции и другие нормативные и методические документы) уполномоченных федеральных органов исполнительной власти.

Федеральные законы и нормативно-правовые акты Российской Федерации предусматривают:

• лицензирование деятельности предприятий, учреждений и организаций в области защиты информации;

• сертификацию средств защиты информации и средств контроля эффективности защиты, используемых в АС;

• аттестацию АИС, обрабатывающих информацию с ограниченным доступом на соответствие требованиям по безопасности информации при проведении работ со сведениями соответствующей степени конфиденциальности;

• возложение решения вопросов организации лицензирования, аттестации и сертификации на органы государственного управления в пределах их компетенции, определенной законодательством РФ;

• создание АИС в защищенном исполнении и специальных подразделений, обеспечивающих защиту информации с ограниченным доступом, являющейся собственностью государства, а также осуществление контроля защищенности информации и предоставление прав запрещать или приостанавливать обработку информации в случае невыполнения требований по обеспечению ее защиты;

• определение прав и обязанностей субъектов в области защиты информации.

5.1. Защищаемая информация

Согласно *Доктрине информационной безопасности Российской Федерации*, утвержденной Указом Президента Российской Федерации от 09.09.2000 № 1895, под *информационной безопасностью* Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Требования по защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности страны — Федеральной службой безопасности (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации — Федеральной службой по техническому и экспортному контролю (ФСТЭК России), в пределах их полномочий.

В области обеспечения безопасности информации в ключевых системах информационной инфраструктуры ФСТЭК России разработала следующие нормативно-методические документы:

• Приказ от 14.03.2014 г. N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;

• Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры;

• Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры;

• Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры;

• Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры;

• Положение о реестре ключевых систем информационной инфраструктуры.

В *Конституции РФ*, а также в *Декларации прав и свобод человека и гражданина Российской Федерации* определено, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29).

Ограничения этого права могут устанавливаться законом только в целях охраны личной, семейной, профессиональной, коммерческой и государственной тайны, а также нравственности.

В Федеральном законе «*Об информации, информационных технологиях и о защите информации*» от 27.07.2006 № 149-ФЗ даны определения информации, информационных технологий, информационной системы, информационно-телекоммуникационной сети и другие, определены права и обязанности обладателя информации.

Закон предусматривает разделение информации на категории свободного и ограниченного доступа (право на тайну). В свою очередь информацию ограниченного доступа подразделяют на информацию, отнесенную к государственной тайне, и конфиденциальную (рис. 5.1).

Условия отнесения информации к сведениям, составляющим коммерческую, служебную или иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение

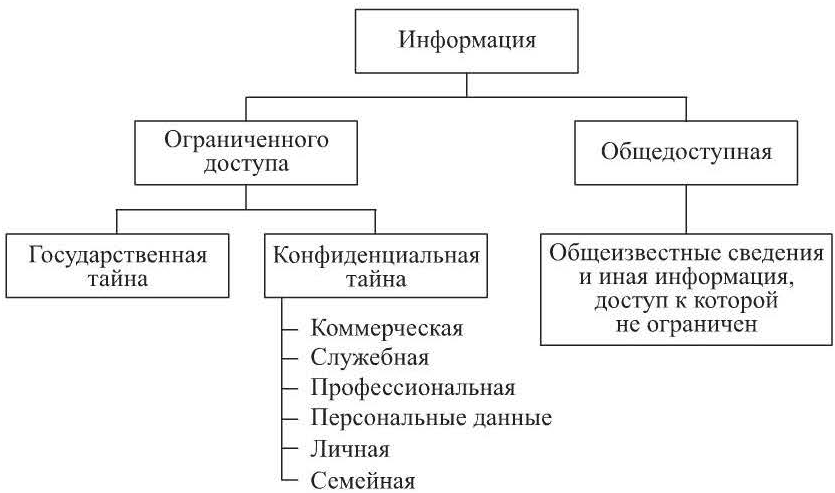

Рис. 5.1. Классификация информации

устанавливаются федеральными законами, в соответствии с которыми предусмотрена следующая классификация тайн:

• по собственнику (государственная, негосударственная и т. п.);

• по владельцу (государственная, коммерческая, банковская, профессиональная, служебная, персональные данные как особый институт охраны неприкосновенности частного лица и т. п.);

• по области применения, в которой извлекается выгода от монопольного владения (коммерческая, политическая, военная и т. п.);

• по степени важности (гриф секретности).

Общедоступная информация. Согласно ст. 8 Федерального закона № 149-ФЗ, не может быть ограничен доступ к информации, касающейся вопросов:

• прав, свобод и обязанностей человека и гражданина, правового положения организаций, полномочий государственных органов, органов местного самоуправления;

• состояния окружающей среды;

• деятельности государственных органов и органов местного самоуправления, использования бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну).

К общедоступной относится информация, накапливаемая в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, и иная информация, недопустимость ограничения доступа к которой установлена федеральными законами.

Информация ограниченного доступа. Перечень сведений конфиденциального характера определен в Указе Президента Российской Федерации от 06.03.1997 № 188 (с изм. от 23.09.2005 № 1111):

• 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, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20.08.2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации;

• служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

• сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами;

• сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);

• сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Государственная тайна. Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации «*О государственной тайне*» от 21.07.1993 № 5485-1.

В соответствии с п. 1 Указа Президента Российской Федерации от 17.03. 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» подключение информационных систем, телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, к информационно-телекоммуникационным сетям международного информационного обмена производится только с использованием сертифицированных средств защиты информации, в том числе шифровальных (криптографических).

Персональные данные. Порядок доступа к персональным данным граждан (физических лиц) устанавливается Федеральным законом *«О персональных данных»* от 27.07.2006 № 152-ФЗ, где даны следующие определения:

• *персональные данные* — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

• *оператор* — государственный или муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

При обработке персональных данных оператор обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Российская Федерация ратифицировала *Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных* (Федеральный закон от 19.12.2005 № 160-ФЗ) и заявила, что:

• не будет применять Конвенцию к персональным данным:
  — обрабатываемым физическими лицами исключительно для личных и семейных нужд;
  — отнесенным к государственной тайне в порядке, установленном законодательством Российской Федерации о государственной тайне;

• будет применять Конвенцию к персональным данным, которые не подвергаются автоматизированной обработке, если применение Конвенции соответствует характеру действий, совершаемых с персональными данными без использования средств автоматизации;

• оставляет за собой право устанавливать ограничения права субъекта персональных данных на доступ к персональным данным о себе в целях защиты безопасности государства и общественного порядка.

В соответствии с Указом Президента Российской Федерации от 30.05.2005 № 609 *«Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»* руководители государственных органов обязаны:

• обеспечить защиту персональных данных государственных гражданских служащих Российской Федерации, содержащихся в их личных делах, от неправомерного использования или утраты;

• определить круг лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных государственных гражданских служащих.

Постановление Правительства РФ от 01.11.2012 № 1119 *«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»* устанавливает требования к защите персональных данных при их обработке в информационных системах и уровни защищенности таких данных.

Система защиты персональных данных (ч. 5 ст. 19 Федерального закона «О персональных данных») включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности — совокупности условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия:

• *угрозы 1-го типа* связаны с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении;

• *угрозы 2-го типа* — в прикладном программном обеспечении;

• *угрозы 3-го типа* — в системном и прикладном программном обеспечении одновременно, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, и выбор средств защиты информации производится оператором, который обрабатывает персональные данные с учетом оценки возможного вреда (п. 5 ч. 1 ст. 181, ч. 4 и 5 ст. 19 ФЗ «О персональных данных»).

При обработке персональных данных в информационных системах устанавливают четыре уровня защищенности персональных данных:

1) для информационной системы актуальны угрозы 1-го типа, и она обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных или для ИС актуальны угрозы 2-го типа, и она обрабатывает специальные категории персональных данных более чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора;

2) для информационной системы актуальны угрозы 1-го типа, и она обрабатывает общедоступные персональные данные или для ИС актуальны угрозы 2-го типа, и она обрабатывает либо специальные категории персональных данных сотрудников оператора, либо специальные категории персональных данных менее чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора, либо биометрические персональные данные, либо общедоступные персональные данные более чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора, или для ИС актуальны угрозы 3-го типа и она обрабатывает специальные категории персональных данных более чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора;

3) для информационной системы актуальны угрозы 2-го типа, и она обрабатывает либо общедоступные или иные персональные данные сотрудников оператора, либо менее чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора, или для ИС актуальны угрозы 3-го типа и она обрабатывает либо специальные категории персональных данных сотрудников оператора или менее чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора, либо биометрические персональные данные, либо иные категории персональных данных более чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора;

4) для информационной системы актуальны угрозы 3-го типа, и она обрабатывает либо общедоступные персональные данные, либо иные категории персональных данных сотрудников оператора или менее чем 100 тыс. субъектов персональных данных, не являющихся сотрудниками оператора.

Для обеспечения четвертого уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

• организация режима ограниченного доступа в помещения, в которых размещена информационная система;

• обеспечение сохранности носителей персональных данных;

• утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей;

• использование сертифицированных средств защиты информации.

Обеспечение третьего уровня защищенности персональных данных предусматривает выполнение всех требований к четвертому уровню и назначение должностного лица, ответственного за обеспечение безопасности персональных данных в информационной системе.

Для обеспечения второго уровня защищенности персональных данных, помимо выполнения требований к третьему уровню, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных обязанностей.

Для обеспечения первого (самого высокого) уровня защищенности персональных данных при их обработке в информационных системах, помимо выполнения требований ко второму уровню, следует обеспечить автоматическую регистрацию в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в ИС, и создать структурное подразделение, ответственное за обеспечение безопасности персональных данных в информационной системе.

Контроль за выполнением перечисленных требований проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Контроль проводится регулярно — не реже одного раза в три года в сроки, определяемые оператором.

Контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации, согласно постановлению Правительства РФ от 16.03.2009 № 228, осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (*Роскомнадзор*).

Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем утверждены *Постановлением Правительства РФ от 06.06.2008 № 512*.

Под *материальным носителем* понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность.

Порядок передачи материальных носителей уполномоченным лицам, учет количества экземпляров материальных носителей, а также присвоение материальному носителю уникального идентификационного номера осуществляет оператор. Оператор вправе устанавливать не противоречащие требованиям законодательства Российской Федерации дополнительные требования к технологиям хранения биометрических персональных данных.

Перечень методических документов ФСТЭК России и ФСБ России, касающихся персональных данных:

• *Приказ ФСТЭК России от 11.02.2013 № 17* «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

• *Приказ ФСТЭК России от 18.02.2013 № 21* «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

• *Приказ ФСБ России от 10.07. 2014 № 378* «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах

персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

• *Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных* (утв. ФСТЭК России 14.02.2008);

• *Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных* (утв. ФСТЭК России 15.02.2008);

• *Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации* (утв. ФСБ России 21.02.2008 № 149/54-144);

• *Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств*, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСБ России 21.02.2008 № 149/6/6-622).

Коммерческая тайна. В Федеральном законе *«О коммерческой тайне»* от 29.07.2004 № 98-ФЗ даны следующие определения:

• *коммерческая тайна* — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

• *информация, составляющая коммерческую тайну*, — сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

• *обладатель информации, составляющей коммерческую тайну*, — лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении нее режим коммерческой тайны;

• *разглашение информации, составляющей коммерческую тайну*, — действие или бездействие, в результате которых информация, составляющая коммерческую тайну в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Режим коммерческой тайны считается установленным после принятия обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации:

• определение перечня информации, составляющей коммерческую тайну;

• ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

• учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и/или лиц, которым такая информация была предоставлена или передана;

• регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

• нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц — полное наименование и место нахождения, для индивидуальных предпринимателей — фамилия, имя, отчество и место жительства).

Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Кроме того, в соответствии с Федеральным законом «О бухгалтерском учете» от 06.12.2011 № 402-ФЗ, не может быть установлен режим коммерческой тайны в отношении бухгалтерской (финансовой) отчетности.

Постановлением Правительства РСФСР от 05.12.1991 № 35 установлено, что коммерческую тайну не могут составлять:

• учредительные документы, устав, лицензии, патенты;

• документы о платежеспособности;

• сведения о численности, составе работающих, их заработной плате и условиях труда, а также о вакансиях;

• документы об уплате налогов и обязательных платежах;

• сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда и др.

К сожалению, Федеральный закон «О коммерческой тайне» не в полной мере обеспечивает неприкосновенность соответствующей информации, так в ст. 6 отмечено, что по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления «обладатель информации, составляющей коммерческую тайну, предоставляет им на безвозмездной основе информацию, составляющую коммерческую тайну». При отказе собственника информационных ресурсов добровольно выдать информацию, составляющую коммерческую тайну, она может быть получена в судебном порядке без возмещения

издержек собственника на предоставление информации. Кроме того, ФЗ не предусматривает отмены ранее принятых нормативных документов по вопросам защиты коммерческой тайны, в том числе и в части, противоречащей ФЗ, что не способствует устранению существующих правовых коллизий.

В настоящее время, согласно Федеральному закону № 35-ФЗ от 12.03.2014 понятия «коммерческая тайна» и «секрет производства» разделены — последнее является более общим понятием. Согласно Гражданскому кодексу РФ, *секретом производства* (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и др.) о результатах интеллектуальной деятельности в научно-технической сфере и способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны.

Существует также ряд методических документов по технической защите информации, составляющей коммерческую тайну, выпущенных ФСТЭК России:

• *Методические рекомендации по технической защите информации, составляющей коммерческую тайну* (утв. ФСТЭК России 25.12.2006);

• *Пособие по организации технической защиты информации, составляющей коммерческую тайну* (утв. ФСТЭК России 25.12.2006).

Служебная тайна. Общий порядок обращения с документами и другими материальными носителями информации (фото-, кино-, видео- и аудиопленки, машинные носители информации и др.), содержащими служебную информацию ограниченного распространения, определен в «Положении о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», утвержденном постановлением Правительства РФ от 03.11.1994 № 1233.

К служебной информации ограниченного распространения относят несекретную информацию, касающуюся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью.

На документах (в необходимых случаях и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования».

Руководитель федерального органа исполнительной власти определяет:

• категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения;

• порядок передачи такой информации другим органам и организациям;

• порядок снятия пометки «Для служебного пользования»;

• организацию защиты служебной информации ограниченного распространения.

Должностные лица, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность такого решения.

За разглашение служебной информации ограниченного распространения, а также нарушение порядка обращения с документами, содержащими такую информацию, государственный служащий (работник организации) может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

Постановлением Правительства Российской Федерации от 03.11.1994 № 1233 установлено, что не могут быть отнесены к служебной информации ограниченного распространения:

- акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов;
- описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;
- порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц;
- решение по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;
- сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностях населения;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан.

Банковская тайна. Регламентация банковской тайны осуществляется в соответствии со ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» и ст. 857 ч. 2 *Гражданского кодекса РФ (Федеральный закон от 25.01.1996 № 14-ФЗ)*.

К основным объектам банковской тайны, согласно действующему законодательству, относят:

- *банковский счет* — сведения о счетах клиентов (расчетный, текущий, бюджетный, депозитный, валютный, корреспондентский и т. п.) и действиях с ними (открытие, закрытие, перевод, переоформление счета и т. п.) в кредитной организации;
- *операции по банковскому счету* — сведения о зачислении поступающих на счет клиента денежных средствах, о выполнении перечислений, выдаче сумм со счета и др.;
- *банковский вклад* — сведения о всех видах вкладов клиента в кредитной организации (срочные, до востребования, в пользу третьих лиц и др.);

• *тайна частной жизни клиента (корреспондента)* — сведения о клиенте (корреспонденте), составляющие его личную, семейную тайну и сохраняемые законом как персональные данные клиента (корреспондента).

5.2. Лицензирование

Законодательство Российской Федерации предусматривает установление Правительством Российской Федерации порядка ведения лицензионной деятельности, перечня видов деятельности, на осуществление которых требуется лицензия, и органов, уполномоченных на ведение лицензионной деятельности.

В Федеральном законе от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» даны следующие определения:

• *лицензирование* — деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования;

• *лицензия* — специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в форме электронного документа.

В ст. 12 Федерального закона приведен перечень видов деятельности в области защиты информации, подлежащих лицензированию:

• разработка, производство и распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием таких криптографических средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием таких средств (за исключением случая, когда техническое обслуживание осуществляется юридическим лицом или индивидуальным предпринимателем для собственных нужд);

• разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации;

• деятельность по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

• разработка и производство средств защиты конфиденциальной информации;

• деятельность по технической защите конфиденциальной информации.

В рамках перечисленных видов деятельности приняты постановления Правительства Российской Федерации, разъясняющие порядок лицензирования:

• от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

• от 03.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»;

• от 16.04.2012 № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

Постановление Правительства РФ № 79 определяет понятие «техническая защита конфиденциальной информации» — это выполнение работ и (или) оказание услуг по защите информации от несанкционированного доступа, утечки по техническим каналам, специальных воздействий в целях уничтожения, искажения или блокирования доступа.

Лицензирование деятельности по технической защите конфиденциальной информации осуществляет Федеральная служба по техническому и экспортному контролю РФ и Федеральная служба безопасности РФ.

Соискатель лицензии (лицензиат) на осуществление деятельности по технической защите конфиденциальной информации (сотрудник юридического лица или индивидуальный предприниматель) должен иметь:

• высшее профессиональное образование в области технической защиты информации или высшее техническое или среднее профессиональное (техническое) образование, а также свидетельство о повышении квалификации по вопросам технической защиты информации;

• помещение для осуществления лицензируемого вида деятельности, соответствующее установленным законодательством Российской Федерации

техническим нормам и требованиям по технической защите информации и принадлежащее соискателю лицензии на праве собственности или ином законном основании;

• контрольно-измерительное оборудование, прошедшее в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку) и маркирование; производственное и испытательное оборудование, соответствующее требованиям по техническим характеристикам и параметрам, устанавливаемым ФСТЭК России на праве собственности или ином законном основании;

• средства контроля защищенности информации от несанкционированного доступа, сертифицированных по требованиям безопасности информации, в соответствии с перечнем, утверждаемым ФСТЭК России на праве собственности или ином законном основании;

• автоматизированные системы, предназначенные для обработки конфиденциальной информации, а также сертифицированные средства защиты такой информации;

• программы для ЭВМ и баз данных, принадлежащие соискателю лицензии на праве собственности или на ином законном основании;

• необходимую техническую документацию, национальные стандарты и методические документы;

• системы производственного контроля.

Таким образом, вся деятельность по обеспечению технической защиты конфиденциальной информации подпадает под обязательное лицензирование, т. е. владелец АС, в рамках которой обрабатывается, хранится или передается конфиденциальная информация, должен либо обладать лицензией на проведение работ по технической защите информации, либо привлекать для проведения подобных работ компании, обладающие такой лицензией.

Постановление Правительства Российской Федерации от 16.04.2012 № 313 определяет перечень шифровальных (криптографических) средств (средств криптографической защиты информации), включая документацию на эти средства:

• *средства шифрования* — аппаратные, программные и программно-аппаратные криптографические средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;

• *средства имитозащиты* — аппаратные, программные и программно-аппаратные криптографические средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модификации, корректуры, для обеспечения ее достоверности и возможности выявления изменений, имитации, фальсификации;

• *средства электронной подписи*;

• *средства кодирования* — средства шифрования, в которых часть криптографических преобразований информации осуществляется вручную или с

использованием автоматизированных средств, предназначенных для выполнения таких операций;

• *средства изготовления ключевых документов* — аппаратные, программные, программно-аппаратные криптографические средства, обеспечивающие возможность изготовления ключевых документов для иных криптографических средств, не входящих в состав данных;

• *ключевые документы* — электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием соответствующих алгоритмов;

• *аппаратные шифровальные (криптографические) средства* — устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для ЭВМ;

• *программные шифровальные (криптографические) средства* — программы для ЭВМ, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных криптографических средствах, информационно-телекоммуникационных системах, защищенных с использованием криптографических средств;

• *программно-аппаратные шифровальные (криптографические) средства* — устройства и их компоненты (за исключением информационно-телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для ЭВМ, предназначенных для осуществления данных преобразований.

Действие постановлений правительства РФ № 79, 171 и 213 не распространяется на деятельность с использованием:

• шифровальных (криптографических) средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну;

• шифровальных (криптографических) средств, а также товаров, содержащих также средства, реализующих либо симметричный криптографический алгоритм, использующий криптографический ключ длиной не более 56 бит, либо ассиметричный криптографический алгоритм, основанный либо на методе разложения на множители целых чисел, размер которых не превышает 512 бит, либо на методе вычисления дискретных логарифмов в мультипликативной группе конечного поля размером не более 512 бит, либо на методе вычисления дискретных логарифмов в иной группе размером не более 112 бит;

• товаров, содержащих шифровальные (криптографические) средства, имеющих либо функцию аутентификации, включающую в себя все аспекты

контроля доступа, где нет шифрования файлов или текстов, за исключением шифрования, которое непосредственно связано с защитой паролей, персональных идентификационных номеров или подобных данных для защиты от несанкционированного доступа, либо имеющих электронную подпись;

• шифровальных (криптографических) средств, являющихся компонентами программных операционных систем, криптографические возможности которых не могут быть изменены пользователями, которые разработаны для установки пользователем самостоятельно без дальнейшей существенной поддержки поставщиком и техническая документация (описание алгоритмов криптографических преобразований, протоколы взаимодействия, описание интерфейсов и т. д.) на которые является доступной;

• персональных смарт-карт для общедоступного применения, криптографические возможности которых недоступны пользователю и которые в результате специальной разработки имеют ограниченные возможности защиты хранящейся на них персональной информации;

• приемной аппаратуры для радиовещания, коммерческого телевидения или аналогичной коммерческой аппаратуры для вещания на ограниченную аудиторию без шифрования цифрового сигнала, кроме случаев использования шифрования исключительно для управления видео- или аудиоканалами и отправки счетов или возврата информации, связанной с программой, провайдерам вещания;

• оборудования, криптографические возможности которого недоступны пользователю, специально разработанного и ограниченного для осуществления следующих функций:

— исполнение программного обеспечения в защищенном от копирования виде;
— обеспечение доступа к защищенному от копирования содержимому, хранящемуся только на доступном для чтения носителе информации, или к информации, хранящейся в зашифрованной форме на носителях, общедоступного применения;
— контроль копирования аудио- и видеоинформации, защищенной авторскими правами;

• шифровального (криптографического) оборудования для банковских или финансовых операций в составе терминалов единичной продажи (банкоматов), POS-терминалов и терминалов оплаты различного вида услуг, криптографические возможности которых не могут быть изменены пользователями;

• портативных или мобильных радиоэлектронных средств гражданского назначения (например, в системах сотовой радиосвязи), которые не способны к сквозному шифрованию (т. е. от абонента к абоненту);

• беспроводного оборудования, осуществляющего шифрование информации только в радиоканале с максимальной дальностью беспроводного действия без усиления и ретрансляции менее 400 м в соответствии с техническими условиями производителя (за исключением оборудования, используемого на критически важных объектах);

• шифровальных (криптографических) средств для защиты технологических каналов информационно-телекоммуникационных систем и сетей связи, не относящихся к критически важным объектам;

• товаров, у которых криптографическая функция гарантированно заблокирована производителем.

Лицензии стали бессрочными, но требования по соблюдению условий лицензирования ужесточились.

5.3. Сертификация средств защиты информации и аттестация объектов информатизации

Согласно Закону Российской Федерации *«О государственной тайне»*, средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Кроме того, в соответствии с *Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам*, утвержденным постановлением Совета Министров — Правительства Российской Федерации от 15.09.1993 № 912-51, информация, содержащая сведения, отнесенные к государственной или служебной тайне, должна обрабатываться с использованием защищенных систем и средств информатизации и связи или с применением технических и программных средств защиты, сертифицированных в установленном порядке. Для оценки готовности систем и средств информатизации и связи к передаче информации, содержащей такие сведения, проводится аттестация указанных систем и средств в реальных условиях эксплуатации на предмет соответствия принимаемых методов, мер и средств защиты требуемому уровню безопасности информации.

Положение о лицензировании деятельности по технической защите конфиденциальной информации, утвержденное постановлением Правительства Российской Федерации от 03.02.2012 № 79, допускает использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и(или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством РФ.

Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» допускает использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Согласно *указу Президента Российской Федерации от 17.03.2008 № 351,* подключение информационных систем, информационно-телекоммуника-

ционных сетей и СВТ, применяемых для хранения, обработки или передачи конфиденциальной информации, к информационно-телекоммуникационным сетям международного информационного обмена производится только с использованием сертифицированных средств защиты информации, в том числе криптографических средств, в специальных помещениях.

Постановление Правительства Российской Федерации от 18.05.2009 № 424 регулирует деятельность операторов федеральных государственных информационных систем, созданных или используемых в целях реализации полномочий федеральных органов исполнительной власти и содержащих сведения, указанные в перечне сведений о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательных для размещения в информационно-телекоммуникационной сети Интернет в соответствии с постановлением Правительства Российской Федерации от 12.02.2003 № 98 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям широкого доступа.

В Федеральном законе от 27.12.2002 № 184-ФЗ «О техническом регулировании» даны основные определения, касающиеся вопросов сертификации и аттестации.

Оценка соответствия — прямое или косвенное определение соблюдения требований, предъявляемых к объекту, — проводится в форме государственного контроля (надзора), аккредитации, испытания, регистрации, подтверждения соответствия и др.

Подтверждение соответствия — документальное удостоверение соответствия продукции или иных объектов, процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Подтверждение соответствия на территории Российской Федерации может носить добровольный или обязательный характер. Добровольное подтверждение соответствия осуществляется в форме добровольной сертификации. Обязательное подтверждение соответствия осуществляется в форме принятия декларации о соответствии или обязательной сертификации.

Порядок применения форм обязательного подтверждения соответствия устанавливается Федеральным законом «О техническом регулировании».

Декларирование соответствия — форма подтверждения соответствия продукции требованиям технических регламентов.

Декларация о соответствии и сертификат соответствия имеют равную юридическую силу и действуют на всей территории РФ в отношении каждой единицы продукции, выпускаемой в обращение на территории РФ во время действия декларации или сертификата, в течение срока годности или срока службы продукции.

Декларирование соответствия осуществляется по одной из следующих схем: 1) на основании собственных доказательств результатов проведенных исследований (испытаний) и измерений, а также иных документов, послуживших мотивированным основанием для подтверждения соответствия продукции требованиям технических регламентов; 2) на основании собственных доказательств и доказательств, полученных с участием органа по сертификации и (или) аккредитованной испытательной лаборатории (центра), в дополнение к собственным доказательствам представляют протоколы исследований и измерений, проведенных в аккредитованной испытательной лаборатории, а также сертификат системы качества, в отношении которого предусматривается контроль (надзор) органа по сертификации, выдавшего данный сертификат, за объектом сертификации.

При декларировании соответствия заявителями могут быть зарегистрированные на территории Российской Федерации юридическое лицо или физическое лицо в качестве индивидуального предпринимателя, либо являющееся изготовителем или продавцом, либо выполняющее функции иностранного изготовителя на основании договора с ним в части обеспечения соответствия поставляемой продукции требованиям технических регламентов и в части ответственности за несоответствие поставляемой продукции требованиям технических регламентов (лицо, выполняющее функции иностранного изготовителя).

Декларация о соответствии оформляется на русском языке и содержит сведения:

- о наименовании и местонахождении заявителя;
- наименовании и местонахождении изготовителя;
- объекте подтверждения соответствия, позволяющие идентифицировать этот объект;
- техническом регламенте, на соответствие требованиям которого подтверждается продукция;
- схеме декларирования соответствия;
- безопасности продукции при ее использовании в соответствии с целевым назначением и принятии заявителем мер по обеспечению соответствия продукции требованиям технических регламентов;
- проведенных исследованиях (испытаниях) и измерениях, сертификате системы качества, а также документах, послуживших основанием для подтверждения соответствия продукции требованиям технических регламентов;
- сроке действия декларации о соответствии и др.

Срок действия декларации о соответствии определяется техническим регламентом.

Оформленная заявителем декларация подлежит регистрации в едином реестре деклараций о соответствии в течение трех дней.

Технический регламент — документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством РФ, или межправительственным соглашением и

устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям или к связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации).

Технический регламент должен содержать перечень и (или) описание объектов технического регулирования, требования к этим объектам (терминологии, упаковке, маркировке или этикеткам) и правила их идентификации (схемы подтверждения соответствия, порядок продления срока действия выданного сертификата соответствия).

Сертификация – форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, правил или условиям договоров.

Обязательная сертификация осуществляется органом по сертификации на основании договора с заявителем.

Соответствие продукции требованиям технических регламентов подтверждается сертификатом соответствия, который включает в себя:

- наименование и местонахождение заявителя;
- наименование и местонахождение изготовителя продукции, прошедшей сертификацию;
- наименование и местонахождение органа по сертификации, выдавшего сертификат соответствия;
- информацию об объекте сертификации, позволяющую идентифицировать этот объект;
- наименование технического регламента, на соответствие требованиям которого проводилась сертификация;
- информацию о проведенных исследованиях (испытаниях) и измерениях;
- информацию о документах, представленных заявителем в орган по сертификации в качестве доказательств соответствия продукции требованиям технических регламентов;
- срок действия сертификата соответствия.

Особенности сертификации средств защиты информации, содержащей сведения, составляющие государственную тайну, рассмотрены в *Постановлении Правительства Российской Федерации от 21.04.2010 № 266*; не содержащей сведения, составляющие государственную тайну — в *Постановлении Правительства Российской Федерации от 15.05.2010 № 330*.

Согласно *Постановлению Правительства Российской Федерации от 26.06.1995 № 608* «О сертификации средств защиты информации», были созданы системы обязательной сертификации пяти федеральных органов исполнительной власти:

- **ФАПСИ** — Система сертификации средств криптографической защиты информации (утверждена генеральным директором ФАПСИ 28.10.1993 г., в соответствии с Указом Президента РФ от 11.03.2003 № 308 в связи с расформированием ФАПСИ соответствующие функции переданы ФСБ РФ);

• **ФСТЭК России** — Положение о сертификации средств защиты информации по требованиям безопасности информации (введено в действие приказом Председателя Гостехкомиссии России от 27.10.1995 № 199);

• **ФСБ России** — Положение о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (утверждено приказом ФСБ России от 13.11.1999 № 564);

• **Минобороны России** — Система сертификации средств защиты информации по требованиям безопасности информации (введено в действие приказом Министра обороны);

• **СВР России** — Положение о системе сертификации средств защиты информации по требованиям безопасности информации (утверждено директором СВР России 05.08.1998).

Необходимой составляющей государственной системы обеспечения информационной безопасности являются национальные (государственные) и другие руководящие, нормативно-технические и методические документы по безопасности информации, утвержденные федеральными органами исполнительной власти в соответствии с их компетенцией, и определяющие нормы защищенности информации и требования в различных направлениях защиты информации.

Приведем некоторые из них (полный перечень документов см. на с. 237) ***в области защиты информации от несанкционированного доступа.***

Национальные стандарты:

• ГОСТ Р 50922–2006. Защита информации. Основные термины и определения;

• ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения;

• ГОСТ Р ИСО/МЭК 27001–2013. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006 №375-ст). Дата введения: 01.02.2008;

• ГОСТ Р ИСО/МЭК 27002–2012. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (утв. приказом Федерального агентства по техническому регулированию и метрологии от 24.09.2012 № 423-ст). Дата введения: 01.01.2014;

• ГОСТ Р ИСО/МЭК 27003–2012. Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. (утв. приказом Федерального агентства по техническому регулированию и метрологии от 15.11.2012 № 812-ст). Дата введения: 01.12.2013;

• ГОСТ Р ИСО/МЭК 27004–2011. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной без-

опасности. Измерения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 01.12.2011 № 681-ст). Дата введения: 01.01.2012;

• ГОСТ Р ИСО/МЭК 27005-2010. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 30.11.2010 № 632-ст). Дата введения: 01.12.2011;

• ГОСТ Р ИСО/МЭК 27006-2008. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18.12.2008 №524-ст). Дата введения: 01.10.2009.

Руководящие документы ФСТЭК России:

• Защита от несанкционированного доступа к информации. Термины и определения;

• Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;

• Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации;

• Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности;

• Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники и др.

Документы в области защиты информации от утечки по техническим каналам:

• ГОСТ Р В50170–2005. Противодействие иностранной технической разведке. Термины и определения;

• ГОСТ Р 50752–95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний и др.

Нормативно-методические документы ФСТЭК России:

• Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К);

• Методические рекомендации по технической защите информации, составляющей коммерческую тайну;

• Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам.

Документы в области криптографического преобразования информации при ее хранении и передаче по каналам связи:

• ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной

цифровой подписи (ранее ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи);

• ГОСТ Р 34.11—2012. Информационная технология. Криптографическая защита информации.Функция хэширования (взамен ГОСТ Р 34.11–94. Функция хеширования) и др.

Документы ФСБ России:

• Положение о разработке, изготовлении и обеспечении эксплуатации шифровальной техники, систем связи и комплексов вооружения, использующих шифровальную технику (ПШ-93);

• Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005);

• Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну и др.

Остановимся более детально на вопросах сертификации средств защиты. Отметим, что после передачи лицензирующих подразделений ФАПСИ в ведение ФСБ России основные принципы системы лицензирования и сертификации не изменились. Все ранее выданные ФАПСИ лицензии и сертификаты оставались действительными на обозначенный в них срок.

Сертификация. Приведем некоторые определения. Под *сертификацией средств защиты информации* по требованиям безопасности информации понимается деятельность по подтверждению их соответствия требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных уполномоченными федеральными органами исполнительной власти в пределах их компетенции.

Сертификат соответствия — документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Знак соответствия — зарегистрированный знак, которым по правилам, установленным в данной системе сертификации, подтверждается соответствие маркированной им продукции определенным требованиям.

Средства защиты информации (СЗИ) — технические, криптографические, программные и другие средства, предназначенные для защиты сведений конфиденциального характера, а также средства контроля эффективности защиты информации.

В соответствии с руководящим документом ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» возможные показатели защищенности (рис. 5.2) разделены на семь классов (наиболее защищенный — 1-й класс). Выбор класса защищенности зависит от секретности обрабатываемой информации, условий эксплу-

атации и расположения объектов системы. Для защиты конфиденциальной информации (персональных данных, служебной тайны и др.) применяют средства защиты 5-го и 6-го классов.

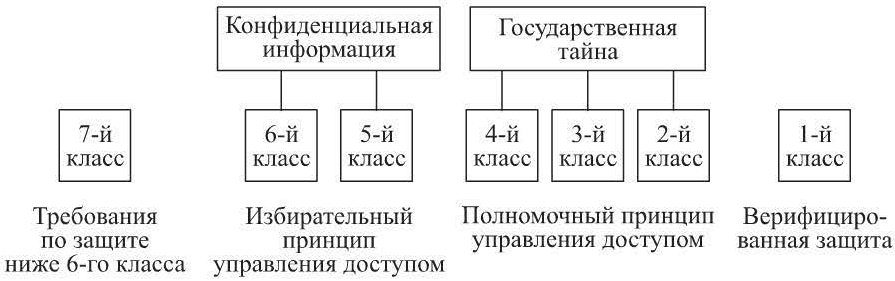

Рис. 5.2. Показатели защищенности СВТ

Классификация программного обеспечения (отечественного и импортного производства), средств защиты информации по уровню контроля отсутствия в нем недекларированных возможностей приведена в руководящем документе ФСТЭК России «Защита от несанкционированного доступа к информации. Ч. 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (рис. 5.3).

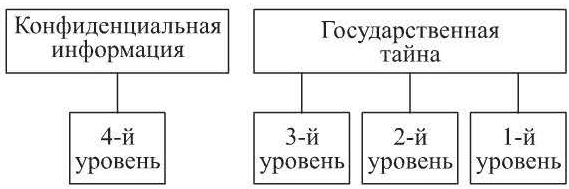

Рис. 5.3. Классификация по уровню контроля отсутствия недекларированных возможностей

Недекларированные возможности (НДВ) — функциональные возможности программного обеспечения (ПО), не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности и целостности обрабатываемой информации.

Классификацию межсетевых экранов (МЭ) по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований устанавливает руководящий документ ФСТЭК России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (рис. 5.4).

Межсетевой экран — локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивающее защиту АС посредством фильтрации информации, т. е. ее анализа по совокупности критериев и принятия решения о ее распространении в АС.

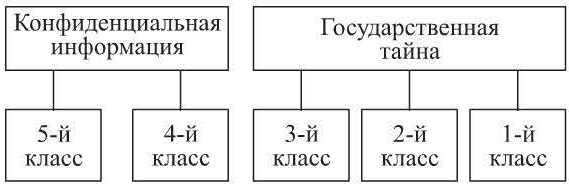

Рис. 5.4. Классификация МЭ по уровню защищенности от НСД

Применение сертифицированных средств защиты информации является обязательным условием при рассмотрении в судебном порядке спорных вопросов, связанных с удостоверением подлинности электронных документов и идентификацией личности пользователей системы.

Аттестация. При проведении работ со сведениями соответствующей степени конфиденциальности (секретности) системы информатизации проходят аттестацию на соответствие требованиям по безопасности информации.

Государственная система аттестации объектов информатизации устанавливает основные принципы, организационную структуру, порядок проведения аттестации, а также контроля и надзора за эксплуатацией аттестованных объектов информатизации.

Под *объектами информатизации*, аттестуемыми по требованиям безопасности информации, понимаются АС различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.

Система аттестации объектов информатизации по требованиям безопасности информации является составной частью единой государственной системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Деятельность системы аттестации организуют уполномоченные федеральные органы по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации в соответствии с нормативно-методическими документами ФСТЭК России.

Под *аттестацией объектов информатизации* понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» — подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных уполномочен-

ными федеральными органами исполнительной власти. Наличие на объекте информатизации действующего Аттестата соответствия дает право обработки информации с определенным уровнем конфиденциальности и в указанный в Аттестате соответствия период времени.

Аттестат соответствия утверждается руководителем органа по аттестации объектов информатизации, который несет юридическую и финансовую ответственность за качество проведенных работ. Кроме того, органы по аттестации несут ответственность за обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонент.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, утечки за счет устройств, встроенных в объекты информации побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие).

Правила аккредитации определяются действующими в соответствующих системах сертификации положениями. В системе сертификации ФСТЭК России разработано и утверждено 25.11.1994 г. «Положение об аккредитации органов по аттестации объектов информатизации по требованиям безопасности информации».

Руководящий документ ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» вводит в рассмотрение девять классов защищенности АС, объединенных в три группы (рис. 5.5).

В зависимости от уровня конфиденциальности, уровня полномочий субъектов доступа АС на доступ к конфиденциальной информации и режима обработки данных в АС (коллективный или индивидуальный) для каждого класса сформулирован определенный набор требований для подсистем, касающихся управления доступом, регистрации и учета, обеспечения конфиденциальности и целостности.

Группа 1 классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всему объему информации АС. Группа содержит пять классов: 1Д, 1Г, 1В, 1Б и 1А.

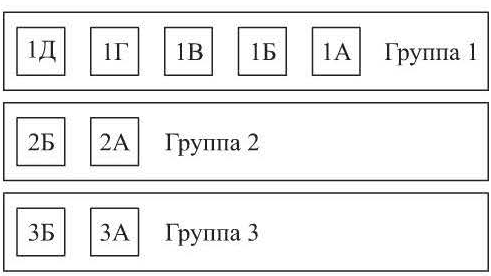

Рис. 5.5. Классы защищенности АС

К группе 2 относят АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всему объему информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа объединяет два класса: 2Б и 2А.

Группа 3 классифицирует АС, в которых работает один пользователь, допущенный ко всему объему информации, размещенной на носителях одного уровня конфиденциальности (классы 3Б и 3А).

Соответствие классов защищенности различным уровням конфиденциальности приведено на рис. 5.6.

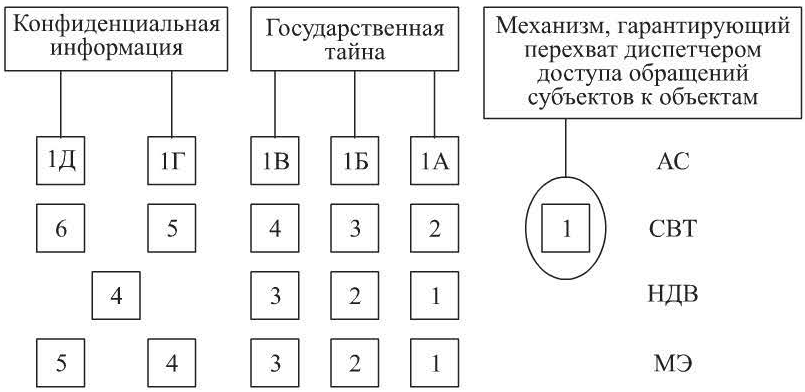

Рис. 5.6. Классы защищенности АС в зависимости от категории информации ограниченного доступа

Качественно новым этапом в развитии нормативной базы оценки безопасности ИТ послужило начало разработки и апробация нового поколения нормативных документов в системе сертификации ФСТЭК России на основе методологии *ГОСТ Р ИСО/МЭК 15408–2013* «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», который содержит полный аутентичный текст Международного стандарта ISO/IEC 15408 «Общие критерии».

Главная тенденция, которая прослеживается на протяжении целого ряда стандартов в области информационной безопасности — отказ от жесткой универсальной шкалы классов безопасности и обеспечение гибкости в подходе к оценке безопасности различных типов ИТ-продуктов. Именно это стремление объясняет столь сложную на первый взгляд логическую структуру стандарта, которая характеризуется:

- четким разделением требований безопасности на функциональные требования и требования доверия к безопасности. Функциональные требования относятся к функциям безопасности (идентификация, аутентификация, управление доступом, аудит и т. д.), а требования доверия — к технологии разработки, тестированию, анализу уязвимостей, поставке, сопровождению, эксплуатационной документации, т. е. ко всем этапам жизненного цикла изделий информационных технологий;
- систематизацией и классификацией требований к безопасности в рамках иерархии «класс» — «семейство» — «компонент» — «элемент»;
- ранжированием компонентов требований в семействах и классах по степени полноты и жесткости, а также их группированием в пакеты функциональных требований и уровнями оценки доверия;

• гибкостью и динамизмом в подходе к заданию требований безопасности для различных типов ИТ-продуктов и условий их применения, обеспечиваемых путем целенаправленного формирования необходимых наборов требований в виде определенных структур (профилей защиты и целевых уровней безопасности).

Понимание методологии позволяет эффективно использовать огромный фактический материал по требованиям безопасности ИТ, порядку их задания и оценке, который содержится в данном стандарте.

Общие критерии разработаны таким образом, чтобы удовлетворить потребности трех групп специалистов: разработчиков, оценщиков и пользователей объекта оценки. Под *объектом оценки* (ОО) понимается аппаратно-программный продукт или информационная система. К таким объектам относятся, например, операционные системы, вычислительные сети, распределенные системы, прикладные программы.

К аспектам безопасности относятся: защита от несанкционированного доступа, модификации или потери доступа к информации при воздействии угроз, являющихся результатом случайных или преднамеренных действий.

Однако, некоторые аспекты безопасности ИТ находятся вне рамок данного стандарта:

• отсутствуют критерии оценки криптографических алгоритмов, а также безопасности, касающиеся административных мер, непосредственно не относящихся к мерам безопасности ИТ. Административные меры безопасности в среде эксплуатации ОО рассматриваются в качестве предположений о безопасном использовании;

• не приведена оценка физических аспектов безопасности ИТ (например, контроль электромагнитного изучения), хотя многие концепции стандарта применимы и в этой области;

• не рассмотрены вопросы, касающиеся методологии оценки и нормативно-правовой базы, на основе которой критерии могут применяться органами оценки;

• отсутствует процедура использования результатов аттестации продуктов и систем ИТ. Данный вопрос является административным актом, посредством которого компетентный орган допускает их применение в конкретных условиях эксплуатации.

Общие критерии предполагается использовать как при задании требований к продуктам и системам ИТ, так и при оценке их безопасности на всех этапах жизненного цикла. Стандарт ГОСТ Р ИСО/МЭК 15408 не меняет сложившейся в России методологии защиты, однако по уровню систематизации, полноте и степени детализации требований, универсальности и гибкости значительно превосходит действующие в настоящее время руководящие документы.

5.4. Специальные требования и рекомендации по технической защите конфиденциальной информации

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Гостехкомиссии России от 30.08.2002 № 282, являются нормативно-методическим докумен-

том, который устанавливает порядок организации работ и техническую защиту информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, на территории Российской Федерации.

Данный документ распространяется на защиту государственных информационных ресурсов некриптографическими методами (служебная тайна), направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и специальных воздействий на информацию в целях ее уничтожения, искажения или блокирования.

Для негосударственных информационных ресурсов, составляющих коммерческую, банковскую и другую тайну, требования документа носят рекомендательный характер.

Документ определяет следующие в о п р о с ы защиты конфиденциальной информации:

- организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;
- состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;
- требования и рекомендации по защите речевой информации при ведении переговоров, в том числе с использованием технических средств, а также представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнито-оптической и иной основе.
- требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;
- порядок обеспечения защиты информации при эксплуатации объектов информатизации;
- особенности защиты информации при разработке и эксплуатации АС, использующих различные типы СВТ и информационные технологии.

Для защиты информации на объекте информатизации выполняют комплекс организационных мероприятий с применением сертификационных СЗИ от НСД и программно-технических воздействий.

При защите информации в локальных вычислительных сетях конфиденциальная информация может обрабатываться только в ЛВС, расположенных в пределах контролируемой зоны. Средства защиты информации от НСД применяются во всех узлах ЛВС независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС и требуют непрерывного квалифицированного контроля настроек СЗИ администратором безопасности информации. Класс защищенности ЛВС определяется в соответствии с требованиями руководящих документов ФСТЭК России (см. рис. 5.5).

5.5. Юридическая значимость электронных документов с электронной подписью

Вопросы юридической значимости электронных документов (ЭД) регулируют Гражданский кодекс РФ, Федеральный закон от 27.07.2006 № 149-ФЗ

«Об информации, информационных технологиях и о защите информации», Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» и др.

Гражданский кодекс РФ определяет понятие сделки в письменной форме (ч. 1, ст. 160) и представляет форму договора и способ обмена документами (ч. 1, ст. 434):

Федеральный закон № 149-ФЗ предписывает порядок документирования информации (ст. 11) при заключении гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, каждое из которых подписано электронной подписью (ЭП) или иным аналогом собственноручной подписи отправителя такого сообщения, рассматривается как обмен документами, право собственности на которые устанавливаются гражданским законодательством.

В Федеральном законе № 63-ФЗ даны определения основных понятий, связанных с ЭП.

В ст. 5 Федерального закона приведены виды электронных подписей:

• простая ЭП — подтверждает факт формирования ЭП определенным лицом посредством использования кодов, паролей или иных средств (для подписания документов, содержащих сведения составляющие государственную тайну, не применяется);

• усиленная ЭП (неквалифицированная и квалифицированная).

Электронный документ считается подписанным простой электронной подписью при выполнении одного из следующих условий (ст. 9):

• простая ЭП содержится в самом электронном документе;

• ключ простой ЭП применяется в соответствии с правилами, установленными оператором ИС, с использованием которой осуществляются создание и (или) отправка электронного документа.

К неквалифицированной ЭП относят подпись, которая:

• получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

• дает возможность определить лицо, подписавшее электронный документ.

Квалифицированная ЭП соответствует всем признакам неквалифицированной ЭП, а также тому, что ключ проверки ЭП указан в квалификационном сертификате.

Квалифицированная ЭП признается действительной до тех пор, пока решением суда не установлено иное, при одновременном соблюдении следующих условий (ст. 11):

• квалификационный сертификат выдан аккредитованным удостоверяющим центром и действителен на момент подписания ЭД;

• имеется положительный результат проверки принадлежности владельцу квалификационного сертификата квалифицированной ЭП и подтверждено отсутствие изменений, внесенных в этот документ после его подписания.

При использовании усиленных электронных подписей участники электронного взаимодействия обязаны (ст. 10):

• обеспечивать конфиденциальность ключей электронных подписей;

• уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа ЭП в течение одного рабочего дня со дня получения информации о таком нарушении;

• не использовать ключ ЭП при подозрении на нарушение конфиденциальности ключа.

5.6. Ответственность за нарушения в сфере защиты информации

За нарушение в области защиты информации предусмотрена административная и уголовная ответственность.

Уголовная ответственность. Уголовный кодекс Российский Федерации (УК РФ) определяет уголовную ответственность (ст. 159.6) за мошенничество в сфере компьютерной информации, т. е. хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, в виде штрафа в размере до 120 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до 360 ч, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

Если мошенничество совершено группой лиц по предварительному сговору и с причинением значительного ущерба гражданину — штраф в размере до 300 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок до 480 ч, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до четырех лет с ограничением свободы на срок до одного года или без такового.

При совершении мошенничества лицом с использованием своего служебного положения, или в крупном размере — штраф от 100 тыс. до 500 тыс. руб. или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере до 80 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

За мошенничество, совершенное организованной группой лиц, либо в особо крупном размере, предусмотрено лишение свободы на срок до 10 лет со штрафом в размере до 1 млн руб. или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз или иным незаконным способом наказывается штрафом в размере до 500 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до одного года, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок (ст. 183 УК РФ).

Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, — наказываются штрафом в размере до 1 млн руб. или в размере заработной платы или иного дохода осужденного за период до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо лишением свободы на тот же срок; при причинении крупного ущерба или из корыстной заинтересованности штраф составляет до 1 млн руб. или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на тот же срок; если действия повлекли тяжкие последствия, то срок лишения свободы составляет до десяти лет.

В гл. 28 УК РФ «Преступления в сфере компьютерной информации» содержатся три статьи, касающиеся неправомерного доступа к компьютерной информации (ст. 272), вредоносных программ для ЭВМ (ст. 273) и нарушения правил эксплуатации ЭВМ (ст. 274).

Если уничтожение, блокирование, модификация, копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети совершено одним лицом, то штраф составляет до 200 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до 18 мес., либо исправительными работами на срок до одного года, либо лишением свободы на срок до двух лет; группой лиц по предварительному сговору или организованной группой либо лицом с использованием служебного положения 100 тыс. — 300 тыс. руб. или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, использование или распространение таких программ или машинных носителей с такими программами наказываются лишением свободы на срок до трех лет со штрафом в размере до 200 тыс. руб. или в размере заработной платы или иного дохода осужденного за период до 18 мес. (если это привело по неосторожности к тяжким последствиям, — лишение свободы на срок до семи лет).

Нарушение правил эксплуатации ЭВМ лицом, имеющим доступ к ЭВМ, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ при причинении существенного вреда наказывается

лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от 180 до 240 ч, либо ограничением свободы на срок до двух лет (если это привело по неосторожности к тяжким последствиям — лишение свободы на срок до четырех лет).

Административная ответственность. Административную ответственность устанавливает *Кодекс об административных правонарушениях Российской Федерации (КоАП)*. В частности нарушение установленного законом порядка сбора, хранения, использования или распространения информации о персональных данных граждан влечет предупреждение или наложение административного штрафа на граждан в размере от 300 до 500 руб.; на должностных лиц — от 500 до 1000 руб.; на юридических лиц — от 5 тыс. до 10 тыс. руб. (ст. 13.11).

Ст. 13.12 предусматривает ответственность за нарушение правил защиты информации:

- нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), предполагает штраф от 300 до 500 руб. для граждан, от 500 до 1000 руб. — для должностных лиц, от 5 тыс. до 10 тыс. руб. — для юридических лиц;
- использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), — штраф 500 –1000 руб. для граждан, 1000 — 2000 руб. для должностных лиц, 10 — 20 тыс. руб. для юридических лиц с конфискацией таких средств или без таковой;
- нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, — штраф в размере от 2 тыс. до 3 тыс. руб. — для должностных лиц, от 15 тыс. до 20 тыс. руб. — для юридических лиц;
- использование несертифицированных средств защиты информации, составляющей государственную тайну, — штраф 3 тыс. — 4 тыс. руб. для должностных лиц и 20 тыс. — 30 тыс. руб. для юридических лиц с конфискацией таких средств или без таковой;
- грубое нарушение условий лицензии на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), — штраф 1000 —1500 руб. для индивидуальных предпринимателей без образования юридического лица или административное приостановление деятельности на срок до 90 сут., 1000 — 1500 руб. для должностных лиц; и от 10 тыс. до 15 тыс. руб. для юридических лиц или административное приостановление деятельности на срок до 90 сут.

Ст. 13.13 устанавливает ответственность за незаконную деятельность в области защиты информации:

• занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без лицензии, если такая лицензия обязательна, влечет наложение штрафа на граждан в размере 500 — 1000 тыс. руб. с конфискацией средств защиты информации или без таковой, на должностных лиц — от 2 тыс. до 3 тыс. рублей с конфискацией средств защиты информации или без таковой, на юридических лиц — от 10 тыс. до 20 тыс. руб. с конфискацией средств защиты информации или без таковой;

• занятие деятельностью, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств защиты такой информации, осуществлением мероприятий и (или) оказанием услуг по защите такой информации, без лицензии — штраф на должностных лиц от 4 тыс. до 5 тыс. руб., на юридических лиц — от 30 тыс. до 40 тыс. руб. с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных ч. 1 ст. 14.33 КоАП, влечет наложение административного штрафа на граждан в размере от 500 до 1000 руб., на должностных лиц — от 4 тыс. до 5 тыс. руб. (ст.13.14).

Гражданский кодекс РФ (ч. IV) в ст. 1253. предусматривает ответственность юридических лиц и индивидуальных предпринимателей за нарушения исключительных прав на результаты интеллектуальной деятельности и средства индивидуализации, в частности суд может в соответствии с п. 2 ст. 61 Гражданского кодекса принять решение о прекращении деятельности такого юридического лица или индивидуального предпринимателя по требованию прокурора.

В ст. 1290 определена ответственность по договорам, заключаемым автором произведения, которая ограничена суммой реального ущерба, причиненного другой стороне, если договором не предусмотрен меньший размер ответственности автора. В случае неисполнения или ненадлежащего исполнения договора авторского заказа, за которое автор несет ответственность, автор обязан возвратить заказчику аванс, а также уплатить неустойку, если она предусмотрена договором. При этом общий размер указанных выплат ограничен суммой реального ущерба, причиненного заказчику.

В случаях нарушения исключительного права на произведение, ст. 1301 (объект смежных прав, ст. 1311), автор (обладатель исключительного права) наряду с использованием других применимых способов защиты и мер ответственности, установленных Гражданским кодексом (ст. 1250, 1252 и 1253), вправе в соответствии с п. 3 ст. 1252 требовать по своему выбору от нарушителя вместо возмещения убытков выплаты компенсации:

• в размере от 10 тыс. до 5 млн руб., определяемом по усмотрению суда;

• в двукратном размере стоимости экземпляров произведения (фонограммы) или двукратном размере стоимости права использования произведения

(объекта смежных прав), определяемой, исходя из цены, которая при сравнимых обстоятельствах обычно взимается за правомерное использование произведения (объекта).

Нарушитель исключительного права на секрет производства (ст. 1472), в том числе лицо, которое неправомерно получило сведения, составляющие секрет производства, и разгласило или использовало эти сведения, а также лицо, обязанное сохранять конфиденциальность секрета производства в соответствии с п. 2 ст. 1468, п. 3 ст. 1469 или п. 2 ст. 1470 Гражданского кодекса, обязано возместить убытки, причиненные нарушением исключительного права на секрет производства, если иная ответственность не предусмотрена законом или договором с этим лицом (лицо, которое использовало секрет производства и не знало о незаконности своих действий, не несет ответственности за это нарушение).

Федеральный закон «О коммерческой тайне» в ст. 11 определяет обязанности работников и работодателя по охране конфиденциальности информации в рамках трудовых отношений.

Работодатель обязан:

• ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой является работодатель и его контрагенты;

• ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и мерами ответственности за его нарушение;

• создать работнику необходимые условия для соблюдения режима коммерческой тайны.

Работник обязан:

• выполнять установленный работодателем режим коммерческой тайны;

• не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;

• передать работодателю при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну.

Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

Нарушение Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации (ст. 14).

Невыполнение обладателем информации, составляющей коммерческую тайну, законных требований органов государственной власти или местного самоуправления о предоставлении им такой информации, как и воспрепятствование получению должностными лицами этих органов указанной информации, влечет за собой ответственность в соответствии с законодательством Российской Федерации (ст. 15).

* * *

Развитие информационного общества в Российской Федерации базируется на принципах минимизации рисков и угроз национальной безопасности России, связанных с враждебным и преступным использованием возможностей информационно-коммуникационных технологий, укреплением доверия и безопасности при их использовании.

Правительство Российской Федерации регулирует требования к обеспечению безопасности данных и отдельных граждан (персональных данных) при их обработке, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Контрольные вопросы

1. Приведите классификацию информации по доступности с точки зрения Федерального закона «Об информации, информационных технологиях и о защите информации».
2. Дайте определения обладателя информации и оператора информационной системы.
3. Перечислите права и обязанности обладателя информации.
4. Дайте определение понятия «коммерческая тайна» в соответствии с Федеральным законом «О коммерческой тайне».
5. Какая информация не может быть отнесена к коммерческой тайне?
6. Каким нормативным актом утвержден Перечень сведений конфиденциального характера?
7. В каком кодексе предусмотрена ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)?
8. В каком кодексе предусмотрена ответственность за «незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»?
9. Какие статьи Уголовного кодекса РФ определяют ответственность за преступления в сфере компьютерной информации?
10. С какого возраста предусмотрена уголовная ответственность за преступления в сфере компьютерной информации?
11. В какой статье Уголовного кодекса РФ определяется ответственность за создание, использование и распространение вредоносных программ для ЭВМ ?
12. Что такое лицензирование?
13. Какие виды лицензирования вам известны?
14. Для кого аттестация АИС по требованиям безопасности информации ФСТЭК России является обязательной?
15. Когда проводится аттестация АИС по требованиям безопасности информации ФСТЭК России?
16. Перечислите классы защищенности СВТ в соответствии с руководящими документами ФСТЭК России.
17. Перечислите классы защищенности АС в соответствии с руководящими документами ФСТЭК России.
18. Какие подсистемы включает в себя комплекс программно-технических средств защиты информации от НСД в АС?

Глава 6. ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Структура государственной системы защиты информации в Российской Федерации, ее задачи и функции, основы организации защиты сведений, отнесенных к государственной или служебной тайне, определены в Положении о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденном *постановлением Совета Министров — Правительства Российской Федерации от 15.09.1993 № 912-51.*

Этот документ обязателен для выполнения при проведении работ по защите информации, содержащей сведения, составляющие государственную или служебную тайну, в органах государственной власти (представительной, исполнительной и судебной властей Российской Федерации, республик в составе Российской Федерации, автономной области, автономных округов, краев, областей, городов Москвы и Санкт-Петербурга) и в органах местного самоуправления, на предприятиях, в учреждениях и организациях независимо от их организационно-правовой формы и формы собственности.

Работы по защите информации в органах государственной власти и на предприятиях проводятся на основе актов законодательства Российской Федерации путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий в целях уничтожения или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также за счет проведения специальных работ, порядок организации и выполнения которых определяются Правительством Российской Федерации.

6.1. Главные направления работ по защите информации

Мероприятия по защите информации — составная часть управленческой, научной и производственной деятельности — осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности проводимых работ.

Главные направления работ по защите информации:

- обеспечение эффективного управления системой защиты информации;
- определение сведений, охраняемых от технических средств разведки, и демаскирующих признаков, раскрывающих эти сведения;
- анализ и оценка реальной опасности перехвата информации техническими средствами разведки, несанкционированного доступа, разрушения (уничтожения) или искажения путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки сведений, подлежащих защите;

• разработка организационно-технических мероприятий по защите информации и их реализация;

• организация и проведение контроля состояния защиты информации.

К основным организационно-техническим м е р о п р и я т и я м по защите информации относят:

• лицензирование деятельности предприятий в области защиты информации;

• аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

• разработку и сертификацию СЗИ систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;

• введение территориальных, частотных, энергетических, пространственных и временны́х ограничений в режимах использования технических средств, подлежащих защите;

• создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

• разработку и внедрение технических решений и элементов защиты информации при проектировании, строительстве и эксплуатации объектов, систем и средств информатизации и связи;

• применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

Конкретные методы, приемы и меры защиты информации разрабатывают в зависимости от степени возможного ущерба в случае ее утечки или уничтожения.

Проведение любых мероприятий и работ с использованием сведений, отнесенных к государственной или служебной тайне, без принятия необходимых мер по защите информации не допускается.

6.2. Структура государственной системы защиты информации

Основные з а д а ч и государственной системы защиты информации:

• проведение единой технической политики, организация и координация работ по защите информации во всех сферах деятельности;

• исключение или существенное затруднение доступа к информации техническими средствами разведки, предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных программно-технических воздействий в целях разрушения или искажения информации в процессе ее обработки, передачи или хранения;

• анализ состояния и прогнозирование возможностей технических средств разведки и способов их применения, формирование системы информационного обмена сведениями по осведомленности иностранных разведок;

• создание СЗИ и контроль за их использованием в органах государственной власти и на предприятиях.

Государственную систему защиты информации в Российской Федерации образуют:

• Федеральная служба по техническому и экспортному контролю Российский Федерации (ФСТЭК России);

• Федеральная служба безопасности Российской Федерации (ФСБ России), Министерство внутренних дел Российской Федерации (МВД России), Министерство обороны Российской Федерации (Минобороны России), Федеральная служба охраны Российской Федерации (ФСО России), Служба внешней разведки Российской Федерации (СВР России), их структурные подразделения по защите информации;

• структурные и межотраслевые подразделения по защите информации органов государственной власти;

• управления ФСТЭК России по федеральным округам;

• головная научно-исследовательская организация в Российской Федерации по защите информации — ФГУП «Научно-исследовательский испытательный институт проблем технической защиты информации»;

• головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские организации по защите информации в органах государственной власти;

• предприятия, проводящие работы с использованием сведений, отнесенных к государственной или служебной тайне, их подразделения по защите информации;

• предприятия, специализирующиеся на выполнении работ в области защиты информации;

• высшие учебные заведения и институты повышения квалификации по подготовке и переподготовке кадров в области защиты информации.

Права и функции *ФСТЭК России* и ее центрального аппарата определяются Положением о Федеральной службе по техническому и экспортному контролю и Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам.

Структурные и межотраслевые подразделения по защите информации органов государственной власти (в пределах их компетенции):

• проводят единую техническую политику, осуществляют координацию и методическое руководство работами по защите информации на подведомственных органу государственной власти предприятиях;

• выполняют функции заказчика по проведению научно-исследовательских и опытно-конструкторских работ по проблемам защиты информации;

• разрабатывают предложения для федеральных программ по защите информации;

• организуют аттестацию подведомственных органу государственной власти объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности, сертификацию средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности ин-

формации от утечки по техническим каналам, проведение специальных проверок и исследований технических средств;

• готовят рекомендации и указания по лицензированию деятельности предприятий в области защиты информации.

Непосредственное руководство работами по защите информации осуществляют руководители органов государственной власти или их заместители.

Подразделения по защите информации могут быть как самостоятельными, так и входить в состав одного из управлений органа государственной власти. Назначение (освобождение) руководителей этих подразделений проводят по согласованию с ФСТЭК России.

Для обеспечения принципа коллегиальности при рассмотрении важнейших вопросов защиты информации в органах государственной власти создают технические комиссии, межотраслевые или отраслевые советы.

Управления ФСТЭК России по федеральным округам:

• проверяют и оценивают состояние защиты информации;

• оказывают методическую помощь на местах в организации и проведении мероприятий по защите информации;

• участвуют в аттестации объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности.

Головная научно-исследовательская организация в Российской Федерации по защите информации, *головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские организации* по защите информации органов государственной власти в пределах своей специализации разрабатывают концепции, проекты федеральных программ, нормативно-технических и методических документов по защите информации, обобщают и анализируют информацию о силах и средствах технической разведки, прогнозируют ее возможности, осуществляют разработку (корректировку) модели иностранной технической разведки и методик оценки ее возможностей, проводят научные исследования и работы по созданию технических СЗИ.

Организацию работ по защите информации на предприятиях осуществляют руководители.

В зависимости от объема работ по защите информации руководителем предприятия создается структурное подразделение по защите информации либо назначаются штатные специалисты по этим вопросам.

Подразделения по защите информации (штатные специалисты) на предприятиях:

• осуществляют мероприятия по защите информации в ходе выполнения работ с использованием сведений, отнесенных к государственной или служебной тайне;

• определяют совместно с заказчиком работ основные направления комплексной защиты информации;

• участвуют в согласовании технических (тактико-технических) заданий на проведение работ;

• дают заключение о возможности проведения работ с информацией, содержащей сведения, отнесенные к государственной или служебной тайне.

Такие подразделения подчиняются непосредственно руководителю предприятия или его заместителю, а работники этих подразделений приравниваются по оплате труда к соответствующим категориям работников основных структурных подразделений организации.

Для проведения работ по защите информации на договорной основе привлекают специализированные предприятия, имеющие лицензию (ФСТЭК России или ФСБ России) на право проведения работ в области защиты информации.

Высшие учебные заведения и институты повышения квалификации по подготовке и переподготовке кадров в области защиты информации осуществляют:

• первичную подготовку специалистов по комплексной защите информации;

• переподготовку (повышение квалификации) специалистов по защите информации органов государственной власти и предприятий;

• усовершенствование знаний руководителей органов государственной власти и предприятий в области защиты информации.

6.3. Организация защиты информации в системах и средствах информатизации и связи

Защита информации в системах и средствах информатизации и связи — составная часть работ по их созданию и эксплуатации, осуществляемых во всех органах государственной власти и организациях, располагающих информацией, содержащей сведения, отнесенные к государственной или служебной тайне.

Требования по защите такой информации определяются заказчиками совместно с разработчиками на стадии подготовки и согласования решений Правительства РФ, приказов и директив, планов и программ работ, технических и тактико-технических заданий на проведение исследований, разработку (модернизацию), испытания, производство и эксплуатацию на основе стандартов, нормативно-технических и методических документов, разработанных Федеральным агентством по техническому регулированию и метрологии (Росстандарт), ФСТЭК России и другими органами государственной власти в соответствии с их компетенцией.

Организация защиты информации, содержащей государственную или служебную тайну, возлагается на руководителей органов государственной власти и предприятий, заказчиков и разработчиков систем и средств информатизации и связи, руководителей подразделений, эксплуатирующих эти системы и средства, а ответственность за обеспечение защиты информации — непосредственно на пользователя (потребителя) информации.

Объектами защиты являются:

• *информационные ресурсы*, содержащие сведения, отнесенные к государственной или служебной тайне, представленные в виде носителей на магнит-

ной и оптической основе, информативных физических полей, информационных массивов и баз данных;

• *средства и системы информатизации*: СВТ, программные средства (ОС, СУБД, другое общесистемное и прикладное программное обеспечение), АСУ, системы связи и передачи данных, технические средства приема, передачи и обработки информации, содержащей сведения, отнесенные к государственной или служебной тайне;

• *технические средства и системы*, не обрабатывающие информацию, но размещенные в помещениях, где циркулирует информация, содержащая сведения, отнесенные к государственной или служебной тайне, а также сами помещения, предназначенные для ведения секретных переговоров.

Защита информации осуществляется следующими способами:

• предотвращением перехвата техническими средствами информации, передаваемой по каналам связи криптографическими и иными средствами защиты, а также проведением организационно-технических и режимных мероприятий за счет применения защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдельных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами;

• исключением НСД к обрабатываемой или хранящейся в технических средствах информации благодаря применению специальных программно-технических средств защиты, криптографических способов защиты, а также организационных и режимных мероприятий;

• предотвращением специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации в результате применения специальных программных и аппаратных средств защиты (антивирусные процессоры, антивирусные программы), организации системы контроля безопасности программного обеспечения;

• выявлением внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств) путем проведения периодических проверок по выявлению таких устройств;

• предотвращением перехвата техническими средствами речевой информации из помещений и объектов с помощью специальных средств защиты, проектных решений, обеспечивающих звукоизоляцию помещений, выявления специальных устройств подслушивания и др.

Соответствие технического средства и его программного обеспечения требованиям защищенности подтверждается сертификатом, выдаваемым предприятием, имеющим лицензию на этот вид деятельности.

Защиту информации, передаваемую по общегосударственным и ведомственным линиям связи, осуществляют потребители, которые по согласованию с подразделениями ФСТЭК России и Министерства связи и массовых коммуникаций РФ разрабатывают инструкции по обеспечению защиты информации и определяют перечень организационных и технических мер по предотвращению утечки информации по техническим каналам.

Необходимость защиты доступных средствам радиоразведки каналов связи, по которым передаются потоки служебной информации, где отдельно взятые сведения не составляют государственную или служебную тайну, определяется решениями ФСТЭК России по согласованию с заинтересованными органами государственной власти.

6.4. Контроль состояния защиты информации

Контроль состояния защиты информации проводят для своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию.

Контроль проводят: ФСТЭК России, ФСБ России, МВД России, Минобороны России, СВР и ФСО России, а также структурные и межотраслевые подразделения органов государственной власти, входящие в государственную систему защиты информации.

Повседневный контроль за состоянием защиты информации в организации осуществляют подразделения по защите информации, находящиеся непосредственно в организации.

Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам. Несоответствие мер требованиям или нормам по защите информации считается нарушением.

Нарушения по степени важности подразделяют на три категории:

1) невыполнение требований или норм привело к реальной возможности утечки информации по техническим каналам;

2) несоблюдение требований по защите информации с созданием предпосылок к ее утечке по техническим каналам;

3) невыполнение других требований по защите информации.

При обнаружении нарушений первой категории руководители органов государственной власти и предприятий обязаны:

- немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения, и принять меры по их устранению;
- организовать расследование причин и условий появления нарушений в целях недопущения их в дальнейшем и привлечения к ответственности виновных лиц;
- сообщить в ФСТЭК России, ФСБ России, руководству органа государственной власти и заказчику о нарушениях и принятых мерах.

Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер.

При обнаружении нарушений второй и третьей категорий руководители проверяемых органов государственной власти и предприятий обязаны принять необходимые меры по их устранению в сроки, согласованные с органом, проводившим проверку, или заказчиком (представителем заказчика). Контроль за устранением нарушений осуществляется подразделениями по защите информации этих органов государственной власти и предприятий.

6.5. Финансирование мероприятий по защите информации

Финансирование мероприятий по защите информации, содержащей сведения, отнесенные к государственной или служебной тайне, а также подразделений по защите информации в органах государственной власти и на бюджетных предприятиях предусматривается в сметах расходов на их содержание.

Обеспечение техническими средствами защиты информации, не требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчиком на научно-исследовательские и опытно-конструкторские работы, связанные с разработкой продукции. Расходы по разработке технических средств защиты включаются в стоимость разработки образца продукции.

Создание технических средств защиты информации, требующее капитальных вложений, осуществляется в пределах средств, выделяемых заказчиком на строительство (реконструкцию) сооружений или объектов.

* * *

Ключевым моментом политики государства в области обеспечения АС является осознание необходимости защиты любых информационных ресурсов и информационных технологий, неправомерное обращение с которыми может нанести ущерб их обладателю (собственнику, владельцу, пользователю) или иному лицу.

Соответствие технического средства и его программного обеспечения требованиям защищенности подтверждается сертификатом, выдаваемым предприятием, имеющим лицензию на этот вид деятельности.

Информация, содержащая сведения, отнесенные к государственной или служебной тайне, должна обрабатываться с использованием либо защищенных систем и средств информатизации и связи, либо технических и программных средств защиты, сертифицированных в установленном порядке.

Контрольные вопросы

1. Назовите главные направления работ по защите информации.
2. Перечислите основные организационно-технические мероприятия в области защиты информации.
3. В чем заключаются основные задачи государственной системы защиты информации?
4. Какова структура государственной системы защиты информации?
5. Каковы цели защиты информации?
6. В чем заключается контроль состояния защиты информации?
7. Каковы источники финансирования мероприятий по защите информации?

РАЗДЕЛ II

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Глава 7. ОРГАНИЗАЦИОННАЯ СТРУКТУРА СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Проблемы безопасности АС каждой конкретной организации «не уникальны», поэтому приведенная далее технология управления безопасностью информации и ресурсов в автоматизированной системе носит универсальный характер, поскольку в ней обобщен опыт специалистов многих организаций и стран.

Целью создания системы обеспечения безопасности информационных технологий является достижение заданного уровня информационной безопасности организации (предприятия), чтобы предотвратить или минимизировать ущерб, наносимый субъектам информационных отношений посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

Основная задача системы защиты — обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов АС соответствующими методами и средствами.

7.1. Технология управления безопасностью информации и ресурсов в автоматизированной системе

Как уже отмечалось, обеспечение безопасности АС есть процесс управления рисками, следовательно, система защиты — это система управления, реализующая технологию обеспечения безопасности (управления безопасностью). Любая технология предусматривает определенный набор операций и процессов взаимодействия их исполнителей, направленный на достижение конечного результата (цели).

При разработке технологии управления решают следующие в о п р о с ы :

• определяют категории сотрудников, входящих в систему безопасности АС организации, и их функции;

• регламентируют порядок взаимодействия подразделений;

• разрабатывают перечень регламентируемых процессов и действий;

• составляют организационно-распорядительные и нормативно-методические документы.

Под *технологией обеспечения безопасности* информации и ресурсов в АС понимается определенное распределение функций и регламентация порядка их исполнения, а также порядка взаимодействия подразделений и сотрудников (должностных лиц) организации по обеспечению комплексной защиты ресурсов АС в процессе ее эксплуатации.

К технологии управления безопасностью предъявляют определенные т р е б о в а н и я :

• соответствие современному уровню развития информационных технологий;

• учет особенностей построения и функционирования различных подсистем АС;

• точная и своевременная реализация политики безопасности организации;

• минимизация затрат на реализацию самой технологии обеспечения безопасности;

• наличие полной и непротиворечивой правовой базы по вопросам обеспечения безопасности ИТ;

• четкое распределение функций и порядка взаимодействия подразделений и должностных лиц организации по вопросам обеспечения безопасности ИТ на всех этапах жизненного цикла подсистем АС;

• наличие подразделения защиты информации, наделенного необходимыми полномочиями, которое отвечает за формирование и реализацию единой политики безопасности ИТ организации и осуществляет контроль и координацию действий подразделений и сотрудников организации по вопросам обеспечения безопасности ИТ.

При реализации технологии управления безопасностью АС осуществляют следующие м е р о п р и я т и я :

• назначение и подготовка сотрудников, ответственных за организацию, реализацию функций и осуществление конкретных практических мероприятий по обеспечению безопасности информации и процессов ее обработки;

• строгий учет всех подлежащих защите ресурсов системы (информации, ее носителей и процессов обработки) с определением требований к организационно-техническим мерам и средствам защиты;

• разработка реально выполнимых и непротиворечивых организационно-распорядительных документов по вопросам обеспечения безопасности информации;

• реорганизация технологических процессов обработки информации в АС с учетом требований по безопасности ИТ;

• поддержание необходимого уровня защищенности и целостности технических средств;

• регламентация процессов обработки подлежащей защите информации с применением средств автоматизации при участии сотрудников структурных подразделений, использующих АС, и персонала, осуществляющего обслуживание и модификацию программных и технических средств АС, в соответствии с организационно-распорядительными документами по вопросам обеспечения безопасности ИТ;

• контроль за соблюдением сотрудниками подразделений — пользователями и обслуживающим АС персоналом — требований по обеспечению безопасности информации;

• проведение постоянного анализа эффективности и достаточности принятых мер и средств защиты информации;

• разработка и реализация предложений по совершенствованию системы защиты информации в АС.

7.2. Институт ответственных за обеспечение информационной безопасности

Обеспечение информационной безопасности — это непрерывный процесс, основное содержание которого составляет управление рисками через управление людьми, ресурсами, средствами защиты и т. п.

Обслуживающий персонал и конечные пользователи АС — неотъемлемая часть АС и от того, каким образом они реализуют свои функции в системе, существенно зависит не только ее функциональность (эффективность решения задач), но и безопасность.

Уровень информационной безопасности организации существенно зависит от деятельности следующих категорий сотрудников и должностных лиц организации (рис. 7.1):

• руководителей организации, определяющих цели и задачи функционирования АС;

• сотрудников подразделения защиты информации, оценивающих состояние безопасности АС, определяющих требования к системе защиты, разрабатывающих организационно-распорядительные документы, внедряющих и администрирующих специализированные дополнительные средства защиты (администраторов безопасности);

• системных администраторов штатных средств защиты (ОС, СУБД и т. п.);

• сотрудников подразделения эксплуатации технических средств (ТС), обеспечивающих нормальную работу и обслуживание, обработки и передачи информации и системного ПО;

• сотрудников подразделения внедрения и сопровождения ПО, обеспечивающих нормальное функционирование и установленный порядок инсталляции и модификации прикладных программ;

• программистов, осуществляющих разработку (приобретение и адаптацию) необходимых прикладных программ для автоматизации деятельности сотрудников организации;

• сотрудников структурных подразделений — конечных пользователей АС, решающих свои функциональные задачи с применением средств автоматизации.

Кроме того, на безопасность ИТ организации могут оказывать влияние посторонние лица и сторонние организации, предпринимающие попытки вмешательства в процесс нормального функционирования АС или несанкционированного доступа к информации как локально, так и удаленно.

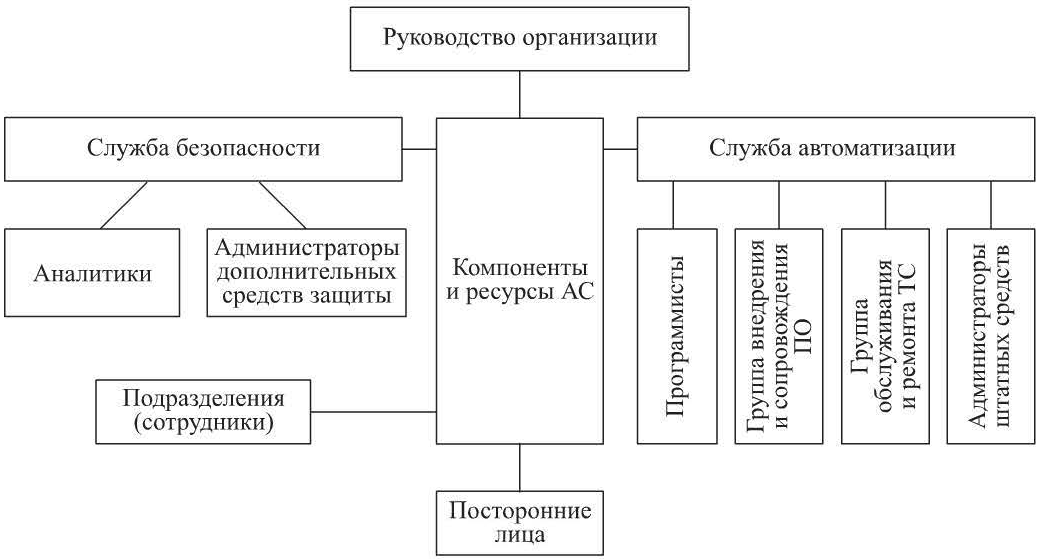

Рис. 7.1. Субъекты, влияющие на состояние безопасности ИТ

Влияние на безопасность информационных технологий руководства организации. Руководство принимает стратегические решения по вопросам обеспечения безопасности ИТ и утверждает основные документы, регламентирующие порядок функционирования и развития АС, обеспечивающий безопасную обработку и использование защищаемой информации.

Руководство определяет критичность процессов, ресурсов и степень их защиты, а также координирует деятельность по управлению и распределению обязанностей по обеспечению безопасности ИТ между службами безопасности и автоматизации.

В соответствии со стандартом ISO 27002 руководство должно показывать свою заинтересованность в вопросах безопасности ИТ, оказывать поддержку в распространении политики безопасности ИТ среди сотрудников организации и проводить регулярные совещания по вопросам корректировки политики безопасности, ИТ, и координации действий персонала.

Для того чтобы добиться понимания и осознания важности проблем безопасности ИТ, руководителями используются различные м е р ы, например такие:

• извлечение максимальной пользы из любых инцидентов с акцентом на важность решений вопросов по обеспечению безопасности ИТ;

• организация показательных мероприятий (например, демонстрация слабости парольной защиты) — проведение подобных мероприятий требует предварительного согласования с руководством, документального оформления и осторожности при реализации;

• демонстрация документов других организаций по вопросам обеспечения безопасности ИТ.

Влияние на безопасность информационных технологий службы безопасности. Наиболее важным звеном, оказывающим влияние на безопасность ИТ организации, являются аналитики и администраторы средств защиты, контроля и управления безопасностью — аналитики отвечают за анализ состояния безопасности ИТ, определение требований к защищенности различных подсистем АС, выбор методов и средств защиты; администраторы средств защиты, контроля и управления безопасностью отвечают за эффективное применение специализированных средств защиты.

Влияние на безопасность информационных технологий подразделения автоматизации. Наиболее существенное влияние на безопасность ИТ организации в подразделении автоматизации оказывают специалисты служб разработки, внедрения и сопровождения ПО, эксплуатации технических средств и общего программного обеспечения, системные администраторы.

Влияние программистов может быть как непреднамеренным (ошибки), так и преднамеренным (закладки, люки). Практика показывает, что ошибки кода присутствуют практически в каждой программе.

Администраторы серверов, приложений и баз данных отвечают за эффективное применение штатных средств защиты и разграничение доступа всех используемых ОС и СУБД.

Для обеспечения безопасности ИТ необходимо повышение ответственности на основе регламентации процессов разработки, отладки и внедрения ПО, т. е. разделение сотрудников на группы разрабатывающих, тестирующих, внедряющих и сопровождающих ПО.

Влияние на безопасность информационных технологий сотрудников структурных подразделений организации. Совершение ошибок сотрудниками структурных подразделений (конечными пользователями системы) способствует порождению угроз, которые затем могут быть использованы злоумышленниками для нанесения вреда организации и ее сотрудникам. К числу таких у г р о з можно отнести:

• создание предпосылок к осуществлению НСД со стороны других лиц (уязвимостей, каналов проникновения) к критичным ресурсам системы;

• разглашение конфиденциальной информации (сведений, составляющих коммерческую тайну организации, персональных данных, паролей и др.);

• заражение рабочих станций вирусами, «троянскими» и другими вредоносными программами (внедрение шпионских кодов);

• создание помех для основных производственных процессов или остановка их работы.

Злоумышленники преследуют определенные ц е л и :

• порча или утрата материального имущества (технических средств);

• искажение или утрата файлов с важной информацией;

• потеря конкурентных преимуществ в результате разглашения сведений, составляющих коммерческую тайну;

• дезорганизация или снижение эффективности производственных процессов (нарушение работоспособности подсистем);

• непроизводительные траты ресурсов (материальных, информационных, операционных, рабочего времени и др.);

• судебные иски к организации, ее руководителям и сотрудникам со стороны государственных органов, других юридических и физических лиц;

• потеря деловой репутации организации (с последующей потерей клиентов, партнеров и т. п.);

• нанесение физического или морального ущерба сотрудникам организации или третьим лицам.

Смысл безопасности ИТ состоит в жесткой регламентации деятельности сотрудников, сочетающейся с высокой исполнительской дисциплиной. Необходимо учитывать, что регламентация деятельности сотрудников, непосредственно не подчиненных службе безопасности, может привести к возникновению конфликтных ситуаций, поэтому дополнительные функции сотрудников должны быть четко определены в соответствующих инструкциях.

7.3. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы

Обслуживающий персонал и пользователи, как неотъемлемая часть АС, сами являются источником внутренних угроз безопасности ИТ организации и одновременно могут быть частью системы защиты АС, поэтому одно из основных направлений обеспечения безопасности, как уже отмечалось, — регламентация действий всех пользователей и обслуживающего персонала АС, проводимая в целях:

• ограничения возможностей лиц из числа пользователей и персонала совершения нарушений (как неумышленных, так и преднамеренных);

• реализации специальных мер противодействия другим внутренним и внешним для системы угрозам (связанным с отказами и сбоями оборудования, ошибками в программах, стихийными бедствиями и действиями посторонних лиц, не являющихся частью АС).

Регламентация предусматривает введение таких ограничений и приемов работы сотрудников, которые без создания помех для исполнения ими своих функциональных обязанностей минимизируют возможности совершения ими нарушений (например, наделение каждого сотрудника (пользователя) минимально необходимыми для выполнения своих служебных обязанностей полномочиями по доступу к ресурсам АС).

Регламентации подлежат также вопросы исполнения сотрудниками дополнительных обязанностей, связанных с усилением режима безопасности ИТ. Так, для защиты от действий посторонних лиц и «подкрепления» вводимых ограничений на действия своих сотрудников на компьютерах АС могут применяться средства защиты, работающие на физическом, аппаратном или программном уровне. Применение таких средств защиты требует регламентации вопросов их использования конечными пользователями и процессов их администрирования сотрудниками подразделений автоматизации и обеспечения безопасности ИТ.

Итак, учитывая приведенные доводы, можно сделать вывод о том, что к обеспечению безопасности информационных технологий организации (и в определенной степени к управлению ее безопасностью) должны привлекаться практически все сотрудники, участвующие в процессах автоматизированной обработки информации, и все категории обслуживающего АС персонала (кроме посторонних лиц).

Роли и функции различных категорий сотрудников и подразделений организации в обеспечении безопасности ИТ существенно различаются (большинство сотрудников лишь исполняют установленные в организации регламенты и правила безопасной работы в АС).

Создание и эффективное функционирование системы безопасности ИТ может быть обеспечено только при наличии следующих с о с т а в л я ю щ и х:

- системы организационно-распорядительных и нормативно-методических документов, определяющих политику безопасности ИТ (регламенты по вопросам безопасности АС для всех категорий сотрудников организации);
- технических средств защиты и контроля эффективности принятых мер защиты;
- специального подразделения (например, отдела технической защиты информации — ОТЗИ), которое отвечает за формирование системы защиты, реализацию единой политики безопасности ИТ организации, контроль и координацию действий всех подразделений и сотрудников по вопросам обеспечения безопасности ИТ.

7.4. Политика безопасности организации

Политика безопасности организации в области ИТ — это совокупность документируемых решений в виде программных, аппаратных, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, регламентирующих все аспекты деятельности организации в области безопасности ИТ.

Основная *цель* политики безопасности — информирование пользователей, сотрудников и руководства о наложенных на них обязательных требованиях по защите технологии и информационных ресурсов.

Все документально оформленные решения, формирующие политику безопасности ИТ, утверждаются руководством и предоставляются сотрудникам организации для ознакомления.

При определении политики безопасности должны соблюдаться следующие условия:

• непрерывность работы и восстановление АС;

• конфиденциальность стандартных сервисов (электронная почта, Интернет, виртуальные частные сети (VPN), мобильные пользователи);

• аутентификация (пароли, рекомендации по аутентификации удаленных субъектов и использованию аутентифицирующих устройств);

• разграничение доступа и привилегии для различных категорий сотрудников (пользователей, системных администраторов, администраторов безопасности, руководителей);

• блокирование вирусов и других вредоносных программ;

• обучение персонала по вопросам безопасности ИТ;

• защита от недекларированных возможностей ПО;

• ликвидация последствий нарушения политики безопасности и ответственность нарушителей;

• аудит и обновление политики безопасности.

К сожалению, на практике после внедрения в организациях систем обеспечения безопасности возможны следующие типичные проблемы:

• отсутствие необходимой организационной основы для согласованных действий подразделений организации по выработке и реализации единой политики безопасности ИТ;

• неполнота, противоречивость и несоответствие требованиям законодательства РФ нормативно-правовой базы организации по вопросам обеспечения безопасности ИТ.

Для оценки текущего состояния ИТ в организации существуют различные методики и модели зрелости или оптимизации ИТ-инфраструктуры, предлагаемые известными исследовательскими и консалтинговыми организациями в области ИТ (например, Infrastructure Maturity Model, Gartner Group, Architecture Maturity Model, MTI, Infrastructure Optimization Model, Microsoft). Набор сервисов в моделях зрелости называют уровнем зрелости. Так, в Infrastructure Maturity Model (Gartner Group) определены четыре уровня зрелости (в сфере обеспечения ИБ):

0-й уровень: информационной безопасностью в компании никто не занимается, руководство компании не осознает важности проблем информационной безопасности; финансирование отсутствует; информационная безопасность реализуется штатными средствами операционных систем, СУБД и приложений (парольная защита, разграничение доступа к ресурсам и сервисам);

1-й уровень: информационная безопасность рассматривается руководством как чисто «техническая» проблема, отсутствует единая концепция развития системы обеспечения информационной безопасности компании; финансирование осуществляется в рамках общего ИТ-бюджета; информационная безопасность реализуется средствами нулевого уровня, а также средствами резервного копирования, антивирусными средствами, межсетевыми экранами, средствами организации VPN (построения виртуальных частных сетей), т. е. используются традиционные средства защиты;

2-й уровень: информационная безопасность рассматривается руководством как комплекс организационных и технических мероприятий; существует понимание важности информационной безопасности для производственных процессов; имеется программа развития системы обеспечения информационной безопасности компании; финансирование осуществляется по отдельной строке бюджета; дополнительно к средствам первого уровня применяют средства усиленной аутентификации, анализа почтовых сообщений и веб-контента, обнаружения вторжений (IDS), анализа защищенности, однократной аутентификации (SSO), инфраструктуру открытых ключей (PKI) и организационные меры (внутренний и внешний аудит, анализ рисков, политика информационной безопасности, положения, процедуры, регламенты и руководства);

3-й уровень: информационная безопасность — часть корпоративной культуры, выделена штатная единица — старший администратор по вопросам обеспечения информационной безопасности (CISA); финансирование ведется в рамках отдельного бюджета, а в дополнение к средствам второго уровня реализована система управления информационной безопасностью; сформирована группа реагирования на инциденты нарушения информационной безопасности (CSIRT); подписано соглашение об уровне сервиса (SLA).

7.5. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты

Организационные и организационно-технические мероприятия подразделяют:

- на *разовые* (однократно проводимые и повторяемые только при полном пересмотре принятых решений);
- *проводимые* по необходимости (при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде);
- *периодически проводимые* (через определенный промежуток времени);
- *постоянно проводимые* (непрерывно или дискретно в случайные моменты времени).

Разовые мероприятия. Эти однократно осуществляемые мероприятия проводят при создании нормативно-методологической базы защиты АС; проектировании, строительстве и оборудовании вычислительных центров и других объектов АС для исключения возможности тайного проникновения в помещения и установки технических средств несанкционированного съема информации; вводе в эксплуатацию технических средств и программного обеспечения для проверки и сертификации используемых технических и программных средств.

При необходимости изменить организацию охраны, пропускной режим доступа сотрудников, уровень защищенности также проводят разовые мероприятия в подразделениях и на технологических участках, осуществляющих организацию и контроль за соблюдением всеми категориями должностных

лиц требований по обеспечению безопасности программно-информационных ресурсов автоматизированной системы обработки информации.

К разовым мероприятиям относят регулярно-проводимые превентивные меры и оперативные действия персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса АС, обновление версий используемых и установка новых системных прикладных программ в критических ситуациях НСД, сбои и отказы СВТ, ошибки в программах и действиях персонала, стихийные бедствия.

Периодически проводимые мероприятия. Если требуется изменить реквизиты разграничения доступа (пароли, ключи шифрования и т. п.), принять меры по обнаруженным нарушениям правил работы, провести анализ состояния и оценки эффективности мер и применяемых средств защиты, то осуществляют периодически проводимые мероприятия.

Мероприятия, проводимые по мере необходимости. По мере необходимости в организациях проводят следующие мероприятия:

- осуществляемые при кадровых изменениях в организации;
- после ремонта и модификации оборудования и программного обеспечения (рассмотрение и утверждение изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т. п.);
- по проверке нового оборудования, предназначенного для обработки закрытой информации, на наличие специально внедренных закладных устройств, инструментальному контролю технических средств на наличие побочных электромагнитных излучений и наводок;
- по защите оборудования систем информатизации от сбоев электропитания и помех в линиях связи и в связи с меняющейся оперативной обстановкой;
- при оформлении юридических документов (договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами) и третьей стороной (арбитражем, третейским судом) о правилах разрешения споров, связанных с информационным обменом.

Постоянно проводимые мероприятия. К таким мероприятиям относят:

- мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АС (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности СВТ, носителей информации и т. п.);
- мероприятия по непрерывной поддержке функционирования используемых средств защиты и управлению (администрированию) ими;
- организацию явного и скрытого контроля за работой пользователей и персонала системы;
- контроль за реализацией выбранных мер защиты на всех этапах жизненного цикла АС;
- анализ состояния и оценка эффективности мер и применяемых средств защиты, осуществляемые постоянно (силами службы безопасности) и периодически сторонними специалистами.

7.6. Распределение функций по обеспечению безопасности автоматизированных систем

Реализация функций по обеспечению безопасности АС осуществляется подразделениями безопасности и автоматизации в соответствии с организационно-распорядительными документами (положениями, инструкциями, должностными обязанностями), а также отдельными сотрудниками организации.

Технология управления безопасностью АС предусматривает взаимодействие подразделений по обеспечению безопасности и должностных лиц организации.

Подразделение безопасности (отдел защиты информации). Служба безопасности представляет собой систему штатных подразделений и нештатных сотрудников, организующих и обеспечивающих комплексную защиту информации и выполнение различных мероприятий по созданию и поддержанию работоспособности системы защиты.

В соответствии с организационно-распорядительными документами подразделение безопасности выполняет следующие р а б о т ы :

• определяет критерии отнесения ресурсов АС к той или иной категории по требуемой степени защищенности и оформляет их в виде «Положения об определении требований по защите (категорировании) ресурсов»;

• формирует типовые конфигурации и настройки программно-аппаратных средств защиты информации для автоматизированных рабочих мест (АРМ) различных категорий (требуемых степеней защищенности);

• по заявкам руководителей структурных подразделений (используя формуляры АРМ и формуляры задач) проводит анализ возможности решения указанных задач на конкретных АРМ (с точки зрения обеспечения безопасности) и принимает решение об отнесении АРМ к той или иной группе по степени защищенности;

• по установке на АРМ программно-аппаратных средств защиты информации совместно с подразделениями технического обслуживания службы автоматизации;

• определяет организацию, методы и средства контроля эффективности противодействия попыткам НСД и незаконного вмешательства в процесс функционирования АС.

Подразделение автоматизации (отдел эксплуатации и отдел телекоммуникаций). В своей деятельности сотрудники отдела эксплуатации руководствуются «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АРМ АС организации».

Подразделение автоматизации принимает участие в заполнении (корректировке сведений) формуляров АРМ и выдаче предписаний на эксплуатацию АРМ для решения конкретных задач и производит:

• установку (развертывание, обновление версий) программных средств, необходимых для решения на АРМ конкретных задач (используя полученные в фонде алгоритмов и программ (ФАП) дистрибутивы и формуляры задач);

• удаление неиспользуемых программных пакетов;

• установку новых АРМ или подключение дополнительных устройств (узлов, блоков) для решения на АРМ конкретных задач;

• изъятие или замену ПЭВМ (отдельных устройств, узлов, блоков), необходимость в использовании которых отпала, предварительно осуществляя затирание остаточной информации на изымаемых машинных носителях.

Подразделение автоматизации (фонд алгоритмов и программ). Данное подразделение ведет общий перечень задач, решаемых в АС организации; совместно с отделами разработки и сопровождения службы автоматизации и отделом защиты информации заполняет формуляры на новые функциональные задачи АС, сдаваемые в ФАП; хранит, осуществляет резервное копирование, контроль целостности и выдачу лицензионных дистрибутивов или эталонных носителей, принятых в ФАП программных пакетов.

Структурные подразделения организации. Ответственный за обеспечение безопасности ИТ в подразделении следит за реализацией разработанных службой безопасности и утвержденных руководством организации регламентов и выполняет следующие обязанности:

• определяет функциональные задачи, которые должны решаться в подразделении с использованием АРМ;

• проверяет проводимые изменения в конфигурации АРМ и полномочия пользователей подразделения на соответствие «Инструкции по внесению изменений в списки пользователей АС организации и наделению их полномочиями доступа к ресурсам системы» и «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АРМ автоматизированной системы организации»;

• заполняет формуляры АРМ и предоставляет их на утверждение в отдел технической защиты службы безопасности;

• обеспечивает надлежащую эксплуатацию установленных на АРМ средств защиты информации.

7.7. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем

К документам, содержащим требования по обеспечению безопасности информации при работе в АС, относят следующие:

• *Устав* организации — основной документ, в соответствии с которым организация осуществляет свою деятельность;

• *Концепция обеспечения безопасности информационных технологий* — на основе анализа современного состояния информационной инфраструктуры организации и интересов организации в области обеспечения безопасности

АС определяет основные задачи по защите информации и процессов ее обработки, намечает подходы и основные пути решения данных задач;

• *Положение об определении требований по защите (категорировании) ресурсов* — отражает вопросы взаимодействия подразделений организации при определении требуемой степени защищенности ресурсов АС организации в зависимости от степени ценности обрабатываемой информации, характера обработки и обязательств по обеспечению безопасности информации перед сторонними организациями и физическими лицами;

• *Перечень информационных ресурсов, подлежащих защите*, — отражает классификацию защищаемой информации не только по уровню конфиденциальности (конфиденциально, строго конфиденциально и т. д.), но и по уровню ценности (определяемой возможными прямыми и косвенными экономическими потерями в случае нарушения ее целостности и несвоевременности предоставления), в Перечне указывают также подразделения организации, являющиеся владельцами конкретной защищаемой информации и отвечающие за установление требований к режиму ее защиты;

• *Инструкция по внесению изменений в списки пользователей АС и наделению их полномочиями доступа к ресурсам системы* — содержит любые изменения состава и полномочий пользователей подсистем АС;

• *Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы* — определяет меры безопасности при вводе в эксплуатацию новых рабочих станций и серверов, а также при изменениях конфигурации технических и программных средств существующих компьютеров в АС;

• *Порядок разработки, проведения испытаний и передачи задач (комплексов задач) в эксплуатацию* — регламентирует разработку ПО задач (комплексов задач), проведение испытаний разработанного и приобретенного ПО, передачу ПО в эксплуатацию;

• *Инструкция по организации антивирусной защиты* — приводит перечень мероприятий по защите АС от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих АС, за их ненадлежащее исполнение;

• *Инструкция по организации парольной защиты* — отражает процессы генерации, смены и прекращения действия паролей пользователей в АС организации, а также порядок проведения контроля за действиями пользователей и обслуживающего персонала системы при работе с паролями;

• *Порядок работы с носителями ключевой информации* — разрабатывается при использовании в некоторых подсистемах АС средств криптографической защиты информации и средств ЭЦП.

Для пользователей защищенных АРМ (на которых обрабатывается защищаемая информация или решаются подлежащие защите задачи и установлены соответствующие средства защиты) разрабатывают необходимые дополнения к функциональным обязанностям и технологическим инструкциям,

закрепляющие требования по обеспечению информационной безопасности при работе в АС и ответственность сотрудников за реализацию мер по обеспечению установленного режима защиты информации.

* * *

Задачи организации и функции по обеспечению безопасности ИТ, ее подразделений и сотрудников должны формулироваться в документах с учетом положений действующего в России законодательства по информатизации и защите информации (федеральных законов, указов Президента Российской Федерации, постановлений Правительства Российской Федерации и других руководящих и нормативно-методических документов).

Организационные (административные) меры регламентируют процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Четкое знание и строгое соблюдение всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства АС, требований организационно-распорядительных документов по вопросам обеспечения безопасности информации, а также персональная ответственность за свои действия дают возможность поддерживать безопасность АС на необходимом уровне.

Контрольные вопросы

1. Что понимается под технологией обеспечения безопасности информации и ресурсов в АС?
2. Каковы условия для реализации технологий обеспечения безопасности информации и ресурсов в АС?
3. Какова цель создания системы обеспечения безопасности АС?
4. Охарактеризуйте влияние на состояние безопасности АС различных категорий сотрудников.
5. Перечислите основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты.
6. В чем заключается политика безопасности организации?

Глава 8. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ И ОТВЕТСТВЕННЫХ ЗА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПОДРАЗДЕЛЕНИЯХ

Пользователь автоматизированной системы является важнейшим информационным ресурсом АС, который реализует критичные функции, настраивает ПО, хранит пароли, управляет безопасностью ИТ. Система безопасности ИТ должна обеспечить защиту АС от нарушений со стороны конечных поль-

зователей, обслуживающего персонала, сетевых и системных администраторов, администраторов безопасности и руководителей.

8.1. Проблема человеческого фактора

Аспекты, связанные с безопасностью ИТ, следует учитывать еще на стадии набора персонала, включать их в должностные инструкции и контракты, а также контролировать в течение всего времени работы сотрудника. Стандарт ISO 27002 определяет обязанности персонала организации и пользователей информационных ресурсов из сторонних организаций:

- хранить конфиденциальные (защищаемые организацией) сведения, ставшие ему известными в силу производственной (служебной) необходимости;
- во время работы в организации и в течение трех лет после увольнения не передавать посторонним лицам ставшие ему известными конфиденциальные сведения;
- соблюдать требования и правила обеспечения безопасности информации в организации в соответствии с должностной инструкцией;
- в случае прекращения работы в организации сразу же возвратить организации все документы (в том числе электронные), носители информации и другие материалы, содержание которых отнесено к конфиденциальной информации, полученные в ходе выполнения своих служебных обязанностей и т. д.

При приеме на работу сотрудник должен подписать обязательство о конфиденциальности, ознакомиться с требованиями обеспечения безопасности информации и подтвердить, что он не имеет никаких обязательств перед кем-либо, которые входят в противоречие с настоящим соглашением или ограничивают его деятельность в организации.

Достижение требуемого уровня безопасности ИТ возможно только при выработке у персонала и пользователей АС определенной дисциплины с установлением персональной ответственности за нарушения регламента безопасной обработки информации, правил хранения и использования находящихся в их распоряжении защищаемых ресурсов системы.

Регламентация работы сотрудников предполагает определение для каждой категории пользователей и обслуживающего персонала обязательных знаний, действий и процедур, необходимых для обеспечения безопасности ИТ при автоматизированной обработке информации и обслуживании компонент АС, а также запрещенных действий, которые могут привести к нарушению нормальной работы АС, конфиденциальности или целостности хранимой и обрабатываемой информации, вызвать непроизводительные затраты ресурсов.

8.2. Общие правила обеспечения безопасности

Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным

автоматизированной системы, несет персональную ответственность за свои действия и обязан:

• производить обработку защищаемой информации в подсистемах АС в соответствии с технологическими инструкциями для данных подсистем;

• соблюдать установленные правила обеспечения безопасности;

• хранить в тайне свой пароль (пароли) и с установленной периодичностью в соответствии с Инструкцией по организации парольной защиты автоматизированной системы менять свой пароль (пароли);

• передавать для хранения индивидуальное устройство идентификации (iButton, Smart Card, Proximity, eToken и т. п.), другие реквизиты разграничения доступа и носители ключевой информации только руководителю своего подразделения или ответственному за информационную безопасность в подразделении;

• немедленно ставить в известность ответственного за безопасность ИТ и руководителя подразделения в случае утери носителей ключевой информации, индивидуального устройства идентификации или при подозрении компрометации личных ключей и паролей.

Сотрудникам организации, имеющим доступ к автоматизированным системам, запрещается:

• использовать компоненты программного и аппаратного обеспечения АС не по назначению (в неслужебных целях);

• самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочей станции или устанавливать дополнительные программные и аппаратные средства;

• осуществлять обработку конфиденциальной информации в присутствии посторонних;

• записывать и хранить конфиденциальную информацию на неучтенных носителях;

• оставлять включенным без присмотра свой компьютер, не активизировав средства защиты от НСД;

• передавать кому-либо свой персональный ключевой носитель, кроме ответственного за информационную безопасность или руководителя своего подразделения установленным порядком, делать неучтенные копии ключевого носителя, снимать с него защиту записи и вносить какие-либо изменения в записанные на носитель файлы;

• использовать свои ключи ЭП для формирования электронной подписи любых электронных документов, кроме электронных документов, регламентированных технологическим процессом.

8.3. Обязанности ответственного за обеспечение безопасности информации в подразделении

Ответственный за обеспечение безопасности информации подразделения назначается из числа штатных сотрудников и непосредственно подчиняется руководителю подразделения, в штате которого он состоит.

Основными обязанностями ответственного за обеспечение безопасности информации являются:

• контроль целостности печатей (пломб) на устройствах защищенных компьютеров подразделения;

• ведение Журнала учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств рабочих станций подразделения;

• контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных;

• работа по выявлению возможных каналов неправомерного вмешательства в процесс функционирования АС и осуществления НСД к информации и техническим средствам ПЭВМ;

• инструктаж сотрудников подразделения по вопросам обеспечения безопасности информации и правилам работы с используемыми СЗИ.

Ответственный за обеспечение безопасности информации имеет право:

• требовать от сотрудников подразделения — пользователей АС соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности информации в АС;

• инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ИТ, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АС;

• обращаться к руководителю подразделения с требованием прекращения работы на рабочих станциях при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности ИТ;

• подавать предложения по совершенствованию организационных, технологических и технических мер защиты на своем участке работы;

• обращаться в подразделение обеспечения безопасности ИТ за необходимой технической и методологической помощью.

8.4. Ответственность за нарушения требований обеспечения безопасности

Для создания *юридической основы* процедур привлечения сотрудников к ответственности за нарушения в области обеспечения безопасности ИТ необходимо выполнение определенных условий:

• в Уставе организации, во всех положениях о структурных подразделениях и должностных инструкциях всех сотрудников, участвующих в процессах автоматизированной обработки информации, приводят требования по обеспечению безопасности ИТ при работе в АС;

• каждый сотрудник при приеме на работу подписывает трудовой договор, в котором определены обязательства по соблюдению установленных требований по сохранению государственной, служебной и коммерческой тайны, а также об ответственности за нарушение правил работы с защищаемой информацией в АС.

Сотрудники организации несут ответственность по действующему законодательству за разглашение сведений, составляющих тайну (государственную, служебную, коммерческую), и сведений ограниченного распространения, ставших им известными в процессе работы.

Любое грубое нарушение порядка и правил работы в АС сотрудниками структурных подразделений необходимо расследовать, а к виновным применять соответствующие меры воздействия.

Нарушения установленных правил и требований по обеспечению безопасности ИТ могут служить основанием для применения к сотруднику административных мер наказания, вплоть до увольнения и привлечения к уголовной ответственности.

Мера ответственности сотрудников за действия, совершенные в нарушение установленных правил обеспечения безопасной автоматизированной обработки информации, должна определяться с учетом нанесенного ущерба, наличия злого умысла и других факторов по усмотрению руководства.

Для реализации принципа персональной ответственности сотрудников осуществляются следующие м е р ы :

• индивидуальная идентификация сотрудников и инициированных ими процессов при работе в АС, т. е. установление за ними уникальных идентификаторов пользователей, на основе которых проводится разграничение доступа и регистрация событий;

• аутентификация пользователей и сотрудников на основе паролей, ключей, специальных устройств, биометрических характеристик личности и т. п.;

• регистрация (протоколирование) работы механизмов контроля доступа пользователей к ресурсам информационных систем с указанием даты и времени, идентификаторов пользователя и запрашиваемых им ресурсов, вида взаимодействия и его результата;

• оперативная реакция на попытки несанкционированного доступа (сигнализация, блокировка и т. д.).

Допуск к работе с подсистемами АС осуществляется после сдачи зачета на знание и умение выполнять требования по обеспечению безопасности ИТ.

В процессе работы *ответственный за обеспечение безопасности ИТ*:

• доводит инструкции по обеспечению безопасности ИТ до сведения сотрудников под роспись (в традиционном виде);

• размещает инструкции в электронном виде на корпоративном портале;

• оповещает о всех изменениях требований в документах;

• периодически повторяет инструктажи и обучение сотрудников.

8.5. Порядок работы с носителями ключевой информации

В некоторых подсистемах АС для обеспечения контроля за целостностью передаваемых по технологическим цепочкам электронных документов, а также для подтверждения их подлинности и авторства может быть использована электронная подпись.

Каждому сотруднику, которому в соответствии с его функциональными обязанностями предоставлено право постановки на ЭД цифровой подписи, выдается персональный ключевой носитель информации (например, диск, флеш-карта), на который записана уникальная ключевая информация («ключ электронной подписи»), относящаяся к категории сведений ограниченного доступа.

Жизненный цикл ключей включает в себя следующие этапы:

- генерация;
- использование;
- хранение;
- передача;
- уничтожение;
- обновление.

Ошибки в технологии распространения ключей, а также их небрежное хранение могут стать причиной доступа злоумышленника к строго конфиденциальной информации.

Для предотвращения подобных ошибок в организации разрабатывают документ по названием *«Политика безопасности при работе с носителями ключевой информации»*, который содержит ответы на следующие основные вопросы:

- кто формирует ключи для пользователей;
- где хранятся ключи;
- должен ли владелец ключей (пользователь) иметь лицензию на деятельность по техническому обслуживанию шифровальных средств;
- как восстановить зашифрованную информацию при потере ключа;
- кто изготовляет ключевые носители;
- как уничтожают ключевые носители;
- кто уничтожает ключевые носители и др.

Следует учитывать, что политика безопасности в отношении ключей ЭП существенно отличается от политики безопасности ключей шифрования. Регламентация порядка работы с ключами шифрования предусматривает при получении доступа к зашифрованным данным передачу копии секретного ключа для хранения агенту восстановления (на случай его утраты без компрометации), а также архивное хранение секретного ключа после истечения срока его использования. Ключ ЭП принадлежит одному лицу и по истечении срока действия уничтожается.

Персональный ключевой носитель изготовляют в центре управления ключевыми системами (ЦУКС) или удостоверяющем центре (УЦ) на основании заявки, подписанной руководителем подразделения исполнителя.

Генерация уникальной ключевой информации и ее запись на носитель осуществляются на специально оборудованном автономном «АРМ генерации ключей», программное обеспечение которого выполняет функции, регламентированные технологическим процессом формирования ключей ЭП, уполномоченными сотрудниками подразделения обеспечения безопасности ИТ — специалистами ЦУКС в присутствии самого исполнителя маркирует-

ся, записывается в Ведомость выдачи ключевых носителей ЦУКС и выдается ему под роспись. Оснащение АРМ генерации ключей должно гарантировать, что уникальная секретная ключевая информация исполнителя записывается только на его персональный носитель и не попадет на какой-либо промежуточный носитель.

Для обеспечения возможности восстановления ключевой информации исполнителя, в случае выхода ключевого носителя из строя, обычно создают его рабочую копию.

На этикетках ключевого носителя указывают регистрационный номер, дату изготовления и подпись уполномоченного сотрудника подразделения обеспечения информационной безопасности, изготовившего носитель, вид ключевой информации — ключевой носитель (эталон) или ключевой носитель (рабочая копия), фамилию, имя, отчество и подпись владельца — исполнителя.

Персональные ключевые носители (эталон и рабочую копию) хранят в опечатанном пенале, в сейфе ответственного за информационную безопасность подразделения и извлекают из сейфа только на время приема (выдачи) рабочих копий ключевых носителей исполнителям.

Ключи проверки электронной подписи исполнителей регистрируются специалистами ЦУКС или УЦ в справочнике ключей проверки ЭП, используемом при проверке подлинности документов по установленным на них ЭП.

Сотрудник, которому в соответствии с его должностными функциями предоставлено право постановки на ЭД электронной подписи, несет персональную ответственность за сохранность и правильное использование вверенной ему ключевой информации и содержание документов, на которых стоит его ЭП; он о б я з а н :

• лично присутствовать в ЦУКС при изготовлении ключевой информации (от момента включения до момента выключения АРМ генерации ключей), чтобы быть уверенным в том, что содержимое его ключевых дисков (эталонной и рабочей копии) не было компрометировано;

• под роспись в Ведомости выдачи ключевых носителей ЦУКС получить эталонный и рабочий ключевые носители и убедиться в их правильной маркировке. Зарегистрировать их у ответственного за безопасность подразделения, положить в пенал, опечатать личной печатью и передать пенал на хранение ответственному за обеспечение безопасности;

• использовать для работы только рабочую копию ключевого носителя;

• получать (в начале рабочего дня)/сдавать (в конце рабочего дня) ответственному за обеспечение безопасности рабочую копию ключевого носителя;

• сдавать персональный ключевой носитель на временное хранение ответственному за безопасность, например на время отсутствия исполнителя на рабочем месте;

• в случае порчи рабочей копии ключевого носителя (например, при ошибке чтения носителя) исполнитель передает ее сотруднику подразделения обеспечения безопасности ИТ, который в присутствии исполнителя и ответственного за обеспечение безопасности подразделения на АРМ генерации

ключей ЦУКС изготовляет новую рабочую копию с имеющегося у исполнителя эталона, а испорченную рабочую копию ключевого носителя уничтожает в присутствии исполнителя. Все эти действия фиксируют в Ведомости выдачи ключевых носителей ЦУКС.

Сотруднику, имеющему право ЭП, запрещено:

- оставлять персональный ключевой носитель без личного присмотра;
- передавать персональный ключевой носитель (эталонную или рабочую копии) другим лицам (за исключением передачи на хранение ответственному за безопасность в опечатанном пенале);
- делать неучтенные копии ключевого носителя, распечатывать или переписывать с него файлы на иной носитель информации (например, жесткий диск ПЭВМ), вносить изменения в файлы, находящиеся на ключевом носителе;
- подписывать персональным ключом ЭП любые электронные сообщения и документы, кроме регламентированных технологическим процессом;
- сообщать кому-либо вне работы, что он является владельцем ключа ЭП для данного технологического процесса.

При *компрометации* ключей, т. е. утрате доверия к тому, что используемые ключи обеспечивают безопасность информации, немедленно прекращают работу с ключевым носителем, сообщают об этом ответственному за обеспечение безопасности, сдают ему скомпрометированный ключевой носитель, соблюдая обычную процедуру с пометкой в журнале о причине компрометации, и пишут объяснительную записку о факте компрометации персонального ключевого носителя на имя начальника подразделения.

Различают явную и неявную компрометацию ключей — явной называют компрометацию, факт которой становится известным на отрезке установленного времени действия данного ключа; при неявной факт компрометации остается неизвестным для законных пользователей данного ключа.

Событиями, квалифицируемыми, как *явная компрометация ключей*, являются:

- утрата ключевого носителя;
- утрата ключевого носителя с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение печати на сейфе с ключевыми носителями;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации и др.

К событиям *неявной компрометации ключей* относят:

- возникновение подозрений на искажение или утечку информации в системе конфиденциальной связи;
- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями и др.

Решение задачи защиты ключей от компрометации направлено либо на исключение компрометаций, либо на сведение неявной компрометации к явной.

В случае перевода сотрудника на другую работу, увольнения и иных обстоятельствах он обязан сдать (сразу по окончании последнего сеанса работы) персональный ключевой носитель ответственному за обеспечение безопасности подразделения под роспись в журнале учета ключевых носителей, который информирует об этом уполномоченного сотрудника ЦУКС для принятия действий по блокированию использования ЭП увольняемого сотрудника.

Уничтожение ключей осуществляют двумя способами: 1) физическим уничтожением ключевого носителя, на котором он расположен; 2) стиранием (разрушением) ключей без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Ключевые носители уничтожаются либо исполнителями (только принадлежащие им ключи), либо ответственными за обеспечение безопасности ИТ под роспись в соответствующих журналах. Централизованное уничтожение ключей по акту производит комиссия, состоящая из сотрудников ЦУКС и ответственного за обеспечение безопасности ИТ.

* * *

Сотрудники — пользователи АС должны знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции, надежно хранить и никому не передавать свои пароли, личные печати и ЭП; немедленно информировать ответственного за обеспечение безопасности ИТ подразделения о некорректном функционировании технических средств защиты.

Контрольные вопросы

1. Каковы общие правила обеспечения безопасности информационных технологий при работе сотрудников с ресурсами АС?
2. Перечислите права и обязанности ответственного за обеспечение безопасности ИТ в подразделении.
3. Что такое явная и неявная компрометация ключей шифрования?
4. Какие действия должен предпринять сотрудник при компрометации ключей?
5. Каков порядок уничтожения ключей шифрования?

ГЛАВА 9. РЕГЛАМЕНТАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Допуск сотрудников подразделений к работе с автоматизированной системой и доступ к ее ресурсам должен быть строго регламентирован. Аппаратно-программная конфигурация автоматизированных рабочих мест, на которых обрабатывается защищаемая информация и с которых возможен доступ к защищаемым ресурсам, должна соответствовать кругу возложенных на сотрудников (пользователей данного АРМ) функциональных обязанностей.

9.1. Регламентация правил парольной и антивирусной защиты

Правила парольной защиты регламентируют организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в автоматизированной системе, а также контроль над действиями пользователей при работе с паролями.

Правила антивирусной защиты определяют требования к организации защиты автоматизированной системы от разрушающего воздействия вредоносного ПО (компьютерных вирусов, сетевых червей, «троянских коней», логических бомб и т. п.) и устанавливают ответственность руководителя и сотрудников обеспечения безопасной эксплуатации АС за их выполнение.

Организация парольной защиты. Организационно-техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями осуществляют сотрудники подразделения обеспечения безопасности АС — администраторы средств защиты, в которых реализованы механизмы идентификации и аутентификации (подтверждения подлинности) пользователей.

При назначении личных паролей самостоятельно должны соблюдаться следующие п р а в и л а:

- длина пароля должна быть не менее установленной (обычно 6...8 символов);
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т. п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов и т. д.), последовательность символов и знаков (111, abcd и т. д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т. п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в заданном числе (например, 6 символов) позиций;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с правилами их составления и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

При централизованном формировании личных паролей пользователей ответственность за правильность их формирования и распределения возложена на сотрудников подразделения обеспечения безопасности ИТ. Для генерации «стойких» значений паролей применяют специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников подразделения обеспечения безопасности ИТ, а также ответственных за обеспечение безопасности информации в подразделениях с паролями других сотрудников подразделений организации (исполнителей).

При наличии технологической необходимости использования имен и паролей некоторых сотрудников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств) такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) передавать на хранение ответственному за безопасность подразделения (либо руководителю подразделения) в запечатанном конверте или опечатанном пенале, которые хранятся в сейфе.

Полная плановая смена паролей пользователей проводится не реже одного раза в месяц.

Неплановую полную смену паролей всех пользователей осуществляют в случае компрометации личного пароля пользователя АС, а также при прекращении полномочий пользователя АС или администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

Хранение сотрудником своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе ответственного за обеспечение безопасности, либо в сейфе руководителя в опечатанном виде.

Организация антивирусной защиты. К использованию в организации допускаются только лицензионные антивирусные средства, централизованно приобретенные у разработчиков указанных средств, рекомендованные к применению подразделениями автоматизации и безопасности информации.

Установка средств антивирусного контроля на компьютерах, серверах и рабочих станциях АС осуществляется сотрудниками подразделения автоматизации в соответствии с Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АС.

Настройку параметров средств антивирусного контроля проводят сотрудники подразделения автоматизации в соответствии с руководствами по применению конкретных антивирусных средств.

Антивирусный контроль всех внешних устройств и файлов рабочих станций проводится ежедневно в начале работы при загрузке компьютера (для серверов — при перезапуске) в автоматическом режиме.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, флеш-картах и т. п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или при условии начальной загрузки операционной системы, в оперативную память компьютера с заведомо «чистого» (не зараженного вирусами) и защищенного от записи системного диска — на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации проводят непосредственно перед архиви-

рованием и отправкой (записью на съемный носитель). Файлы, помещаемые в электронный архив, также проходят антивирусный контроль. Периодические проверки электронных архивов проводят не реже одного раза в месяц.

Установку (изменение) системного и прикладного ПО осуществляют на основании «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации».

Устанавливаемое (изменяемое) программное обеспечение должно быть проверено на отсутствие вирусов перед установкой и непосредственно после установки (изменения).

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) сотрудник подразделения (самостоятельно или вместе с ответственным за обеспечение безопасности) проводит внеочередной антивирусный контроль и при необходимости привлекает специалистов подразделения автоматизации.

При обнаружении зараженных компьютерными вирусами файлов сотрудники подразделений о б я з а н ы :

• приостановить работу;

• поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за обеспечение безопасности владельца зараженных вирусом файлов, а также смежные подразделения, использующие эти файлы в работе;

• совместно с владельцем зараженных вирусом файлов провести анализ возможности их дальнейшего использования;

• провести коррекцию или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов подразделения автоматизации);

• в случае обнаружения неизвестного вируса передать зараженный вирусом файл на магнитном носителе в подразделение автоматизации для дальнейшей отправки в обслуживающую организацию, с которой заключен договор на антивирусную поддержку;

• по факту обнаружения зараженных вирусом файлов составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т. д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия и передать ее в отдел обеспечения безопасности информации.

Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем подсистему АС, возложена на руководителя подразделения; за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований инструкции — на ответственного за обеспечение безопасности и всех сотрудников подразделения, являющихся пользователями АС.

9.2. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы

В рамках разрешительной системы (системы авторизации) допуска устанавливаются:

• условия, ресурсы и круг лиц, имеющих право выдавать разрешения;

• система санкционирования и разграничения доступа, которая предполагает определение для всех пользователей информационных и программных ресурсов, доступных им для чтения, модификации, удаления и т. п.;

• порядок реализации процедуры допуска.

Систему санкционирования доступа целесообразно строить на основе структурно-функционального подхода к разделению всего множества защищаемых ресурсов АС на отдельные задачи с описанием всех используемых при ее решении ресурсов (файлов, каталогов, таблиц баз данных и т. п.), всех категорий пользователей (роли в задаче) и прав доступа для каждой категории к ресурсам задачи.

Полномочия руководителей подразделений давать разрешения на допуск к решению определенных задач закрепляют решениями (приказами) высшего руководства организации.

Любые изменения состава и полномочий пользователей подсистем АС проводят согласно «Инструкции по внесению изменений в списки пользователей АС и наделению их полномочиями доступа к ресурсам системы», в которой должны быть отражены правила именования пользователей и процедура авторизации сотрудников.

Правила именования пользователей. Соблюдение принципа персональной ответственности каждого сотрудника, допущенного к работе с конкретной подсистемой АС, предполагает наличие персонального уникального имени (учетной записи пользователя), под которым его регистрируют в автоматизированной системе. В случае производственной необходимости сотрудник может иметь несколько учетных записей. Запрещается использование одного имени пользователя («группового имени») несколькими сотрудниками при работе в АС.

Функции распределения имен, генерации паролей, сопровождения правил разграничения доступа к базам данных возложены на администраторов баз данных.

Учетные записи всех пользователей должны быть «привязаны» к конкретным рабочим станциям (номерам сетевых карт) или сегменту сети (группе рабочих станций), закрепленных за конкретным подразделением организации. При этом могут использоваться как основные (штатные) средства защиты СУБД и операционных систем, так и дополнительные.

Для всех пользователей устанавливают режим принудительного запроса смены пароля не реже одного раза в месяц.

Процедура авторизации сотрудников. Процедура регистрации (создания учетной записи) пользователя для сотрудника и предоставления ему прав

доступа к ресурсам АС инициируется *заявкой начальника подразделения* (отдела, сектора), в которой указывается:

• содержание запрашиваемых изменений (регистрация нового пользователя АС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам АС ранее зарегистрированного пользователя);

• наименование подразделения, должность, фамилия, имя и отчество сотрудника;

• имя пользователя (при изменении полномочий и прав доступа);

• полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач на конкретных рабочих станциях АС). Наименования задач рабочих станций указывают в соответствии с формулярами задач.

Если полномочий начальника подразделения недостаточно, то заявку может завизировать руководитель организации, утверждая таким образом производственную необходимость допуска (изменения прав доступа) конкретного сотрудника к ресурсам АС.

Представленную заявку рассматривают руководители подразделений автоматизации и обеспечения безопасности АС, а затем составляют и подписывают задание системным администраторам (серверов, баз данных) и администратору специальных средств защиты информации от несанкционированного доступа на внесение необходимых изменений в списки пользователей.

На основании заявки системный администратор в соответствии с формулярами указанных задач, которые хранятся в архиве эталонных дистрибутивов (АЭД) программ, и документацией на средства защиты сетевых операционных систем производит необходимые действия по созданию (удалению) учетной записи пользователя, присвоению ему начального пароля и заявленных прав доступа к сетевым ресурсам АС.

Аналогичные операции для систем управления базами данных (СУБД) выполняет администратор баз данных.

Администратор СЗИ НСД в соответствии с формулярами указанных задач и Руководством администратора системы защиты от НСД производит необходимые действия по регистрации нового пользователя, присвоению ему начального пароля (возможна также регистрация персонального идентификатора, например, iButton) и прав доступа к ресурсам указанных в заявке рабочих станций, включению его в соответствующие задачам системные группы пользователей и др.

После внесения изменений в списки пользователей администратор СЗИ НСД обеспечивает настройки средств защиты, соответствующие категориям защиты указанных рабочих станций. Проверка правильности настроек средств защиты осуществляется с участием сотрудника, ответственного за эксплуатацию конкретной рабочей станции, в соответствии с «Порядком проверки работоспособности системы защиты после установки (обновления) программных средств АС и внесения изменений в списки пользователей».

Сотруднику, зарегистрированному в качестве нового пользователя системы, под роспись сообщается имя соответствующего ему пользователя (учетная запись), выдается персональный идентификатор, личные ключевые диски (для работы в режиме усиленной аутентификации и работы со средствами криптографической защиты) и начальный пароль, который он обязан сменить при первом же входе в систему (при первом подключении к АС).

Исполненная заявка передается в подразделение и хранится в архиве у ответственного за безопасность ИТ подразделения (при его отсутствии — у руководителя подразделения). Копии исполненных заявок хранят в подразделении автоматизации (у системных администраторов) и в подразделении обеспечения безопасности ИТ и впоследствии могут использоваться:

• для восстановления бюджетов и полномочий пользователей после аварий в АС;

• контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам автоматизированной системы при разборе конфликтных ситуаций;

• проверки правильности настройки средств разграничения доступа к ресурсам автоматизированной системы.

9.3. Регламентация порядка изменения конфигурации аппаратно-программных средств автоматизированной системы

В соответствии с принципом «минимизации полномочий» все неиспользуемые в работе устройства ввода-вывода информации на АРМ, где обрабатывается защищаемая информация, отключают, а ненужные для работы программные средства и данные с дисков АРМ удаляют.

Подлежащие защите аппаратные и программные ресурсы системы (информационные файлы, задачи, программы, АРМ) заносят в соответствующие формуляры или специализированные базы данных с определением требуемого уровня защищенности.

Программное обеспечение (разработанное специалистами организации, полученное централизованно или приобретенное у фирм-производителей) проходит испытания и передается в фонд алгоритмов и программ — АЭД (в подсистемах АС устанавливают и применяют только учтенные в АЭД программные средства).

На всех АРМ, подлежащих защите, должны быть установлены необходимые технические средства защиты (соответствующие категории данных АРМ).

Для упрощения сопровождения, обслуживания и организации защиты автоматизированные рабочие места оснащают программными средствами и унифицируют (в соответствии с установленными правилами).

Контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Физическая охрана объектов информатизации (компонентов компьютерных систем) включает в себя следующие мероприятия:

• определение границ контролируемой зоны объекта, подлежащего защите;

• организация и обеспечение внутриобъектного и пропускного режимов;

• установка инженерных и технических сооружений и устройств защиты периметра объекта системы видеонаблюдения, охранной и пожарной сигнализации, а также систем контроля допуска на объект и в помещения;

• введение дополнительных средств и мер, ограничивающих свободный допуск лиц на объект и в помещения, где размещаются защищаемые ресурсы АС (формирование и утверждение списков лиц, допущенных в помещения);

• применение средств для опломбирования и опечатывания и др.).

Узлы и блоки оборудования СВТ, доступ к которым обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с монтажом схем, закрывают и опечатывают. Факты вскрытия блоков ПЭВМ отражают в «Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания блоков ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств АРМ подразделения».

Повседневный контроль за целостностью и соответствием пломб на системных блоках ПЭВМ осуществляют пользователи АРМ и ответственные за обеспечение безопасности ИТ; периодический контроль — сотрудники подразделения обеспечения безопасности ИТ.

Обслуживание и модификация аппаратных и программных средств автоматизированной системы. Ввод в эксплуатацию новых АРМ и все изменения в конфигурации технических и программных средств существующих АРМ в АС осуществляются согласно «Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств АРМ АС». В инструкции регламентированы функции и взаимодействия подразделений организации по обеспечению безопасности при проведении модификаций и обслуживании программного обеспечения и технических средств АС.

Изменения конфигурации технических и программных средств защищенных рабочих станций и серверов (различных уровней защищенности в соответствии с «Положением о категорировании ресурсов АС») проводятся на основании заявок руководителей структурных подразделений организации или руководителя подразделения автоматизации, согласованных с руководителем подразделения обеспечения безопасности ИТ.

Право внесения изменений в конфигурацию аппаратно-программных средств защищенных рабочих станций и серверов АС имеет уполномоченный сотрудник (обычно издается соответствующий приказ) подразделения:

• *авторизации* — в отношении системных и прикладных программных средств, а также аппаратных средств;

• *обеспечения безопасности ИТ* — в отношении программно-аппаратных средств защиты;

• *службы (отдела) связи (телекоммуникации)* — в отношении программно-аппаратных средств телекоммуникации.

Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций АС организации, не требующих защиты, может быть

предоставлено как сотрудникам подразделения автоматизации (на основании заявок), так и сотрудникам подразделений, в которых они установлены, на основании распоряжений руководителей данных подразделений.

Внесение изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций. Процедура внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций АС может инициироваться либо заявкой руководителя данного подразделения, либо заявкой руководителя подразделения автоматизации.

Заявка руководителя подразделения, в котором требуется изменить конфигурацию рабочей станции, оформляется на имя руководителя подразделения автоматизации.

Заявка руководителя подразделения автоматизации, которое отвечает за плановое развитие АС и проведение изменений (обновлений версий) ПО, оформляется на имя руководителя структурного подразделения, использующего подсистему АС, требующую модификации.

В заявках указывают виды необходимых изменений в составе конфигурации аппаратных и программных средств рабочих станций и серверов подразделения:

- установка в подразделении новой ПЭВМ (развертывание новой рабочей станции или сервера);
- замена или изъятие ПЭВМ (рабочей станции или сервера подразделения), узла, блока;
- установка или обновление (замена) на конкретной рабочей станции или сервере программных средств, необходимых для решения определенной задачи (добавление или обновление версий, используемых для решения данной задачи);
- удаление с конкретной рабочей станции или сервера программных средств, необходимых для решения определенной задачи (исключение возможности решения данной задачи на данной рабочей станции).

В заявке отражают условные наименования рабочих станций и серверов в соответствии с их формулярами (при развертывании новой рабочей станции ее наименование устанавливается позднее — при заполнении формуляра новой рабочей станции). Наименования задач указывают в соответствии с формулярами задач или перечнем задач АЭД подразделения автоматизации, которые можно решать с использованием АС.

Модификация ПО на подлежащих защите серверах осуществляется уполномоченными сотрудниками подразделения автоматизации в присутствии уполномоченного сотрудника подразделения обеспечения безопасности ИТ. После установки модифицированных модулей на сервер сотрудник подразделения безопасности ИТ в присутствии сотрудников подразделения автоматизации настраивает средства контроля целостности модулей на сервере (производит пересчет контрольных сумм эталонов модулей), проверяет их работоспособность, а также отсутствие опасных функций, проводит антивирусный контроль в соответствии с Инструкцией по антивирусной защите.

Установка (обновление) общего ПО (системного, тестового и т. п.) рабочих станций и сервера осуществляется с оригинальных лицензионных дистрибутивных носителей (дисков, флеш-карт, и т. п.) или с эталонных копий программных средств, полученных из АЭД.

В случае установки части компонент на дисках сетевых серверов к работам привлекаются администраторы сети (серверов) и администраторы баз данных.

Устанавливаемое (изменяемое) ПО как предварительно, так и после установки (изменения) проверяют на отсутствие вирусов.

После установки (обновления) ПО администратор СЗИ НСД проводит настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с формуляром и совместно с сотрудником подразделения автоматизации и пользователем рабочей станции проверяет работоспособность ПО и правильность настройки средств защиты.

После завершения работ по внесению изменений в состав аппаратных средств защищенной рабочей станции помещение, где расположен системный блок, закрывает сотрудник подразделения автоматизации и опечатывает сотрудник подразделения обеспечения безопасности ИТ.

Уполномоченные исполнители работ от подразделений автоматизации и обеспечения безопасности ИТ производят соответствующую запись в Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств рабочих станций подразделения (Журнал учета нештатных ситуаций) с отметкой о выполнении задания на модификацию по следующей форме:

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи	ФИО ответственного пользователя РС, подпись	Подпись ответственного за обеспечение безопасности информации подразделения	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

При изъятии компьютера из состава рабочих станций подразделения его передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как специалист подразделения обеспечения безопасности ИТ снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на жестком диске компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью ответственного за обеспечение безопасности информации в подразделении.

Допуск новых пользователей к решению задач с применением вновь развернутого ПО (либо изменение их полномочий доступа) осуществляется в соответствии с Инструкцией по внесению изменений в списки пользователей системы и наделению пользователей полномочиями доступа к ресурсам АС.

Оригиналы заявок (документов), на основании которых вносились изменения в состав технических или программных средств рабочей станции с отметками о внесенных изменениях в состав аппаратно-программных средств, хранятся вместе с оригиналами формуляров рабочих станций и Журналом учета нештатных ситуаций в подразделении (у ответственного за обеспечение безопасности информации подразделения или руководителя подразделения). Копии исполненных заявок и актов хранятся в подразделениях автоматизации и обеспечения безопасности ИТ и могут впоследствии использоваться:

- для восстановления конфигурации рабочей станции после аварий;
- контроля правомерности установки на конкретной рабочей станции средств для решения соответствующих задач при разборе конфликтных ситуаций;
- проверки правильности установки и настройки средств защиты рабочей станции.

Экстренная модификация. В исключительных случаях (перечень которых определяет руководство организации), требующих срочного изменения ПО и модификации технических средств, сотрудник подразделения автоматизации ставит в известность непосредственного руководителя и руководителя подразделения обеспечения безопасности ИТ (в случае их отсутствия — дежурного сотрудника подразделения обеспечения безопасности ИТ и пользователя рабочей станции) о необходимости такого изменения для получения соответствующего разрешения (список лиц, которым предоставлено право разрешать выполнение работ, связанных с форс-мажорными обстоятельствами, составляет руководитель организации).

Факт внесения изменений в ПО и технические средства защищенных рабочих станций и серверов фиксируется актом за подписями ответственного за обеспечение безопасности информации в подразделении и пользователя данной рабочей станции, сотрудников подразделений автоматизации и обеспечения безопасности ИТ. В акте указывают причину модификации, перечисляют файлы, подвергшиеся изменению, и приводят список лиц, принявших решение о проведении работ и проводивших эти работы. Факт модификации ПО и корректировки настроек системы защиты фиксируется в Журнале учета нештатных ситуаций того подразделения, в котором установлены рабочие станции (серверы).

В течение следующего дня после составления акта руководство подразделений автоматизации и обеспечения безопасности ИТ проводит совещание с участием сотрудников структурных подразделений, на котором выясняются причины и состав проведенных экстренных изменений и принимается решение о необходимости подготовки новой модификации ПО или восстановления ПО рабочей станции (сервера) с эталонной копии (из АЭД). Протокол совещания оформляется в виде согласованного решения и хранится в подразделении автоматизации, копии передаются в подразделение обеспечения безопасности ИТ и в структурное подразделение.

9.4. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач

В большинстве организаций ответственность за решение вопросов, связанных с защитой информации, на этапах проектирования и разработки прикладных программ традиционно возлагают на те же подразделения (и специалистов), которые отвечают за создание и внедрение данных прикладных программ. При этом требования к характеристикам средств защиты в разрабатываемых подсистемах определяют сами разработчики — прикладные программисты, а не специалисты по защите информации. Разработчики действуют, исходя из собственных, не всегда верных в силу специфики вопроса, представлений о достаточности средств и механизмов защиты, т. е. самостоятельно принимают решения по удовлетворению этих требований, и самостоятельно оценивают качество реализации необходимых защитных механизмов.

Все это в итоге приводит к недопустимым упрощениям в вопросах обеспечения безопасности информации в разрабатываемых прикладных подсистемах.

Поскольку применение дополнительных средств защиты создает определенные ограничения при эксплуатации и использовании прикладных программ, требует дополнительных затрат системных ресурсов компьютеров (для создания качественных средств защиты необходимы существенные затраты времени и сил, наличие специальных знаний и опыта), разработчики прикладного программного обеспечения, отвечающие прежде всего за своевременность и качество решения задач по автоматизации технологических процессов, не заинтересованы в создании надежных средств защиты.

Порядок приема разработанных программных продуктов в промышленную эксплуатацию обычно сводится к проведению испытаний и подписанию акта сдачи-приемки. Нередко внедрение ПО и особенно его модернизация осуществляются без передачи эталонных копий ПО и всей необходимой документации в ФАП (АЭД) или это происходит с большим отставанием по времени. В результате документация, имеющаяся в архиве, по многим подсистемам либо неполная и не соответствует реальным версиям ПО, либо отсутствует.

Данное обстоятельство приводит к возникновению ситуаций, когда сопровождение прикладного ПО или реализация дополнительных мер по обеспечению безопасности ИТ затруднены или невозможны по причине увольнения создавших данное ПО программистов и отсутствия необходимых описаний и исходных текстов программ. Кроме того, это позволяет разработчикам достаточно свободно осуществлять замену версий ПО, находящегося в эксплуатации.

Для устранения отмеченных недостатков необходим переход к такому порядку взаимодействия подразделений, при котором определение требований по защите информации в прикладных подсистемах и контроль за качеством реализации механизмов защиты в них должны осуществляться специалиста-

ми по защите информации вне подразделений, разрабатывающих ПО и эксплуатирующих технические средства, исходя из единых для организации целей и задач защиты информации.

Процессы разработки ПО задач (комплексов задач), проведения испытаний разработанного и приобретенного ПО, передачи ПО в эксплуатацию должны осуществляться в соответствии с утвержденным Порядком разработки, проведения испытаний и передачи задач (комплексов задач) в эксплуатацию.

Документ включает требования по номенклатуре и содержанию нормативных документов, разрабатываемых специалистами подразделения обеспечения безопасности ИТ совместно со специалистами подразделения автоматизации, порядку определения требований по обеспечению безопасности ИТ и проведению экспертизы реализации механизмов защиты в прикладных системах.

Разработка и отладка программ должны быть организованы на специальном опытном участке АС таким образом, чтобы исключать возможность доступа программистов в эксплуатируемые подсистемы АС (к реальной информации и базам данных).

Порядок разработки комплексов задач предусматривает передачу разработанных (доработанных) программ в эксплуатацию через архив эталонных дистрибутивов программ (фонд алгоритмов и программ) подразделения, ответственного за эксплуатацию ПО.

В связи с тем, что вопросами закупок средств защиты занимаются, как правило, несколько подразделений организации, разрабатывают также Порядок согласования выбора и приобретения средств защиты информации в АС для нужд организации и Порядок инспекторского контроля специалистами подразделения обеспечения безопасности ИТ за соблюдением технических условий и сертификатов ФСТЭК России и ФСБ России на приобретенные средства защиты и прикладные системы.

Взаимодействие подразделений при проектировании и разработке средств защиты. Специалисты подразделения обеспечения безопасности совместно со специалистами отдела разработки программ и представителями подразделения заказчика участвуют в разработке постановки задач и технического задания (спецификаций) в части определения требований ИБ.

На основе анализа категории пользователей, а также информации, создаваемой и используемой при решении задачи, ее размещения на носителях, характера осуществляемых преобразований информации и других особенностей проектируемой технологии обработки данных, с учетом требований Концепции безопасности организации специалисты подразделения обеспечения безопасности ИТ проводят анализ рисков и формируют требования к защите ресурсов разрабатываемой подсистемы.

При этом учитываются реальные возможности организации по реализации требований обеспечения безопасности ИТ организационными мерами и аппаратно-программными средствами защиты системного и прикладного уровней и другие особенности создаваемой подсистемы. При необходимости определяется потребность в приобретении или разработке дополнительных средств защиты.

Согласованные с начальником подразделения обеспечения безопасности требования должны включаться отдельным разделом в проектную документацию (постановку задачи, техническое задание, рабочий проект и т. п.).

Подразделение обеспечения безопасности участвует также в процессе выбора аппаратно-программных средств (системных, инструментальных, базовых и т. п.), планируемых к приобретению и использованию в разрабатываемой подсистеме.

Специалисты подразделения обеспечения безопасности совместно со специалистами подразделения технического сопровождения и представителями подразделений разработки выносят на обсуждение предложения по конфигурации (правила коммутации, маршрутизации и т. п.) телекоммуникационной сети организации в части требований по обеспечению безопасности ИТ. Требования формируются на основе анализа коммуникационных потребностей прикладных задач подсистемы и категорий сведений, используемых при решении данных задач.

Взаимодействие подразделений при проведении испытаний. Специалисты подразделения обеспечения безопасности ИТ совместно со специалистами подразделений разработки и системного сопровождения ПО и представителями подразделения-заказчика принимают участие в подготовке программ и методик испытаний задач и программных средств в части проверки реализации требований по обеспечению безопасности ИТ, проводят испытания, проверяют контрольные суммы сдаваемого в ФАП ПО и подписывают акты по результатам испытаний.

Взаимодействие подразделений при сдаче в промышленную эксплуатацию. Специалисты подразделения обеспечения безопасности ИТ совместно со специалистами подразделений разработки и системного сопровождения ПО участвуют в разработке формуляра для задачи (разработанного или приобретенного программного средства), передаваемой в ФАП.

Формуляр (карта разграничения доступа) задачи (программного средства) содержит перечень и размещение всех программных, информационных и других ресурсов, используемых при решении задачи (применении программного средства), список категорий пользователей данной задачи (программного средства) и указание их прав по доступу к перечисленным ресурсам. Данный формуляр необходим при настройке средств разграничения доступа на этапе внедрения задачи (при восстановлении системы после сбоев). Кроме того, формуляры могут использоваться при контрольных проверках правильности настройки и работы средств защиты.

В процессе установки (развертывания) подсистем (задач) специалисты подразделения автоматизации осуществляют настройку штатных средств защиты, а специалисты подразделения обеспечения безопасности ИТ контролируют правильность их настройки и настраивают дополнительные средства защиты в соответствии с формулярами задач (программных средств).

Специалисты подразделения обеспечения безопасности ИТ совместно со специалистами подразделений разработки и системного сопровождения, под-

разделения-заказчика участвуют в разработке специальных требований по обеспечению безопасности ИТ в должностных инструкциях пользователей АС.

Взаимодействия подразделений в процессе эксплуатации (сопровождения). Изменения настроек средств защиты в соответствии с утвержденными заявками на изменение полномочий пользователей осуществляют специалисты, системные администраторы и администраторы безопасности, отвечающие за эксплуатацию соответствующих подсистем (комплексов задач).

Изменения в конфигурацию аппаратно-программных средств подсистемы (в том числе при снятии задач с эксплуатации и передаче аппаратных средств в ремонт) вносят специалисты подразделений эксплуатации и технического сопровождения на основании утвержденных и согласованных с подразделением обеспечения безопасности ИТ заявок (заданий) от руководителей операционных подразделений в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации».

В экстренных случаях (в кризисных ситуациях) основанием для принятия решений специалистами подразделений эксплуатации и технического сопровождения является План обеспечения непрерывной работы и восстановления (ПОНРВ).

* * *

Конечные пользователи (специалисты операционных подразделений) при работе с АС руководствуются должностными инструкциями и инструкцией пользователя по вопросам обеспечения безопасности ИТ и должны соблюдать правила парольной и антивирусной защиты.

Правильность функционирования и настройки системы защиты периодически контролируется специалистами подразделений эксплуатации (системными администраторами), а также специалистами подразделения обеспечения безопасности ИТ (администраторами информационной безопасности).

Физическая охрана объектов информации предусматривает организацию и обеспечение визуального и технического контроля за контролируемой территорией объекта защиты, установку механических, кодовых и электронных замков и др.

Контрольные вопросы

1. Каковы требования к пользовательским паролям?
2. Перечислите недостатки парольной аутентификации.
3. Какова периодичность плановой смены пароля?
4. В каких случаях проводится неплановая смена пароля?
5. Охарактеризуйте в общих чертах требования к технологии антивирусной защиты.
6. Опишите алгоритм действий при обнаружении вирусов.
7. Дайте определение авторизации.
8. Что устанавливается в рамках разрешительной системы (системы авторизации)?

9. Опишите алгоритм авторизации пользователя.

10. Какие сотрудники участвуют в процессе авторизации пользователя?

11. Какова процедура авторизации?

12. Каковы цели изготовления копий заявки об авторизации?

13. Что включает в себя физическая охрана объектов информатизации?

14. Опишите процедуру внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и рабочих станций системы.

15. Какие категории сотрудников имеют право внесения изменений в системное и прикладное ПО?

16. Кто имеет право вносить изменения в конфигурацию аппаратно-программных средств защиты?

17. Каков порядок экстренной модификации технических средств?

18. Кто определяет требования к характеристикам средств защиты в разрабатываемых подсистемах?

19. Что такое фонд алгоритмов и программ?

20. Опишите порядок взаимодействия подразделений на этапах проектирования, разработки, испытания и внедрения новых автоматизированных подсистем.

Глава 10. КАТЕГОРИРОВАНИЕ И ДОКУМЕНТИРОВАНИЕ ЗАЩИЩАЕМЫХ РЕСУРСОВ

Наибольшую сложность при решении вопросов обеспечения безопасности информационных технологий представляет задача определения требований к защите конкретной информации, ее носителей и процессов обработки. Ключом к решению данной задачи для общего случая служит учет интересов всех затрагиваемых технологией субъектов информационных отношений.

10.1. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов

Сложившийся подход к классификации государственной информации (данных) по уровням требований к ее защищенности основан на рассмотрении и обеспечении только одного свойства информации — ее конфиденциальности (грифа секретности). Требования по обеспечению целостности и доступности информации, как правило, лишь косвенно фигурируют среди общих требований к системам обработки этих данных. Считается, что поскольку к информации имеет доступ узкий круг доверенных лиц, вероятность ее искажения (несанкционированного уничтожения) незначительна.

Если такой подход в некоторой степени оправдан в силу существующей приоритетности свойств безопасности важной государственной информации, то это вовсе не означает, что его механический перенос в другую предметную область (с другими субъектами и их интересами) будет иметь успех.

Во многих областях деятельности (предметных областях) доля конфиденциальной информации сравнительно мала. Для коммерческой и персональной информации, равно как и для государственной информации, не подлежащей засекречиванию, приоритетность свойств безопасности информации может быть совершенно иной. Для открытой информации, ущерб от разглашения которой несущественен, важнейшими могут быть такие качества, как доступность, целостность, защищенность от неправомерного тиражирования. Так, для платежных (финансовых) документов самым важным является свойство их целостности (достоверности, неискаженности). Затем, по степени важности, следует свойство доступности (потеря платежного документа или задержка платежей могут приводить к значительным финансовым потерям). Требования к обеспечению конфиденциальности платежных документов, как правило, стоят на третьем месте. Попытка решить вопросы защиты такой информации с позиций традиционного обеспечения только конфиденциальности, не достигает успеха. Основные причины этого состоят в узости традиционного подхода к защите информации, отсутствии опыта и соответствующих проработок в плане обеспечения целостности и доступности информации, не являющейся конфиденциальной.

Развитие системы классификации информации по уровням требований к ее защищенности предполагает введение категорий (градаций, степеней) требований по обеспечению каждого из свойств безопасности информации: доступности, целостности, конфиденциальности.

Количество дискретных градаций и вкладываемый в них смысл могут различаться. Главное, чтобы требования к защищенности различных свойств информации указывались отдельно и достаточно конкретно (исходя из серьезности возможного ущерба, наносимого субъектам информационных отношений, от нарушения каждого из свойств безопасности информации и системы ее обработки).

Далее *информационным пакетом* будем называть любой отдельный функционально законченный документ, содержащий определенные сведения, вне зависимости от вида носителя, на котором он находится.

К одному типу будем относить информационные пакеты (типовые документы), имеющие сходство по некоторым признакам (структуре, технологии обработки, типу сведений и т. п.).

Задача состоит в определении реальных уровней заинтересованности (высокая, средняя, низкая, отсутствует) субъектов в обеспечении требований к защищенности каждого из свойств различных типов информационных пакетов, циркулирующих в АС.

Порядок определения требований к защищенности циркулирующей в системе информации. Вначале составляют перечень типов информационных пакетов (документов, таблиц и т. п.), для чего с учетом предметной области системы пакеты информации разделяют на типы по тематике, функциональному назначению, сходности технологии обработки и другим признакам.

На последующих этапах первоначальное разделение информации (данных) на типы пакетов уточняют в зависимости от требований к их защищенности.

Затем для каждого типа пакетов и каждого критического свойства информации (доступности, целостности, конфиденциальности) определяют (например, методом экспертных оценок):

• перечень и важность (значимость по отдельной шкале) субъектов, интересы которых затрагиваются при нарушении данного свойства информации;

• уровень наносимого им при этом ущерба (незначительный, малый, средний, большой, очень большой и т. п.) и соответствующий уровень требований к защищенности.

Определение ущерба. При определении уровня наносимого ущерба учитывают:

• стоимость возможных потерь при получении информации конкурентом;

• стоимость восстановления информации при ее утрате;

• затраты на восстановление нормального функционирования АС и т. д.

Для каждого типа информационных пакетов с учетом значимости субъектов и уровней наносимого им ущерба устанавливают степень необходимой защищенности по каждому из свойств информации (при равенстве значимости субъектов выбирают максимальное значение уровня).

Пример оценки требований к защищенности некоторого типа информационных пакетов приведен в табл. 10.1.

Таблица 10.1

Оценка требований к защищенности информации

Субъект	Уровень ущерба по свойствам информации		
	Конфиденциальность	Целостность	Доступность
1	Нет	Средняя	Средняя
2	Высокая	Средняя	Средняя
m	Низкая	Низкая	Низкая
Итого	Высокая	Средняя	Средняя

10.2. Категорирование защищаемых ресурсов

Категорирование защищаемых ресурсов АС—необходимый элемент организации работ по обеспечению безопасности информации — предполагает:

• установление градаций важности (категорий) обеспечения защиты ресурсов;

• отнесение конкретных ресурсов к соответствующим категориям.

Ц е л и категорирования ресурсов (определение требований к защите ресурсов) АС:

• создание нормативно-методической основы для дифференцированного подхода к защите ресурсов автоматизированной системы (информации, задач, компьютеров) на основе их классификации по степени риска в случае нарушения их доступности, целостности или конфиденциальности;

• типизация принимаемых контрмер;

• распределение физических и аппаратно-программных средств защиты по компьютерам АС (рабочим станциям и серверам);

• унификация настроек защитных механизмов.

Категории защищаемой информации. Исходя из необходимости обеспечения различных уровней защиты разных видов информации (не содержащей сведений, составляющих государственную тайну), хранимой и обрабатываемой в АС, вводится несколько категорий конфиденциальности и несколько категорий целостности защищаемой информации.

Категории конфиденциальности защищаемой информации:

• *строго конфиденциальная* — информация, являющаяся конфиденциальной в соответствии с требованиями действующего законодательства (банковская тайна, персональные данные), а также информация, ограничения на распространение которой введены решениями руководства организации (коммерческая тайна), а ее разглашение может привести к тяжким финансово-экономическим последствиям для организации (нанесению тяжкого ущерба жизненно важным интересам клиентов, корреспондентов, партнеров или сотрудников, вплоть до банкротства);

• *конфиденциальная* — информация, не отнесенная к категории «строго конфиденциальная», ограничения на распространение которой вводятся решением руководства организации в соответствии с предоставленными ему как собственнику (уполномоченному собственником лицу) информации действующим законодательством правами, разглашение которой может привести к значительным убыткам и потере конкурентоспособности организации (нанесению ощутимого ущерба интересам его клиентов, корреспондентов, партнеров или сотрудников);

• *открытая* — информация, обеспечения конфиденциальности (введения ограничений на распространение) которой не требуется.

Категории целостности защищаемой информации:

• *высокая* — к данной категории относят информацию, несанкционированная модификация (искажение, подмена, уничтожение) или фальсификация (подделка) которой может привести к нанесению значительного прямого ущерба организации, целостность и аутентичность (подтверждение подлинности источника) такой информации должна обеспечиваться гарантированными методами (средствами электронной подписи) в соответствии с обязательными требованиями действующего законодательства, приказов, директив и других нормативных актов;

• *низкая* — данная категория включает в себя информацию, несанкционированная модификация, подмена или удаление которой может привести к нанесению незначительного косвенного ущерба организации, ее клиентам, партнерам или сотрудникам, целостность должна обеспечиваться решениями руководства, основанными на проведении анализа с использованием методов подсчета контрольных сумм, хеш-функций;

• *нет требований* — к данной категории относится информация, к обеспечению целостности (и аутентичности) которой требований не предъявляется.

Категории функциональных задач. В зависимости от периодичности решения функциональных задач и максимально допустимой задержки получения результатов их решения вводятся следующие категории доступности функциональных задач:

• *беспрепятственная доступность* — доступ к задаче должен обеспечиваться в любое время (задача решается постоянно, задержка получения результата не превышает нескольких секунд или минут);

• *высокая доступность* — доступ к задаче осуществляется без существенных временны́х задержек (задача решается ежедневно, задержка получения результата не превышает нескольких часов);

• *средняя доступность* — доступ к задаче может обеспечиваться с существенными временны́ми задержками (задача решается один раз в несколько дней, допустимая задержка получения результата не превышает нескольких дней);

• *низкая доступность* — временны́е задержки при доступе к задаче практически не лимитированы (задача решается с периодом в несколько недель или месяцев, допустимая задержка получения результата — несколько недель).

Категории компьютеров. Категории защиты компьютеров устанавливают в зависимости от категорий конфиденциальности и целостности хранимой или обрабатываемой информации и категорий доступности решаемых на компьютерах задач.

Обычно при определении категории компьютера указывают: максимальную категорию конфиденциальности хранимой или обрабатываемой на компьютере информации/максимальную категорию целостности информации/максимальную категорию доступности задач, решаемых на компьютере (например, «конфиденциально»/«высокая»/«беспрепятственная доступность»).

Порядок определения категорий защищаемых ресурсов автоматизированной системы. Категорирование ресурсов автоматизированной системы (компьютеров, задач, информации) проводят на основе их инвентаризации, составляя перечни ресурсов АС, подлежащих защите.

Ответственность за составление и ведение перечней ресурсов АС организации возлагают:

• на *подразделение автоматизации организации* — в части составления и ведения перечня компьютеров (с указанием их размещения, закрепления за подразделениями организации, состава и характеристик входящих в его состав технических средств — формуляров компьютеров);

• *отделы программирования, внедрения, сопровождения и эксплуатации ПО* подразделения автоматизации организации — в части составления и ведения перечня системных (общих) и прикладных (специальных) задач, решаемых на компьютерах (с указанием перечней используемых при их решении ресурсов — устройств, каталогов, файлов с информацией).

Функциональные подразделения организации, которые непосредственно решают задачи на данных компьютерах, и *подразделение обеспечения безопасности ИТ* (компьютерной безопасности) — отвечают за определение требований к обеспечению конфиденциальности, целостности, доступности и присвоение соответствующих категорий ресурсам конкретных компьютеров (информационным ресурсам и задачам).

Утверждение назначенных категорий ресурсов АС осуществляет *руководитель подразделения обеспечения безопасности ИТ*.

Инициаторами категорирования компьютеров и получения соответствующих предписаний на эксплуатацию (формуляров ПЭВМ) должны выступать *руководители подразделений организации*, в которых используются данные ПЭВМ.

Контроль за правильностью категорирования ресурсов АС и законностью эксплуатации (наличием утвержденных формуляров — предписаний на эксплуатацию) защищенных рабочих станций и серверов АС организации в подразделениях организации осуществляют *сотрудники подразделения обеспечения безопасности ИТ*.

Категорирование ресурсов АС организации осуществляется последовательно для конкретного компьютера с последующим объединением и формированием общего перечня ресурсов АС организации, подлежащих защите:

- информационных ресурсов АС организации — Перечень информационных ресурсов, подлежащих защите, в котором устанавливают категории конфиденциальности и целостности конкретных видов информации;
- задач (совокупности формуляров задач), решаемых в АС организации, — Перечень задач, подлежащих защите, категорирование всех функциональных задач, решаемых на данной ПЭВМ;
- компьютеров (совокупности формуляров ПЭВМ), эксплуатируемых в организации, — Перечень компьютеров с установлением категории компьютера, исходя из максимальных категорий обрабатываемой информации и задач, решаемых на нем.

10.3. Проведение информационных обследований и документирование защищаемых ресурсов

Категорирование предполагает проведение работ по выявлению (инвентаризации) и анализу всех ресурсов подсистем АС организации, подлежащих защите.

Для выполнения данных работ формируют рабочую группу, в состав которой включают специалистов подразделения обеспечения безопасности ИТ и других подразделений организации (осведомленных в вопросах технологии автоматизированной обработки информации в организации).

Для придания необходимого статуса рабочей группе издается соответствующее распоряжение руководства организации с указанием руководителям структурных подразделений организации оказывать содействие и необходимую помощь в проведении работ по анализу ресурсов компьютеров АС. Для оказания такой помощи на время работы группы в подразделениях выделяют сотрудников, владеющих детальной информацией по вопросам автоматизированной обработки информации в данных подразделениях.

При обследовании подразделений и подсистем АС выполняют следующие этапы.

1. Категорирование информации. Выявляются все виды входящей, исходящей, хранимой и обрабатываемой информации, причем не только той, которая может быть отнесена к конфиденциальной (банковской и коммерческой тайне, персональным данным), но и информации, подлежащей защите в силу того, что нарушение ее целостности (искажение, фальсификация) или доступности (уничтожение, блокирование) может нанести ощутимый ущерб организации.

При выявлении всех видов информации, циркулирующей и обрабатываемой в подсистемах, желательно проводить оценку серьезности последствий, к которым могут привести нарушения ее свойств (конфиденциальности, целостности). Для получения первоначальных оценок серьезности таких последствий целесообразно проводить опрос (например, в форме анкетирования) специалистов, работающих с данной информацией с выяснением круга лиц, заинтересованных в данной информации, возможностями ее незаконного использования и последствиями. При сложности количественной оценки вероятного ущерба проводят качественную оценку серьезности последствий, к которым могут привести нарушения их доступности (блокирование возможности решения задач). В случае невозможности количественной оценки вероятного ущерба проводится качественная оценка.

Выявленные в ходе обследования различные виды информации заносят в Перечень информационных ресурсов, подлежащих защите.

Определяется (и затем указывается в Перечне), к какому типу тайны (банковская, коммерческая, персональные данные, не составляющая тайны) относится каждый из выявленных видов информации (на основании требований действующего законодательства и предоставленных организации прав).

Первоначальные предложения по оценке категорий обеспечения конфиденциальности и целостности конкретных видов информации выясняются у руководителей (ведущих специалистов) структурного подразделения (на основе их личных оценок вероятного ущерба от нарушения свойств конфиденциальности и целостности информации). Данные оценки категорий информации заносят в Перечень.

Затем Перечень передают на согласование руководителю подразделения автоматизации и обеспечения безопасности ИТ (компьютерной безопасности) и после этого — на рассмотрение руководства организации.

2. Категорирование функциональных задач. На основе требований по доступности, предъявляемых руководителями подразделений организации и согласованных с подразделением автоматизации, категорируются все специальные (прикладные) функциональные задачи, решаемые в подразделениях с использованием АС. Информация о категориях специальных задач заносится в формуляры задачи. Категорирование общих (системных) задач и программных средств вне привязки к конкретным компьютерам и прикладным задачам не производится.

Далее, с участием специалистов подразделений автоматизации и обеспечения безопасности ИТ, уточняют состав информационных и программных ресурсов каждой задачи и вносят в ее формуляр сведения по группам пользователей задачи и указания по настройке применяемых при ее решении средств

защиты (полномочия доступа групп пользователей к перечисленным ресурсам задачи). Эти сведения будут использованы в качестве эталона настроек средств защиты соответствующих компьютеров, на которых будет решаться данная задача, и для контроля правильности их установки;

3. Категорирование компьютеров. Категория компьютера устанавливается исходя из максимальной категории специальных задач, решаемых на нем, и максимальных категорий конфиденциальности и целостности информации, используемой при решении данных задач. Информацию о категории компьютера (триаду) заносят в его формуляр.

* * *

В ходе обследования конкретных подразделений организации и автоматизированных подсистем выявляются и анализируются все функциональные задачи, решаемые с использованием АС, а также все виды информации (сведений), применяемые при решении этих задач в подразделениях. Одновременно с этим ведется учет программных средств (общих, специальных), с помощью которых решают функциональные задачи подразделения.

При составлении перечня и формуляров функциональных задач, решаемых в организации, необходимо выяснять периодичность их решения, максимально допустимое время задержки получения результатов решения задач и степень серьезности последствий, к которым могут привести нарушения их доступности (блокирование возможности решения задач). В случае невозможности количественной оценки вероятного ущерба проводится качественная оценка.

Контрольные вопросы

1. Каков примерный порядок определения требований к защищенности циркулирующей в системе информации?
2. Что необходимо учитывать при определении уровня возможного ущерба?
3. Перечислите цели категорирования ресурсов.
4. Приведите примеры категорий защищаемой информации и функциональных задач.
5. Опишите порядок проведения информационного обследования и документирования защищаемых ресурсов.

Глава 11. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПЛАНЫ ЗАЩИТЫ И ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ И ВОССТАНОВЛЕНИЯ ПОДСИСТЕМ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Концепция информационной безопасности организации (далее – Концепция) определяет порядок обеспечения безопасности информации в орга-

низации и представляет собой систематизированное изложение целей и задач защиты, принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в АС.

Основные положения и требования Концепции распространяются на все структурные подразделения организации, в которых осуществляется автоматизированная обработка конфиденциальной информации, а также на подразделения сопровождения, обслуживания и обеспечения нормального функционирования АС.

Один из способов управления рисками информационной безопасности — уменьшение вероятности наступления нежелательного события и/или снижение потерь в случае, если это событие все-таки наступит. Для уменьшения вероятности наступления нежелательного события разрабатывают *план защиты информации*, а для снижения потерь — *план обеспечения непрерывной работы и восстановления подсистем АС*.

11.1. Концепция информационной безопасности организации

Назначение и статус документа. Концепция является *методологической основой* для:

- формирования и проведения единой политики в области обеспечения безопасности информации в АС;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности и ликвидации последствий реализации различных видов угроз безопасности информации;
- координации деятельности структурных подразделений при проведении работ по созданию, развитию и эксплуатации АС с соблюдением требований обеспечения безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности АС.

Правовой основой Концепции является Конституция Российской Федерации, Гражданский кодекс РФ, Уголовный кодекс РФ, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК России, ФСБ России и другие нормативные документы, регламентирующие вопросы защиты информации в АС.

При разработке Концепции учитывают основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации, а также текущее состояние и перспективы развития информационных технологий.

Основные положения Концепции базируются на качественном осмыслении вопросов безопасности информации, при этом не проводится экономический (количественный) анализ рисков и обоснование необходимых затрат на защиту информации.

Положения Концепции предусматривают существование в рамках проблемы обеспечения безопасности информации в АС двух относительно самостоятельных направлений с единым замыслом: 1) защита информации от утечки по техническим каналам; 2) защита информации в автоматизированных системах от НСД.

Содержание Концепции информационной безопасности. В Концепции должны быть отражены следующие вопросы:

• характеристика АС организации как объекта безопасности ИТ; структура, состав и размещение основных элементов АС организации; категории информационных ресурсов, подлежащих защите; категории пользователей АС организации, режимы использования и уровни доступа к информации; интересы субъектов информационных отношений затрагиваемых при эксплуатации АС организации и др.;

• цели и задачи обеспечения безопасности ИТ организации и основные пути их достижения (решения задач системы защиты);

• перечень основных опасных внешних и внутренних воздействующих факторов и значимых угроз безопасности ИТ (утечка информации по техническим каналам, неформальная модель возможных нарушителей, подход к оценке риска в АС организации и др.);

• основные положения технической политики в области обеспечения безопасности информации АС организации;

• принципы обеспечения безопасности ИТ организации;

• основные способы защиты от угроз, средства обеспечения требуемого уровня защищенности ресурсов АС (организационные, физические, технические);

• первоочередные мероприятия по обеспечению безопасности информации АС организации;

• перечень нормативных документов, регламентирующих деятельность в области защиты информации;

• основные термины и определения.

11.2. План защиты информации

План защиты информации, разрабатываемый в целях конкретизации положений Концепции информационной безопасности для конкретных подсистем АС, содержит следующие сведения:

• описание подсистемы АС как объекта защиты: назначение, перечень решаемых задач, конфигурация, характеристики и размещение технических средств и программного обеспечения, перечень категорий информации (пакетов, файлов, наборов и баз данных, в которых они содержатся), подлежащих защите, требований по обеспечению доступности, конфиденциальности, целостности этих категорий информации, список пользователей с указанием их полномочий по доступу к ресурсам системы и т. п.;

• цель защиты и пути обеспечения безопасности ресурсов подсистемы АС и циркулирующей в ней информации;

• перечень значимых угроз безопасности и наиболее вероятных путей нанесения ущерба подсистеме АС;

• требования к организации процесса функционирования подсистемы АС и мерам обеспечения безопасности обрабатываемой информации;

• требования к условиям применения и определение зон ответственности установленных в системе штатных и дополнительных технических средств защиты;

• основные правила, регламентирующие деятельность пользователей и персонала по вопросам обеспечения безопасности в подсистеме.

11.3. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы

План обеспечения непрерывной работы и восстановления определяет основные меры, методы и средства сохранения (поддержания) работоспособности АС при возникновении различных кризисных ситуаций, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности АС и ее основных компонентов. Кроме того, в плане содержится перечень действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий и минимизации наносимого ущерба.

Классификация кризисных ситуаций. Ситуацию, возникающую в результате нежелательного воздействия на АС, не предотвращенного средствами защиты, называют *кризисной*. Кризисная ситуация может возникнуть либо вследствие злого умысла, либо случайно.

Под *умышленным нападением* понимается кризисная ситуация, которая возникла по причине выполнения злоумышленниками в определенные моменты времени заранее обдуманных и спланированных действий; под *случайной (непреднамеренной) кризисной ситуацией* понимается кризисная ситуация, которая не была результатом заранее обдуманных действий, а возникла вследствие субъективных причин случайного характера (непреднамеренные действия, халатность, небрежность) или объективных причин (аварии, стихийные бедствия и т. п.).

По *степени серьезности и размерам наносимого ущерба* различают следующие категории кризисных ситуаций:

• *угрожающая* — приводящая к полному выходу АС из строя или уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации:

— нарушение подачи электроэнергии;

— выход из строя сервера (с потерей или без потери информации);

— частичная потеря информации на сервере без потери его работоспособности;

— выход из строя локальной сети (физической среды передачи данных);

• *серьезная* — приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа:

— выход из строя рабочей станции (с потерей или без потери информации);

— частичная потеря информации на рабочей станции без потери ее работоспособности;

• *критическая* — возникающая в результате нежелательных воздействий, не наносящих ощутимого ущерба, но, тем не менее, требующая внимания и адекватной реакции (несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации). Зафиксированные неудачные попытки проникновения или несанкционированного доступа к ресурсам системы к критическим не относятся. Действия в случае возникновения ситуаций, требующих внимания, предусмотрены планом защиты информации (для контроля действий персонала назначают ответственных за безопасность в подразделениях и на технологических участках).

К источникам информации о возникновении кризисной ситуации относят:

• пользователей, обнаруживших несоответствия плану защиты информации или другие подозрительные изменения в работе или конфигурации системы или средств ее защиты в своей зоне ответственности;

• средства защиты, обнаружившие предусмотренную планом защиты кризисную ситуацию;

• системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

Меры обеспечения непрерывной работы АС. Для непрерывности процесса функционирования АС и своевременности восстановления ее работоспособности применяют следующие мероприятия:

• разработка организационно-распорядительных документов по вопросам обеспечения непрерывности вычислительного процесса;

• регламентация процесса обработки информации с применением ЭВМ и действий персонала системы, в том числе в кризисных ситуациях;

• назначение и обучение должностных лиц, отвечающих за организацию и осуществление практических мероприятий;

• применение различных способов резервирования аппаратных ресурсов, эталонного копирования программных и страхового копирования информационных ресурсов системы;

• поддержание необходимого уровня защищенности компонентов системы, управление и административная поддержка корректного применения средств защиты;

• непрерывный анализ эффективности принятых мер, разработка и реализация предложений по их совершенствованию.

Общие требования. Все пользователи, работа которых может быть нарушена в результате возникновения угрожающей или серьезной кризисной ситуации, должны быть немедленно оповещены. Дальнейшие действия по устранению причин нарушения работоспособности АС, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

Каждая кризисная ситуация должна быть проанализирована администрацией безопасности с последующей выработкой предложений по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т. п.

Серьезная и угрожающая кризисные ситуации могут требовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

Оперативное восстановление программ (эталонное копирование) и данных (страховое копирование) в случае их уничтожения или порчи в серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность системы и выполнение ею своих задач (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т. д.

Все программные средства, используемые в системе, должны иметь эталонные (дистрибутивные) копии, местонахождение и сведения об ответственных за их создание, хранение и использование которых должны быть приведены формулярах на каждую ЭВМ (рабочую станцию, сервер). Там же указывают перечни наборов данных, подлежащих страховому копированию, периодичность копирования, место хранения и ответственных за создание, хранение и использование страховых копий данных.

Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала.

Каждый носитель, содержащий резервную копию, должен иметь метку с данными о классе, ценности, назначении хранимой информации, ответственном за создание, хранение и использование, дате последнего копирования, месте хранения и др.

Дублирующие аппаратные ресурсы предназначены для обеспечения работоспособности системы при выходе из строя всех или отдельных компонентов в результате угрожающей кризисной ситуации. Количество и характеристики дублирующих ресурсов должны обеспечивать выполнение основных задач системой в любой кризисной ситуации.

Ликвидация последствий угрожающей или серьезной кризисной ситуации подразумевает восстановление программных, аппаратных, информационных и других поврежденных компонентов системы.

Для любой кризисной ситуации проводят расследование причин ее возникновения, определяют причиненный ущерб, устанавливают виновных и принимают соответствующие меры.

Расследование причин кризисной ситуации осуществляется группой лиц, назначаемой руководством организации и возглавляемой администратором безопасности.

Если причиной угрожающей или серьезной кризисной ситуации явились недостаточно жесткие меры защиты и контроля, а ущерб превысил установленный уровень, то такая ситуация служит основанием для полного пересмотра плана защиты информации и плана обеспечения непрерывной работы и восстановления подсистемы АС.

Средства обеспечения непрерывной работы и восстановления подсистем АС. Резервному копированию (РК) подлежит следующая информация:

• системные программы и наборы данных — невозобновляемому (однократному, эталонному) РК;

• прикладное программное обеспечение и наборы данных — невозобновляемому (эталонному) РК;

• наборы данных, генерируемые в процессе работы и содержащие ценную информацию (журналы транзакций, системный журнал и т. д.) — периодическому возобновляемому РК.

Программные и информационные ресурсы, подлежащие резервному копированию, заносят в соответствующие списки, которые могут быть оформлены в виде таблицы:

Наименование информационного ресурса	Место размещения ресурса в системе	Вид резервного копирования (период возобновляемого копирования)	Ответственный за резервное копирование и порядок создания резервной копии (используемые технические средства)	Место хранения резервной копии (ФИО ответственного, номер телефона)	Порядок использования резервной копии

Безопасность резервных копий обеспечивается:

• хранением резервных копий вне системы (в других помещениях, на другой территории);

• соблюдением мер физической защиты резервных копий;

• строгой регламентацией порядка использования резервных копий.

Дублированию (резервированию) в АС подлежат и используемые в подсистемах АС технические средства, списки которых оформляются также в виде таблицы:

Наименование дублируемого (резервируемого) технического средства	Место размещения средства в системе	Вид резерва (групповой или индивидуальный, холодный или горячий), время готовности резерва	Ответственный за готовность резервного средства (период проверки работоспособности)	Порядок использования резервного средства (включение, настройки) для различных кризисных ситуаций	Место хранения резервного средства (ФИО и номер телефона ответственного)

Обязанности и действия персонала по обеспечению непрерывной работы и восстановлению подсистем АС. Действия персонала в кризисной ситуации зависят от ее категории.

Анализ критической кризисной ситуации администратор безопасности подсистемы проводит собственными силами и ставит в известность руководство подразделения о фактах систематического возникновения таких ситуаций и принятых мерах.

В случае возникновения угрожающей или серьезной критической ситуации осуществляется следующий порядок действий персонала:

- немедленная реакция;
- частичное восстановление работоспособности подсистемы и возобновление обработки информации;
- полное восстановление подсистемы и возобновление обработки информации в полном объеме;
- расследование причин кризисной ситуации и установление лиц, виновных в ее возникновении.

Немедленная реакция предусматривает выполнение действий:

- *оператор*, обнаруживший факт возникновения кризисной ситуации, обязан немедленно оповестить об этом администратора безопасности;
- *администратор безопасности* доводит до сведения операторов всех смежных подсистем факт возникновения кризисной ситуации для перехода на аварийный режим работы (приостановку работы);
- вызывает ответственных системного программиста и системного инженера;
- определяет степень серьезности и масштабы кризисной ситуации, размеры и область поражения;
- оповещает персонал взаимодействующих подсистем о характере кризисной ситуации и ориентировочном времени возобновления работы.

При *частичном восстановлении работоспособности* подсистем (минимально необходимой для возобновления работы системы в целом, возможно с потерей производительности) администратор безопасности подсистемы, системный программист и системный инженер выполняют действия:

- отключают пораженные компоненты или переключают на использование дублирующих ресурсов (горячего резерва);
- если не произошло повреждения программ и данных, возобновляют обработку информации и оповещают об этом персонал взаимодействующих подсистем;
- восстанавливают работоспособность поврежденных критичных аппаратных средств и другого оборудования, при необходимости производят замену отказавших узлов и блоков резервными;
- восстанавливают поврежденное критичное программное обеспечение и данные, используя страховые копии;
- проверяют работоспособность поврежденной подсистемы, удостоверившись в том, что последствия кризисной ситуации не оказывают воздействия на дальнейшую работу системы;
- уведомляют операторов смежных подсистем о готовности к работе.

Для *полного восстановления подсистемы* следует:

• восстановить работоспособность всех поврежденных аппаратных средств, при необходимости произвести замену отказавших узлов и блоков резервными;

• восстановить и настроить все поврежденные программы, используя эталонные (страховые) копии;

• восстановить все поврежденные данные, используя страховые копии и журналы транзакций;

• настроить средства защиты подсистемы в соответствии с планом защиты информации;

• уведомить администратора системы (базы данных) о результатах восстановления.

Далее необходимо провести расследование причин возникновения кризисной ситуации и ответить на вопросы:

• случайная или преднамеренная кризисная ситуация;

• учитывалась ли возможность возникновения кризисной ситуации в плане защиты информации и плане обеспечения непрерывной работы и восстановления подсистем АС;

• можно ли было ее предусмотреть;

• вызвана ли она слабостью средств защиты и регистрации;

• превысил ли ущерб от нее установленный уровень;

• есть ли невосполнимый ущерб и велик ли он;

• это первая кризисная ситуация такого рода;

• есть ли возможность точно определить круг подозреваемых лиц;

• есть ли возможность точно установить виновника;

• какова причина возникновения кризисной ситуации и др.

Ответственным за расследование является администратор безопасности подсистемы. Отчет о результатах расследования и предложениях по совершенствованию системы направляют администратору системы (базы данных) и руководству организации.

* * *

Концепция информационной безопасности организации разрабатывается на основе нормативно-правовой базы, регламентирующей вопросы защиты информации в АС и служит руководящим документом при формировании политики безопасности в организации. Планы защиты информации и обеспечения непрерывной работы и восстановления подсистем АС составляют для конкретизации положений Концепции информационной безопасности.

Контрольные вопросы

1. Каково назначение Концепции информационной безопасности?
2. Какие факторы учитываются при разработке Концепции?
3. Что служит правовой основой для разработки Концепции?
4. Какие вопросы отражены в Концепции?

5. Охарактеризуйте статус Концепции.

6. Охарактеризуйте цель разработки и содержание плана защиты информации.

7. Охарактеризуйте цель разработки и содержание плана обеспечения непрерывной работы и восстановления.

8. Что такое кризисная ситуация?

9. Назовите категории кризисных ситуаций.

10. Перечислите меры обеспечения непрерывной работы и восстановления работоспособности подсистем АС.

11. Приведите перечень обязанностей и действий персонала по обеспечению непрерывной работы и восстановлению работоспособности подсистем АС.

РАЗДЕЛ III

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Глава 12. НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В зависимости от вида мер противодействия угрозе безопасности АС (правовые, морально-этические, организационные и др., см. гл. 4) применяют различные защитные механизмы.

12.1. Основные механизмы защиты автоматизированных систем

Для защиты АС от НСД к информации используются следующие механизмы:

- идентификация (именование и распознавание) и аутентификация (подтверждение подлинности) пользователей системы;
- разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователей;
- регистрация и оперативное оповещение о событиях, происходящих в системе;
- криптографическое шифрование хранимых и передаваемых по каналам связи данных;
- контроль целостности и аутентичности (подлинности и авторства) данных;
- резервирование и резервное копирование;
- фильтрация трафика и трансляция адресов;
- обнаружение вторжений (атак);
- выявление и нейтрализация компьютерных вирусов;
- затирание остаточной информации на носителях;
- выявление уязвимостей «слабых мест» системы;

• маскировка и создание ложных объектов;

• страхование рисков.

В конкретных технических средствах перечисленные механизмы защиты могут применяться в различных комбинациях.

Рассмотрим наиболее важные защитные механизмы.

Идентификация и аутентификация пользователей. Для разграничения доступа к ресурсам АС и возможности регистрации событий такого доступа каждый субъект (сотрудник, пользователь, процесс) и объект (ресурс) защищаемой АС должен быть однозначно идентифицирован. Для этого в системе хранятся специальные признаки каждого субъекта (объекта), по которым их можно опознать.

Идентификация — это, с одной стороны, присвоение индивидуальных имен, номеров (идентификаторов) субъектам и объектам системы, а с другой — распознавание субъектов (объектов) по присвоенным им уникальным идентификаторам. Наличие идентификатора позволяет упростить процедуру выделения конкретного субъекта (объекта) из множества однотипных. Обычно в качестве идентификаторов применяют номера или условные обозначения в виде набора символов.

Аутентификация — проверка (подтверждение) подлинности идентификации субъекта (объекта) системы.

Идентификация и аутентификация пользователей проводится при каждом входе в систему, а также при возобновлении работы после кратковременного перерыва (после периода неактивности без выхода из системы или выключения компьютера).

Формы аутентификации пользователей весьма разнообразны — пароли, PIN-коды, ключевые слова, смарт-карты, отпечатки пальцев, особенности радужной оболочки глаз, сертификаты и др.

Системы аутентификации могут быть двух видов — *с взаимной* и *односторонней аутентификацией*. Пример взаимной аутентификации — аутентификация веб-сервера, которая предполагает предъявление сертификата, доказывающего взаимодействие с определенным оборудованием, которое находится под управлением определенных физических или юридических лиц.

Простейшая форма аутентификации — *парольная*, при которой ввод значений идентификатора и пароля осуществляется, как правило, с клавиатуры. Считается, что данная форма аутентификации небезопасна, поскольку пользователи нередко применяют короткие, легко подбираемые пароли и во многих системах существуют многочисленные возможности перехвата паролей (установка клавиатурного «шпиона» (рис. 12.1), перехват в открытых сетях и т. д.).

Рис. 12.1. Клавиатурный «шпион»

Международным стандартом ISO/IEC 27002 рекомендуется использовать сервисы, не допускающие передачу пароля в открытом виде, поэтому современные информационные системы применяют, как правило, хеширование и шифрование передаваемых паролей, а также одноразовые пароли.

Эффективное средство против подбора паролей — систематическая смена пароля пользователями.

Одно из достоинств парольной аутентификации — интеллектуальная составляющая, т. е. связь с разумом и сознанием пользователя. В совершенных с точки зрения безопасности информационных системах пароли хранят исключительно в памяти человека без записи на любой материальный носитель информации.

Еще одна форма аутентификации — использование уникальных элементов пользователя (смарт-карт, дисков, ключевых контейнеров, радиочастотных бесконтактных карточек, электронных таблеток iButton и т. п.) — аутентификация «владения». Как правило, подобный механизм защиты применяется в совокупности с дополнительной парольной аутентификацией (вводом PIN-кода), образуя *двухфакторную систему аутентификации* (например, защита с помощью ключевых контейнеров на различных носителях — смарт-картах, USB-ключах, e-Token и Guardant ID и PIN-кода; технология RSA SecureID, рис. 12.2).

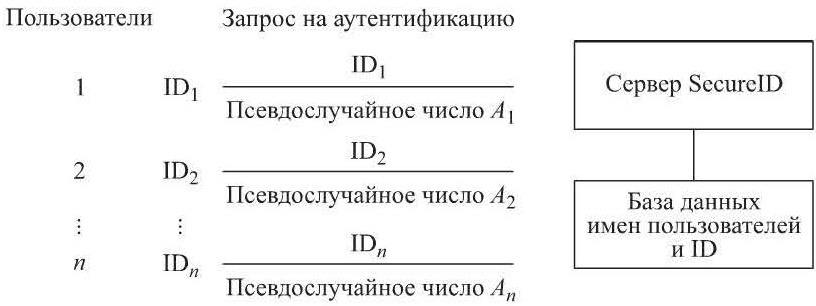

Рис. 12.2. Технология двухфакторной аутентификации RSA SecureID

Одной из форм аутентификации «владения» является *аутентификация по адресу* (IP-адресу, адрес электронной почты, телефонному номеру), активно применяющаяся в системах клиент-банк и сотовой телефонии.

Альтернативой аутентификации «владения», недостаток которой состоит в возможности потери (кражи) аутентификатора, служит *биометрическая аутентификация*.

В основе данного способа лежит биометрическое распознавание субъекта по его аналогичным характеристикам, хранящимся в базе данных.

Наряду с достоинствами биометрической аутентификации — относительной трудностью потери аутентификатора и высоким уровнм достоверности опознавания пользователей, способу присущи недостатки — проблема получения ключа из биометрических параметров; возможность исключения из процесса аутентификации субъектов при компрометации электронного

аутентификатора, высокая стоимость реализации биометрических систем; ошибки распознавания первого и второго рода (пропуск или ложная тревога); возможность изготовления относительно дешевых муляжей для биопараметров.

Для реализации рассмотренных форм аутентификации необходим первоначальный контакт между субъектом и объектом, в процессе которого стороны обмениваются аутентификатором. В ряде случаев такой контакт невозможен, например в системах электронного бизнеса B2C.

Система B2C — это краткосрочное взаимодействие бизнеса и потребителя бизнес-продукта, сопровождаемое большим количеством разовых сделок, при котором ни поставщики, ни потребители не имели ранее деловых контактов. Для подобных заочных транзакций наиболее эффективна аутентификация с использованием различных форм *рекомендаций от доверенного посредника*, например сертификата или билета.

В частности, широко известны сертификаты X509, связывающие открытый ключ клиента и его уникальный идентификатор, которые подписаны ЭЦП доверенного центра сертификации (см. п. 12.2).

Перспективой развития технологий аутентификации является создание многофакторных систем аутентификации с комбинированным применением паролей, биопараметров, отчуждаемых элементов и сертификатов.

Разграничение доступа пользователей к ресурсам автоматизированной системы. Разграничение (контроль) доступа к ресурсам АС — это такой порядок использования ресурсов автоматизированной системы, при котором субъекты получают доступ к объектам системы в строгом соответствии с установленными правилами.

Авторизация пользователей осуществляется с применением следующих механизмов реализации разграничения доступа:

- *избирательного управления доступом* с помощью атрибутивных схем, списков разрешений и т. п.;
- *полномочного управления доступом* с помощью меток конфиденциальности ресурсов и уровней допуска пользователей;
- *замкнутой среды доверенного программного обеспечения* (индивидуальных для каждого пользователя списков разрешенных программ), поддерживаемой механизмами идентификации и аутентификации пользователей при входе в систему.

Технические средства разграничения доступа к ресурсам АС рассматривают как составную часть единой системы контроля доступа субъектов на контролируемую территорию, в отдельные здания и помещения организации, к элементам АС, СИЗ, информационным и программным ресурсам АС.

Механизмы управления доступом субъектов к объектам доступа выполняют основную роль в обеспечении внутренней безопасности компьютерных систем. Их работа строится на концепции единого диспетчера доступа, сущность которого состоит в том, что диспетчер доступа выступает в роли посредника-контролера при обращении субъектов к объектам.

Диспетчер доступа выполняет следующие функции:

• проверяет права доступа субъекта к объекту на основании информации, содержащейся в базе данных системы защиты;

• производит авторизацию субъекта и разрешает доступ субъекта к объекту (при соблюдении правил разграничения доступа), либо запрещает доступ;

• регистрирует факт попытки доступа и его параметры в системном журнале (в том числе НСД с превышением полномочий).

Диспетчер доступа, контролируя множество событий безопасности, происходящих в системе, тесно взаимодействует с подсистемами регистрации событий и оперативного оповещения об их наступлении. Он обнаруживает и регистрирует до нескольких сотен типов событий, среди которых:

• вход пользователя в систему (сеть);

• неудачная попытка входа в систему или сеть (неправильный ввод имени или пароля);

• запуск и завершение программы;

• попытка открытия файла, недоступного для чтения или записи;

• попытка удаления или изменения файла, недоступного для модификации;

• попытка запуска программы или чтения/записи информации с диска, недоступного пользователю;

• вывод на устройства печати документов с грифом (при полномочном управлении доступом);

• нарушение целостности программ и данных системы защиты и др.

При реализации диспетчера доступа необходимо соблюдать требования:

• полноты контролируемых операций — проверке должны подвергаться все операции всех субъектов над всеми объектами системы, т. е. обход диспетчера невозможен;

• изолированности диспетчера, т. е. защищенность от изменений субъектами доступа в целях влияния на процесс функционирования;

• минимизации используемых диспетчером ресурсов.

Основной принцип работы средств разграничения доступа субъектов к объектам основан на проверке сведений, хранимых в базе данных защиты.

Под *базой данных защиты (security database)* понимают базу данных, хранящую информацию о правах доступа субъектов к объектам.

Внесение изменений в базу данных защиты, добавление и удаление объектов и субъектов, просмотр и изменение соответствующих прав доступа субъектов к объектам осуществляется с помощью средств для привилегированных пользователей (администраторов безопасности, владельцев объектов и т. п.)

Основу базы данных средств разграничения доступа в общем случае составляет абстрактная матрица доступа или ее реальные представления, строки которой соответствуют субъекту, а столбцы — объекту АС. Каждый элемент матрицы представляет собой кортеж (упорядоченную совокупность значений), определяющий права доступа (для всех возможных видов доступа — чтение, модификация, удаление и т. п.) определенного субъекта к определенному объекту (рис. 12.3).

Сложность управления доступом в реальных системах связана не только с большим размером матрицы доступа (большим числом субъектов и объектов) и высоким динамизмом ее корректировки, но и с необходимостью постоянно отслеживать большое число зависимостей между значениями определенных кортежей. Наличие таких зависимостей связано с ограничениями и правилами наследования полномочий в иерархии объектов и субъектов (например, при наследовании пользователем полномочий групп, в которые он входит, его права доступа к каталогам и файлам не должны превышать соответствующие права по доступу к диску, на котором они размещены).

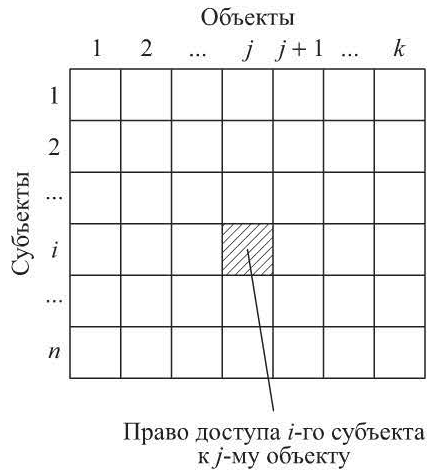

Рис. 12.3. Матрица избирательного управления доступом

Ограничения и зависимости между полномочиями существенно усложняют процедуру ведения матриц доступа, поэтому стали разрабатываться способы неявного задания матрицы (списки доступа, перечисление полномочий, атрибутные схемы).

Основные критерии оценки эффективности различных способов неявного задания матрицы доступа следующие:

- затраты памяти на хранение образа матрицы доступа;
- время на выборку (или динамическое вычисление) значений полномочий (элементов кортежей);
- удобство ведения матрицы при наличии ограничений и зависимостей между значениями ее кортежей (простота и наглядность, количество требуемых операций при добавлении/удалении субъекта или объекта, назначении/модификации полномочий и т. п.).

Рассмотрим основные способы неявного задания матрицы доступа.

Списки управления доступом к объекту. В данной схеме полномочия по доступу к объекту представляют в виде списков (цепочек) кортежей для всех субъектов, имеющих доступ к данному объекту. Это равносильно заданию матрицы по столбцам с исключением кортежей, имеющих все нулевые значения.

Такой вид представления матрицы называют «список управления доступом» (Access Control List — ACL) и реализуют в большинстве версий ОС Windows .

Достоинства способа состоят в экономии памяти, так как матрица доступа обычно сильно разрежена, и удобстве получения сведений о субъектах, имеющих доступ к объекту.

Недостатками являются неудобство отслеживания ограничений и зависимостей по наследованию полномочий субъектов, а также получения сведений об объектах, к которым имеет доступ данный субъект.

Поскольку списки управления доступом связаны с объектом, при удалении субъекта возможно возникновение ситуации, при которой объект будет доступен несуществующему субъекту.

Списки полномочий субъектов. В данной модели полномочия доступа субъекта представлены в виде цепочек кортежей для всех объектов, к которым он имеет доступ, что равносильно заданию матрицы по строкам с исключением кортежей, имеющих нулевые значения.

Данный вид задания матрицы доступа называют «профилем» (*profile*) субъекта.

В системах с большим числом объектов профили могут иметь значительные размеры и, вследствие этого, становятся трудно управляемыми. Изменение профилей нескольких субъектов может потребовать большого числа операций и привести к трудностям в работе системы.

Достоинства способа состоят в экономии памяти, так как матрица доступа обычно сильно разрежена, и удобстве получения сведений об объектах, к которым имеет доступ данный субъект.

Недостатки заключаются в сложности отслеживания ограничений и зависимостей по наследованию полномочий доступа к объектам, а также получении сведений о субъектах, имеющих доступ к заданному объекту.

Так как списки управления доступом связаны с субъектом, при удалении объекта может возникнуть ситуация, при которой субъект будет иметь право на доступ к несуществующему объекту.

Атрибутивные схемы. Атрибутивные способы задания матрицы доступа основаны на присвоении субъектам (объектам) определенных меток, содержащих значения атрибутов, на основе сопоставления которых определяют права доступа, т. е. осуществляется авторизация субъекта. Наиболее известный пример неявного задания матрицы доступа — реализация атрибутивной схемы в операционной системе UNIX.

Достоинствами данных схем являются экономия памяти, так как элементы матрицы не хранятся, а динамически вычисляются при попытке доступа для конкретной пары субъект-объект на основе их меток или атрибутов; удобство корректировки базы данных защиты, т. е. модификации меток и атрибутов и отслеживания ограничений и зависимостей по наследованию полномочий субъектов; отсутствие потенциальной противоречивости при удалении отдельных субъектов (объектов).

Недостатки состоят в дополнительных затратах времени на динамическое вычисление значений элементов матрицы при каждом обращении любого субъекта к любому объекту и затрудненном задании прав доступа конкретного субъекта к конкретному объекту.

Полномочное управление доступом. Механизм полномочного управления доступом, разработанный в 1980-х годах в интересах Министерства обороны США для обработки информации с различными грифами секретности, предусматривает присвоение каждому объекту системы метки критичности, определяющей ценность содержащейся в нем информации, а также уровня

прозрачности (уровня допуска), определяющего максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Цель системы защиты — не только контролировать доступ пользователя к объектам АС, но и следить за тем, чтобы пользователь не получил доступ к данным более высокого уровня конфиденциальности, чем позволяет его форма допуска и не произвел копирование этих данных на носители с меньшими уровнями секретности.

Выделяют две системы присвоения меток конфиденциальности — иерархическая и неиерархическая.

Полномочный метод управления доступом не получил широкого распространения в коммерческих организациях в связи с отсутствием в таких организациях четкой классификации хранимой и обрабатываемой информации, относительно высокой стоимостью реализации метода и большими накладными расходами.

Замкнутая программная среда. Механизм замкнутой программной среды предусматривает формирование жесткого списка программ, разрешенных системе для запуска, при выполнении определенных требований:

- «запрещено все, что явно не разрешено»;
- указание полных путей доступа к исполняемым файлам;
- запрет модификации файлов;
- формирование списка по журналам регистрации;
- наличие «мягкого» режима работы.

Регистрация и оперативное оповещение о событиях безопасности, происходящих в АС. Механизмы регистрации предназначены для получения и накопления (в целях последующего анализа) информации о состоянии ресурсов системы и действиях субъектов, признанных администрацией АС потенциально опасными для системы. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, характер и степень воздействия на систему, методы расследования, поиска нарушителя и исправления ситуации.

При регистрации событий безопасности в системном журнале обычно фиксируют следующую информацию:

- дату и время события;
- идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
- действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

Механизмы регистрации непосредственно связаны с другими защитными механизмами (например, сигналы о происходящих событиях и детальная информация о них поступает от механизмов контроля: подсистем разграничения доступа, контроля целостности ресурсов и др.).

В современных системах защиты подсистема оповещения сопряжена с механизмами оперативного автоматического реагирования на определенные события:

• подача сигнала тревоги;
• извещение администратора безопасности;
• извещение владельца информации о НСД к его данным;
• снятие программы (задания) с дальнейшего выполнения;
• отключение (блокирование работы) терминала или компьютера, с которого были осуществлены попытки НСД к информации;
• исключение нарушителя из списка зарегистрированных пользователей и т. п.

Криптографические методы защиты информации. Криптографическое преобразование информации, основанное на некотором алгоритме, зависящем от изменяемого параметра (обычно называемого секретным ключом), обладает свойством невозможности восстановления исходной информации по преобразованной без знания действующего ключа с трудоемкостью, меньше заранее заданной.

К криптографическим (шифровальным) средствам защиты относят: средства шифрования, имитозащиты, электронной подписи; кодирование; изготовление ключевых документов; аппаратные; программные и программно-аппаратные.

С помощью криптографических технологий можно решать з а д а ч и :
• аутентификации абонентов;
• контроля целостности данных;
• закрытия данных, хранимых в АС или передаваемых по каналам связи;
• разграничения ответственности на основе обеспечения аутентичности и неотказуемости.

Основное достоинство криптографических методов состоит в обеспечении высокой гарантированной стойкости защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей).

К числу недостатков относят значительные затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации; трудности совместного использования обычной и зашифрованной (подписанной) информации, связанные с управлением ключами (генерация, распределение и т. д.); высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены.

Различают криптографию с симметричными ключами и криптографию с открытыми ключами.

Криптография с симметричными ключами. Это классическая криптография, в которой абоненты используют общий ключ для шифрования и расшифрования данных.

Достоинствами криптографии данного класса являются высокая производительность и криптографическая стойкость алгоритмов на единицу длины ключа; недостатками — сложный механизм распределения ключей и технологические трудности обеспечения неотказуемости.

Криптография с открытыми ключами. Для решения задач распределения ключей и ЭП были использованы идеи асимметричности преобразований

и открытого распределения ключей Диффи и Хеллмана. В результате была создана криптография с открытыми ключами — не с одним секретным ключом, а парой ключей: открытым (публичным) и секретным (личным, индивидуальным), известным только одной взаимодействующей стороне. В отличие от секретного ключа, который должен сохраняться в тайне, открытый ключ может распространяться публично.

Схема шифрования данных с использованием открытого ключа состоит из двух этапов (рис. 12.4): на первом происходит обмен по несекретному каналу открытыми ключами при обеспечении подлинности передачи ключевой информации; на втором реализуется собственно шифрование сообщений, при котором отправитель зашифровывает сообщение открытым ключом получателя. Зашифрованный файл может быть прочитан только владельцем секретного ключа, т. е. получателем. В схеме расшифрования, реализуемой получателем сообщения, используется секретный ключ получателя.

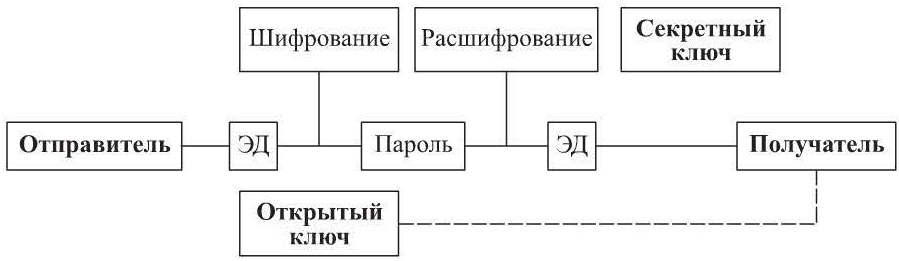

Рис. 12.4. Схема шифрования в криптографии с открытыми ключами

Реализация схемы ЭП связана с вычислением хеш-функции (дайджеста) данных, которая представляет собой уникальное число, полученное из исходных данных путем его сжатия (свертки) с помощью сложного, но известного алгоритма. Хеш-функция является однонаправленной, т. е. по хеш-значению невозможно восстановить исходные данные, и чувствительна к всевозможным искажениям данных. Кроме того, очень сложно отыскать два набора данных, обладающих одним и тем же значением хеш-функции.

Схема формирования подписи электронного документа его отправителем включает вычисление хеш-функции ЭД и шифрование этого значения посредством секретного ключа отправителя. Результатом шифрования является значение ЭП ЭД (реквизит ЭД), которое пересылается вместе с самим ЭД получателю. При этом получателю сообщения должен быть предварительно передан открытый ключ отправителя сообщения (рис. 12.5).

Алгоритм проверки (верификации) ЭП, осуществляемой получателем сообщения, состоит из следующих ш а г о в:

1) расшифрование блока ЭП посредством открытого ключа отправителя;

2) вычисление хеш-функции ЭД;

3) сравнение результата вычисления с результатом расшифровки блока ЭП — при совпадении результатов принимается решение о соответствии ЭП ЭД.

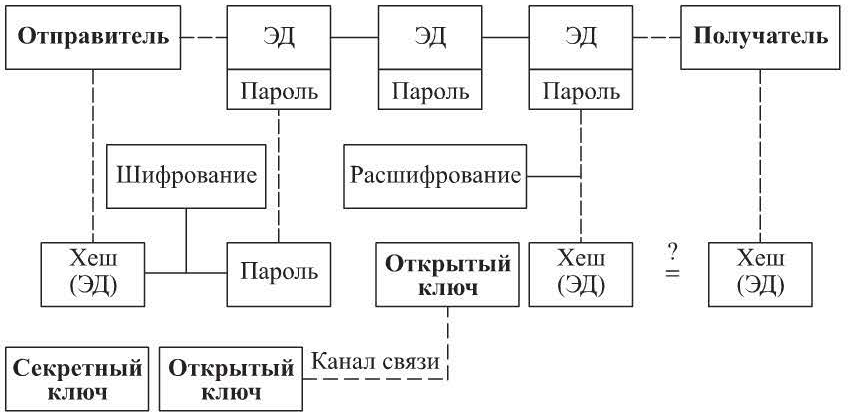

Рис. 12.5. Схема ЭП в криптографии с открытыми ключами

Несовпадение результатов возможно по следующим причинам:

- в процессе передачи по каналу связи была потеряна целостность ЭД;
- при формировании ЭП использовали поддельный секретный ключ;
- при проверке ЭП применили другой открытый ключ (в процессе передачи по каналу связи или при дальнейшем его хранении открытый ключ был модифицирован или подменен).

Реализация криптографических алгоритмов с открытыми ключами требует бóльших по сравнению с симметричными алгоритмами затрат процессорного времени, поэтому криптографию с открытыми ключами обычно применяют для решения задач распределения ключей и ЭП, а симметричную — для шифрования.

В схеме комбинированного шифрования, сочетающей в себе высокую безопасность криптосистем с открытым ключом и преимущества скорости работы симметричных криптосистем, для шифрования используется случайно вырабатываемый симметричный (сеансовый) ключ, который, в свою очередь, шифруют посредством открытой криптосистемы для секретной передачи по каналу в начале сеанса связи (рис. 12.6).

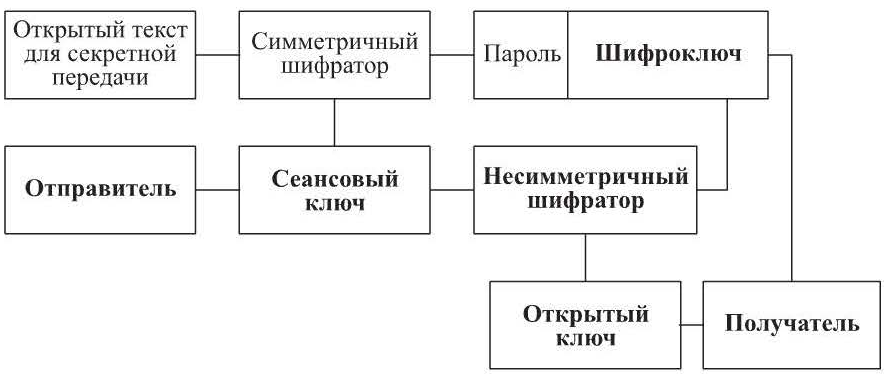

Рис. 12.6. Схема комбинированного шифрования

Доверие к открытому ключу и цифровые сертификаты. Главным вопросом схемы открытого распределения ключей является вопрос доверия к полученному открытому ключу партнера. Для большого класса практических систем (системы электронного документооборота, системы клиент — банк, межбанковских систем электронных расчетов), в которых возможна личная встреча партнеров до начала обмена ЭД, данная задача имеет относительно простое решение — взаимная сертификация открытых ключей.

Процедура сертификации заключается в том, что каждая сторона при личной встрече удостоверяет подписью уполномоченного лица и печатью бумажный документ — распечатку содержимого открытого ключа другой стороны. Этот бумажный сертификат является, во-первых, обязательством стороны использовать для проверки подписи под входящими сообщениями данный ключ и, во-вторых, обеспечивает юридическую значимость взаимодействия, поскольку позволяет однозначно идентифицировать мошенника среди двух партнеров, если один из них захочет подменить ключи.

В системах, где отсутствует возможность предварительного личного контакта партнеров, необходимо использовать цифровые сертификаты, выданные и заверенные ЭП доверенного посредника — центра сертификации.

На предварительном этапе каждый из партнеров лично посещает ЦС и получает сертификат — своеобразный электронный аналог гражданского паспорта, где содержатся данные:

- открытый ключ пользователя;
- серийный номер сертификата;
- индентификатор пользователя;
- период действия сертификата;
- идентификатор эмитента;
- ЭП эмитента;
- идентификатор алгоритма ЭП.

В бумажном виде сертификат содержит рукописные подписи уполномоченных лиц и печати. Сертификат может быть выпущен только уполномоченным эмитентом и содержит единственную ЭП эмитента.

После посещения ЦС каждый из партнеров становится обладателем открытого ключа ЦС, который позволяет проверить подлинность открытого ключа партнера путем установления подлинности ЭП удостоверяющего центра под сертификатом открытого ключа партнера.

В ЦС созданы условия безопасного хранения секретных ключей, а также администрирования доступа к ним.

В соответствии с Федеральным законом «Об электронной подписи» владелец сертификата проверки ключа ЭП — исключительно физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа и которое владеет соответствующим закрытым ключом ЭП.

В реальных системах каждым партнером может использоваться несколько сертификатов, выданных различными ЦС, которые могут быть объединены инфраструктурой открытых ключей или PKI (Public Key Infrastructure). ЦС в

рамках PKI обеспечивает не только хранение сертификатов, но и управление ими (выпуск, отзыв, проверку доверия). Наиболее распространенная модель PKI — иерархическая, достоинство которой состоит в том, что проверка сертификатов требует доверия только относительно малому числу корневых (root) ЦС, но при этом позволяет иметь различное число ЦС, выдающих сертификаты.

Контроль целостности программных и информационных ресурсов. В правильно спроектированных системах защиты все механизмы контроля используют единый механизм регистрации. Применение разнородных средств защиты разных производителей, в каждом из которых имеются свои механизмы и ведутся свои журналы регистрации, усложняет администрирование системы защиты.

Механизм контроля целостности ресурсов системы, предназначенный для своевременного обнаружения модификации ресурсов системы, обеспечивается средствами:

- разграничения доступа, запрещающими модификацию или удаление защищаемого ресурса;
- сравнения критичных ресурсов с их эталонными копиями;
- подсчета контрольных сумм (сигнатур, имитовставок и т. п.);
- ЭП.

К контролируемым ресурсам относят файлы и каталоги, элементы реестра, сектора дисков.

При этом контролируют такие параметры, как:

- содержимое ресурса;
- списки управления доступом;
- атрибуты файлов.

Контроль осуществляют либо до загрузки ОС, либо непосредственно в момент наступления события, либо по расписанию.

Обнаружение вторжений (атак). Это процесс мониторинга событий, происходящих в АС, в целях поиска признаков нарушений безопасности. Например, просматривая журнал регистрации событий и обнаружив там большое количество неудачных попыток аутентификации за короткий промежуток времени, можно сделать вывод, о том что произошла атака «*подбор пароля*». В данном случае определенное число неудачных попыток аутентификации за определенный период времени и есть признак нарушения безопасности.

Теоретически поиск признаков атак может выполняться вручную (в этом случае он сводится к рассмотренному анализу собранной средствами регистрации информации, что позволяет выявить факты совершения нарушений), но суть механизма обнаружения атак состоит именно в автоматизации данного процесса.

Таким образом, система (средство) обнаружения атак — это программное (или программно-аппаратное) обеспечение, автоматизирующее данный процесс.

Для примера, приведенного на рис. 12.7, это означает, что система будет непрерывно осуществлять мониторинг журнала «Security» и при обнаруже-

нии там определенного количества записей, свидетельствующих о неудачных попытках аутентификации за единицу времени, осуществит соответствующее оповещение.

Tag Name	Severity	Status	Event Count	Sc
Brute_force_login_attack	High	Detected event	1	
Registry_eventlog_settings_changed	Medium	Detected event	3	
Audit_policy_change	Medium	Detected event	2	
Failed_login-bad_username_or_password	Low	Detected event	13	
Windows_Access_Error	Low	Detected event	13	
Privileged_service_called	Low	Detected event	8	
SMB_Auth_Failed	Low	Detected event	3	
SensorStatistics	Low	Detected event	1	
SensorStatistics_Cumulative	Low	Detected event	1	

Рис. 12.7. Консоль системы обнаружения атак

Считается, что впервые вопрос о механизме обнаружения атак был затронут в работе Дж. Андерсена (James Anderson) «Computer Security Threat Monitoring and Surveillance», где он предложил автоматизировать анализ результатов работы механизма регистрации событий в целях сокращения времени реагирования на нарушения.

Таким образом, появившись как дополнительная «надстройка» над механизмом регистрации событий, обнаружение атак стало вполне самостоятельным защитным механизмом.

В настоящее время системы обнаружения атак осуществляют поиск признаков нарушений в сетевом трафике, журнале событий и действиях субъектов системы.

12.2. Защита периметра компьютерных сетей и управление механизмами защиты

Развитие сетевых технологий привело к созданию нового типа СЗИ. Это межсетевые экраны (Firewall), обеспечивающие безопасность при электронном обмене информацией с другими автоматизированными системами и внешними сетями, разграничение доступа между сегментами корпоративной сети, а также защиту от проникновения и вмешательства в работу АС нарушителей из внешних систем.

Межсетевые экраны, установленные в точках соединения с сетью Интернет, обеспечивают защиту внешнего периметра сети организации и защиту собственных интернет-серверов, открытых для общего пользования, от несанкционированного доступа.

В межсетевых экранах применяются специальные средства защиты; основные из них:

• трансляция адресов для сокрытия структуры и адресации внутренней сети;

• фильтрация проходящего трафика;

• управление списками доступа на маршрутизаторах;

• дополнительная идентификация и аутентификация пользователей стандартных служб (на проходе);

• ревизия содержимого (вложений) информационных пакетов, выявление и нейтрализация компьютерных вирусов;

• виртуальные частные сети (для защиты потоков данных, передаваемых по открытым сетям, для обеспечения конфиденциальности информации применяются криптографические методы);

• противодействие атакам на внутренние ресурсы.

Управление механизмами защиты. Конкуренция в области разработки средств защиты АС приводит к унификации требований к таким средствам, в частности, к обеспечению управления всеми имеющимися защитными механизмами.

В настоящее время в большинстве случаев средства защиты устанавливают на функционирующие АС, что требует приостановления технологического процесса (на этапе внедрения), а также перерывов в работе АС при переналадке оборудования, изменении состава технических средств, программного обеспечения, персонала и пользователей и т. д.

Для обеспечения удобства переналадки средств защиты необходимо предусмотреть следующие возможности:

• выборочное подключение имеющихся защитных механизмов, что позволит реализовать режим поэтапного усиления степени защищенности АС;

• использовать так называемый «мягкий» режим функционирования средств защиты, при котором несанкционированные действия пользователей (действия с превышением полномочий) фиксируются в системном журнале, но не пресекаются, т. е. не запрещаются системой защиты. Такой режим дает возможность выявить некорректности настроек средств защиты без нарушения работоспособности АС и существующей технологии обработки информации;

• автоматизированного изменения полномочий пользователя с учетом информации, накопленной в системных журналах (при работе как в «мягком», так и в обычном режимах).

С увеличением объема защищаемой АС усиливаются требования к организации удаленного управления средствами защиты, поэтому решения, приемлемые для автономного компьютера или небольшой сети из 10 — 15 рабочих станций, непригодны для больших сетей, объединяющих несколько сотен рабочих станций. Решение проблем управления средствами защиты таких сетей предусматривает дополнительные требования:

• управление механизмами защиты проводится как централизованно (удаленно, с рабочего места администратора безопасности сети), так и децентрализованно (непосредственно с конкретной рабочей станции), т. е. любые

изменения настроек защитных механизмов, произведенные централизованно, автоматически распространяются на все рабочие станции (независимо от состояния рабочей станции на момент внесения изменений в центральную базу данных). Аналогично, часть изменений, произведенных децентрализованно, автоматически отражается в центральной базе данных (например, при смене пароля пользователем на одной из рабочих станций, новое значение пароля поступает в центральную базу данных защиты сети и рассылается на все рабочие станции, на которых данному пользователю разрешено работать);

• управление механизмами защиты рабочей станции осуществляется независимо от активности данной станции;

• оперативный контроль за состоянием рабочих станций и работой пользователей в сети.

Для облегчения работы системных администраторов при увеличении количества рабочих станций и использовании новых программных средств, включающих большое количество разнообразных программ (например, MS Windows), предусматривают следующие возможности:

• установку подсистемы реализации запросов, позволяющую выбирать из собранных системных журналов данные об определенных событиях (по имени пользователя, дате, времени и категории события и т. п.);

• автоматическое разбиение и хранение системных журналов по месяцам и дням в пределах заданного количества последних дней. Причем во избежание переполнения дисков по истечении установленного количества дней просроченные журналы, если их не удалил администратор, должны автоматически уничтожаться;

• наличие в системе защиты средств автоматической подготовки отчетных документов установленной формы о работе станций сети и имевших место нарушениях, а также механизмов семантического сжатия данных в журналах регистрации, позволяющих укрупнять регистрируемые события без существенной потери их информативности (например, заменять все многократно повторяющиеся в журнале события, связанные с выполнением командного файла autoexec.bat, одним событием).

12.3. Страхование информационных рисков

Утрата или искажение данных в результате компьютерных преступлений и мошенничества, несанкционированных действий третьих лиц, воздействия программ-вирусов, отказов и сбоев аппаратных средств, ошибок программного обеспечения, неквалифицированных и преднамеренных действий обслуживающего персонала и других причин способны повлечь за собой значительный материальный ущерб. Одним из эффективных методов компенсации ущерба, наступившего в результате перечисленных событий, является страхование.

В соответствии с Федеральным законом «Об организации страхового дела в Российской Федерации» *страхование* представляет собой отношения по защите интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов (страховых премий).

Страховой случай. К страховым случаям относят уничтожение или повреждение застрахованных активов вследствие наступления следующих с о б ы т и й :

- действие вирусов, «червей» и «троянских коней»;
- компьютерные атаки со стороны внешних злоумышленников (хакеров);
- хищение денежных средств в электронной форме внешними злоумышленниками (с помощью сфальсифицированного финансового поручения, посланного электронным способом страхователю или от имени страхователя, путем модификации программного обеспечения, непосредственным вводом команд);
- несанкционированные действия со стороны сотрудников организации;
- сбои системы из-за ошибок, допущенных при проектировании, разработке, создании, установке, настройке и эксплуатации АС;
- временное прекращение деятельности вследствие любого из перечисленных страховых случаев.

Принятие решения о применении страхования. При выборе страхования как метода защиты информации проводится оценка рисков. После принятия решения об использовании страхования в качестве метода защиты информации специалист по защите информации (информационной безопасности) составляет справку по объектам, подлежащим страхованию, рискам и возможным потерям, вероятности реализации рисков и размерам возможных убытков и принимает решение по поводу вида страхования, типа договора, условий страхования и т. п.

После выбора вида страхования агент страховой компании оформляет договор.

Процедура страхования информационных рисков. Процедура страхования информационных рисков состоит из следующих э т а п о в :

- переговоры, определяющие условия страхования;
- разработка и согласование предложений по страхованию;
- проведение экспертизы страхователя;
- выполнение рекомендаций, полученных в результате экспертизы;
- подписание договора о страховании.

Непременным условием страхования информационных рисков является проведение экспертизы по анализу рисков страхового объекта. Эта экспертиза, называемая «сюрвей» (от англ. *survey* — осмотр), проводится экспертами в области информационной безопасности — независимыми специалистами, которые не работают ни в застрахованной, ни в страховой компании.

Половина стоимости такой экспертизы компенсируется страховой компании при заключении соответствующего договора страхования.

К параметрам, влияющим на ставку страхования, относят:

• стоимость застрахованных ресурсов;

• используемые средства защиты —чем известнее система защиты, тем ниже ставка страхования;

• статистика атак для аналогичных организаций отрасли.

* * *

Таким образом, универсальные механизмы защиты, которыми располагают специалисты по безопасности, обладают как достоинствами, так и недостатками, и могут применяться в различных вариациях и совокупностях в конкретных методах и средствах защиты. Повышать уровень стойкости системы защиты за счет применения более совершенных физических и технических средств можно только до уровня стойкости персонала из ядра безопасности системы. Успех или неудача масштабного применения систем защиты информации зависит от наличия в них развитых средств управления режимами работы защитными механизмами и реализации функций, позволяющих существенно упрощать процессы установки, настройки и эксплуатации средств защиты.

Контрольные вопросы

1. Назовите этапы идентификации и аутентификации. В чем их различие и как они связаны между собой?

2. Приведите примеры различных идентификаторов и аутентификаторов пользователя.

3. Что понимают под авторизацией пользователя?

4. Перечислите недостатки парольных подсистем идентификации и аутентификации.

5. Перечислите основные виды угроз парольных подсистем идентификации и аутентификации.

6. Приведите примеры технических устройств, с помощью которых может решаться задача идентификации пользователя.

7. Приведите примеры технических устройств, с помощью которых может решаться задача идентификации и аутентификации пользователя.

8. Перечислите основные задачи, решаемые криптографией.

9. Опишите традиционные симметричные криптосистемы и укажите их недостатки.

10. Сколько секретных ключей используется при взаимном обмене зашифрованными (симметричным алгоритмом) сообщениями двух сторон?

11. Что понимают под ЭП?

12. Какой ключ используется для формирования ЭП почтового сообщения?

13. Что понимают под инфраструктурой открытых ключей?

14. Как осуществляется защита периметра компьютерных сетей и каковы основные средства защиты?

15. Какие события относят к страховым случаям?

Глава 13. АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

С момента создания и начала функционирования системы сертификации средств защиты информации по требованиям безопасности информации ФСТЭК России было сертифицировано несколько десятков СЗИ НСД. Далее будут приведены рекомендации по выбору СЗИ НСД, рассмотрены некоторые из существующих на рынке СЗИ НСД (полный перечень сертифицированных средств защиты информации опубликован на сайте ФСТЭК России).

13.1. Рекомендации по выбору средств защиты информации от несанкционированного доступа

Выбор средств защиты информации зависит от потребности организации в определенном уровне защищенности автоматизированной системы, количества компьютеров, их технических характеристик, применяемых операционных систем и других факторов.

При выборе соответствующих уровню защищенности АС конкретных средств защиты необходимо пользоваться руководящими документами ФСТЭК России: 1) Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации; 2) Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.

Защищенность СВТ определяется их способностью предотвращать или существенно затруднять НСД к информации при использовании СВТ в составе АС.

Защита АС и СВТ обеспечивается комплексом программно-технических средств (КСЗ) и соответствующих организационных мер.

Требования ФСТЭК России к защищенности АС приведены в табл. 13.1, СВТ — в табл. 13.2.

Таблица 13.1

Распределение показателей защищенности по классам для автоматизированных систем

Подсистемы и требования	Класс защищенности								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									
в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-	-	+	-	+	+	+	+
к программам	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+

Окончание табл. 13.1

Подсистемы и требования	Класс защищенности								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
2. Подсистема регистрации и учета									
2.1. Регистрация и учет:									
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+	+	+	+	+	+
выдачи печатных документов	-	+	-	+	-	+	+	+	+
запуска (завершения) программ и процессов	-	-	-	+	-	+	+	+	+
доступа к защищаемым файлам (создание, удаление, передача по линиям и каналам связи)	-	-	-	+	-	+	+	+	+
доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, файлам	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	-	+	-	+	-	+	+	+	+
2.4. Сигнализация о попытках нарушения защиты	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема									
3.1. Шифрование конфиденциальной информации	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа на разных ключах	-	-	-	-	-	-	-	-	+
3.3. Использование сертифицированных криптографических средств	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности									
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты	-	+	-	+	-	-	+	+	+

Примечание: «-» — требования к классу отсутствуют.

Таблица 13.2

Требования руководящих документов ФСТЭК России к средствам защиты информации от несанкционированного доступа

№ п/п	Показатель	Класс защищенности					
		6	5	4	3	2	1
1	Дискреционный принцип контроля доступа	+	+	+	=	+	=
2	Мандатный принцип контроля доступа	-	-	+	=	=	=
3	Очистка памяти	-	+	+	+	=	=
4	Изоляция модулей	-	-	+	=	+	=

Окончание табл. 13.2

№ п/п	Показатель	Класс защищенности					
		6	5	4	3	2	1
5	Маркировка документов	-	-	+	=	=	=
6	Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
7	Сопоставление пользователя с устройством	-	-	+	=	=	=
8	Идентификация и аутентификация	+	=	+	=	=	=
9	Гарантии проектирования	-	+	+	+	+	+
10	Регистрация	-	+	+	+	=	=
11	Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
12	Надежное восстановление	-	-	-	+	=	=
13	Целостность КСЗ	-	+	+	+	=	=
14	Контроль модификации	-	-	-	-	+	=
15	Контроль дистрибуции	-	-	-	-	+	=
16	Гарантии архитектуры	-	-	-	-	-	+
17	Тестирование	+	+	+	+	+	=
18	Руководство пользователя	+	=	=	=	=	=
19	Руководство по КСЗ	+	+	=	+	+	=
20	Тестовая документация	+	+	+	+	+	=
21	Конструкторская (проектная) документация	+	+	+	+	+	+

Примечание: «-» — требования к классу отсутствуют; «=» — требования совпадают с требованиями к СВТ предыдущего класса.

При выборе СЗИ НСД необходимо учитывать следующие моменты:

• цель применения СЗИ НСД и задачи, которые необходимо решать с их помощью;

• существующие на рынке СЗИ НСД, обратив внимание на длительность существования данных СЗИ НСД на рынке (чем дольше СЗИ находится на рынке, тем выше вероятность того, что бóльшая часть ошибок разработчиками СЗИ устранена с уточнением конфигурации технических и программных средств);

• получив у поставщика опытный образец с ограниченным сроком действия, проверить совместимость с существующими программно-аппаратными средствами (чем больше организаций, в которых установлены данные СЗИ, тем больше перечень программных средств, с которыми они совместимы);

• определить удобство эксплуатации и наличие необходимой документации на СЗИ.

Приобретение дополнительных средств защиты требуется в следующих случаях:

• при использовании на компьютерах средств криптографической защиты (для защиты ключей ЭП и шифрования);

• регламентации действий пользователей, работающих на компьютерах, и протоколировании их действий;

• введении ограничений доступа пользователей, работающих на компьютерах, к локальным ресурсам системы (локальным дискам, каталогам, файлам или внешним устройствам).

Разработчики СЗИ НСД могут реализовать две схемы управления:

• «*длинные руки*» — управление полномочиями пользователя осуществляется администратором удаленно на каждом компьютере (недостатками схемы являются ее децентрализованный характер — для смены, например, пароля пользователя необходимо вручную изменить его пароль на всех компьютерах, на которых он зарегистрирован, и зависимость от того, включен ли компьютер пользователя);

• *отложенного централизованного управления доступом* — полномочия пользователя меняются один раз в центральной базе данных, и затем их изменение на конкретном компьютере берет на себя система защиты (при этом администратору безразлично состояние ПК на момент внесения изменений в центральную базу данных. Все изменения на компьютер передаются во время сеанса синхронизации). В последнее время при разработке СЗИ для платформы Windows все большее распространение получает подход, когда в качестве центральной базы данных по настройкам СЗИ на компьютере используется Active Directory, а для распространения настроек — механизм групповых политик.

13.2. Обзор существующих на рынке средств защиты информации от несанкционированного доступа

Приведем краткий перечень предприятий-разработчиков СЗИ НСД, включенных в Государственный реестр сертифицированных средств защиты информации.

Ассоциация защиты информации «Конфидент»[1] (Санкт-Петербург). Ассоциация разрабатывает семейство программных комплексов Dallas Lock следующих сертифицированных версий:

• Dallas Lock 6.0 для Windows 95OSR2/98/ME (сертификат ФСТЭК России по 4-му классу для СВТ и 3-му уровню контроля отсутствия НДВ[2]);

• Dallas Lock 7.0 для Windows 2000/XP (сертификат ФСТЭК России по 4-му классу для СВТ и 3-му уровню контроля отсутствия НДВ);

• Dallas Lock 7.5 для Windows 2000(SP4)/XP(SP2)/2003(SP1) (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия НДВ);

• Dallas Lock 7.7 для Windows XP/2003/Vista/2008/7 (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия НДВ);

• Dallas Lock 8.0-К.

---

[1] http://www.confident.ru

[2] НДВ — недекларированные возможности.

Основные возможности СЗИ НСД Dallas Lock 7.7:

• запрос пароля и аппаратных идентификаторов происходит до начала загрузки ОС, т. е. загрузка ОС возможна только после проверки идентификационных данных пользователя в СЗИ НСД;

• запрет загрузки компьютера посторонними лицами;

• двухфакторная авторизация по паролю и аппаратным идентификаторам (USB eToken, смарт-карты eToken, ruToken, iButton);

• разграничение прав пользователей на доступ к локальным и сетевым ресурсам по мандатному и дискреционному методам;

• контроль работы пользователей со сменными накопителями;

• организация замкнутой программной среды;

• аудит действий пользователей;

• контроль целостности ресурсов компьютера с помощью контрольных сумм, вычисленных по одному из алгоритмов;

• очистка остаточной информации — невозможность восстановления удаленных данных;

• возможность автоматической печати штампов (меток конфиденциальности) на всех распечатываемых документах;

• защита содержимого дисков путем «прозрачного» преобразования по алгоритмам XOR32 или ГОСТ 28147 — 89;

• удаленное администрирование;

• выделенный центр управления, работа в составе домена безопасности и др.

Разграничение прав доступа к ресурсам файловой системы реализуется следующими методами:

• *дискреционный* — предоставляет доступ к защищаемым объектам файловой системы на основании списков контроля доступа. В соответствии с содержимым списков определяются права доступа для каждого пользователя;

• *мандатный* — каждому пользователю присваивается максимальный уровень мандатного доступа. Пользователь получает доступ к объектам, мандатный уровень которых не превышает его текущий уровень;

• *замкнутая программная среда* — режим, в котором пользователь может запускать только программы, определенные администратором.

Для осуществления централизованного управления защищенными компьютерами в ЛВС в состав СЗИ НСД входит Сервер безопасности (СБ), который позволяет централизованно управлять учетными записями пользователей, политиками безопасности, осуществлять просмотр и автоматический сбор журналов, назначать права доступа к ресурсам, управлять «прозрачным» преобразованием и выполнять команды оперативного управления.

Модуль «Менеджер серверов безопасности» объединяет несколько СБ в «Лес Безопасности», с помощью которого осуществляется централизованное управления несколькими доменами безопасности (получение журналов, управление политиками и учетными записями пользователей).

Научно-исследовательский отдел проблем информационной безопасности Санкт-Петербургского института информатики и автоматизации РАН[1]

[1] http://www.cobra.ru

(Санкт-Петербург). Отдел разрабатывает средства программных комплексных СЗИ НСД следующих сертифицированных в е р с и й :

• *СЗИ «Аура»* для Windows 2000 Professional SP4/ 2000 Server SP4/ XP Professional SP3/ Server 2003 Standard Edition SP2/ Server 2003 Enterprise Edition SP2/ Server 2008 Standard Edition SP2/ Server 2008 Enterprise Edition SP2/ Vista Business SP2/ Vista Ultimate SP2 (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия НДВ);

• *СЗИ «Щит-РЖД»* для Windows 2000/XP (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия недекларированных возможностей (НДВ).

Основные функциональные возможности СЗИ НСД «Аура»:

• идентификация и аутентификация пользователей в доверенной среде с применением электронных устройств ruToken (на данный момент используется ruToken версии 1.0. При установке новых драйверов функция блокировки консоли доступна и с ruToken версии 2.0/3.0);

• многоуровневый контроль целостности информационных объектов вычислительной системы;

• контроль доступа к устройствам, файлам и папкам;

• управление печатью, автоматическая маркировка и учет документов;

• достоверное уничтожение информационных объектов;

• регистрация действий пользователя в системных журналах.

Основные функциональные возможности СЗИ НСД «Щит-РЖД»:

• поставляется совместно с электронным ключом Guardant (по согласованию возможна поставка системы без электронного ключа);

• идентификация и аутентификация пользователей в доверенной среде с применением электронных устройств ruToken (в настоящее время используется ruToken версии 1.0);

• динамический контроль целостности системы защиты, компонентов ОС, прикладных программ и управляющих данных;

• контроль доступа к устройствам, файлам и папкам;

• управление печатью, автоматическая маркировка и учет документов и др.

Компания ООО «ГАЗИНФОРМСЕРВИС»[1] (Санкт-Петербург). Компания разрабатывает семейство программных и программно-технических СЗИ НСД следующих сертифицированных в е р с и й :

• *СЗИ «Блокпост-2000/XP» v.1.0* (локальный вариант) для Windows 2000/XP (сертификат ФСТЭК России по 4-му классу для СВТ и 3-му уровню контроля отсутствия НДВ);

• *СЗИ «Блокхост-сеть»* для Windows 2000/XP/2003 (сертификат ФСТЭК России по 3-му классу для СВТ и сертификат ФСТЭК России по 3-му уровню контроля отсутствия НДВ).

Версия «Блокпост-2000/XP» v.1.0 дополняет стандартные защитные механизмы операционных систем MS Windows ф у н к ц и я м и , обеспечивающими:

[1] http://www.gaz-is.spb.ru

• идентификацию пользователей с помощью специальных аппаратных средств (iButton);

• дискреционное и мандатное управление доступом пользователей к информационным ресурсам ПК;

• оперативный контроль за работой пользователей ПК путем регистрации событий, связанных с безопасностью информационной системы, с помощью средств просмотра и представления зарегистрированной информации;

• контроль целостности программ, используемых пользователями и ОС;

• возможность создания для любого пользователя замкнутой программной среды (списка разрешенных для запуска программ) и др.

Серверная часть СЗИ «Блокхост-сеть» обеспечивает *централизованную защиту* информации, включая:

• разграничение удаленного доступа пользователей к защищаемой информации, содержащейся на рабочих станциях на основе мандатного механизма;

• удаленное администрирование клиентской части СЗИ «Блокхост-сеть» на рабочих станциях;

• удаленное ведение оперативного контроля;

• аутентификация и идентификация пользователей с помощью аппаратных средств eToken, ruToken и других USB-устройств;

• оперативный контроль за событиями, связанными с безопасностью защищаемой информации.

ЗАО Научно-производственный центр «Модуль»[1] (Москва). НПЦ разрабатывает семейство программных СЗИ от НСД следующих сертифицированных версий:

• *СЗИ «Страж NT» (версия 2.5)* для Windows NT 4.0, 2000, XP, 2003 Server (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия НДВ);

• *СЗИ «Страж NT» (версия 3.0)* для 32-разрядных операционных систем Windows 2000 (Server и Professional), Windows XP (Professional и Home Edition), Windows Server 2003, Windows Vista, Windows Server 2008 (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия НДВ).

Основные функциональные возможности СЗИ «Страж NT» (версия 2.5):

• вход в систему пользователей только при предъявлении специального идентификатора (iButton или USB-ключа типа eToken и GuardantID) и ввода пароля;

• возможность идентификации пользователей без перезагрузки ОС при использовании однотипных идентификаторов;

• избирательное разграничение доступа пользователей к защищаемым ресурсам (дискам, каталогам, файлам и др.);

• разграничение доступа пользователей к информации различных уровней конфиденциальности в соответствии с имеющимися допусками;

[1] http://www.npcmodul.ru

• управление и настройка механизмов защиты как локально, так и удаленно;

• возможность гарантированной очистки содержимого всех файлов на локальных жестких дисках при их удалении;

• возможность запуска хранителя экрана, блокировка рабочей станции при удалении USB-ключа или при предъявлении iButton и др.

Основные отличия СЗИ НСД «Страж NT» (версия 3.0) от предыдущих версий:

• устанавливается как на автономных рабочих станциях, так и рабочих станциях в составе рабочей группы или домена, серверах, в том числе в составе кластера;

• функционирует на одно- и многопроцессорных компьютерных системах на базе архитектуры x86 под управлением 32-разрядных операционных систем Windows Vista, Windows Server 2008;

• осуществляет контроль устройств, подключенных к компьютеру путем задания дескрипторов безопасности для групп однотипных устройств;

• имеет дополнительный механизм защиты съемных носителей (дисков и флэш-карт) путем «прозрачного» преобразования информации, записываемой на носитель по ГОСТ 28147–89;

• имеет механизм, позволяющий создавать списки настроек и свободно тиражировать их на другие компьютеры;

• помимо устройств iButton, USB-ключей eToken и Guardant ID, реализована поддержка ключей ruToken и др.;

ЗАО «ОКБ САПР»[1] (Москва). Организация разрабатывает семейство программно-технических СЗИ НСД следующих сертифицированных версий:

• комплекс СЗИ НСД *«Аккорд-NT/2000» v.3.0* для ОС Windows в системах терминального доступа, построенных на базе терминальных служб сетевых операционных систем семейства Microsoft Windows, и программного обеспечения Citrix, является совместной разработкой ЗАО «ОКБ САПР» и ООО «Фирма «ИнфоКрипт» (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия НДВ);

• подсистема распределенного аудита и управления «*Аккорд-РАУ*», функционирующая на ПЭВМ, совмещенных с IBM PC AT, под управлением ОС Windows NT/2000/XP/2003/Vista (сертификат ФСТЭК России по 3-му уровню контроля отсутствия НДВ);

• комплекс *«Аккорд-Рубеж» v.1.5* — совместная разработка ЗАО «ОКБ САПР» и ООО «Фирма «ИнфоКрипт» (сертификат ФСТЭК России по 4-му классу для СВТ).

Основные функциональные возможности комплекса СЗИ НСД «Аккорд»:

• идентификация и аутентификация пользователей до загрузки операционной системы;

• аппаратный контроль целостности системных файлов и критичных разделов реестра;

[1] http://www.okbsapr.ru

• контроль целостности программ и данных, их защита от несанкционированных модификаций;

• запрет запуска неразрешенных программ;

• разграничение доступа пользователей к массивам данных и программам с помощью дискреционного и мандатного контроля доступа;

• автоматическое ведение протокола регистрируемых событий в энергонезависимой памяти аппаратной части комплекса.

Комплекс СЗИ НСД «Аккорд-Рубеж» решает проблему защиты информации путем создания программно-изолированной среды на рабочих станциях под управлением ОС Windows 2000 и Windows XP. Для фиксации списка защищаемых объектов (информационных файлов и запускаемых модулей) создается так называемый белый список с помощью режима автоматического сбора статистики.

При защите корпоративных АС комплексы «Аккорд-Рубеж» используются совместно с комплексом «АккордСеть-NDS» (сертификат ФСТЭК России по 4-му классу для СВТ) и позволяют решать з а д а ч и:

• защиты гетерогенных АС, используя как внутреннюю трехзвенную архитектуру «клиент-приложения-данные», так и службы единого каталога (например, Active Directory, Open LDAP);

• интеграции средств защиты разнородных прикладных и информационных компонентов гетерогенных АС и управления защитой всей гетерогенной АС из единой консоли администратора информационной безопасности АС;

• поддержки серверных сетевых ОС (Windows, Linux, Sun Solaris и др.).

ООО «Код Безопасности» /ГК «Информзащита»[1] (Москва). Компания разрабатывает семейство программно-аппаратных и программных СЗИ НСД следующих сертифицированных в е р с и й:

• *СЗИ Secret Net 5.0 (мобильный вариант)* для Windows 2000/XP/2003 (сертификаты ФСТЭК России по 4-му уровню контроля отсутствия НДВ и оценочный уровень доверия (усиленный), для АС класса 1Г включительно);

• *Secret Net 5.0*—С для Windows 2000/XP/2003 (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия НДВ);

• *Secret Net 5.0*—С (сетевой вариант) для Windows 2000/XP/2003 (сертификат ФСТЭК России по 4-му классу для СВТ и 3-му уровню контроля отсутствия НДВ);

• *Secret Net 5.1* (автономный вариант) для Windows 2000/XP/2003/Vista (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия НДВ);

• *Secret Net 5.1* (сетевой вариант) для Windows 2000/XP/2003/Vista (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия НДВ);

• *Secret Net 6* (вариант К) для Windows 2000/XP/2003/Vista/7/2008 (сертификат ФСТЭК России по 5-му классу для СВТ и 4-му уровню контроля отсутствия НДВ);

[1] http://www.securitycode.ru

• *Secret Net 6* для Windows 2000/XP/2003/Vista/7/2008 (сертификат ФСТЭК России по 3-му классу для СВТ и 2-му уровню контроля отсутствия НДВ);

• *SecretNet Studio* для Windows 2000/XP/2003, а также систем терминального доступа, построенных на базе терминальных служб сетевых ОС Microsoft Windows (сертификат ФСТЭК России по 5-му классу для СВТ и 4-му уровню контроля отсутствия НДВ).

Комплекс Secret Net 6 сочетает в себе необходимые возможности по защите информации, средства централизованного управления, средства оперативного реагирования и возможность мониторинга безопасности информационной системы в реальном времени и имеет следующие возможности:

• идентификация и аутентификация пользователя при входе в систему с помощью устройств iButton, eToken, ruToken;

• разграничение доступа к информации в целях предотвращения несанкционированного копирования информации с защищаемого компьютера (существует возможность запретить или разрешить пользователям работу с любыми портами/устройствами);

• контроль подключения устройств на шинах USB, PCMCIA, IEEE1394 по типу и серийному номеру;

• возможность запрета использования сетевых интерфейсов;

• создание доверенной информационной среды;

• запрет загрузки ОС с внешних съемных носителей (в качестве аппаратной поддержки используется программно-аппаратный комплекс «Соболь» или Secret Net Card);

• создание замкнутой программной среды (для каждого пользователя компьютера формируется определенный перечень программ, разрешенных для запуска, что позволяет исключить распространение вирусов, «червей» и шпионского ПО, а также использования компьютера в качестве игровой приставки);

• контроль целостности (слежение за неизменностью контролируемых объектов для защиты их от модификации в автоматическом режиме в соответствии с заданным расписанием);

• контроль аппаратной конфигурации компьютера;

• функциональный самоконтроль подсистем;

• защита информации в процессе хранения;

• контроль печати конфиденциальной информации (при разрешенном выводе конфиденциальной информации на печать документы автоматически маркируются в соответствии с принятыми в организации стандартами. Факт печати отображается в журнале защиты Secret Net 6);

• гарантированное уничтожение данных;

• регистрация всех событий;

• импорт и экспорт параметров (после проверки корректности работы защитных механизмов на компьютере, принимаемом за эталонный, выполняется экспорт значений параметров в файл, а затем их импорт на необходимое количество компьютеров).

13.3. Средства аппаратной поддержки

Аппаратная поддержка осуществляется с помощью специальной платы, обеспечивающей чтение аппаратурой компьютера информации из микросхемы расширения BIOS. Плата содержит разъем для системной шины PCI, панель для установки микросхемы с расширением BIOS и разъем для подключения считывателя персональных идентификаторов.

Изделия такого класса (Secret Net Card и программно-аппаратный комплекс (ПАК) «Соболь») входят в состав разработок компании «Код Безопасности» и поставляются в качестве одного из вариантов аппаратной поддержки для СЗИ НСД Secret Net.

Возможности *Secret Net Card* (не является самостоятельным средством защиты информации; поставляется как плата аппаратной поддержки для СЗИ НСД Secret Net):

- идентификация и аутентификация пользователей с использованием персональных идентификаторов;
- защита от загрузки операционной системы с внешних съемных носителей информации;
- автоматическое определение времени срабатывания сторожевого таймера (индивидуально для каждого изделия Secret Net Card);
- поддержка работы платы Secret Net Card с современными версиями BIOS Intel и других производителей.

В отличие от Secret Net Card *ПАК «Соболь»* (рис. 13.1) может быть использован как самостоятельное средство защиты информации, функционирующее под управлением ОС семейства Windows, FreeBSD, Trustverse Linux XP Desktop 2008 Secure Edition, МСВС и VMWare ESX, и имеет следующие возможности:

- идентификация и усиленная (двухфакторная) аутентификация пользователей с использованием персональных идентификаторов (iButton, eToken PRO, смарт-карта eToken PRO через USB-считыватель Athena ASEDrive IIIe USB V2, iKey 2032, ruToken S, ruToken RF S);
- блокировка загрузки ОС со съемных носителей на аппаратном уровне для всех пользователей компьютера, кроме администратора после успешной загрузки штатной копии ОС доступ к этим съемным носителям восстанавливается. Администратор имеет возможность задать режим работы ПАК, при котором будет блокирован вход пользователей в систему при нарушении целостности контролируемых файлов (контроль целостности функционирует под управлением операционных систем, использующих файловые системы NTFS5, NTFS, FAT32, FAT16 и FAT12);
- контроль целостности программной среды (позволяет контролировать неизменность файлов и физических секторов жесткого диска до загрузки ОС, для чего вычисляются некоторые контрольные значения проверяемых объектов и сравниваются с ранее рассчитанными для каждого из этих объектов эталонными значениями);
- контроль целостности системного реестра Windows — повышает защищенность рабочих станций от несанкционированных действий внутри операционной системы;

• сторожевой таймер (срабатывает, если после включения компьютера и по истечении заданного интервала времени управление не передано расширению BIOS ПАК);

• регистрация попыток доступа к АС.

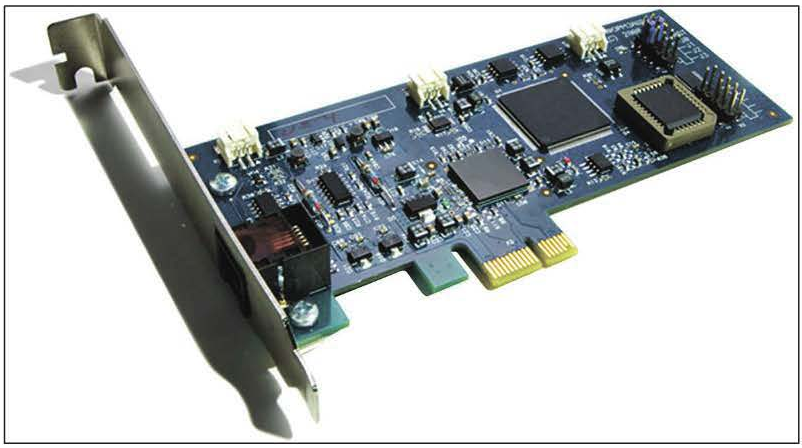

Рис. 13.1. ПАК «Соболь 3.0»

Среди других продуктов с аналогичной функциональностью (их обычно называют аппаратно-программными модулями доверенной загрузки) следует отметить:

• *ПАК семейства «Аккорд»* (разработчик — ЗАО «ОКБ САПР», Москва);

• *ПАК семейства «Dallas Lock»* (разработчик — компания «Конфидент», Санкт-Петербург);

• аппаратно-программные модули доверенной загрузки *«КРИПТОН-ЗАМОК»*[1] (разработчик — ООО Фирма «АНКАД», Зеленоград);

• аппаратно-программные средства криптографической защиты информации *М-502 и «Щит»*[2] (разработчик — ФГУП «Концерн «Системпром»);

• аппаратно-программные комплексы доверенной загрузки *«Лабиринт-ДЗ»*[3] (разработчик ЗАО НИИ «Центрпрограммсистем», Тверь).

13.4. Способы аутентификации

Дальнейшее увеличение вычислительной мощности доступных на рынке компьютеров усугубило проблему, связанную с использованием чисто парольной аутентификации, поскольку пароль можно подобрать, забыть, потерять и т. д.

Для обеспечения должного уровня защиты начали применять схемы с использованием аппаратных идентификаторов и комбинированные схемы многофакторной аутентификации.

[1] http://www.ancud.ru

[2] http://www.fstec.ru/_doc/perech/_perech_cfo.htm)

[3] http://cps.tver.ru

Выделяют несколько основных типов аппаратно-программных средств аутентификации:

- на базе смарт-карт и USB-токенов;
- на базе пассивных контактных и бесконтактных идентификаторов;
- биометрические;
- комбинированные.

Устройства аутентификации на базе смарт-карт и/или USB-токенов. Поддержка такого рода средств встроена штатно в Microsoft Active Directory Windows 2000, Windows Server 2003 и 2008.

Аутентификация на базе смарт-карт и USB-токенов (фактически, USB-токен — это смарт-карта, совмещенная в одном корпусе со считывателем, подключаемым к разъему USB) основана на проверке сертификатов открытого ключа. Ключевая пара генерируется смарт-картой, соответствующий закрытый ключ хранится в смарт-карте, возможны такие настройки, при которых закрытый ключ не может быть экспортирован. Сертификат открытого ключа также хранится в смарт-карте, но наряду с этим возможно централизованное хранение сертификатов в каталоге (это может быть Microsoft Active Directory или другая служба каталога, поддерживающая LDAP). Все сопутствующие криптографические вычисления производятся процессором смарт-карты. ОС через считыватель передает в смарт-карту запрос, который шифруется на секретном ключе и передается ОС, ответ расшифровывается на открытом ключе и сравнивается с исходным запросом.

Данная схема может быть усложнена дополнительными техническими мерами, если необходимо осуществлять аутентификацию по сети (например, протокол аутентификации Kerberos — RFC 1510, EAP TLS — RFC 2716), но в основе всегда лежит проверка того, что проходящий аутентификацию субъект обладает секретным ключом, соответствующим проверяемому сертификату открытого ключа.

Для реализации схем аутентификации с использованием смарт-карт требуются смарт-карты и подходящие считыватели (либо USB-токены), а также сопутствующее ПО (драйверов) на компьютерах, где планируется проводить аутентификацию с использованием смарт-карт. Кроме того, требуется развернуть в АС организации инфраструктуру открытых ключей, в рамках которой будут выпускаться сертификаты для смарт-карт.

В качестве программных средств, реализующих инфраструктуру открытых ключей, можно использовать *Крипто-Про УЦ*[1] (Крипто-Про, Москва), *Notary Pro*[2] (Сигнал-КОМ, Москва) либо другое ПО для удостоверяющего центра, в которое можно встроить сертифицированные ФСБ России криптопровайдеры (например, Crypto-CSP (Крипто-Про), Крипто-Ком (Сигнал-Ком), ViPNet CSP (компании ОАО «ИнфоТеКС»).

Смарт-карты и токены с поддержкой криптографии ГОСТ выпускает компания «Аладдин Р.Д.»[3], токены ruToken ЭЦП — совместная разработка

[1] http://www.cryptopro.ru
[2] http://www.signal-com.ru
[3] http://www.aladdin-rd.ru

Фирмы «АНКАД» и компании «Актив» и изделия ШИПКА от ОКБ САПР (в них совмещена функциональность смарт-карты и съемного диска, содержимое которого зашифровано на аппаратном уровне).

КриптоПро Winlogon предназначен для ОС семейства Windows 2000/XP/2003/Vista/7/2008R2 и реализует первоначальную аутентификацию пользователя протокола Kerberos V5 (RFC 4120) по сертификату и ключевому носителю КриптоПро CSP 3.0 (смарт-карта, USB-токен) или КриптоПро CSP 3.6.

КриптоПро Winlogon построен на основе сертифицированного СКЗИ КриптоПро CSP 3.0 и входит в состав СКЗИ КриптоПро CSP 3.6.

Открытые ключи и ЭП по ГОСТ Р 34.10–2001 используются для аутентификации и авторизации пользователя домена Windows в соответствии с проектом документа IETF (Draft-Ietf-Smime-Gost).

В настоящее время наличие аппаратной поддержки отечественной сертифицированной криптографии стало особо актуально в связи с государственными программами по предоставлению различных услуг гражданам России через Интернет, в частности, решения ведущих российских производителей смарт-карт и токенов компаний «Аладдин Р.Д.» и «Актив» востребованы на портале государственных услуг.

eToken ГОСТ. Это персональное средство формирования электронной подписи с неизвлекаемым закрытым ключом, предназначенное для разработчиков систем дистанционного банковского обслуживания, электронных торгов и других целей, спроектировано в соответствии с требованиями ФСБ России к криптографическим средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, по классу КС1, КС2 и реализует следующие криптографические функции:

- формирование и проверку электронной подписи для блоков данных, передаваемых в электронный ключ согласно ГОСТ Р 34.10–2001;
- вычисление значения хеш-функции блоков данных в соответствии с ГОСТ Р 34.11–94;
- формирование и хранение ключевой пары, сертификатов X.509 по стандарту ISO/IEC 9594–8 и др.

Доступны следующие варианты исполнения eToken ГОСТ:

- USB-ключ eToken ГОСТ;
- смарт-карта eToken ГОСТ;
- комбинированный USB-ключ eToken ГОСТ с генератором одноразовых паролей;
- комбинированный USB-ключ eToken ГОСТ с flash-памятью объемом до 16 Гбайт;
- USB-ключ eToken PRO Anywhere.

Для встраивания eToken ГОСТ в различные приложения могут использоваться следующие программные интерфейсы:

- высокоуровневый интерфейс PKCS#11 версии 2.30, включающий расширения для российских криптографических алгоритмов и позволяющий

Рис. 13.2. Рутокен

работать на любых операционных системах (Windows 32/64-бит, Linux 32/64-бит, Mac OS);

• сертифицированные библиотеки, позволяющие делегировать функции цифровой подписи ключу eToken ГОСТ;

• низкоуровневый интерфейс /система APDU-команд, позволяющий использовать eToken ГОСТ на любых платформах и операционных системах (Windows 32/64-бит, Linux 32/64-бит, Mac OS).

Рутокен[1]. Это российское средство аутентификации и защиты информации (рис. 13.2), предназначенное для безопасного хранения и использования паролей, цифровых сертификатов, ключей шифрования и электронной подписи; имеет сертификаты ФСТЭК России (№ 1461, № 1395) и ФСБ России (№ СФ/124-0999).

Основные функциональные возможности:

• неизвлекаемые ключи шифрования и ЭП;

• поддержка международных стандартов;

• интеграция с решениями, использующими технологии смарт-карт, и инфраструктурой открытых ключей (PKI);

• расширенная поддержка сертифицированных российских средств криптографической защиты информации (СКЗИ).

Программно-аппаратное СКЗИ КриптоПро Рутокен CSP объединяет возможности российского криптопровайдера КриптоПро CSP и идентификатора Рутокен ЭП:

• поддержка всего функционала СКЗИ КриптоПро CSP 3.6;

• интеграция с инфраструктурой PKI, основанной на КриптоПро УЦ;

• генерация ключей и формирование ЭЦП по ГОСТ Р 34.10 — 2001;

• вычисление ключа согласования Диффи — Хеллмана (RFC 4357);

• безопасное хранение и использование закрытых ключей внутри ключевого носителя без возможности извлечения (срок действия закрытого ключа — до трех лет).

Аутентификация с использованием одноразовых паролей. Рассмотрим принцип работы eToken PASS производства компании «Аладдин Р.Д.» (рис. 13.3), где реализован алгоритм генерации одноразовых паролей (One-Time Password — OTP). Этот алгоритм основан на алгоритме HMAC и хеш-функции SHA-1. Для расчета значения OTP принимают два входных параметра — секретный ключ (начальное значение для генератора) и текущее значение счетчика (количество необходимых циклов генерации). Начальное значение хранится как в самом устройстве, так и на сервере в системе eToken TMS. Счетчик в устройстве

Рис. 13.3. eToken PASS

[1] http://www.rutoken.ru, www.aktiv-company.ru

увеличивается при каждой генерации OTP, на сервере — при каждой удачной аутентификации по OTP.

При запросе на аутентификацию проверка OTP осуществляется сервером RADIUS (Microsoft IAS, FreeRadius и др.), который обращается к системе eToken TMS, осуществляющей генерацию OTP на стороне сервера. Если введенное пользователем значение OTP совпадает со значением, полученным на сервере, аутентификация считается успешной, и сервер RADIUS отправляет соответствующий ответ.

Алгоритм аутентификации пользователя с помощью OTP-токена eToken PASS очень прост:

- пользователь активизирует свой OTP-токен, который генерирует OTP, шифруя количество прохождений процедуры аутентификации данным пользователем, с помощью своего секретного ключа и вводит свое имя и OTP на рабочей станции;
- имя пользователя и OTP передаются по сети в открытом виде;
- аутентификационный сервер находит запись пользователя и шифрует количество раз прохождений процедуры аутентификации данным пользователем с помощью хранимого им секретного ключа пользователя, получая в результате OTP;
- сервер сравнивает OTP, представленный пользователем, и OTP, вычисленный им самим.

Партия устройств eToken PASS поставляется с зашифрованным файлом, содержащим начальные значения для всех устройств партии. Этот файл импортируется администратором в систему eToken TMS. После этого для назначения устройства пользователю необходим ввод его серийного номера (печатается на корпусе устройства).

В случае нарушения синхронизации счетчика генерации в устройстве и на сервере, система eToken TMS позволяет легко восстановить синхронизацию. Для этого администратор системы или сам пользователь (при наличии соответствующих разрешений) должен сгенерировать два последовательных значения OTP и отправить их на сервер через веб-интерфейс eToken TMS.

В целях усиления безопасности система eToken TMS позволяет использовать дополнительное значение OTP PIN — в этом случае для аутентификации пользователь помимо имени пользователя и OTP вводит дополнительное секретное значение OTP PIN. Возможна интеграция генератора одноразовых паролей в комбинированные решения, например eToken NG-OTP (Java), или в мобильные телефоны с использованием технологии MobilePASS.

Аутентификация с использованием пассивных идентификаторов. Пассивные идентификаторы, в отличие от смарт-карт, ничего сами внутри себя не вычисляют, а представляют собой только хранилище идентификационной информации, к которому обращается соответствующее ПО. Простейший пассивный идентификатор — это диск, на котором записаны какие-то данные (в частности, это один из возможных вариантов персональных идентификаторов, присваиваемых сотруднику в системе Secret Net; обращение к ней про-

исходит после ввода пароля пользователя). В роли такого идентификатора может выступать флеш-карта (или любое устройство, опознаваемое системой как съемное), изделия iButton, бесконтактные Proximity-карты или RFID-метки.

Наиболее распространены изделия iButton (рис. 13.4) — их используют все разработчики электронных замков. В зависимости от модели iButton и электронного замка, в iButton может быть записана дополнительная вспомогательная информация (например, Secret Net позволяет хранить на iButton пароль пользователя, при этом его не требуется вводить с клавиатуры — решение о целесообразности использования данной возможности следует принимать в зависимости от контингента пользователей). Если компьютер оснащен ПО CryptoPro CSP, в iButton может храниться ключевая информация (реализовано для средств «Соболь», Аккорд, Dallas Lock).

В случае с Proximity-картами (рис. 13.5) и RFID-метками обмен данными между идентификатором и считывателем происходит по радиоканалу: излучение считывателя возбуждает электрический ток в бесконтактном идентификаторе, который питает его микросхему с приемником/передатчиком, передатчик идентификатора по запросу считывателя передает уникальный номер изделия (уникальность гарантируется компанией-производителем), который и является идентификационной информацией. Радиус действия подобных устройств невелик (в случае Proximity-карт — несколько сантиметров, в случае RFID-меток — несколько метров), если только желающий подслушать этот радиообмен не обзавелся направленной антенной (аналогичные направленные антенны позволяют устанавливать, а значит и перехватывать обмен данными по BlueTooth на расстоянии до 1500 км[1] на открытой местности вместо заявленных нескольких десятков метров). Следовательно, при использовании бесконтактных идентификаторов необходимо принять меры по экранированию помещений.

Рис. 13.4. Идентификаторы iButton

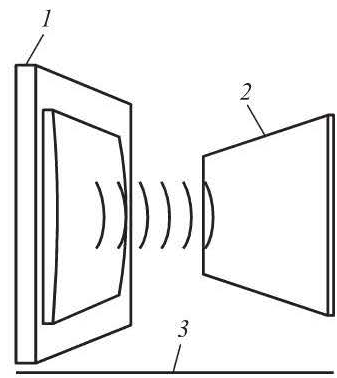

Рис. 13.5. Идентификатор и считыватель Proximity:
1 — считыватель; *2* — карточка Proximity; *3* — идентификатор

[1] http://www.google.ru/

Биометрическая аутентификация. К достоинствам биометрических сканеров обычно относят то, что они никак не зависят от пользователя (например, можно ошибиться при вводе пароля) и никто не может передать свой биологический идентификатор другому человеку, в отличие от пароля. Однако, как показали проведенные в США исследования, биометрические сканеры, основанные на отпечатках пальцев, довольно легко обмануть с помощью муляжа. Или ситуация с отказом в доступе, осуществляемом на основании распознавания голоса, в случае если человек простужен.

Биометрические методы подразделяют на две группы:

• *статические* — основаны на физиологической (статической) характеристике человека, т. е. уникальном свойстве, данном ему от рождения (форма ладони, отпечатки пальцев, радужная оболочка глаз, форма лица, расположение вен на кисти руки и т. д.);

• *динамические* — в их основе лежит поведенческая (динамическая) характеристика человека — подпись, речь, динамика клавиатурного набора.

Идентификация по статическим характеристикам более надежна, так как не зависит от психоэмоционального состояния человека.

Рассмотрим биометрические методы идентификации подробнее. *Распознавание по отпечаткам пальцев* — самый распространенный статический метод биометрической идентификации, в основе которого лежит уникальность для каждого человека рисунка папиллярных узоров на пальцах. Изображение отпечатка пальца, полученное с помощью специального сканера, преобразуется в цифровой код (свертку) и сравнивается с ранее введенным шаблоном (эталоном) или набором шаблонов (в случае аутентификации).

Среди ведущих производителей[1] сканеров отпечатков пальцев можно выделить BioLink, Bioscrypt, DigitalPersona и др.

Ведущие производители сенсоров[2] (считывающих элементов для сканирующих устройств): Atmel, AuthenTec.

Распознавание по форме руки возможно с помощью специального устройства, позволяющего получать трехмерный образ кисти руки с дальнейшим преобразованием в уникальную цифровую свертку. Ведущие производители[3] подобных устройств — фирмы Recognition Systems и BioMet Partners.

Распознавание по радужной оболочке глаз возможно при наличии камеры, позволяющей получить изображение глаза человека с достаточным разрешением, и специализированное ПО для выделения из полученного изображения рисунка радужной оболочки глаза, по которому строится цифровой код для идентификации человека.

Крупнейшим производителем в данной области является компания Iridian[4], а также компании LG, Panasonic, OKI, Saflink и др.

---

[1] http://www.biolink.ru, http://www.biolinkusa.com, http://www.bioscrypt.ru, http://www.digitalpersona.com

[2] http://www.atmel.com, http://www.authentec.com

[3] http://www.recogsys.com, http://www.biomet.ch

[4] http://www.iridiantech.com

Распознавание по клавиатурному почерку предлагает использование кодового слова, а из оборудования требуется только стандартная клавиатура. Основная характеристика, по которой строится свертка для идентификации, — динамика набора кодового слова.

Среди ведущих производителей выделяют компании BioPassword Security Software[1] и Checco[2].

Распознавание по голосу основано на различных сочетаниях частотных и статических характеристик голоса.

Ведущими производителями ПО для этих целей являются компании Nuance[3], Voicevault[4].

Помимо перечисленных производителей на рынке биометрии появилась новая группа компаний, чьи решения называют промежуточными. Как правило, это система «программное обеспечение — посредник между оборудованием и программными средствами, в которые интегрируются процедуры биометрической идентификации». Причем посредник может реализовать как просто регистрацию в системе с использованием измерений биометрического сканера (например, Windows Logon), так и самостоятельные функции (например создание криптографических контейнеров с помощью ключа, получаемого только по определенному отпечатку пальца).

Следует отметить, что в чистом виде биометрические средства аутентификации не позволяют построить 100 %-ную систему защиты — существует определенный процент ложных срабатываний, причем в обе стороны — как принятие своих за чужих, так и принятие чужих за своих, кроме того возможна компрометация таких систем[5]. Появился даже новый термин «Biologger» (биометрический кейлоггер). Британский исследователь М. Льюис (M. Lewis) разработал биометрический кейлоггер[6], который позволяет получать отпечатки пальцев, необходимые для разблокировки дверей зданий, доступа к компьютерным сетям и иным системам с ограничением доступа. Но исследователи, которые работают с управлением ИБ-рисками, предупреждают, что атака биометрических систем может стать обычным явлением с возможностью перехвата передаваемых между устройствами данных с помощью ноутбука, а по полученным данным воспроизвести изображение отпечатков пальцев.

Комбинированные схемы и многофакторная аутентификация. Многофакторная аутентификация — это проверка нескольких секретов для аутентификации субъекта (например, проверка смарт-картой PIN-кода, вводимого пользователем, только после которой смарт-карта открывает доступ к ключевому материалу и возможна проверка сертификата).

Ведутся разработки по совмещению функциональности смарт-карты и SIM-карты мобильного телефона. В Японии компанией NTT DoCoMo пред-

[1] http://www.biopassword.com
[2] http://www.biochec.com
[3] http://www.nuance.com
[4] http://www.voicevault.com
[5] http://www.kinnet.ru/cterra/445/18034.html
[6] http://www.securitylab.ru/news/349668.php

лагается основанная на SIM-картах система безналичных платежей «ID». Существуют планы по внедрению в Москве системы для оплаты проезда в метро через мобильный телефон со специальной SIM-картой. Вероятно появление в ближайшем будущем технических решений и для аутентификации пользователей по мобильному телефону в корпоративных АС, вся необходимая для этого элементная база уже существует.

Рис. 13.6. Карт-ридер ASEDrive IIIe Bio Combo F2

Любое внедрение электронных замков подразумевает использование двухфакторной аутентификации: проверяется наличие индивидуального идентификатора и соответствующего пароля пользователя.

Существуют решения, использующие биометрические факторы в качестве одного из проверяемых секретов в схемах многофакторной аутентификации. Например, подразделение EMC по обеспечению безопасности (Компания RSA) предлагает USB-токены, оснащенные считывателем отпечатка пальца: отпечаток пальца используется вместо PIN-кода для доступа к содержащимся в токене ключам, аналогичное решение имеется у компании Athena Smartcard Solutions (рис. 13.6).

* * *

При выборе системы защиты следует оценить ее функциональность, соответствие возможностей требованиям к защите ресурсов АС конкретной организации и стоимость. Для повышения обоснованности выбора целесообразно учесть состояние и перспективы развития парка компьютеров, подлежащих защите, применяемых операционных систем и другого программного обеспечения, задачи, решаемые персоналом с применением АС в различных сферах деятельности организации.

Следует иметь в виду, что аппаратные средства аутентификации предоставляют инструмент, позволяющий решить главным образом первую из задач, возлагаемых на СЗИ НСД, — задачу защиты от вмешательства посторонних лиц в процесс нормального функционирования АС. При этом аутентификация осуществляется применительно к трем моментам работы: загрузке компьютера (при наличии на компьютере электронного замка загрузить компьютер может только зарегистрированный пользователь), регистрации в системе (начать сеанс работы может только зарегистрированный пользователь, для которого в системе имеется учетная запись) и разблокировке консоли (если в ходе сеанса работы пользователь заблокировал консоль, разблокировать консоль может только этот пользователь либо пользователь, обладающий на данном компьютере административными полномочиями; в последнем случае сеанс работы пользователя, заблокировавшего консоль, прерывается с принудительным закрытием всех запущенных пользователем программ, и если какие-либо файлы не были сохранены, вся введенная в них после последнего сохранения информация теряется).

Эффективное использование данного инструмента возможно в том случае, если соблюдаются еще, по крайней мере, два условия, требующие организационных мер. Для пользователей внутренними нормативными документами организации установлен запрет на передачу своих реквизитов входа другому лицу либо их запись в доступном для других лиц месте (классический пример — стикер с паролем, наклеенный на монитор). Другой возможный вариант — разработка некоторой бюрократической процедуры передачи реквизитов входа, с тем чтобы по соответствующим данным бумажного учета можно было однозначно установить, какой сотрудник воспользовался указанной учетной записью в данный момент.

Контрольные вопросы

1. Какие факторы влияют на выбор конкретных средств защиты информации?
2. Что определяет класс защищенности АС или СВТ?
3. Сколько и какие подсистемы образуют систему защищенности АС?
4. Охарактеризуйте классы защищенности СВТ.
5. Каковы критерии выбора СЗИ от НСД?
6. Какие СЗИ от НСД вам известны?
7. Перечислите задачи, решаемые средствами аппаратной поддержки систем защиты информации от НСД.
8. Охарактеризуйте существующие средства аппаратной поддержки.
9. Какие устройства аутентификации на базе смарт-карт и/или USB-токенов вам известны?
10. Каков алгоритм аутентификации пользователя с использованием OTP-токена?
11. Что понимается под биометрической аутентификацией пользователя? Приведите примеры биометрических характеристик.
12. Назовите основные отличия методов биометрической аутентификации пользователя от других (например, парольных).

Глава 14. ПРИМЕНЕНИЕ ШТАТНЫХ И ДОПОЛНИТЕЛЬНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Рассмотренные в гл. 13 средства идентификации и аутентификации позволяют решить только одну из задач, возлагаемых на СЗИ НСД, — задачу защиты от вмешательства посторонних лиц в процессы нормального функционирования АС. После того, как сеанс работы пользователя начат либо разблокирован, вступают в действие другие защитные механизмы, реализованные в составе штатных средств ОС и дополнительных средствах защиты от НСД, позволяющие, при соблюдении определенных условий (при внедрении необходимых организационных мер), решить остальные задачи по защите АС.

14.1. Стратегия безопасности Microsoft

Компания Microsoft уделяет обеспечению безопасности своих пользователей пристальное внимание. Общая концепция продуктов и технологий компании Microsoft представляет собой решение вопросов защиты информации от несанкционированного доступа, вредоносного воздействия, искажения и т. д. В частности, для обеспечения защиты от вирусов и нежелательной почты и спама серверов и приложений, а также клиентских и серверных ОС предлагается целая линейка решений марки Forefront. Для защиты периметра сети используется межсетевой экран Forefront Threat Management Gateway 2010 (наследник ISA Server), а также шлюз аутентификации и обеспечения сервиса единой точки доступа. Также в платформу Microsoft Windows встроены технологии, которые обеспечивают соблюдение политик безопасности при работе с документами и важными данными с помощью шифрования — Encrypted file system, BitLocker, ADRMS. Решения, базирующиеся на Windows Server AD services, позволяют управлять учетными записями пользователей.

Семейство решений System Center дает возможность управлять как аппаратными, так и программными конфигурациями в рамках корпоративной сети.

Все перечисленные продукты совместимы между собой, дополняют друг друга и могут обеспечить защиту информации, обрабатываемой и хранящейся в корпоративной сети.

Компания Microsoft сертифицирует свои продукты на соответствие требованиям информационной безопасности: в области сертификации криптографических алгоритмов — ФСБ России, в области сертификации, не связанной с криптографией, — ФСТЭК России с учетом мнения Министерства обороны России.

В настоящее время компании Microsoft выдано множество сертификатов соответствия, среди последних: Microsoft Windows Server 2012 Standart — сертификат № 2949; Microsoft Office 2013 Professional Plus — сертификат № 3161; Microsoft Windows 8 Professional — сертификат № 2960).

Актуальную информацию по сертифицированным продуктам можно найти на сайтах: http://www.microsoft.com/Rus/Security/Certificate/results.aspx, http://www.microsoft.com/rus/government/certificate/.

14.2. Защита от вмешательства в процесс нормального функционирования автоматизированной системы

Для того чтобы отличать своих от чужих, необходимо провести аутентификацию. В Microsoft Windows встроена штатная проверка по паролю, которая используется по умолчанию. В Windows 2000/2003 на базе Active Directory (AD) была лишь одна политика для пароля и блокировки учетной записи (account lockout policy) для всего домена. Поэтому у некоторых компаний возникала необходимость в использовании нескольких доменов, чтобы

иметь возможность применять разные политики пароля (password policy) для различных пользователей либо необходимо было разрабатывать собственные фильтры для паролей или приобретать решения сторонних производителей. В операционной системе Windows Server 2008 имеется возможность указать разные политики паролей для различных пользователей и групп. Данная технология, называемая «Подробные политики паролей» (Fine-Grained Password Policies), позволяет создавать следующие настройки для разных групп пользователей в рамках одного домена Active Directory:

- вести журнал паролей;
- определять максимальный и минимальный сроки действия пароля;
- ограничивать минимальную длину пароля;
- соблюдать определенную сложность пароля;
- хранить пароли, используя обратимое шифрование.

Однако во многих организациях существуют инструкции по парольной защите, в которых сформулированы правила формирования паролей. Например, персональные пароли должны генерироваться специальными программными средствами административной службы либо выбираться пользователями информационной системы организации самостоятельно с учетом определенных требований (см. гл. 9).

Встроенными средствами Windows Server 2008 эта задача не решается, но может быть решена с помощью дополнительного ПО сторонних разработчиков. Например, Specops Password Policy[1] имеет следующий функционал:

- возможность любых комбинаций ограничений пароля: нижний регистр, верхний регистр, числовые и специальные символы;
- различные правила срока годности пароля для каждой политики;
- запрет последовательных символов в пароле;
- автоматическая отправка даты окончания срока действия пароля на адрес электронной почты и др.

Но практика показывает, что парольная защита не очень надежна, поэтому возникает необходимость в применении двухфакторных вариантов аутентификации. В Windows 7/2008R2 вход по смарт-картам с применением сертификатов существенно упростился благодаря поддержке многими поставщиками ПО спецификации Microsoft CCID Smart Card Minidriver, которая не требует установки отдельного драйвера с сайта производителя, а позволяет использовать встроенные в Windows драйверы или те, которые загружаются автоматически через службу Windows Update.

Компания Microsoft продолжает работу по усовершенствованию биометрической идентификации. В Windows 10 (по сравнению с Windows 8) добавлено сканирование радужной оболочки глаза (помимо отпечатка пальца).

Датчики компании Fingerprint Cards, с которой сотрудничает компания Microsoft, предполагалось встроить в клавиатуру ПК, ноутбуков, планшетов новых версий ОС семейства Windows (последняя версия — Windows 10), но до настоящего времени биометрические методы не получили широкого распространения.

[1] http://www.specopssoft.com

14.3. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы

Как было упомянуто ранее, существует три подхода к разграничению доступа: избирательное, полномочное (мандатное) и разграничение доступа к ПО путем создания замкнутой программной среды. В современных многопользовательских ОС избирательное разграничение доступа реализовано штатными средствами. Кроме того, во всех сертифицированных дополнительных СЗИ НСД, согласно требованиям руководящих документов ФСТЭК России, существует реализация всех трех подходов к разграничению доступа.

Избирательное разграничение доступа. Поскольку избирательное разграничение доступа реализовано штатно в многопользовательских ОС (в частности, в Windows NT/2000/XP/2003/Vista/7/2008 предусмотрено разграничение доступа путем контроля списков управления доступом, связанных с защищаемыми объектами), данный подход порождает меньше всего проблем с функционированием ПО, поскольку практически во все современное ПО заложена возможность корректного функционирования в условиях, когда среда работы ОС может блокировать попытки модификации каких-то данных. Поэтому проблема использования избирательного разграничения доступа сводится к тому, чтобы реализовать его средствами корректного ограничения доступа к ресурсам АС для соблюдения принципа минимально необходимых полномочий.

Полномочное (мандатное) разграничение доступа. Принцип полномочного разграничения доступа состоит в том, что сотрудникам присваивается уровень допуска к конфиденциальной информации, ресурсам АС — уровень конфиденциальности. После этого система препятствует попыткам доступа к ресурсам, уровень конфиденциальности которых превышает уровень допуска сотрудника, а при открытии конфиденциальных ресурсов — попыткам переноса данных в ресурс с более низким уровнем конфиденциальности (контроль потоков данных).

Компания Microsoft в операционных системах Windows Server 2008 и Windows Vista предложила модель безопасности (так называемый «механизм целостности»), которая обеспечивает защитный барьер вокруг процессов с повышенными привилегиями и состоит из обязательного контроля целостности (Mandatory Integrity Control — MIC) и изоляции привилегий пользовательского интерфейса (UIPI). Наиболее существенный эффект MIC — отображение сообщения контроля учетных записей, когда текущих привилегий недостаточно для выполнения операций. Фактически учетные записи и группы имеют предустановленный уровень доверия, и, таким образом, когда программа запускается в определенной учетной записи, она автоматически получает ее уровень доверия.

Механизм целостности использует шесть уровней доверия, которые он назначает объектам (в данном случае под объектами подразумевается все — от файлов и папок до процессов и пользователей):

• *доверенный инсталлятор* — объекты со статусом доверенного инсталлятора имеют наивысший уровень доверия из возможных и могут вносить изменения в ОС;

• *системный* — объекты с данным статусом являются общими службами или объектами, составляющими часть ОС (данный приоритет характерен для учетных записей локальных или сетевых служб);

• *высокий* — учетные записи администратора, продвинутых пользователей — оператора архива или оператора шифрования запускаются с высоким уровнем доверия, позволяющим вносить изменения в ОС;

• *средний* — обычный уровень для стандартных учетных записей и связанных с ними данных;

• *низкий* —для учетных записей Everyone и временных файлов;

• *недоверенный* — такой статус присваивается анонимным и гостевым учетным записям.

Политика доверия NO_WRITE_UP предусматривает основное ограничение между уровнями доверия — по умолчанию ни один объект одного уровня не может редактировать объект более высокого уровня.

Политика доверия NEW_PROCESS_MIN предотвращает запуск приложения более низкого уровня доверия с более высоким уровнем (в предыдущих версиях Windows запускаемый процесс получал уровень того, кто его запустил, несмотря на уровень самого приложения).

Политика доверия NO_READ_UP предотвращает чтение объектами с низким уровнем участков памяти объектов с более высоким уровнем доверия (который по умолчанию не активирован), а политика NO_EXECUTE_UP позволяет выбранной программе быть вызванной только объектом того же или более высокого уровня.

Необходимо отметить, что объекты с одинаковым уровнем доверия не имеют никаких ограничений по взаимодействию, по крайней мере, с точки зрения механизма целостности.

Дополнением к механизму управления доступом защиты служит механизм, который оценивает доступ с помощью уровней целостности перед проверками прав доступа и выполняет список управления доступом на уровне пользователей (DACL). Субъектам безопасности и объектам, подлежащим защите, назначаются уровни целостности, определяющие их уровень защиты или доступа (например, Internet Explorer® 7, работающий в защищенном режиме Internet Explorer).

Механизм изоляции процессов UIPI, который обозначается в окнах сообщений в виде щита Windows, предотвращает использование повышения привилегий путем внедрения кода в различные процессы одного и того же сеанса.

Применяемая по умолчанию политика целостности позволяет процессам открыть любой объект для чтения, за исключением объектов-процессов и объектов-потоков. Это означает, что процесс, работающий с низким уровнем целостности Integrity Level (IL), может открыть любые файлы, доступные для учетной записи пользователя, под которой он работает. С помощью IL-уровней обозреватель Internet Explorer защищенного режима предотвра-

щает блокировку изменения параметров учетной записи пользователя вредоносной программой, но не может помешать ей читать документы пользователя.

Объекты-процессы и объекты-потоки — исключения, поскольку их политика целостности содержит также компонент «Нет чтения». Это означает, что IL-уровень процесса должен быть выше уровня целостности открываемого процесса или потока (или равен ему), а DACL объекта представляет возможность такого доступа. На рис. 14.1 показаны варианты доступа процессов, работающих со средним и низким IL, к другим процессам и объектам.

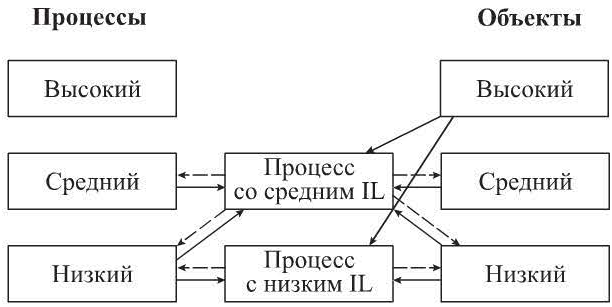

Рис. 14.1. Доступ к объектам и процессам:
⟶ — чтение; ⇢ — запись

Подсистема сообщений Windows также использует уровни целостности для реализации UIPI, препятствуя отправлению процессом всех сообщений, кроме нескольких информационных сообщений, в окна, принадлежащие процессу с более высоким IL. Это позволяет предотвратить разрушение процесса с повышенными правами отправкой ему неправильно сформированных сообщений, вызывающих переполнение внутреннего буфера.

Требования руководящих документов ФСТЭК России (выпущенных в начале 1990-х годов) предусматривают контроль потоков данных на уровне ОС применительно к запуску любого ПО и только в отношении файловых операций. Соблюдение этих требований в современных условиях порождает ряд п р о б л е м:

1) современные приложения открывают, как правило, не один файл, а несколько и могут быть построены таким образом, что для их корректной работы эти вспомогательные файлы должны быть доступны для записи. В условиях функционирования полномочного доступа в режиме контроля потоков система блокирует запись данных в такого рода файлы. Данный факт модулем самодиагностики приложения может быть расценен как аварийная ситуация, и, как минимум, потребуется дополнительная нетривиальная настройка приложений;

2) в настоящее время минимальной логической единицей хранения информации не обязательно является файл, это может быть запись в базе данных, письмо в почтовом ящике корпоративной почтовой системы и т. п. В данном случае разграничение доступа реализуется уже не ОС, а соответ-

ствующим серверным приложением, в которое не всегда технически возможно встроить дополнительные модули разграничения доступа (во всяком случае, подобные модули отсутствуют среди сертифицированных СЗИ НСД);

3) контроль потоков на уровне файловых операций позволяет блокировать запись данных в неконфиденциальные файлы и не в состоянии блокировать несанкционированный перенос данных другими способами, например с использованием прикладных интернет-протоколов, таких как FTP или HTTP.

Для решения перечисленных проблем целесообразно использовать систему электронного документооборота организации, заложив в реализуемые бизнес-процессы контроль потоков уже на этапе проектирования системы, а также систему управления правами, поддержка которой должна быть встроена в прикладное ПО. В этой системе служебный заголовок файла содержит информацию о том, каким субъектам какие действия разрешены в отношении содержащихся в файле данных. Эта информация, а также защищаемое содержимое, зашифрована, и для получения доступа к ключам необходимо обратиться на сервер управления правами, функционирующий в составе АС.

Подобное решение предлагает компания Microsoft: сервер Microsoft Windows Rights Management Services (RMS) функционирует на платформе Windows Server 2008 (в последнем случае он включен в состав дистрибутива для лицензии Enterprise и называется Active Directory Rights Management Services (AD RMS)), клиентская часть устанавливается на Windows 2000 (все версии), Windows XP Professional и Windows Server 2003 (все версии), или входит в состав Windows Vista (Business или Ultimate), Windows 7 и Windows Server 2008 (все версии, кроме Core Edition), в качестве прикладного ПО выступает Office 2013.

Служба управления правами Active Directory (AD RMS) предназначена для защиты доступа к цифровым файлам организации, работает с различными приложениями и позволяет создавать решения для защиты веб-данных, документов и почтовых сообщений. AD RMS работает со всеми поддерживающими данную технологию приложениями для обеспечения политик постоянного использования секретных данных. Служба AD RMS может использоваться для защиты веб-узлов интрасети (Интранета), почтовых сообщений и документов от несанкционированного использования.

Владельцы содержимого могут точно определить, как получателю разрешается использовать информацию (например, указать, кто может ее открывать, вносить изменения, печатать, выполнять другие действия). Организации могут создавать собственные шаблоны прав использования (например, «Конфиденциально — только для чтения»), применимые непосредственно к информации (например, к финансовым отчетам, техническим характеристикам продуктов, данным о заказчиках и почтовым сообщениям). Алгоритм схемы работы AD RMS представлен на рис. 14.2.

Разграничение доступа к программному обеспечению в режиме замкнутой программной среды. Замкнутая программная среда (ЗПС) — это «бе-

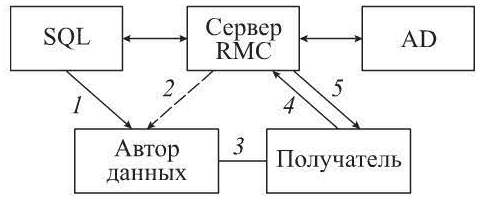

Рис. 14.2. Схема работы Active Directory Rights Management Services:
1 — автор получает сертификат; *2* — автор шифрует файл; *3* — автор распространяет файл; *4* — при открытии файла получателем приложение соединяется с сервером RMS, который проверяет права доступа пользователя; *5* — приложение при работе с файлом обеспечивает исполнение правил

лый» список приложений, которые пользователю разрешается запускать на компьютере. В этот список включаются все компоненты ПО: исполняемые файлы, программные библиотеки, драйверы, оверлейные модули, исполняемые сценарии, экранные заставки и т. п. Система должна обеспечивать блокирование возможности использования программных модулей, не входящих в «белый» список, а также исключать возможность внесения изменений в сами программные модули, включенные в список.

Штатные средства Windows, позволяющие организовать работу в режиме замкнутой программной среды, появились начиная с Windows XP, где они фигурируют под названием «политики ограниченного использования программ» (Software Restriction Policies). Эти политики настраиваются среди прочих параметров безопасности в групповых политиках Active Directory, что позволяет легко тиражировать указанные настройки на большое количество компьютеров. Следует отметить, что эту функцию, во-первых, не поддерживает Windows 2000, поэтому для ее реализации приходится искать альтернативные решения, а во-вторых, процесс настройки ограничений ПО в групповых политиках чрезвычайно трудоемок: каждый модуль, включаемый в список, приходится вносить вручную (с помощью стандартного системного диалога выбора файла, при этом отсутствует возможность выделить и выбрать несколько файлов одновременно).

Механизм Software Restriction Policies, встроенный в Windows начиная с XP, может быть задействован для контроля целостности содержимого любых файлов путем вычисления хеш-функции от этих файлов (используется алгоритм MD5 или SHA1) либо проверкой ЭП для программных файлов (технология Authenticode; администратор может подписывать любые файлы, воспользовавшись утилитой командной строки Signcode, бесплатно загружаемой с сайта Microsoft). Контроль происходит в момент обращения к файлам, при выявлении расхождений доступ блокируется.

В составе Windows 7 и Windows Server 2008 R2 появилось новое приложение AppLocker (табл. 14.1), которое предназначено для замены Software Restriction Policies (политики ограниченного использования программ) и позволяет:

- контролировать, как пользователи применяют исполнимые файлы, скрипты, файлы msi (файлы Windows Installer) и DLL;
- определять правила, основанные на атрибутах файлов, таких как ЭП, наименование производителя данного ПО, имя файла, версия ПО;

• определять правила для группы пользователей или индивидуального пользователя;

• создавать исключения из правил;

• использовать правила в режиме «только аудит», для понимания сути заданных изменений до их непосредственного применения;

• импортировать и экспортировать правила.

Таблица 14.1

Различия между AppLocker и Software Restriction Policies

Особенность	Software Restriction Policies	AppLocker
Состав участников	Все пользователи	Определенные пользователи или группы
Применение правил	Файл-hash, путь, сертификат, раздел реестра, правила зоны Интернет	Файл-hash, путь, издатель
Типы правил	Разрешить/Запретить	Разрешить/Запретить
Правило по умолчанию	Разрешить/Запретить	Разрешить
Режим аудита	Нет	Да
Группировка правил	Нет	Да
Мастер для создания правил	Нет	Да
Импорт/Экспорт политик	Нет	Да
Поддержка PowerShell	Нет	Да
Сообщения об ошибках	Нет	Да

Следует иметь в виду, что наряду с настройкой ЗПС среды нужно внести и другие дополнения в рабочую среду пользователя, например, убрать из интерфейса все элементы, провоцирующие пользователя на попытку запуска программ, не включенных в ЗПС. В состав необходимых настроек входит запрет объектов на рабочем столе, исключая кнопки «Пуск», команды «Поиск» и «Выполнить», запрет отображения общих групп программ. Это осуществляется изменением стандартных настроек Windows через групповые политики либо с помощью технологии Group Policy Preferences, которые дают возможность управлять средой, в которой работает пользователь.

Кроме Software Restriction Policies и AppLocker, реализация замкнутой программной среды включается в состав программной части всех сертифицированных ФСТЭК России СЗИ НСД. Во времена однозадачных ОС это было реализовано через формирование меню, с помощью которого пользователи могли запустить только ограниченный перечень программ, при этом инструкции запрещали включать в число пунктов меню программы типа Norton Commander, позволявшие в свою очередь запустить любую программу. В современных многозадачных ОС в состав СЗИ НСД входит специальный системный драйвер, фильтрующий обращения к программным компо-

нентам, не включенным в список, ассоциированный на данном компьютере с данным пользователем.

Дополнительная защита доверенной программной среды осуществляется либо встроенными в СЗИ НСД средствами контроля целостности, на которые ставятся модули, включенные в список замкнутой программной среды для пользователя, либо контролем атрибутов доступа, т. е. включенные в список файлы не должны быть доступны для записи.

14.4. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа

Встроенные средства регистрации событий, связанных с безопасностью, в соответствии с требованиями руководящих документов ФСТЭК России, имеются в составе ОС Windows NT/2000/XP/2003 Server/Vista/7/2008 Server. Отметим, что если в прежних версиях для реализации защитного механизма необходимо применять *дополнительные* СЗИ НСД, то в Windows NT/2000/XP/2003 Server/Vista/7/2008 Server защитные механизмы встроены в саму ОС. Программы просмотра встроенных в СЗИ НСД журналов регистрации позволяют просматривать и журналы Windows, а имеющаяся в Windows (начиная с Windows 2000) возможность добавлять к приложениям свои журналы формата EVT, дает возможность встроить дополнительную регистрацию событий в СЗИ НСД более естественным образом.

Общая проблема применительно к любым журналам регистрации (как штатным, так и дополнительным) заключается в том, что данные этих журналов по умолчанию сохраняются на том компьютере, где регистрируются события. Это дает возможность злоумышленнику скрыть следы своих действий, если он, имея физический доступ к компьютеру, загрузит ОС со сменного носителя и подменит файлы журналов. К тому же анализ журналов всегда происходит уже после инцидента, т. е. после того, как события зарегистрированы.

Решение этих двух проблем состоит во внедрении системы сбора журналов регистрации в некоторое централизованное хранилище.

Компания Microsoft использует новый формат событий начиная с Windows Vista — изменен как физический формат файла журналов событий Windows с EVT на XML, так и логические поля, которые составляют каждое событие, пересылаемое в журнал.

Появилась также функция перенаправления событий на другие серверы для централизованного управления событиями. Сбор журналов из многих компьютеров — сложная задача, и метод на основе HTTP, применяемый в Windows 2008 для перенаправления событий, пригоден только для малых массивов событий, определенных узкими критериями, поэтому для крупных организаций пользуются дополнительными специализированными продуктами — далее представлены некоторые из них.

Службы ACS (Audit Collection Services). Учитывая новые возможности Windows Server 2008, решение долгосрочного управления информацией жур-

нала событий безопасности и ее архивации заключается в создании централизованной базы данных информации аудита — службы ACS, предоставляющей механизм для пересылки, сбора, хранения и анализа данных событий безопасности (рис. 14.3).

Служба ACS состоит из трех основных компонентов:

1) служба пересылки, являющаяся частью агента диспетчера операций (SCOM agent), передающей данные журнала событий от клиента инфраструктуре служб ACS;

2) служба сбора данных (ACS Collector), которая служит прослушивателем на стороне сервера. Службы пересылки ACS подключаются через порт 51909 TCP для безопасного сообщения с назначенной им службой сбора. Перед пересылкой данные журнала событий нормализуются в XML, т. е. происходит избавление от лишней информации и сведение информации о событии в размеченные поля;

3) база данных служб ACS (ACS Database), которая предназначена для долговременного хранения информации о событиях безопасности. Информацию можно извлекать напрямую через запросы SQL или визуализировать с помощью отчетов HTML, использующих службы отчетов SQL Server®.

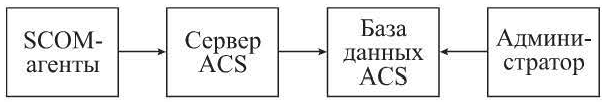

Рис. 14.3. Схема работы ACS

Максимальная производительность службы сбора ACS равна 100 тыс. событий/с (обычная — 2,5 тыс. событий/с). При планировании учитывают, что одна служба сбора ACS способна поддерживать до 150 контроллеров домена, 3 тыс. серверов или 20 тыс. рабочих станций.

Система защиты информации от несанкционированного доступа Secret Net 6. Имеющийся в составе системы сервер безопасности исполняет три основные функции: централизованного хранения и распространения настроек, сетевой аутентификации, дополняющей штатную аутентификацию в домене Windows, и сбора журналов регистрации. В состав СЗИ, в рамках пакета программ для централизованного администрирования, включены:

- программа мониторинга, на которой отображаются оповещения о событиях НСД, зарегистрированных на клиентских компьютерах, с указанием их местоположения;
- возможность просмотра журнала регистрации событий на компьютере (эта информация должна быть предварительно внесена в систему);
- возможность дистанционного выключения компьютера, перезагрузки или завершения сеанса работы пользователя.

Подсистема «Аккорд РАУ». Подсистема «Аккорд-РАУ»[1] совмещена с другими продуктами ЗАО «ОКБ САПР» и объединяет автоматизированное

[1] http://www.accord.ru

рабочее место администратора безопасности информации (АРМ АБИ) и пользовательские терминалы, оснащенные СЗИ семейства «Аккорд».

Администратор безопасности информации наблюдает за работой пользователей, изучает список задач, которые выполняются на данной станции в текущий момент времени, просматривает диски рабочих станций (до уровня файлов и др.) и управляет работой пользователей (посылает пользователю сообщения, обменивается с ним файлами, редактирует базы данных и т. д.).

14.5. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования

Защита от несанкционированной модификации (контроль целостности) программ и данных встроена во все сертифицированные ФСТЭК России СЗИ НСД — наличие реализации данного защитного механизма входит в требования РД Гостехкомиссии России.

Встроенные в Windows штатные средства шифрования, основанные на технологии Encrypting File System (шифрующая файловая система), позволяют передавать файлы в зашифрованном виде с использованием протокола SMB v2.

Сотрудничество компаний «КриптоПро» и «Microsoft» привело к появлению новых интересных продуктов — «КриптоПро EFS» и «КриптоПро IPsec».

«КриптоПро EFS» (при использовании совместно с «КриптоПро CSP») обеспечивает:

- конфиденциальность информации, хранящейся на компьютере, шифрованием файлов системы NTFS по алгоритму ГОСТ 28147–89;
- контроль целостности информации вычислением имитовставки в соответствии с ГОСТ 28147-89;
- организацию совместного доступа к данным зашифрованного файла ограниченной группе пользователей;
- организацию удаленной работы с защищенными файлами;
- восстановление данных в случае удаления пользователей из системы, компрометации или утраты закрытого ключа пользователя.

В отличие от встроенного в ОС Windows EFS ПО «КриптоПро EFS»:

- использует российские стандарты криптографической защиты данных (КриптоПро CSP 3.0 или 3.6);
- обеспечивает контроль целостности файлов;
- предоставляет пользователю интерфейс для выбора текущего ключа шифрования, ключа, по умолчанию используемого для шифрования файлов;
- позволяет одновременно администрировать произвольное число защищенных файлов. Проверять целостность множества файлов, производить одновременное перешифрование многих файлов.

«КриптоПро IPsec» решает з а д а ч и защиты соединения узлов корпоративной вычислительной сети (Site-to-Site VPN):

• подключения удаленных пользователей или малых офисов;

• передачи конфиденциальной информации в ЛВС от нарушителей, не являющихся пользователями автоматизированных систем, но имеющих доступ к ЛВС и/или нарушителей-пользователей, не имеющих необходимых полномочий.

* * *

Сервер безопасности, кроме работы с клиентами (агентами), должен обеспечивать взаимодействие со средствами централизованного управления и оперативного контроля, размещаемыми на компьютерах администраторов безопасности.

Изменение различных составляющих управляющей информации производится по-разному: одна часть информации корректируется централизованно (в групповых политиках) с рабочего места администратора, другая — децентрализованно (в локальной политике безопасности) с соответствующих рабочих станций. В локальной политике безопасности для корректировки доступны только те параметры, которые не заданы через групповые политики. Для параметров СЗИ действуют те же правила наследования, что и для стандартных настроек, назначаемых через групповые политики.

Контрольные вопросы

1. Охарактеризуйте стратегию безопасности Microsoft.
2. Какие сертифицированные ФСТЭК России решения Microsoft в области безопасности вам известны? Охарактеризуйте их.
3. Каковы направления работы компании Microsoft в области биометрии?
4. Какие подходы к разграничению доступа пользователей вам известны? Кратко опишите их.
5. Опишите алгоритм работы AD RMS.
6. Какова схема работы ACS?
7. Какие средства шифрования позволяют обеспечить защиту данных от копирования и перехвата?

РАЗДЕЛ IV

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Глава 15. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

В настоящее время корпоративные компьютерные сети играют важную роль в деятельности большинства организаций. Многие из них подключены к глобальной сети — Интернет. Если раньше сеть Интернет объединяла небольшое число людей, доверявших друг другу, то в настоящее время количество ее пользователей составляет уже сотни миллионов. В связи с этим все серьезнее становится угроза внешнего вмешательства в процессы нормального функционирования корпоративных сетей и несанкционированного доступа к их ресурсам со стороны злоумышленников — так называемых хакеров.

15.1. Типовая корпоративная сеть

Сеть организации может быть как изолированной от внешнего мира (что весьма условно), так и иметь соединение с другими сетями, например с Интернетом.

Подключение к сетям общего пользования осуществляется организациями для решения следующих задач:

- обеспечить внутренним пользователям доступ к внешним ресурсам www-ресурсам, FTP-архивам и т. п.;
- предоставить доступ пользователям из внешней сети к некоторым внутренним ресурсам (корпоративному веб-серверу, FTP-серверу и т. д.);
- обеспечить взаимодействие с удаленными филиалами и отделениями;
- организовать доступ к ресурсам внутренней сети мобильных пользователей.

При решении перечисленных задач у руководства организации возникают проблемы, связанные с безопасностью (например, проблема разграничения доступа пользователей к ресурсам). Предоставление всеобщего доступа

к внутренним ресурсам порождает угрозу внешних вторжений, имеющих целью получения конфиденциальной информации или выведения из строя узлов внутренней сети. При взаимодействии с удаленными филиалами и мобильными пользователями по открытым каналам возможна угроза перехвата передаваемой информации. Дополнительные сложности при обеспечении безопасности вносит интеграция с сетевой инфраструктурой мобильных технологий. Появление беспроводных сетей делает периметр сети все более «размытым».

15.2. Уровни информационной инфраструктуры корпоративной сети

Корпоративная сеть — сложная система, состоящая из нескольких взаимодействующих у р о в н е й, или «слоев»:

• *персонал* — пользователи и обслуживающий персонал;

• *приложения* — программное обеспечение веб-серверов, различные офисные приложения, браузеры и т. п.;

• *система управления базами данных* (СУБД) — предназначена для хранения в упорядоченном виде основной корпоративной информации;

• *операционная система* — установленные на узлах корпоративной сети операционные системы (Windows, UNIX, мобильные платформы и т. д.) — это основа для функционирования различных приложений;

• *сеть* — сетевые протоколы и технологии (TCP/IP и т. п.).

Такой подход очень удобен для рассмотрения вопросов безопасности, поскольку позволяет учесть не только сетевое взаимодействие, но и другие составляющие (приложения, операционные системы и т. д.).

В некоторых случаях уровни приложений, СУБД и ОС объединяют и называют уровнем узла. Отсюда возникает распространенное деление средств защиты на два типа — «network-based» и «host-based».

15.3. Уязвимости и их классификация

Наряду с рассмотренным ранее понятием угрозы, нередко, когда речь идет о сетевой безопасности, используются понятия «уязвимость» и «атака».

Как отмечалось ранее, при создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей.

Далее будут рассмотрены уязвимости и атаки применительно к компьютерным системам и сетям.

Уязвимость — это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

Атака — действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей информационной системы.

Взаимосвязь этих определений с рассмотренным ранее понятием угрозы (см. гл. 3) иллюстрирует рис. 15.1.

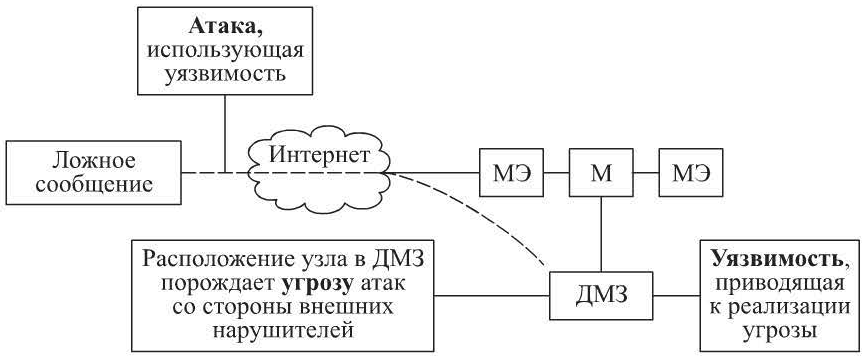

Рис. 15.1. Взаимосвязь определений «атака», «уязвимость», «угроза» (М — маршрутизатор; ДМЗ — демилитаризованная зона)

Предположим, что к узлу, расположенному в демилитаризованной зоне, осуществляется доступ по протоколу RDP. Уязвимость, приводящая к реализации угрозы, — ошибка реализации сервиса удаленного доступа Remote Desktop Protocol, делающая возможным выведение этого сервиса из строя (номер этой уязвимости в каталоге — CVE-2012-0002). Атака, использующая данную уязвимость, — запуск специальной программы-эксплойта и выведение сервиса RDP из строя. В качестве способа нейтрализации уязвимости можно рекомендовать установку соответствующего обновления.

Источники возникновения уязвимостей. В настоящее время существует несколько оснований классификации уязвимостей компьютерных систем и сетей, один из наиболее распространенных — разделение на классы по источнику возникновения («по этапам жизненного цикла системы»: уязвимости проектирования, реализации и эксплуатации).

Уязвимости проектирования возникают на этапе проектирования. Например, значительная часть прикладных сервисов стека TCP/IP (TELNET, FTP, электронная почта и др.) не предусматривает шифрования данных при передаче по сети. В результате критичная информация (имя пользователя и пароль) передается по сети в открытом виде.

Как правило, уязвимости, возникшие на этапе проектирования, с трудом поддаются устранению. Так, для сервисов прикладного уровня для устранения уязвимостей можно либо отказаться от использования соответствующего протокола в пользу другого, более защищенного, либо применять криптографические защитные механизмы.

Уязвимости реализации возникают на этапе реализации (программирования). Например, уязвимость в реализации протокола Remote Desktop Protocol (RDP) более известна как MS12-020.

Уязвимость делает возможным удаленное внедрение произвольного кода, что, в свою очередь, как минимум, приводит к созданию ситуации отказа в обслуживании или, как максимум, к получению полного контроля над объектом атаки.

Атака осуществляется путем отправки уязвимому сервису специальным образом сформированных RDP-пакетов, при обработке которых происходит обращение к уже удаленному объекту (такой механизм иногда называют «use after free» — «использование после освобождения»). Вместо удаленного объекта в этой области памяти находится подготовленный нарушителем код.

Уязвимости данного класса в основном и пополняют публично доступные каталоги.

Уязвимости эксплуатации — следствие ошибок, допущенных в процессе эксплуатации информационной системы:

- использование конфигураций «по умолчанию»;
- некорректно заданные параметры защитных механизмов;
- неиспользуемые сетевые сервисы, доступные удаленно.

Устранение уязвимостей данного класса обычно сводится к внесению соответствующих изменений в конфигурацию системы (например, уязвимость CVE-2009-0243, заключающаяся в том, что функционал «autorun», часто используемый вредоносным ПО, как один из способов распространения, не удается выключить окончательно, даже следуя рекомендациям Microsoft).

Подробная инструкция для устранения данной уязвимости представлена координационным центром CERT. Уязвимости данного типа даже выделены в отдельный каталог[1] Common Configuration Enumeration (CCE).

Типы уязвимости с точки зрения технических особенностей. С любой уязвимостью связаны какие-либо технические особенности, например, в основе уязвимостей реализации нередко лежит возможность создания ситуации переполнения буфера (buffer overflow) или так называемые «гонки» (race condition); уязвимости эксплуатации могут быть следствием неправильного использования различных защитных механизмов: разграничения доступа, криптографии и т. п.

Практическое использование такого подхода к классификации приведено в каталоге NVD[2] (National Vulnerability Database). Помимо стандартных характеристик, здесь в секции «Technical Details» можно увидеть тип уязвимости (Vulnerability Type).

Некоторые типы уязвимостей CWE (Common Weakness Enumeration) приведены в табл. 15.1.

Следует еще раз подчеркнуть, что «тип уязвимости» указывает на ее характер и имеет вполне определенный практический смысл.

---

[1] http://nvd.nist.gov/cce/index.cfm

[2] http://nvd.nist.gov

Таблица 15.1

Типы уязвимостей

Тип	Идентификатор CWE	Описание
Проблемы с проверкой подлинности (Authentication Issues)	CWE-287	Уязвимости, являющиеся следствием неправильного использования механизма аутентификации
Управление учетными данными (Credentials Management)	CWE-255	Уязвимости, связанные с процессами управления учетными записями (создание, хранение, использование)
Контроль разрешений привилегий доступа (Permissions, Privileges and Access Control)	CWE-264	Ошибки в процедуре разграничения доступа
Буфер ошибок (Buffer Errors)	CWE-119	Ошибки реализации программного обеспечения, приводящие к возможности записи за пределы выделенной коду области памяти (так называемое «переполнение буфера»)

Классификация уязвимостей по степени риска. Информация о степени риска той или иной уязвимости в компьютерной системе — важный параметр для выполнения повседневных задач специалиста по информационной безопасности. На основе этих данных проводится более детальный анализ риска, связанного именно с данной уязвимостью в конкретной сети или информационной системе, и, соответственно, принимается решение о целесообразности и оперативности устранения проблемы.

Это вполне понятный, но в то же время довольно «расплывчатый» и субъективный критерий классификации, поскольку степень опасности может зависеть от многих факторов, включая особенности среды эксплуатации уязвимого приложения.

Для уязвимостей, занесенных в доступные каталоги и базы, степень риска выбирается либо вендором[1], либо тем, кто занимается поддержкой каталога уязвимостей.

Например, в базе данных *IBM XForce* уязвимости имеют три уровня риска:

• *высокий* — уязвимости позволяют атакующему сразу получить доступ к узлу с правами суперпользователя или делают возможным обход межсетевых экранов или иных средств защиты;

[1] Крупные вендоры (Microsoft, Cisco Systems и др.) публикуют собственные бюллетени с информацией об уязвимостях в их продуктах. Присваивая степень риска уязвимости, они отражают собственный взгляд на ее степень опасности.

• *средний* — уязвимости дают возможность атакующему получить информацию, которая с высокой степенью вероятности позволит получить доступ к узлу, или приводят к повышенному расходу ресурсов системы (так называемый «отказ в обслуживании»);

• *низкий* — уязвимости позволяют осуществлять сбор критичной информации (например, уязвимость сервера Internet Information Server, позволяющая с помощью специальным образом построенного запроса узнать его внутренний IP-адрес даже при наличии механизма трансляции адресов).

Компания *Microsoft* в своих уведомлениях об обновлениях программного обеспечения использует четыре уровня критичности уязвимостей (табл. 15.2).

Таблица 15.2

Уровни риска (классификация компании Microsoft)

Уровень риска	Определение
Критичный (Critical)	Уязвимость может быть использована для создания интернет-«червя», распространяющегося без вмешательства пользователя
Важный (Important)	Атака с применением уязвимости может привести к снижению уровню целостности, доступности или конфиденциальности данных пользователя или целостности или доступности обрабатываемых ресурсов
Умеренный (Moderate)	Возможность использования уязвимости затруднена различными факторами, такими как настройки по умолчанию, детективные средства защиты или сложность эксплуатации
Низкий (Low)	Устранить уязвимость очень легко, либо последствия устранения минимальны

Компания *SANS* при анализе уязвимостей (SANS Critical Vulnerability Analysis) присваивает критический уровень тем уязвимостям, для которых существует общедоступный эксплойт и/или использование которых не требует специальных навыков. Приведем факторы, рекомендуемые SANS при оценке степени критичности уязвимости:

• распространенность уязвимой системы;

• уровень привилегий, получаемый нарушителем при использовании уязвимости;

• конфигурация «по умолчанию»;

• степень важности уязвимой системы;

• доступность эксплойта;

• сложность использования уязвимости (удаленно/локально и т. п.);

• требуется ли использование методов социальной инженерии (например, «жертва» должна перейти по ссылке и т. п.).

В соответствии с этой оценкой, SANS предлагает, как и Microsoft, 4-балльную шкалу (табл. 15.3).

Руководствуясь информацией о критичности обнаруженной уязвимости, можно планировать и оперативность ее устранения (см. табл. 15.3).

Таблица 15.3

Уровни риска и время реагирования (классификация компании SANS)

Степень риска	Описание	Время реагирования
Критичный (Critical)	Уязвимости, найденные в конфигурациях по умолчанию или в распространенных системах, в результате — получение прав администратора на узле-объекте атаки. При этом эксплойт общедоступен, не требуется применять методы социальной инженерии	48 ч
Высокий (High)	Уязвимость, подобная уязвимости уровня «Critical», для которой имеется хотя бы один фактор, усложняющий ее использование, например требуется какой-либо уровень привилегий	5 раб. дн
Умеренный (Moderate)	Уязвимость, последствия использования которой не так значительны; (например, возможно получение доступа, но с минимальными привилегиями; требуется быть в одном сегменте с объектом атаки; уязвимость есть только в нестандартной конфигурации; использование уязвимости приводит лишь к выведению службы (узла) из строя)	15 раб. дн
Низкий (Low)	Уязвимость, последствия использования которой минимальны, или её применение сильно затруднено (например, требуется физический доступ к узлу). К этой же категории относится возможность получения информации о системе (программные версии служб, топология сети и т. п.)	По усмотрению администратора

Компания *CERT*[1] предлагает методику расчета степени US-CERT риска уязвимости, которая предполагает присвоение уязвимости уровня риска в виде числового значения от 0 до 180 в зависимости от следующих критериев:

- доступность информации об уязвимости;
- наличие случаев использования уязвимости;
- подверженность уязвимости критичных для сети интернет-узлов;
- количество уязвимых узлов сети;
- последствия использования уязвимости;
- легкость использования уязвимости;
- условия применения уязвимости.

[1] http://www.kb.cert.org/vuls/html/fieldhel

Начиная с 2012 г. компания CERT использует методику CVSS[1] (Common Vulnerability Scoring System), позволяющую получать более точные результаты для оценки уязвимостей. Система CVSS предполагает разбиение характеристик (Metrics) уязвимости на три группы, для каждой из которых определен перечень параметров, имеющих набор возможных значений (рис. 15.2). В результате применения методики для каждой из групп получается числовое значение от 0 до 10.

Рис. 15.2. Классификация уязвимостей по методике CVSS

Таблица 15.4

Варианты использования уязвимостей

Значение показателя (Metric Value)	Варианты использования	Коэффициент
Местный Local (L)	Только локально при локальном доступе к системе	0,395
Смежный сетевой Adjacent Network (A)	Удаленно, но находясь в одном сегменте с объектом атаки	0,646
Сетевой Network (N)	Удаленно	1,000

В настоящий момент многие производители используют методику CVSS для оценки риска уязвимостей в своих продуктах, поскольку простота применения методики позволяет на основе общедоступной информации (например, уведомлений от производителя) рассчитать необходимые значения самостоятельно.

[1] http://www.first.org/cvss/cvss-guide

Таблица 15.5

Определение потенциального ущерба

Степень уязвимости	Количество уязвимых систем, %	Весовые коэффициенты
None (ни одной)	0	0
Low (низкий)	До 15	0,10; 0,25
Medium (средний)	16...49	0,30; 0,75
Hight (высокий)	Более 50	0,50; 1,00

Получение информации по уязвимостям. Существует несколько крупнейших общедоступных источников, где можно найти информацию об известных обнаруженных уязвимостях (табл. 15.6).

Таблица 15.6

Источники информации об уязвимости

База уязвимостей	Описание	Ссылка
Securityfocus (Bugtraq)	Содержит информацию об уязвимостях в программном обеспечении. Существует с 1999 г., в 2002 г. приобретена компанией Symantec. Уязвимости, помещаемые в базу Bugtraq, обозначаются уникальным индексом Bugtraq ID (BID), который используется многими программными продуктами для ссылок на уязвимости или атаки	http://www.securityfocus.com/bid
X-Force	Команда исследователей и разработчиков, занимающаяся как анализом программного обеспечения на наличие уязвимостей, так и мониторингом информации об уязвимостях, поступающей из различных источников: списков рассылки, сайтов эксплойтов или непосредственно от производителя ПО. Создана компанией Internet Security Systems (ISS) для обновления баз сигнатур своих продуктов. В 2006 г. ISS приобретена компанией IBM. Уязвимости присваивается уникальный номер и идентификатор, состоящий из ключевых слов, характеризующих уязвимость	http://xforce.iss.net
US-CERT Vulnerability Notes Data	Координационный центр CERT (CERT Coordination Center, CERT/CC) был создан как команда реагирования на инциденты в области информационной безопасности. Однако параллельно с реагированием на инциденты центр занимается также собственными исследованиями в области выявления уязвимостей, результатом которых стала база US-CERT Vulnerability Notes Database	http://www.kb.cert.org/vuls

«Стандартные» обозначения уязвимостей. Ранее были перечислены источники информации по уязвимостям, в основном поддерживаемые компаниями, занимающимися собственными исследованиями в данной области или разработкой соответствующего программного обеспечения. При этом каждый из перечисленных ресурсов располагает собственной системой обозначений для уязвимостей и форматом их описания, в то время как не всегда имеются соответствующие ссылки, позволяющие быстро найти информацию по определенной уязвимости в разных источниках.

Common Vulnerabilities and Exposures (CVE). На рис. 15.3 приведены различные варианты названия уязвимости CVE-2008-4250[1], которая привела к массовому заражению Windows-систем вирусом Kido/Conficker. Обозначение уязвимости включает в себя префикс «CVE», год обнаружения и уникальный номер.

Проект CVE был запущен в 1999 г. и в настоящее время фактически стал промышленным стандартом в части обозначения уязвимостей (см. рис. 15.3).

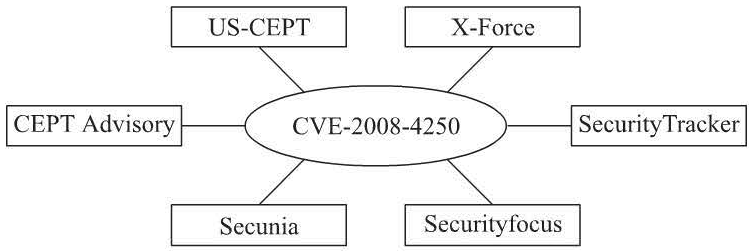

Рис. 15.3. Варианты названия уязвимости CVE

Обеспечить совместимость между разными источниками поможет каталог уязвимостей CVE, который содержит уникальный индекс, краткое описание уязвимости и ссылки на источники, где можно получить более подробную информацию.

National Vulnerability Database[2] — еще один каталог уязвимостей, основанный на CVE, в котором помимо примерно такой же информации, как и в CVE, приведены числовые показатели, характеризующие степень опасности уязвимости. Для расчета используется рассмотренная ранее система.

15.4. Классификация атак

Существуют классификации атак по различным основаниям.

Классификация атак по целям. В зависимости от цели различают:

- нарушение нормального функционирования объекта атаки (например, вызов ситуации отказа в обслуживании);
- получение контроля над объектом атаки (установка серверной части «троянского коня»);

[1] http://cve.mitre.org
[2] http://nvd.nist.gov

• получение конфиденциальной и критичной информации (перехват сетевого трафика и поиск в нем имен и паролей, передаваемых в открытом виде);

• модификация и фальсификация данных (например, изменение информационного наполнения веб-сервера).

Классификация по местонахождению нарушителя. В зависимости от местонахождения нарушителя различают атаки:

• *локальные* — физический, консольный доступ или командная строка узла;

• *внутрисегментные* — нарушитель находится в одном сетевом сегменте с объектом атаки (в этом случае могут быть затронуты все уровни сетевой модели, включая канальный);

• *межсегментные* — нарушитель находится в разных сегментах с объектом атаки (в этом случае вектор атаки распространяется на сетевой уровень и выше).

Кстати, эти три ситуации были упомянуты при рассмотрении системы расчета степени опасности уязвимостей CVSS и назывались Local, Adjacent Network и Network соответственно (см. табл. 15.4).

Локальные атаки обычно предполагают наличие доступа к системе с правами обычного пользователя. Затем, в результате использования какой-либо уязвимости, уровень привилегий может быть повышен. Такие атаки характерны для UNIX-систем, их называют «local root», поскольку в результате такой атаки обычный пользователь получает права «root».

Например, уязвимость CVE 2013-1858[1] позволяет нарушителю, используя системный вызов clone() с параметрами CLONE_NEWUSER|CLONE_FS, получить права суперпользователя.

Самый типичный пример внутрисегментной атаки — «ARP Spoofing», используемый для прослушивания трафика в сетях, где общая среда передачи «сведена к минимуму» посредством использования коммутаторов. Фактически в процессе атаки происходит нарушение навигации на канальном уровне: трафик от одного узла к другому идет не напрямую, а через промежуточный узел.

Атака «ARP-Spoofing» в общем случае имеет следующие э т а п ы :

• ожидание ARP-запросов от участников взаимодействия (поскольку запрос передается широковещательно, он достигнет всех узлов сети, включая узел нарушителя);

• передача ложных ARP-ответов взаимодействующим узлам, в которых в качестве искомого MAC-адреса указывается адрес сетевого адаптера атакующего;

• прием, анализ, модификация и передача пакетов обмена между взаимодействующими узлами (досылка через посредника, в качестве которого выступает узел нарушителя).

Очевидно, что бóльшая часть сетевых атак может быть выполнена межсегментно, т. е. нарушитель и объект атаки находятся в разных сегментах (например, любая атака на ресурс, расположенный в ДМЗ и доступный удаленно, является межсегментной).

Классификация атак по механизмам реализации. В зависимости от механизма реализации различают следующие виды атак:

[1] http://lwn.net/Articles/543273/

- пассивное прослушивание;
- подозрительная активность;
- бесполезное расходование вычислительного ресурса;
- нарушение навигации;
- выведение сервиса из строя;
- запуск кода на объекте атаки.

Рассмотрим перечисленные виды атак подробнее.

Пассивное прослушивание — механизм, при котором со стороны нарушителя не производится каких-либо активных действий (например, в сеть не передается какой-либо подозрительный трафик). Поэтому обнаружение таких атак — сложная задача (например, перехват трафика беспроводного сетевого сегмента и последующий поиск в нем конфиденциальной информации).

Для этого достаточно перевести беспроводной адаптер в режим мониторинга, настроить на нужный канал и осуществлять перехват трафика беспроводных сетей, находящихся в радиусе действия антенны.

Подозрительная активность — механизм, используемый как правило для сбора информации о предполагаемом объекте атаки (рис. 15.4). Но, в отличие от предыдущего механизма, подразумевает какие-то действия со стороны нарушителя (например, сканирование портов (служб) объекта атаки, попытки определения операционной системы путем анализа стека TCP/IP, появление в сети нестандартных пакетов — нетипичный размер, неиспользуемый протокол и т. д.).

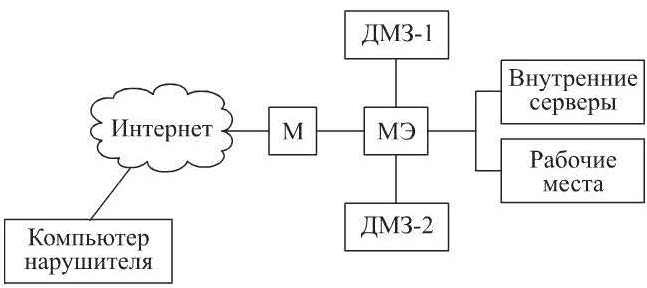

Рис. 15.4. Подозрительная активность

Использование данного механизма в большинстве случаев легко может быть обнаружено.

Бесполезное расходование вычислительного ресурса — разновидность отказа в обслуживании или так называемой DoS-атаки. «Отказ в обслуживании» (Denial of Service, DoS) применительно к компьютерным системам означает намеренное создание условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен. С точки зрения информационной безопасности — это один из механизмов реализации атаки, в ходе которой происходит нарушение доступности системы. Для атак, направленных на исчерпание ограниченных ресурсов, характерно применение нескольких источ-

ников для усиления эффекта атаки. Такой тип атак называют распределенным отказом в обслуживании (Distributed Denial of Service, DDoS). Ограниченными ресурсами обычно являются: пропускная способность канала связи, аппаратные и программные ресурсы конечной системы (объекта атаки) — процессорное время, оперативная память. Принципиальная особенность данного вида сетевых атак — отсутствие уязвимости, устранив которую, можно было бы сделать атаку невозможной. Можно сказать, что в данном случае уязвимостью является сам факт существования ограниченного ресурса (например, сервис, защищенный протоколом SSL, может быть выведен из строя путем отправки большого числа сообщений Client Hello, содержащих случайные данные (рис. 15.5).

Рис. 15.5. Бесполезное расходование вычислительного ресурса.

Обработка этих данных сервером потребует вычислительных операций, после чего сервер сформирует сообщение об ошибке (Illegal Parameter). Таким образом, в данном случае создание нагрузки на сервер осуществляется путем отправки запросов, требующих для их обработки выполнения ресурсоемких криптографических операций. Наиболее масштабная DDoS-атака такого типа выполнялась узлами ботсети Pushdo[1], при этом каждый узел мог отправлять до одного запроса в минуту.

Нарушение навигации (создание ложных объектов и маршрутов) — изменение маршрута сетевых пакетов таким образом, чтобы они проходили через узел нарушителя, изменение соответствия информации различных уровней стека TCP/IP (DNS-имен и IP-адресов, MAC-адресов и IP-адресов и т. п.). Например появление в сети неавторизованного DHCP-сервера может не только вызвать нарушения в работе сети, но и позволить нарушителю реализовать атаку «человек посередине».

Путем передачи клиенту неправильного IP-адреса шлюза по умолчанию нарушитель может осуществлять перехват трафика клиента, а передача неправильного адреса сервера DNS может позволить нарушителю перенаправить клиента на ложный веб-сервер.

Выведение из строя, т. е. создание ситуации отказа в обслуживании путем деструктивного воздействия (выведение сервиса из строя, физическое повреждение элемента инфраструктуры, перенаправление запросов клиента на несуществующий адрес, создание условий для срабатывания защитных механизмов и т. д.), в отличие от рассмотренного ранее намеренного исчер-

[1] https://isc.sans.edu/diary/Pushdo+Update/8131

пания ограниченного вычислительного ресурса, вызывается какой-либо уязвимостью. Например, нарушитель разрывает установленное TCP-соединение путем отправки пакетов ICMP Destination Unreachable от имени одного из участников взаимодействия (рис. 15.6).

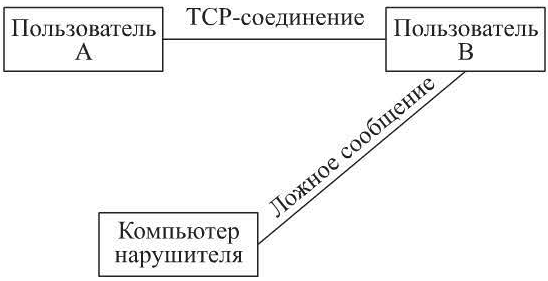

Рис. 15.6. Выведение из строя

Уязвимость CVE-2004-0790, делающая эту атаку возможной, была обнаружена в 2004 г.

Запуск кода на объекте атаки — наиболее опасный механизм реализации сетевых атак. В самом худшем случае нарушитель получает полный контроль над объектом атаки. В настоящее время в основе подобных атак лежат уязвимости реализации клиентских приложений и компонентов. Подобные атаки осуществляются обычно в несколько шагов (рис. 15.7):

1) нарушитель размещает специально подготовленный контент на популярном ресурсе (социальные сети, фотовидеоресурсы), который рассчитан на обработку уязвимым клиентским приложением. При этом довольно популярны Java-эксплойты, например Java/Exploit.CVE-2011-3544, позволяющий выполнить вредоносный код за пределами сети;

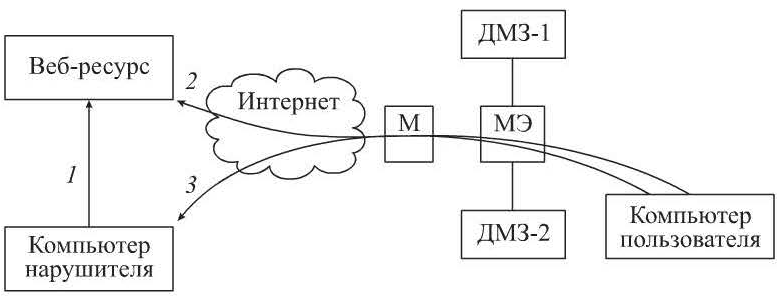

Рис. 15.7. Запуск кода на объекте атаки:
1 — 3 — шаги (этапы) атаки

2) пользователь, посещающий веб-ресурс, при просмотре контента инициирует загрузку соответствующих клиентских приложений, включая уязвимое. В результате на узле пользователя запускается подготовленный нарушителем

код, например обеспечивающий удаленное управление узлом (так называемый reverse shell);

3) нарушитель незаметно для пользователя выполняет подключение к своему узлу, возможно происходит загрузка дополнительных модулей вредоносного программного обеспечения, и получает контроль над объектом атаки.

15.5. Средства защиты сетей

Для защиты корпоративной сети обычно используется комплекс средств безопасности, реализующий основные защитные механизмы и состоящий из нескольких подсистем:

- защиты рабочих станций и серверов от НСД;
- межсетевого экранирования при необходимости с выделением отдельной подсистемы защищенного доступа к ресурсам сети Интернет;
- криптографической защиты сетевого трафика;
- антивирусной защиты;
- анализа защищенности;
- обнаружения атак.

* * *

В основе функционирования всемирной сети Интернет лежат стандарты IP-сетей. Огромный потенциал IP- и интернет-технологий только начинает использоваться. Все бóльшую популярность приобретает технология передачи голоса поверх IP (Voice over IP, VoIP), для связи между офисами все шире применяются виртуальные частные сети. Электронная коммерция из абстрактного понятия все более превращается в реальность.

Контрольные вопросы

1. Охарактеризуйте уровни информационной инфраструктуры корпоративной сети.
2. Дайте определения угрозы, уязвимости и атаки. Охарактеризуйте на примерах взаимосвязь между этими понятиями.
3. Приведите классификационные схемы уязвимостей и атак.
4. Какой из механизмов реализации сетевых атак наиболее сложен с точки зрения обнаружения?
5. Какой из механизмов реализации сетевых атак не подразумевает использования какой-либо уязвимости?
6. Какие средства защиты сетей вам известны?

Глава 16. ЗАЩИТА ПЕРИМЕТРА КОРПОРАТИВНОЙ СЕТИ

Периметр корпоративной сети должен быть защищен и в то же время иметь взаимодействие с окружающим миром.

Возможными точками взаимодействия с окружающим миром могут быть:

- точка подключения к сети Интернет;
- выделенные каналы, соединяющие филиалы друг с другом или обеспечивающие взаимодействие с сетями партнеров;
- клиентские приложения, нередко имеющие постоянное соединение с ресурсами, расположенными в недоверенных сетях;
- сегменты, обеспечивающие удаленный доступ к сети, включая доступ посредством виртуальных частных сетей (Virtual Private Network, VPN);
- беспроводные сегменты, позволяющие нарушать границы сети на физическом и канальном уровнях.

Виртуальные частные сети позволяют предоставить удаленным мобильным пользователям, где бы они ни находились, безопасный доступ к корпоративным ЛВС, а партнерам и клиентам — безопасный доступ к определенным внутренним информационным ресурсам организации за счет создания криптографически защищенных туннелей для пересылки данных из одной конечной точки в другую.

В современных условиях границы сетей становятся все более «размытыми». Иногда говорят, что точка периметра находится на границе между двумя сетями с разными политиками безопасности. Возможные названия этих областей приведены на рис. 16.1.

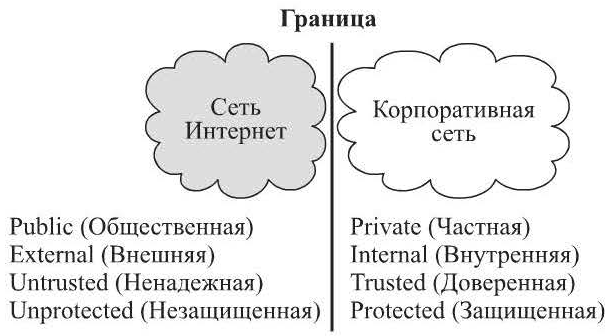

Рис. 16.1. Граница между двумя сетями с разными политиками безопасности

На рис. 16.2 перечислены каналы, через которые в корпоративную сеть может попасть какая-либо информация или, наоборот, уйти из нее.

Разумеется, информация может попасть в сеть (или «уйти» из нее) и через различные портативные устройства (флэш-карты, диски и т. п.), однако эти вопросы касаются физической безопасности и в рамках данного курса не рассматриваются.

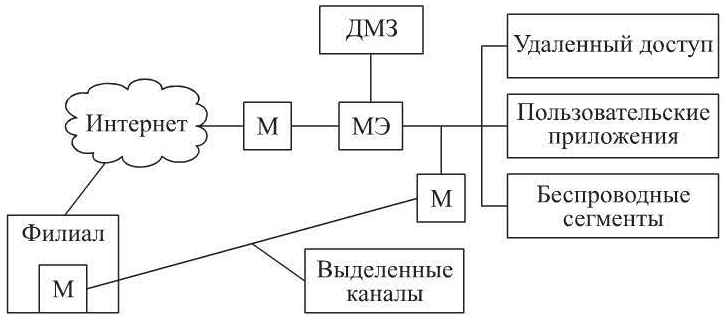

Рис. 16.2. Каналы поступления информации в корпоративную сеть

16.1. Угрозы, связанные с периметром корпоративной сети

Задачи, которые требуется решать в ходе защиты периметра сети, вытекают из тех угроз, источником которых и является существование сетевого периметра.

Прежде всего, это атаки на внешние *ресурсы*, находящиеся в *демилитаризованной зоне* (рис. 16.3).

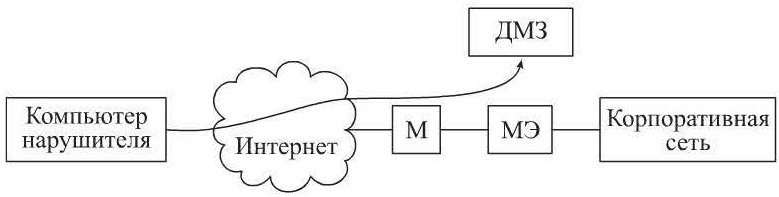

Рис. 16.3. Атаки на внешние ресурсы

К таким ресурсам, например, относят почтовый сервер, DNS-сервер и т. п.

Отдельно следует упомянуть проблему *спама*, которая частично может быть решена средствами защиты периметра.

Поскольку точкой периметра можно считать и клиентские приложения, одной из угроз является возможность *проникновения в сеть вредоносного кода* — вирусов, «червей», шпионского ПО (рис. 16.4).

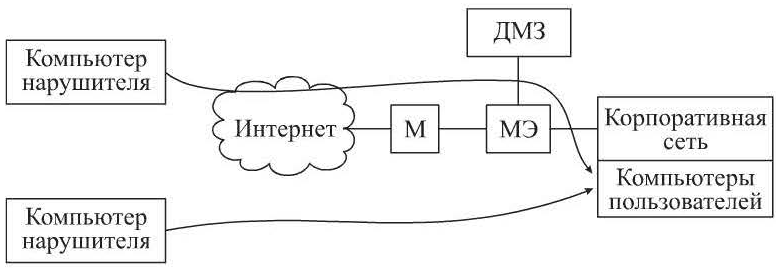

Рис. 16.4. Атаки на клиентское программное обеспечение

Еще одна точка подключения к корпоративной сети — *удаленный доступ*, обычно осуществляющийся с использованием технологий VPN. При этом *незащищенные клиенты* VPN могут представлять собой дополнительную угрозу, поскольку, с одной стороны, они имеют соединение с внутренней сетью, с другой — с той сетью, из которой осуществляется подключение.

Сети, с которыми осуществляется связь по выделенным каналам, могут иметь разный уровень доверия, соответственно, здесь также нужен контроль.

Беспроводные устройства (точка доступа или просто ноутбук, имеющий как проводной, так и беспроводной сетевые интерфейсы) также являются частью сетевого периметра. К тому же они делают возможным нарушение границ на канальном или физическом уровне, поскольку точка доступа может быть «продолжением» коммутатора, а это значит, что для подключения к сети уже не потребуются кабель и розетка.

Наконец, стоит упомянуть и *угрозу утечки критичной информации*, вследствии того, что точка периметра, как уже отмечалось, лежит на границе между доверенной и недоверенной сетями.

16.2. Составляющие защиты периметра

Защита периметра — это обеспечение безопасности при осуществлении электронного обмена информацией с другими сетями, разграничение доступа между сегментами корпоративной сети, а также защита от проникновения и вмешательства в работу корпоративной сети нарушителей из внешних систем.

Для нейтрализации угроз механизм защиты периметра имеет несколько составляющих:

• *фильтрация трафика* — позволяет «отсечь» лишний трафик и оставить только разрешенные сетевые протоколы. Это своеобразное разграничение доступа, работающее на сетевом уровне. Обычно фильтрация трафика сопровождается также трансляцией сетевых адресов, что позволяет скрыть структуру защищаемой сети.

Помимо фильтрации трафика, возникает задача его защиты при передаче по недоверенным сетям, что подразумевает обеспечение его конфиденциальности, аутентичности и целостности. Для этого обычно используются технологии построения виртуальных частных сетей;

• *противодействие сетевым атакам*, с помощью которого в оставшемся (разрешенном) сетевом трафике осуществляется поиск признаков атак;

• *анализ содержимого* (Content Security) — для более тщательного анализа некоторых разновидностей трафика (например, HTTP, POP3, SMTP, FTP).

Задача анализа содержимого распадается на несколько подзадач:

• веб-фильтр;
• антивирусная защита;
• защита от спама;
• контроль утечек критичной информации;
• контроль беспроводных сегментов.

Несанкционированно установленная в сети точка доступа позволяет подключиться к корпоративной сети и использовать ее ресурсы в обход средств защиты периметра.

16.3. Межсетевые экраны

Как было отмечено, задача защиты периметра заключается в контроле его отдельных точек. Обычно для этого устанавливают межсетевые экраны.

Имеется огромное количество определений межсетевого экрана, одно из них, кажущееся вполне логичным, представлено в документе RFC 4949 (Internet Security Glossary), где МЭ (firewall) определяется как шлюз, ограничивающий прохождение сетевого трафика между подключенными к нему сегментами.

Шлюз (gateway) — устройство, обеспечивающее обмен информацией между двумя или несколькими подключенными к нему компьютерными сетями (сетевыми сегментами) со схожими функциями, но с различной реализацией (различные сетевые технологии или различные стеки протоколов) и позволяющее узлам из различных сегментов связываться друг с другом.

Необходимо сделать несколько уточнений: 1) взаимодействие может быть как однонаправленным, так и двунаправленным; 2) возможен широкий спектр различий между взаимодействующими сетями — от используемых протоколов до защитных механизмов.

Теоретически шлюзы могут быть реализованы на любом уровне модели OSI. На практике обычно применяют шлюзы канального (мосты), сетевого (маршрутизаторы) и прикладного (прокси-серверы) уровней.

Межсетевой экран в основном защищает небольшую сеть (корпоративную ЛВС или даже отдельный узел) от большой сети (например, Интернет).

С точки зрения *архитектуры*, МЭ — не всегда отдельный узел (например, МЭ может состоять из двух пакетных фильтров и одного или нескольких посредников (proxy), подключенных к выделенной локальной сети, расположенной между двумя пакетными фильтрами). Внешний пакетный фильтр блокирует атаки на уровне IP, в то время как proxy блокируют атаки на уровнях выше IP. Внутренний маршрутизатор перенаправляет трафик из внутренней сети на посредников различных типов.

С точки зрения *защищаемых ресурсов* МЭ классифицируют следующим образом:

- периметровые или сетевые (network-based, защищающие целую сеть);
- персональные (host-based, контролирующие трафик отдельного узла).

Помимо МЭ общего характера, имеются *специализированные МЭ* (например, для веб-приложений, виртуальных инфраструктур).

Периметровые МЭ выполняют в основном в виде отдельного устройства, имеющего несколько сетевых интерфейсов; персональные МЭ представляют собой программное обеспечение, установленное на защищаемом узле.

Простейшая схема включения периметрового МЭ приведена на рис. 16.5.

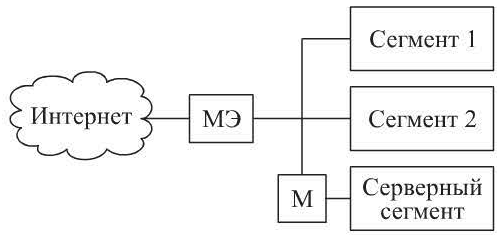

Рис. 16.5. Схема включения периметрового МЭ

В данном случае один из интерфейсов МЭ подключен к внешней (недоверенной) сети, другой — к внутренней (доверенной) сети. МЭ на данной схеме обеспечивает функции маршрутизатора между внешней и внутренней сетями. Внутренняя сеть состоит из нескольких областей, одна из которых (серверный сегмент) отделена маршрутизатором.

Еще одна конфигурация (рис. 16.6) имеет демилитаризованную зону.

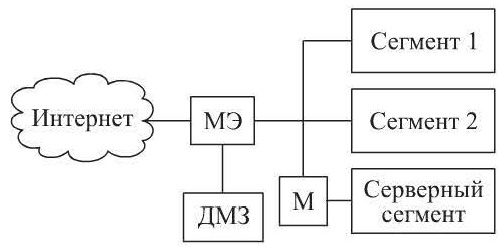

Рис. 16.6. Схема включения периметрового МЭ с ДМЗ — это изолированный сегмент, прохождение трафика через который регламентируется правилами, заданными на МЭ (или другом устройстве разграничения доступа)

Существует две разновидности ДМЗ:

• *граничная сеть* (экранированная подсеть, ДМЗ типа «сэндвич») — сетевой сегмент, расположенный между двумя МЭ;

• *тупиковая сеть* — сетевой сегмент, подсоединенный к отдельному интерфейсу МЭ.

Прохождение трафика через ДМЗ регламентировано правилами установки МЭ, а трафик Интернета и внутренней сети не регулируется.

Основное назначение ДМЗ — предоставление доступа к различным службам клиентов, которые не входят в число доверенных лиц. В качестве примера можно привести:

1) размещение в ДМЗ таких узлов, как веб-сервер, почтовый сервер и разрешение доступа к ним со стороны пользователей;

2) разделение информационных потоков между внутренними сегментами корпоративной сети.

Таким образом, ДМЗ позволяет обеспечить безопасность серверов и разграничение доступа между сегментами внутренней сети. Кроме того, в ДМЗ можно сосредоточить средства обнаружения атак и дополнительно укрепить расположенные там узлы.

С помощью ДМЗ может быть организован гостевой беспроводной доступ. Трафик беспроводных клиентов маршрутизируется в Интернет, а межсетевой экран препятствует подключению к ресурсам внутренней сети.

Периметровые МЭ могут быть дополнены персональными МЭ, установленными на узлах, требующих введения дополнительного уровня защиты:

- отдельные внутренние серверы;
- VPN-клиенты;
- беспроводные клиенты;
- рабочие станции.

Систему персональных МЭ можно использовать, если нет возможности выделить в отдельный сегмент группу узлов, нуждающуюся в таком выделении.

Поскольку МЭ по своей природе это шлюз, который может быть реализован на любом уровне модели OSI, различают следующие типы МЭ по уровню, на котором он «вмешивается» в сетевое взаимодействие:

- мосты (мостовые МЭ);
- пакетные фильтры;
- посредники (шлюзы) уровня соединения;
- посредники (шлюзы) прикладного уровня.

Мостовые МЭ. Мостовые МЭ выполняют анализ фреймов канального уровня и перенаправляют их на нужный сетевой интерфейс. Они подключаются как бы «в разрыв кабеля» и не требуют изменения сетевых настроек (на уровне IP).

К достоинствам мостовых МЭ относят: «прозрачность» (мостовой МЭ просто пересылает фреймы после их анализа между сетевыми интерфейсами, поэтому нет необходимости в изменении существующих сетевых настроек и маршрутизации); защищенность от атак (сетевые интерфейсы мостового МЭ не имеют IP-адреса и поэтому невидимы для окружающего мира).

Пакетные фильтры. Это маршрутизатор, перенаправляющий сетевые пакеты в соответствии с заданной на нем политикой безопасности. Пакетный фильтр «вмешивается» в сетевое взаимодействие на сетевом уровне модели OSI, при этом в качестве критериев фильтрации используется информация из заголовков протоколов сетевого и транспортного уровней (IP, TCP, UDP, ICMP).

Принятие решения происходит на основе правил фильтрации, которые можно представить в виде таблицы. Момент срабатывания правил может варьироваться, обычно это происходит до принятия решения о маршрутизации.

Схема алгоритма работы пакетного фильтра представлена на рис. 16.7.

После поступления очередного пакета происходит просмотр значимых полей, т. е. тех, которые имеют значение при применении критериев фильтрации (например, это могут быть отдельные поля заголовков сетевого и транспортного уровней).

Затем к пакету применяются имеющиеся правила (по очереди, до первого подошедшего). Если правило явно разрешает прохождение пакета, то просмотр правил прекращается и пакет пропускается. Если правило явно запре-

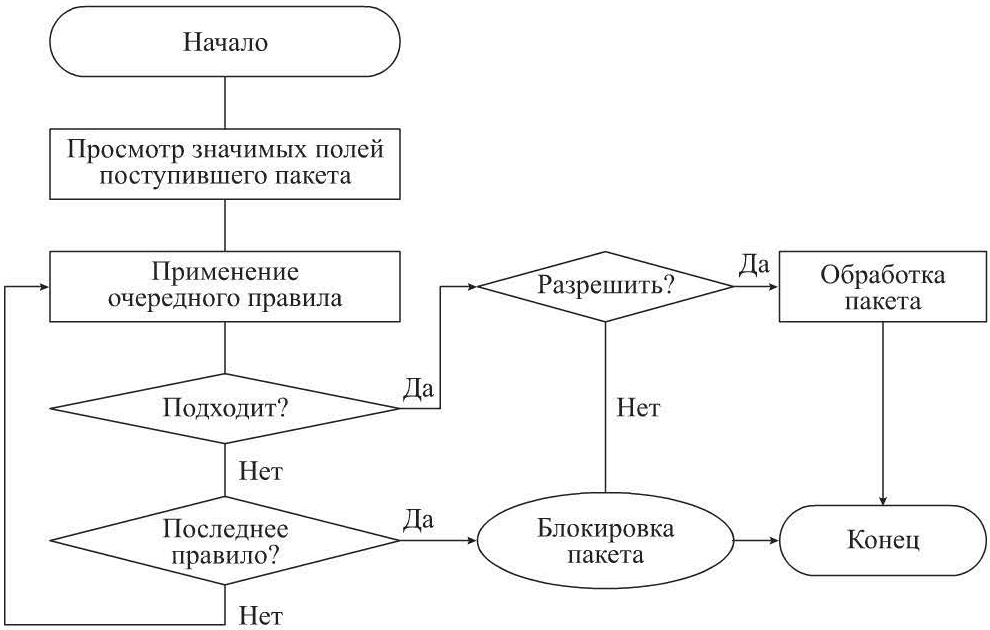

Рис. 16.7. Алгоритм работы пакетного фильтра

щает прохождение пакета, он отбрасывается, просмотр правил прекращается. Если ни одно из имеющихся правил не подошло, пакет также отбрасывается.

Работа алгоритма пакетного фильтра основана на принципе «Запрещено все, что не разрешено».

Правила фильтрации следуют в строго определенном порядке и применяются к пакету в соответствии с этим порядком.

Простейшие пакетные фильтры имеют ряд недостатков, основным из которых является отсутствие контроля соединения (статичность). Это означает, что пакетный фильтр манипулирует отдельными пакетами, не учитывая принадлежности пакета к какому-либо соединению, ни, тем более, сопоставляя данные нескольких (взаимосвязанных между собой) соединений.

Следующий пример иллюстрирует этот основной недостаток пакетных фильтров (рис. 16.8).

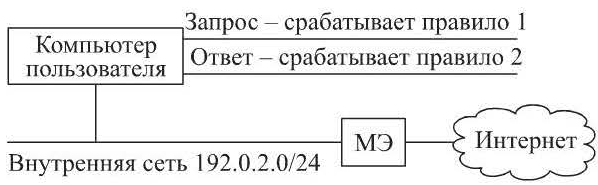

Рис. 16.8. Статичность пакетного фильтра

Правила, приведенные в табл. 16. 1, обеспечивают возможность отправки почты из сети 192.0.2.0/24 на любой внешний SMTP-сервер.

Несмотря на возможность инициирования соединения только из сети 192.0.2.0/24, прохождение ответов с 25-го порта TCP (с любого внешнего узла) разрешено, даже если не было запроса. Таким образом, нарушитель может посылать большое количество ответов, создавая тем самым ситуацию бесполезного расходования вычислительных ресурсов (рис. 16.9).

Таблица 16.1

Правила фильтрации

Номер правила	Действие	Узел-источник	Порт	Узел-получатель	Порт TCP	Флаги TCP Опции IP	Комментарий
1	Разрешить	192.0.2.0/24	1024-65535	*	25	TCP	Запрос
2	Разрешить	*	25	192.0.2.0/24	1024-65535	TCP ACK=1	Ответ

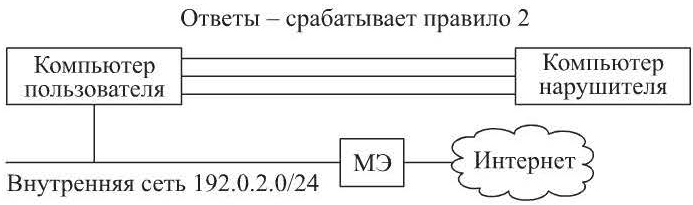

Рис. 16.9. Бесполезное расходование вычислительных ресурсов

Поскольку пакетный фильтр блокирует подключения к узлу, основываясь на наличии флага SYN в заголовке, пакеты с флагом ACK будут пропущены. Развитие этой идеи в свое время привело к появлению троянцев[1], клиентская часть которых подключалась к серверной, используя только ACK-пакеты, без флагов SYN.

Пакетная фильтрация свойственна многим операционным системам, а также сетевому оборудованию. В частности, встроенные в ядро возможности пакетных фильтров всегда были сильной стороной UNIX-систем.

Для BSD-систем наиболее популярным в настоящее время является пакетный фильтр pf, а в ОС Linux используется iptables.

Еще один классический пример – МЭ CheckPoint, архитектура которого базируется на технологии Stateful Inspection. Ядро архитектуры – модуль FireWall INSPECT engine, выполняющий перехват и анализ сетевых пакетов, располагаясь между драйвером сетевого адаптера и стеком TCP/IP. Модуль

[1] http://www.ntsecurity.nu/toolbox/ackcmd/

INSPECT работает в режиме ядра ОС (в виде драйвера). Несмотря на то, что CheckPoint выполняет анализ трафика прикладного уровня, дополнительную аутентификацию и содержит «встроенных» посредников, по «своей природе» это пакетный фильтр с технологией Stateful Inspection.

Технология «Stateful Inspection». Очевидно, что для решения проблемы статичности, т. е. принятия окончательного решения о пропуске или запрете очередного анализируемого пакета, недостаточно лишь просматривать отдельные пакеты, должна быть использована информация о предыдущих соединениях. В зависимости от типа проверяемого пакета, для принятия решения важными могут быть как текущее состояние соединения, которому он принадлежит (полученное из его истории), так и состояние приложения, его использующего.

Технология «Stateful Inspection» обеспечивает сбор информации из пакетов, сохранение и накопление ее в специальных контекстных таблицах, которые динамически обновляются.

Таким образом, обработка нового соединения происходит с записью параметров этого соединения в таблицы соединений.

Обработка последующих пакетов соединения осуществляется на основе анализа этих таблиц.

Для разных типов соединений в таблицах запоминается разная информация (табл. 17.2).

Таблица 16.2

Запоминаемая информация

Протокол	Тайм-аут	Адреса	Порты	Флаги	SEQ number и ACK number	Идентификаторы
TCP	+	+	+	+	+	–
UDP	+	+	+	+	–	–
ICMP	+	+	–	–	–	+
Другой	+	+	–	–	–	–

Технология «Stateful Inspection» может быть распространена и на прикладной уровень. Если прикладная служба использует несколько взаимосвязанных соединений, то технология «Stateful Inspection» обеспечивает динамическое открытие/закрытие необходимых портов.

Посредники уровня соединения. Решить проблему статичности можно также с помощью посредника (proxy) — узла, выполняющего запрос на установление соединения по инициативе другого узла.

В отличие от пакетных фильтров, посредник не позволяет узлам, находящимся по разные стороны МЭ, связываться напрямую. Вместо этого устанавливаются два соединения: одно между клиентом и посредником, другое — между посредником и сервером.

Посредник (аналогично пакетному фильтру) руководствуется набором правил для определения того, какой трафик разрешен, а какой запрещен, при этом контроль соединения осуществляется «по определению».

Внутреннее устройство посредника упрощенно проиллюстрировано на рис. 16.10.

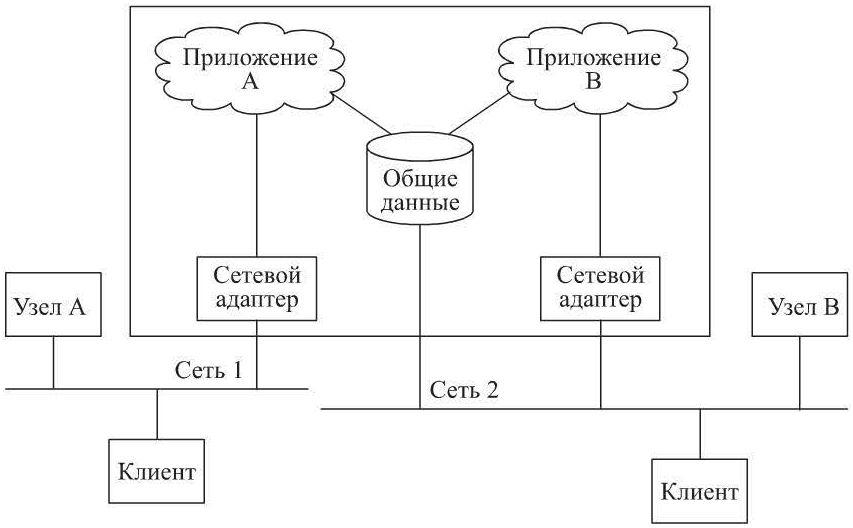

Рис. 16.10. Внутреннее устройство посредника

Узел A в сети 1 имеет доступ к приложению A на представленном узле, а приложение B — к узлу B. Оба приложения имеют общий буфер, через который узлы A и B могут взаимодействовать. Когда клиент внутренней сети обращается, например, к веб-серверу, его запрос попадает к посреднику (или перехватывается им). Последний устанавливает связь с сервером от имени клиента, а полученную информацию передает клиенту.

Различают посредники: универсальные — уровня соединения (circuit-level proxy) и специализированные — прикладного уровня (application-level proxy).

Посредник уровня соединения не учитывает особенностей конкретных служб (HTTP, FTP и пр.) и перенаправляет трафик одинаковым образом для любых прикладных сервисов. Для такого посредника прикладной сервис обычно ассоциируется лишь с номером порта (например, протокол SOCKS).

Шлюзы прикладного уровня, называемые также proxy-серверами (рис. 16.11), контролируют и фильтруют информацию на прикладном уровне модели OSI; различаются по поддерживаемым протоколам прикладного уровня (наиболее часто поддерживаются службы веб (HTTP), FTP, SMTP, POP3/IMAP, NNTP, DNS, RealAudio/RealVideo).

Для внешнего сервера посредник выступает в качестве клиента HTTP, а для внутреннего клиента — в качестве сервера HTTP.

Работа посредников прикладного уровня основана на типе протокола прикладного уровня, в отличие от шлюзов уровня соединения, базирующих-

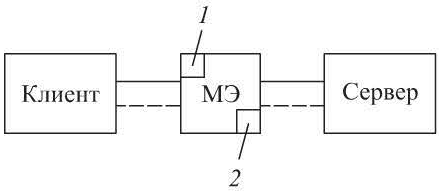

Рис. 16.11. Шлюзы прикладного уровня:
1, 2 — серверная и клиентская часть прикладной службы соответственно

ся обычно на номерах портов (например, proxy-сервер SQUID).

Посредник, в отличие от пакетного фильтра, «заметен» для клиента, что создает некоторые неудобства: необходимость настройки клиентских узлов или приложений. С этой точки зрения посредники подразделяют на классические (classical proxy) и прозрачные (transparent proxy). *Классические посредники* требуют явной настройки клиентских приложений или установки специального программного обеспечения (например, в настройках браузера можно явно указать адрес и номер порта посредника, рис. 16.12).

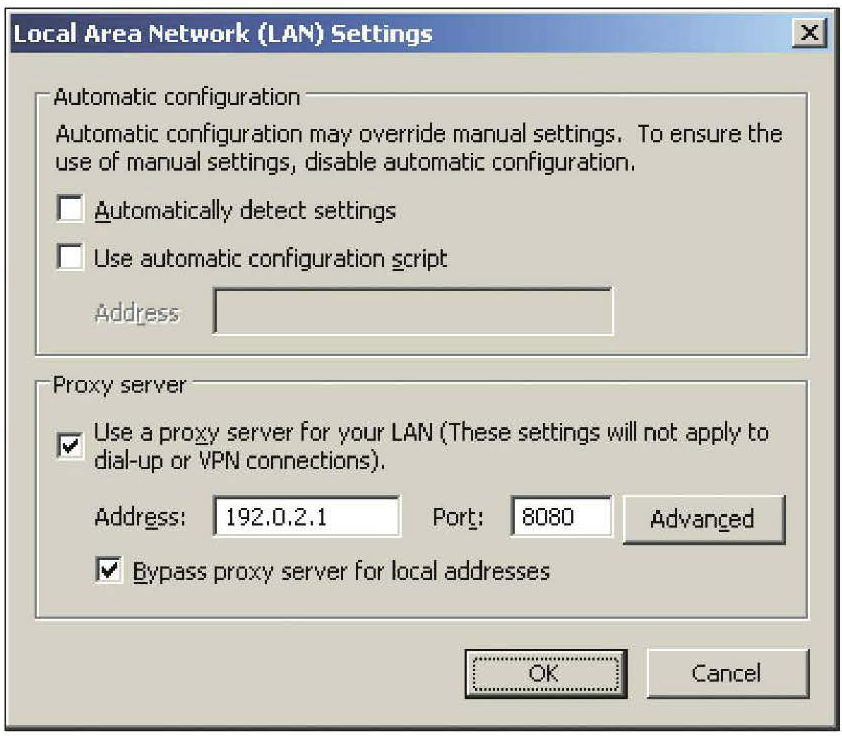

Рис. 16.12. Windows интерфейс настройки классического посредника

Прозрачный посредник с точки зрения пользователя создает иллюзию прямого соединения. Для клиента прозрачный посредник «кажется» пакетным фильтром. Для решения этой задачи стек TCP/IP посредника модифицируется таким образом, что SYN-пакет от клиента обрабатывается именно посредником, и устанавливается соединение с целевым сервером.

В ряде случаев возникает необходимость использования сертифицированных средств защиты, в том числе и МЭ. В России имеется две системы сертификации МЭ: ФСТЭК и ФСБ. Первая система сертификации более известна и описана в руководящем документе ФСТЭК России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации», где установлено шесть классов защищенности МЭ, каждый из которых характеризуется определенной минимальной совокупностью требований по защите информации. Самый низкий класс защищенности — класс 5, самый высокий — класс 1.

16.4. Анализ содержимого почтового и веб-трафика

Для фильтрации трафика служб прикладного уровня возможностей межсетевых экранов может оказаться недостаточно, особенно для контроля электронной почты и HTTP-трафика. Сложность задачи заключается в том, что для осуществления такого контроля недостаточно анализа заголовков указанных протоколов прикладного уровня, здесь требуется просмотр данных, передаваемых в нескольких пакетах различного формата, и т. д.

Задача анализа содержимого сводится к просмотру передаваемой информации следующего характера:

- содержимое электронной почты (в том числе прикрепленные файлы);
- содержимое HTTP-трафика;
- передаваемые файлы (например, по протоколу FTP).

Для решения этой задачи применяют два подхода (данные подходы могут быть реализованы на базе МЭ CheckPoint Fire Wall-l):

1) анализ содержимого средствами МЭ (многие МЭ имеют возможности фильтрации на основе адреса отправителя, получателя и т. д.);

2) антивирусное программное обеспечение.

Такие решения имеют недостатки, которые заключаются в поддержке небольшого числа критериев фильтрации и форматов передаваемых файлов. Кроме того, немаловажное значение имеет вопрос производительности, поскольку для детального анализа содержимого требуется значительное количество ресурсов.

Электронная почта. Электронная почта, наряду с очевидными преимуществами (удобство для бизнеса, оперативность, продуктивность), имеет ряд недостатков, среди которых возможности:

- создания ситуации отказа в обслуживании (пересылка файлов большого размера, спам, подмена адреса отправителя);
- пересылки вирусов в сообщении или прикрепленных файлах;
- пересылки конфиденциальной информации и информации неэтичного характера;
- использования электронной почты в личных целях.

Таким образом, средства анализа содержимого электронной почты должны противодействовать перечисленным угрозам.

Критериями фильтрации для таких средств должны быть:

- адреса отправителя и получателя;
- параметры прикрепленных файлов (тип, размер);
- наличие вирусов;
- содержимое письма и прикрепленных файлов;
- подлинность адреса отправителя.

HTTP-трафик. С HTTP-трафиком связаны следующие угрозы:

- «опасное» содержимое — мобильный код, вирусы;
- пересылка информации через веб-интерфейс;
- использование трафика в личных целях;
- загрузка материалов недопустимого характера (нелицензионное программное обеспечение, порнография и т. д.).

Следовательно, критериями фильтрации в данном случае являются:

- параметры загружаемых файлов (имя, тип, размер);
- наличие вирусов;
- содержимое загружаемых файлов;
- URL;
- почта с веб-интерфейсом;
- разрешенные часы работы;
- направление загрузки файлов.

Системы анализа содержимого — это фактически посредники прикладного уровня с расширенными возможностями фильтрации трафика прикладного уровня, работающие аналогично МЭ (фактически это разновидность МЭ).

Размещение такой системы в корпоративной сети зависит от следующих факторов:

- схема подключения к сети Интернет;
- расположение МЭ (пакетного фильтра или посредника).
- назначение системы анализа содержимого (проверка электронной почты или HTTP-трафика)

16.5. Виртуальные частные сети

Виртуальные частные сети предназначены для обеспечения безопасного обмена данными между удаленными пользователями и удаленными друг от друга ЛВС организации через сети с низким уровнем доверия, например через Интернет.

Виртуальные частные сети (VPN) позволяют предоставить удаленным мобильным пользователям, где бы они ни находились, безопасный доступ к корпоративным ЛВС, а партнерам и клиентам — безопасный доступ к определенным внутренним информационным ресурсам организации за счет создания криптографически защищенных туннелей для пересылки данных из одной конечной точки в другую.

Существует несколько способов классификации виртуальных частных сетей. По решаемым с помощью VPN задачам различают:

• *внутрикорпоративные VPN (Intranet VPN)* — для организации связей между филиалами одной организации;

• *VPN с удаленным доступом (Remote Access VPN)* — для организации доступа к корпоративной сети мобильных сотрудников;

• *межкорпоративные VPN (Extranet VPN)* — для организации связей с партнерами и клиентами.

Кроме того, возможны следующие топологии VPN:

• смешанная (Mesh);

• звезда (Star).

Главными элементами для построения VPN являются криптографические устройства, располагаемые на входах в удаленных друг от друга ЛВС и на компьютерах удаленных (мобильных) пользователей.

Варианты реализации виртуальных частных сетей:

• VPN на основе межсетевых экранов — использует только один программно-аппаратный комплекс для защиты потоков данных для всех узлов каждой ЛВС;

• VPN на основе службы, встроенной в операционную систему сетевых узлов, — наиболее доступный вариант, так как реализуется стандартными средствами ОС, однако для защиты самих узлов сети все равно необходим межсетевой экран;

• VPN на основе специальных криптографических шлюзов между внутренними сетями и сетью общего пользования (например, VPN на основе маршрутизатора с криптографическими возможностями) — отличаются высокой производительностью, но имеют высокую стоимость.

Рассмотрим продукт отечественного производства, разработанный НИП «Информзащита» — программно-аппаратный шифратор IP-протокола (криптошлюз) «Континент-К», который реализует защиту данных по ГОСТ 28147–89. Достоинства криптошлюза состоят в том, что он незначительно увеличивает размер передаваемых пакетов данных, не требует дополнительного взаимодействия сторон при установлении каждого логического соединения и позволяет сжимать передаваемые данные.

Техническая характеристика

Общая пропускная способность криптошлюза (имитовставка, шифрование, туннелирование), Мбит/с	30 (Celeron/500)
Увеличение размера пакета с учетом дополнительного IP-заголовка, байт	24 — 36
Максимальное количество криптошлюзов в сети с одним ЦУС	Не более 5000
Максимальное количество консолей управления	Не ограничено
Максимальное количество абонентских пунктов для одного криптошлюза	Не более 500

Виртуальные частные сети обеспечивают защиту трафика, передаваемого по открытой (недоверенной) сети, при этом компоненты, участвующие в ее работе (VPN-шлюзы и клиенты), сами нуждаются в защите. Атаки злоумышленников могут быть направлены как на VPN-шлюзы, так и на клиентов VPN, а также на передаваемый трафик. Следовательно, угрозы VPN можно подразделить на три г р у п п ы :

- «незащищенные» клиенты;
- атаки на VPN-шлюзы;
- перехват и анализ трафика VPN.

Рассмотрим перечисленные группы подробнее

«Незащищенные клиенты». Клиенты VPN, подключающиеся к VPN-шлюзу, имеют два сетевых соединения: защищенное (соединение с корпоративной сетью) и незащищенное — с той сетью, в которой они находятся в данный момент.

Для защиты клиента на сетевом уровне рекомендуется использовать следующие технологии:

- *фильтрация трафика* — позволяет отсечь лишний трафик, не требующийся клиенту для работы (например, можно блокировать весь входящий трафик, за исключением того, который необходим для функционирования ПО VPN-клиента);
- *обнаружение и блокирование атак* — в разрешенном трафике (как входящем, так и исходящем) необходимо искать признаки атак и при их обнаружении блокировать трафик;
- *блокировка попыток использования переполнения буфера* — обычно сопутствует ряду сетевых атак, не обнаруженных системой противодействия атакам;
- *защита клиента на прикладном уровне* (антивирусная система, контроль используемых приложений, «поведенческий» анализ).

Атаки на VPN-шлюзы можно разделить на три п о д г р у п п ы :

1) сбор информации о VPN-шлюзе (программное обеспечение, версия, конфигурация, поддерживаемые протоколы, открытые порты и т. п.);

2) бесполезное расходование вычислительного ресурса;

3) атаки с использованием уязвимостей.

Защита сервера VPN может быть осуществлена установкой системы обнаружения атак, кроме того, необходимо регулярно обновлять ПО сервера VPN.

Атаки на VPN-трафик. Конечно, значительная часть VPN-трафика зашифрована. Тем не менее, некоторые данные, в частности служебные, используемые на этапе согласования, не шифруются (например, в открытом виде передается имя пользователя, что позволяет использовать его для подбора пароля).

* * *

Периметр корпоративной сети, которая всегда имеет связь с другими сетями, имеющими более низкий уровень политики безопасности (например, Интернет), требует защиты, т. е. контроля поступающей (выходящей) информации. Для этой цели применяют межсетевые экраны (пакетные фильтры, посредники, а также

МЭ с технологией «stateful inspection»), которые должны быть сертифицированы в соответствии с требованиями ФСТЭК России или ФСБ России.

Дополнительный контроль циркулирующей в системе информации необходим для почтового и веб-трафика.

При выборе средств для построения VPN прежде всего необходимо обращать внимание на следующие вопросы: какой протокол туннелирования поддерживает криптографический модуль (межсетевой экран, криптошлюз и т. п.), какие криптографические алгоритмы используются для шифрования, какие механизмы сжатия туннелируемых данных применяются, какова способность системы работать с отдельным удаленным пользователем.

Контрольные вопросы

1. Почему необходимо защищать периметр корпоративной сети?
2. Перечислите составляющие механизма защиты периметра сети.
3. Что такое демилитаризованная зона в применении к компьютерным сетям?
4. Дайте определение понятия межсетевого экрана. В чем заключается его функция?
5. Перечислите основные типы межсетевых экранов. Охарактеризуйте функции МЭ каждого типа, их достоинства и недостатки.
6. В чем состоит главный недостаток пакетных фильтров — разновидности межсетевых экранов?
7. В чем разница между обычным пакетным фильтром и пакетным фильтром с контролем состояния «stateful»?
8. В чем разница между пакетным фильтром с контролем состояния «stateful» и классическим посредником сеансового уровня?
9. Каковы особенности анализа содержимого электронной почты?
10. Перечислите критерии фильтрации содержимого электронной почты.
11. Каковы особенности анализа содержимого HTTP-трафика?

ГЛАВА 17. ОБНАРУЖЕНИЕ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ. ВОЗМОЖНОСТИ СКАНЕРОВ БЕЗОПАСНОСТИ

Подсистема управления уязвимостями представляет собой комплекс организационно-технических мероприятий, направленных на предотвращение использования известных уязвимостей, потенциально существующих в защищаемой системе или сети. В частности, в рамках управления уязвимостями проводятся такие мероприятия, как периодический мониторинг защищенности информационных систем и устранение обнаруженных уязвимостей.

17.1. Управление уязвимостями

Контроль состояния защищенности относится к категории так называемых превентивных защитных механизмов, главное назначение которых —

своевременно «заметить» уязвимость в защищаемой системе и предотвратить возможные атаки.

Создать абсолютно защищенную систему принципиально невозможно. Согласно статистическим данным[1], число уязвимостей, обнаруживаемых ежегодно, составляет в среднем — 5 — 6 тыс.:

Число обнаруженных уязвимостей

2005	4 933
2006	6 608
2007	6 514
2008	5 632
2009	5 732
2012	4 639
2013	4 150
2014	5 289

И это только уязвимости реализации, а есть еще ошибки проектирования и эксплуатации.

В ходе контроля защищенности информационных систем приходится решать следующие основные з а д а ч и :

- инвентаризация информационных активов;
- оценка защищенности;
- контроль соблюдения требований политик и стандартов безопасности.

Средства анализа защищенности (так называемые сканеры безопасности — security scanners) помогают обнаруживать уязвимости на узлах корпоративной сети и своевременно устранять их (до того, как ими воспользуются злоумышленники).

Сканеры безопасности классифицируют по различным критериям.

17.2. Архитектура систем управления уязвимостями

Распределенная архитектура систем управления уязвимостями предполагает наличие как минимум двух типов к о м п о н е н т о в :

- агенты сканирования;
- компоненты управления.

Агенты сканирования в свою очередь могут быть классифицированы п о р а с п о л о ж е н и ю о т н о с и т е л ь н о о б ъ е к т а с к а н и р о в а н и я :

- *сетевые* (network-based) — выполняют проверки дистанционно, не требуя наличия агента на сканируемом узле;
- *локальные* (host-based) — устанавливают непосредственно на контролируемый узел, работают от имени учетной записи с максимальными привилегиями и все проверки выполняют локально;

[1] http://web.nvd.nist.gov

• *пассивные* (passive) — в качестве источника данных используют сетевой трафик, а выводы о наличии уязвимостей делаются на основе анализа сетевых взаимодействий (например, Passive Vulnerability Scanner от компании Tenable).

По назначению агенты сканирования подразделяют на:

• *специализированные* — применяются для сканирования таких систем, как СУБД, веб-приложения, ERP-системы и т. п. ;

• *общего назначения* — содержат проверки разных типов.

Например, в состав решения от компании eEye Digital Security (США) входят два агента сканирования: сканер общего назначения (Retina Network Security Scanner) и специализированный сканер для веб-приложений (Retina Web Security Scanner).

В составе решения от компании Safety. Lab (Россия) используется три типа агентов сканирования: сканер общего назначения (Shadow Security Scanner), сканер веб-приложений (Shadow Web Analyzer), сканер СУБД (Shadow Database Scanner).

В некоторых системах нет явного деления агентов сканирования по назначению (например, агент сканирования от компании Positive Technologies[1] (Россия) содержит различные сканирующие модули, в том числе модули анализа безопасности веб-приложений и СУБД).

17.3. Особенности сетевых агентов сканирования

Сетевые сканеры имеют следующие особенности:

• выполняют проверки дистанционно, т. е. по сети, что влияет как на скорость сканирования (сравните, например, удаленный подбор пароля и локальный), так и на достоверность результатов[2];

• используют разные методы для выявления одной и той же уязвимости (системные сканеры руководствуются только косвенными признаками наличия уязвимости (например, проверкой версий файлов);

• применяют различные учетные записи для подключения к службам сканируемого узла (системные сканеры, как правило, представляют собой сервис, работающий от имени учетной записи с максимальными привилегиями).

Проверки, выполняемые по сети, затрагивают не только сетевые сервисы, но и уровни приложений, сетевых служб, ОС, СУБД.

К наиболее известным программным продуктам для выполнения дистанционного анализа защищенности (network-based) относят:

• Nessus Security Scanner[3];

• Internet Scanner[4];

---

[1] http://www.ptsecurity.ru/mp_eval.asp

[2] В некоторых случаях получение результатов вообще невозможно, например нет доступа к ресурсу ADMINS — нет результата проверки.

[3] www.nessus.org

[4] www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php

• XSpider[1] и др.

Задача анализа защищенности на сетевом уровне — ответить на вопрос: «что нарушитель может сделать с узлом, получив доступ к нему по сети (удаленно)?» При этом попутно решаются задачи инвентаризации сетевого оборудования, обнаружения неизвестных устройств, идентификации сетевых служб и т. д.

Проверки (Check), выполняемые сканером безопасности, подразделяют на две категории:

• *выводы* (Inference) — проверки, выполняемые по косвенным признакам (без «участия» уязвимости);

• *тесты* (Test) — проверки, выполняемые путем проведения атаки в отношении узла (явное использование уязвимости).

При этом часть проверок второй категории может приводить к выведению из строя тестируемой службы (узла).

Наиболее очевидный способ поиска уязвимости — попытаться применить ее, т. е. сымитировать атаку, ее использующую, — такие проверки называют тестами. С другой стороны, наличие уязвимости в системе можно определить и по косвенным признакам, например по баннеру сканируемой службы или версии какого-либо файла — такие проверки называют инференцией, что означает умозаключение, вывод, сделаный на основе анализа полученных сообщений, поэтому результаты таких проверок (по косвенным признакам) весьма существенно зависят от результатов сбора информации (идентификация открытых портов, служб, приложений и т. д.). В некоторых сканерах существует возможность выбора способа выявления уязвимости (например, в сканере безопасности Nessus имеется режим «Safe checks», при включении которого все проверки выполняются по косвенным признакам).

В сканере базопасности Internet Scanner для выявления одной и той же уязвимости может быть предусмотрено две проверки: одна с реализацией атаки (например, проверка WinLsassBo), другая — по косвенным признакам (например, проверка WinMs04011).

Сетевые сканеры безопасности применяют для решения следующих задач:

1) *инвентаризация ресурсов сети*: узлов, сетевых служб, приложений. Инвентаризационное сканирование предоставляет обобщенную (базовую) информацию о сети. Параллельно решается задача обнаружения несанкционированно подключенных устройств;

2) *тестирование сети на устойчивость к взлому* — может осуществляться как внутри сети, так и снаружи. В последнем случае это часто называют анализом защищенности периметра. В процессе проведения такого исследования могут быть использованы и другие инструменты (сетевые анализаторы, «троянцы», «руткиты» и пр.), но сканеры уязвимостей, как правило, используются всегда[2];

---

[1] http://www.ptsecurity.ru/xs7.asp

[2] Для проведения такого тестирования рекомендуется использовать два сканера безопасности.

3) *аудит безопасности сети* или отдельных ее областей на соответствие заданным требованиям — осуществляется периодически в целях, например, проверки правильности и своевременности установки обновлений.

Для решения второй задачи, как правило, привлекаются сторонние организации, а первую и третью задачи выполняют обычно собственными силами.

17.4. Средства анализа защищенности системного уровня

Сканеры системного уровня выполняют поиск уязвимостей более тщательно и достоверно по сравнению с сетевыми сканерами, поскольку установлены на сканируемом узле и работают от имени учетной записи с максимальными привилегиями (root, SYSTEM).

Сканеры уровня узла помимо проверок, аналогичных проводимым сетевыми сканерами (например, поиск работающих на узле устройств, таких как модемы, обнаружение установленных на узле приложений или контроль режима работы сетевого адаптера — селективный или неселективный), выполняют проверки, которые невозможно или сложно осуществить с использованием сетевых сканеров (например, оценка стойкости паролей, контроль целостности, анализ журналов ОС и приложений для поиска следов нарушителя).

Средства сканирования на уровне узла используются для защиты наиболее важных серверов: почтовых, веб, удаленного доступа, управления базами данных. Эти узлы нередко содержат наиболее критичные данные для ведения бизнеса, и сканирование на системном уровне помогает обнаружить уязвимости высокой степени риска и предоставить администратору информацию для устранения найденных проблем. Сканирование на системном уровне применяется и при защите межсетевых экранов, которые содержат известные уязвимости и конфигурации, установленные по умолчанию.

Сканеры уровня узла имеют обычно распределенную архитектуру состоящую из агентов, расставленных на защищаемых узлах, и консоли, контролирующей работу агентов и осуществляющей сбор данных от них.

Перечислим и с т о ч н и к и д а н н ы х для сканеров уровня узла:

• *файловая система узла* — нередко признаком наличия уязвимости считается номер версии того или иного файла. Кроме того, изменения некоторых важных файлов могут служить признаками следов нарушителя;

• *журналы регистрации*;

• *конфигурация, параметры, влияющие на безопасность*, — для ОС Windows основной источник таких данных — реестр. К этой же категории относится информация о пользователях, работающих на узле, службах, установленных приложениях.

Таким образом, проверки, выполняемые на системном уровне, осуществляют поиск уязвимостей следующим образом:

• сравнением версий файлов или их атрибутов с имеющимися значениями в базе данных проверок;

• поиском файлов или ключей реестра, свидетельствующих о наличии в узле того или иного приложения (вируса и т. п.);

• сравнением текущих значений параметров конфигурации с требуемыми значениями (в этом случае пользователь должен задать эти значения, которые обычно являются частью политики безопасности).

* * *

Для обнаружения и устранения уязвимостей применяют сканеры безопасности сетевого и системного уровня, грань между которыми весьма тонка (многие проверки, выполняемые сетевыми сканерами, доступны системным сканерам).

Сканеры уровня узла используют только пассивные методы идентификации уязвимостей, поскольку их, как правило, устанавливают на важном сервере и они должны оказывать на него минимальное влияние.

Контрольные вопросы

1. В чем особенности распределенной архитектуры систем управления уязвимостями?
2. Какие задачи могут быть решены сетевым сканером безопасности?
3. Перечислите типы проверок, используемых в сетевых сканерах безопасности
4. Какую дополнительную критичную информацию может получить злоумышленник в результате сканирования портов?
5. Какая причина затрудняет использование в организациях сетевых сканеров безопасности?

Глава 18. МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ

Среди многочисленных перечисленных ранее механизмов защиты имеются два, которые направлены на выявление случаев удачных и неудачных попыток нарушений безопасности, т. е. относящихся к категории «детективных» (позволяющих как можно более оперативно зафиксировать факт атаки):

• регистрация и оперативное оповещение о событиях безопасности;

• обнаружение атак.

И в том, и другом случае накапливается информация о событиях безопасности, анализ которой позволяет выявить факты совершения нарушений, характер воздействий на систему, определить степень нарушения, метод расследования, способы поиска нарушителя и исправления ситуации.

18.1. Введение в управление журналами событий

Регистрация событий безопасности обычно предполагает их размещение в каком-либо журнале.

Обычно *журнал событий* (лог, log) — это совокупность записей (entries), каждая из которых содержит информацию, относящуюся к отдельному событию, которое произошло с системой или сетью.

Изначально механизм ведения логов служил для выявления причин сбоев, однако в настоящее время его роль может быть различной. Здесь рассмотрим этот механизм с точки зрения безопасности как средство, предоставляющее данные для последующего изучения подозрительной активности пользователей.

Один из аспектов ведения журналов состоит в их многообразии, которое породило понятие управления журналами событий (computer security log management). В это понятие вкладывается процесс создания (генерации) лог-файлов, их передачи, хранения, а также последующего анализа.

18.2. Категории журналов событий

В контексте безопасности наибольший интерес обычно представляют две категории журналов событий:

1) журналы средств защиты — результат работы средств защиты уровня сети или отдельного узла межсетевых экранов, средств противодействия вредоносному коду, систем обнаружения и предотвращения атак, систем управления уязвимостями, серверов аутентификации и контроля доступа к сети;

2) журналы операционных систем, приложений и СУБД — системные события (например, запуск или выключение системы), события аудита (например, доступ к файлам, вход в систему и т. п.), события, связанные с работой приведенных средств защиты и таких приложений, как веб-серверы, шлюзы VPN, почтовые серверы и т. п.

18.3. Инфраструктура управления журналами событий

Ведение журналов характеризуется многообразием как их источников, так и форматов, что значительно усложняет задачу управления ими, но тем не менее, следует придерживаться определенных р е к о м е н д а ц и й :

- выделить наиболее важные и приоритетные задачи по регистрации событий;
- разработать политику в отношении лог-файлов;
- создать и поддерживать инфраструктуру управления лог-файлами;
- поддерживать на необходимом уровне квалификацию персонала, участвующего в процессе управления лог-файлами.

Инфраструктура управления журналами событий включает в себя аппаратное и программное обеспечение, используемое для генерации, передачи, хранения, анализа и накопления помещаемых в журналы данных. В данной инфраструктуре выделяют три у р о в н я :

1) генерация журналов;

2) объединение и централизованное хранение;

3) централизованный анализ.

Инфраструктура управления выполняет следующие основные ф у н к ц и и :

• *фильтрацию* событий по различным критериям;

• *объединение* событий;

• *нормализацию* (приведение к единому формату);

• *корреляцию*.

Кроме перечисленных основных функций, инфраструктура управления журналами событий предоставляет дополнительные возможности, облегчающие анализ собранных данных:

• *парсинг журналов* (Log Parsing) — обработка данных, обычно сопровождаемая преобразованием из одного формата в другой (например, из XML в текстовый);

• *просмотр журналов* (Log Viewing) — отображение записанных в журнал данных в удобном для восприятия формате;

• *анализ* (Log Analysis) — поиск в журналах наиболее значимых событий или событий, отвечающих определенным требованиям (этот поиск обычно выполняется средствами защиты, например, системами обнаружения атак уровня узла);

• *ротацию* (Log Rotation) — смена журналов, например закрытие заполненного журнала и открытие нового;

• *архивирование* (Log Archival);

• *уменьшение* (Log Reduction), т. е. оптимизацию — удаление из журналов лишних записей;

• *чистку* (Log Clearing);

• *контроль целостности* (Log File Integrity Checking).

Выделяют два в а р и а н т а инфраструктуры управления журналами событий:

• на основе протокола syslog (syslog-based);

• специализированного программного обеспечения (Security event management software, SEM).

Протокол syslog. В случае инфраструктуры на основе протокола syslog процесс генерации журналов выполняется одинаковым образом в одном формате. Помимо передачи данных, подлежащих журналированию, на сервер, источник событий обычно сохраняет их и у себя (локально).

Протокол syslog это, прежде всего, механизм передачи логов от отдельных узлов на сервер (в место их централизованного хранения). Однако syslog, по сути дела, представляет собой стандартизованный механизм генерации, передачи и хранения событий от различных источников.

К достоинствам построения инфраструктуры управления журналами событий на основе протокола syslog относят простоту реализации и большой выбор программного обеспечения, реализующего необходимый функционал; к недостаткам — ограниченность числа источников, отсутствие аутентификации источника сообщения; возможные нарушения последовательности доставки сообщений, целостности, повторная пересылка (replay), отправка некорректных сообщений.

Инфраструктура «SEM». По сравнению с инфраструктурой syslog-based, SEM — относительно новый способ управления журналами событий.

Обязательный элемент данной инфраструктуры — сервер анализа и обработки данных. Журналы сохраняются в базе данных на сервере хранения. Обычно такая инфраструктура предполагает наличие агентов на каждом источнике журналов, но возможна архитектура и без агентов — в этом случае сервер самостоятельно подключается к источникам журналов и переписывает их.

Независимо от способа получения журналов, сервер SEM выполняет анализ событий, корреляцию, помогает выделить наиболее значимые события и обычно поддерживает различные механизмы реагирования (см. п. 18.5).

Продукты SEM имеют следующие возможности:

- графический интерфейс;
- настраиваемая база сигнатур;
- средства управления инцидентами;
- корреляция.

В сфере продуктов SEM отсутствуют какие-либо стандарты, поэтому каждый разработчик использует собственные форматы данных и протоколы взаимодействия.

Дополнительные компоненты инфраструктуры управления журналами. В процессе управления журналами событий может оказаться полезным программное обеспечение, реализующее следующие функции:

- *сбор данных и анализ сетевого трафика* — помимо традиционных сетевых систем обнаружения атак (Network Intrusion Detection Systems, NIDS) трафик может быть получен и с межсетевых экранов, а также серверов аутентификации;
- *обнаружение атак уровня узла* — помимо анализа трафика защищаемого узла, выполняют контроль запускаемых приложений, осуществляют антивирусную защиту и т. п.;
- *дополнительные утилиты и инструменты* — инструменты визуализации данных, утилиты ротации, конвертирования.

18.4. Введение в технологию обнаружения атак

Обнаружением атак называют процесс идентификации и реагирования на подозрительную деятельность, направленную на вычислительные ресурсы.

Системы обнаружения атак (Intrusion Detection Systems, IDS) предназначены для своевременного выявления факта нарушения и реагирования на него. Технология обнаружения атак может быть использована либо как часть инфраструктуры мониторинга событий, либо как самостоятельный механизм защиты.

Необходимость использования данной технологии может быть проиллюстрирована следующими примерами.

Ситуация 1. Затруднено или невозможно обращение к расположенному в ДМЗ веб-серверу компании.

Причиной такой ситуации может быть успешно проведенная DDoS-атака с одной из так называемых бот-сетей (ботнетов — от англ. *botnet*), которые распространяют спам, содержащий вредные вложения.

Ситуация 2. Резкий рост нагрузки на межсетевой экран.

Причиной ситуации может быть использование популярных в настоящее время P2P-сетей — файлообменных сетей.

Алгоритм (технология) обнаружения атак имеет три составляющие:

1) признаки атак (понимание ожидаемого поведения контролируемого объекта, знание возможных атак и их модификаций);

2) источники информации об атаках (сетевой график, журналы, действия субъектов и т. д.);

3) механизмы реагирования (оповещение, блокировка, вызов внешней программы и др.).

Рассмотрим механизмы реагирования более подробно.

Возможны следующие варианты оповещения:

- звуковой сигнал;
- электронная почта;
- телефон;
- консоль управления;
- система сетевого управления.

Блокировка предполагает «активное вмешательство» системы обнаружения атак и может быть выполнена следующими способами:

- аварийное завершение TCP-соединения;
- посылка ICMP Destination Unreachable для блокировки взаимодействия по протоколу UDP;
- блокировка трафика, содержащего признаки атак;
- карантин.

Механизм блокировки «превращает» систему обнаружения атак в систему противодействия атакам, что накладывает дополнительные требования:

- сценарий действий в случае выхода из строя для Network IPS;
- наличие «мягкого» режима;
- отсутствие влияния на производительность;
- качество сигнатур, минимизация ложных срабатываний;
- понимание ожидаемого поведения контролируемого объекта, знание возможных атак и модификаций.

18.5. Классификация систем обнаружения атак

Существует несколько вариантов классификации систем обнаружения атак.

Классификация по источнику данных (по принципу реализации) показывает, что именно защищает система обнаружения атак. Исполнение подобных систем возможно в двух вариантах:

- на базе сетевого сегмента (Network-based) — системы, анализирующей трафик сетевого сегмента (подобно сетевому анализатору) в целях поиска

признаков атак. К данному виду относится бóльшая часть систем обнаружения атак;

• на базе узла (host-based) — системы, ориентированной на защиту отдельного узла (в некоторых случаях удобнее поместить систему обнаружения атак непосредственно на защищаемом узле). Входными данными для таких систем являются журналы регистрации и действий пользователей защищаемого узла.

Классификация по технологии обнаружения показывает, произошла атака или нет:

• обнаружение злоупотреблений (Misuse Detection) — известен перечень атак;

• обнаружение аномалий (Anomaly Detection) — известно поведение контролируемого объекта и любое отклонение считается атакой.

Данными для построения *профиля поведения* могут служить:

• объемы трафика;

• отношения между узлами и группами узлов;

• архив потоков данных.

* * *

В журналах фиксируются события, которые происходят на уровне операционной системы или отдельного приложения с различными сетевыми устройствами. Многообразие журналов требует управления ими. Инфраструктура управления журналами реализует дополнительные функции, связанные с обнаружением атак на систему по различным признакам. Методы анализа информации об атаках позволяют использовать разнообразные механизмы реагирования, такие как оповещение, блокировка и др.

Контрольные вопросы

1. Дайте определение инфраструктуры управления журналами событий.
2. Перечислите категории журналов событий.
3. Дайте характеристику протоколов syslog и SEM.
4. Опишите классификационные схемы систем обнаружения атак.
5. Какие механизмы реагирования на атаки вам известны?

ГЛОССАРИЙ

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

Авторизация – предоставление аутентифицированному субъекту соответствующих (предписанных установленным порядком) прав на доступ к объектам системы: какие данные и как он может использовать (какие операции с ними осуществлять), какие программы может выполнять, когда, как долго и с каких терминалов может работать, какие ресурсы системы может использовать и т. п.

Авторизованный субъект доступа – субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

Аппаратные шифровальные (криптографические) средства — устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин.

Аттестация объектов информатизации — комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных уполномоченными федеральными органами исполнительной власти.

Аутентификация — проверка (подтверждение) подлинности идентификации субъекта или объекта системы.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Владелец сертификата ключа проверки электронной подписи — лицо, которому в установленном законом порядке выдан сертификат ключа проверки электронной подписи.

Доступ к информации — ознакомление с информацией (чтение, копирование, модификация (корректировка), уничтожение (удаление) и т. п.).

Доступ к ресурсу — получение субъектом возможности манипулировать данным ресурсом (использовать, управлять, изменять настройки и т. п.).

Журнал событий (лог, log) — объект (например, файл), содержащий перечень событий, произошедших с различными активами организации (с системами или сетями).

Идентификация — это, с одной стороны, присвоение индивидуальных имен, номеров (идентификаторов) субъектам и объектам системы, а с другой — их распознавание (опознавание) по присвоенным им уникальным идентификаторам.

Демилитаризованная зона (ДМЗ) (англ. Demitlitarized Zone (DMZ)) — сегмент сети, который содержит общедоступные сервисы и отделяет их от частных. Служит для повышения уровня безопасности в локальной сети и минимизации ущерба в случае атаки злоумышленника.

Документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная корпоративная система — информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Информационная система общего пользования — информационная система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные технологии (ИТ) — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация — сведения (сообщения, данные) независимо от формы их представления.

Информация, составляющая коммерческую тайну, — сведения любого характера (производственные, технические, экономические, организационные

и др.), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Квалифицированный сертификат ключа проверки электронной подписи – сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

Ключ электронной подписи — уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключевые документы — электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах.

Коммерческая тайна — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Криптографическое преобразование — преобразование информации, основанное на некотором алгоритме, зависящем от изменяемого параметра (обычно называемого секретным ключом) и обладающее свойством невозможности восстановления исходной информации по преобразованной без знания действующего ключа, с трудоемкостью меньше заранее заданной.

Лицензия — специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности (выполнения работ, оказания услуг, составляющих лицензируемый вид деятельности), которое подтверждается документом, выданным лицензирующим органом на бумажном носителе или в форме электронного документа, подписанного электронной подписью, в случае, если в заявлении о предоставлении лицензии указывалось на необходимость выдачи такого документа в форме электронного документа.

Маршрутизатор (англ. *router*) — сетевой компьютер, который имеет два или более сетевых интерфейсов и пересылает пакеты данных между различными сегментами сети. Выполняет логистические и охранные функции.

Межсетевой экран (англ. *firewall*) — шлюз (gateway), разделяющий несколько сетевых сегментов и ограничивающий прохождение сетевого трафика к (от) одному (го) из них (говорят, что он расположен за МЭ, «inside») и таким образом защищающий его ресурсы от угроз, исходящих от других подключенных сегментов (расположенных перед МЭ, «outside»).

Несанкционированный доступ (НСД) — доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Обладатель информации, составляющей коммерческую тайну, — лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании ограничило доступ к этой информации и установило в отношении нее режим коммерческой тайны.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Объект — пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т. п.), доступ к которому регламентируется правилами разграничения доступа.

Оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Патч (от англ. *patch* — заплатка) — информация, предназначенная для автоматизированного внесения определенных изменений (обновлений) в компьютерные файлы. Размер патчей составляет от нескольких килобайт до сотен мегабайт. Патч больших объемов называют Service park.

Персональные данные — любая информация, относящаяся прямо или косвенно к определенному физическому лицу (субъекту персональных данных).

Посредник (proxy) — узел, выполняющий запрос на установление соединения по инициативе другого узла.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

Предоставление информации — действия, направленные на получение или передачу информации определенному кругу лиц.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или кругу лиц.

Программно-аппаратные шифровальные (криптографические) средства — устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для ЭВМ, предназначенных для осуществления этих преобразований информации или их части.

Программные шифровальные (криптографические) средства — программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств.

Разглашение информации, составляющей коммерческую тайну, – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Разграничение доступа к ресурсам АС — порядок использования ресурсов автоматизированной системы, при котором субъекты получают доступ к объектам системы в строгом соответствии с установленными правилами.

Распространение информации – действия, направленные на получение или передачу информации неопределенному кругу лиц.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Сертификация — форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие при-

надлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат соответствия — документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Средства защиты информации (СЗИ) — технические, криптографические, программные и другие средства, предназначенные для защиты сведений конфиденциального характера, а также средства контроля эффективности защиты информации.

Средства изготовления ключевых документов — аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств.

Средства имитозащиты — аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации.

Средства кодирования — средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций.

Средства шифрования — аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче.

Средства электронной подписи — шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Субъект — активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.

Технический регламент — документ, который принят международным договором Российской Федерации, ратифицирован в порядке, установленном законодательством Российской Федерации, или межправительственным соглашением, заключенным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президен-

та Российской Федерации, или постановлением Правительства Российской Федерации, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию, и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям или к связанным с требованиями к продукции процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации).

Трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Удостоверяющий центр — юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей.

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Электронная подпись — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

ЛИТЕРАТУРА

Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум. М.: КноРус, 2013. 136 с.

Будаковский Д.С. Способы совершения преступлений в сфере компьютерной информации // Российский следователь. 2011. № 4.

Волков П.П. Экспертный анализ методов защиты информации от утечки по техническим каналам // Эксперт-криминалист. 2009. № 4.

Воронцова С.В. Киберпреступность: проблемы квалификации преступных деяний. Российская юстиция. 2011. № 2.

Воротников В.Л. О правовой защите компьютерной информации // Администратор суда. 2009. № 2.

Гафнер В.В. Информационная безопасность. Ростов н/Д: Феникс, 2012. 324 с.

Громов Ю.Ю., Драчев В.О., Иванова О.Г. Информационная безопасность и защита информации. Ст. Оскол: ТНТ, 2013. 384 с.

Забегайло Л.А., Назарова И.А. Актуальные вопросы охраны коммерческой тайны в отношениях с органами государства // Современное право. 2011. № 7.

Загузов Г.В. Административно-правовые средства обеспечения информационной безопасности и защиты информации в Российской Федерации // Административное и муниципальное право. 2010. № 5.

Кузнецова Т.В. Организация работы с персональными данными // Трудовое право. 2011. № 5.

Маркарьян Р.В. Об основных направлениях совершенствования законодательства о развитии Интернета в Российской Федерации // Международное публичное и частное право. 2011. № 4.

Палехова Е.А. Конфиденциальная информация и институт персональных данных в банковской деятельности // Предпринимательское право. 2010. № 3.

Партыка Т.Л., Попов И.И. Информационная безопасность. М.: Форум, 2012. 432 с.

Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи. 2006. 400 с.

Петров С.В., Слинькова И.П., Гафнер В.В. Информационная безопасность. АРТА, 2012. 296 с.

Савчишкин Д.Б. Административная ответственность как средство обеспечения информационной безопасности // Административное и муниципальное право. 2011. № 6.

Семененко В.А. Информационная безопасность. М. 2010. 277 с.

Станскова У.М. Правовой анализ локальных нормативных актов работодателя по защите информации ограниченного доступа // Трудовое право в России и за рубежом. 2011. № 2.

Терещенко Л.К. О соблюдении баланса интересов при установлении мер защиты персональных данных // Журн. российского права. 2011. № 5.

Чеботарева А.А. Электронное государственное управление как новая форма взаимоотношений личности, общества и государства // Государственная власть и местное самоуправление. 2011. № 6.

Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: ИД «ФОРУМ, ИНФРА-М», 2013. 416 с.

Ярочкин В.И. Информационная безопасность. М.: Акад. Проект, Гаудеамус, 2008. 544 с.

[Электронный ресурс] Internet Security Glossary, Version 2 (http://www.ietf.org/rfc/rfc4949.txt)

[Электронный ресурс] Benchmarking Terminology for Firewall Performance (http://www.ietf.org/rfc/rfc2647.txt)

[Электронный ресурс] Behavior of and Requirements for Internet Firewalls (http://www.ietf.org/rfc/rfc2979.txt)

[Электронный ресурс] http://aluigi.altervista.org/adv/termdd_1-adv.txt

ПРИЛОЖЕНИЕ

НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные законы

Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.).

О Декларации прав и свобод человека и гражданина (принята Постановлением Верховного Совета РСФСР от 22 ноября 1991 № 1920-1).

Доктрина информационной безопасности Российской Федерации» (утв. Президентом РФ 09 сентября 2000 г. №Пр-1895).

Уголовный кодекс Российской Федерации (принят Федеральным законом от 13 июня 1996 г. № 63-ФЗ).

Кодекс Российской Федерации об административных правонарушениях (принят Федеральным законом от 30 декабря 2001 г. №195-ФЗ).

Гражданский кодекс Российской Федерации (принят Федеральным законом от 18 декабря 2006 г. № 230-ФЗ).

Трудовой кодекс Российской Федерации (принят Федеральным законом от 30 декабря 2001 г. № 197-ФЗ).

Воздушный кодекс Российской Федерации (принят Федеральным законом от 19 марта 1997 г. № 60-ФЗ).

Федеральные законы

Закон Российской Федерации от 02 декабря 1990 г. № 395-1 «О банках и банковской деятельности».

Закон Российской Федерации «Об организации страхового дела в Российской Федерации» от 27 ноября 1992 г. № 4015-I.

Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1.

Федеральный закон «О Федеральной службе безопасности» от 03 апреля 1995 г. № 40-ФЗ .

Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. №144-ФЗ.

Федеральный закон «О техническом регулировании» от 27 декабря 2002 г. № 184-ФЗ.

Федеральный закон «О связи» от 07 июля 2003 г. № 126-ФЗ .

Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ.

Федеральный закон «О государственной гражданской службе Российской Федерации» от 27 июля 2004 г. № 79-ФЗ.

Федеральный закон «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 19 декабря 2005 г. № 160-ФЗ.

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ .

Федеральный закон «О муниципальной службе в Российской Федерации» от 02 марта 2007 г. № 25-ФЗ. (Ст. 29. Персональные данные муниципального служащего).

Федеральный закон «О безопасности» от 28 декабря 2010 г. № 390-ФЗ .

Федеральный закон «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ.

Федеральный закон «О лицензировании отдельных видов деятельности» от 04 мая 2011 г. № 99-ФЗ .

Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации» от 11 июля 2011 г. № 200-ФЗ.

Федеральный закон «О бухгалтерском учете» от 06 декабря 2011 г. № 402-ФЗ.

Федеральный закон «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации и отдельные законодательные акты Российской Федерации» от 12 марта 2014 г. № 35-ФЗ.

Указы Президента Российской Федерации

Указ Президента Российской Федерации от 03 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации (с изм. Указа Президента Российской Федерации от 25 июля 2000 г. № 1358)».

Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изм. от 23 сентября 2005 г. № 1111).

Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

Указ Президента Российской Федерации от 30 мая 2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела».

Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».

Постановления Правительства Российской Федерации

Постановление Правительства РСФСР от 05 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

Постановление Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» (Извлечения).

Постановление Правительства Российской Федерации от 03 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации».

Постановление Правительства Российской Федерации от 06 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Постановление Правительства Российской Федерации от 16 марта 2009 г. № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

Постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

Постановление Правительства Российской Федерации от 04 марта 2010 г. № 125 «О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию».

Постановление Правительства Российской Федерации от 21 апреля 2010 г. № 266 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации».

Постановление Правительства Российской Федерации от 15 мая 2010 г. № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг)».

Постановление Правительства Российской Федерации от 03 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

Постановление Правительства Российской Федерации от 03 марта 2012 г. № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации».

Постановление Правительства Российской Федерации от 21 марта 2012 г. №211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением

случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Иные информативные акты

Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 25.11.1994).

Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 27.10.1995, приказ № 199).

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (утв. Государственной технической комиссией при Президенте РФ от 30.08.2002, приказом № 282).

Методические рекомендации управлениям ФСТЭК России по федеральным округам об организации работ по аттестации объектов информатизации по требованиям безопасности информации (утв. ФСТЭК России 25.04. 2006).

Методические рекомендации по технической защите информации, составляющей коммерческую тайну (утв. ФСТЭК России 25.12.2006).

Пособие по организации технической защиты информации, составляющей коммерческую тайну (утв. ФСТЭК России 25.12.2006).

Методические документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007 и 19.11.2007).

Руководящие документы

Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения (утв. председателем Гостехкомиссии России от 30.03.1992).

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации (утв. председателем Гостехкомиссии России от 30.03.1992).

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утв. председателем Гостехкомиссии России от 30.03.1992).

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (утв. председателем Гостехкомиссии России от 30.03.1992).

Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники (утв. председателем Гостехкомиссии России от 30.03.1992).

Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации (утв. председателем Гостехкомиссии России от 25.07.1997).

Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования (утв. председателем Гостехкомиссии России от 25.07.1997).

Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей (утв. приказом председателя Гостехкомиссии России от 04.06.1999 № 114).

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (утв. Приказом Гостехкомиссии России от 19.06.2002 № 187).

Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05. 2007).

Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007).

Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007).

Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 19.11.2007).

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 14.02.2008).

Ведомственные приказы

Об утверждении Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (Приказ ФСБ России от 21.02.2008 № 149/54-144).

Об утверждении типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, со-

ставляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСБ России от 21.02. 2008. № 149/6/6-622).

Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну (Приказ ФАПСИ России от 13.06.2001 № 152).

Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Приказ ФСБ России от 09.02.2005 № 66).

Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Приказ ФСТЭК России от 18.02.2013 № 21).

Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (Приказ ФСТЭК России от 11.02.2013 № 17).

Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности (Приказ ФСБ России от 10.07.2014 № 378).

Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (Приказ ФСТЭК России от 14.03.2014 № 31).

Национальные и международные стандарты

ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

ГОСТ 29099–91. Сети вычислительные локальные. Термины и определения.

ГОСТ Р 34.11–94. Информационная технология. Криптографическая защита информации. Функция хеширования.

ГОСТ 30373–95/ГОСТ 50414-92. Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний.

ГОСТ Р 50739–95. Средства вычислительной техники. Защита от НСД к информации. Общие технические требования.

ГОСТ Р 50752–95. Информационная технология. Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний.

ISO/IEC 27001–2005 (2013). Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.

ISO/IEC 27002–2005 (2012). Информационные технологии. Методы обеспечения безопасности. Практическое руководство по управлению информационной безопасностью.

ГОСТ Р В50170–2005. Противодействие иностранной технической разведке. Термины и определения.

ГОСТ Р 50922–2006. Защита информации. Основные термины и определения.

ГОСТ Р 51275–2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Требования.

ISO/IEC 27006–2007. Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью.

ГОСТ Р ИСО/МЭК 27006–2008. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27005–2010. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

ГОСТ Р ИСО/МЭК 27004–2011. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

ГОСТ Р 34.10–2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

ГОСТ Р ИСО/МЭК 15408-1–2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий: в 3. Ч. 1. Введение и общая модель.

ГОСТ Р ИСО/МЭК 27002–2012. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

ГОСТ Р ИСО/МЭК 27003–2012. Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 15408-2–2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий: в 3. Ч. 2. Функциональные компоненты безопасности.

ГОСТ Р ИСО/МЭК 15408-3–2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий: в 3. Ч. 3. Компоненты доверия к безопасности.

ОГЛАВЛЕНИЕ

Предисловие 3

Р а з д е л I. Основы безопасности автоматизированных систем 5
Глава 1. Актуальность проблемы обеспечения безопасности автоматизированных систем 5
1.1. Место и роль автоматизированных систем в управлении бизнес-процессами 5
1.2. Обострение проблемы обеспечения безопасности автоматизированных систем на современном этапе 6
1.3. Защита автоматизированных систем как процесс управления рисками 9
1.4. Методы оценки целесообразности затрат на обеспечение безопасности 10
1.5. Особенности современных автоматизированных систем как объектов защиты 13
Глава 2. Основные понятия в области безопасности автоматизированных систем 15
2.1. Определение безопасности автоматизированных систем 15
2.2. Информация и информационные ресурсы 16
2.3. Субъекты информационных отношений, их безопасность 17
2.4. Цель защиты автоматизированной системы и циркулирующей в ней информации 19
Глава 3. Угрозы безопасности автоматизированных систем 20
3.1. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем 20
3.2. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений 22
3.3. Классификация угроз безопасности 24
3.4. Классификация каналов проникновения в автоматизированную систему и утечки информации 27
3.5. Неформальная модель нарушителя 28
Глава 4. Меры и основные принципы обеспечения безопасности автоматизированных систем 33
4.1. Виды мер противодействия угрозам безопасности 33
4.2. Принципы построения системы обеспечения безопасности информации в автоматизированной системе 35

Глава 5. Правовые основы обеспечения безопасности автоматизированных систем 39
5.1. Защищаемая информация 41
5.2. Лицензирование 52
5.3. Сертификация средств защиты информации и аттестация объектов информатизации 57
5.4. Специальные требования и рекомендации по технической защите конфиденциальной информации 68
5.5. Юридическая значимость электронных документов с электронной подписью 69
5.6. Ответственность за нарушения в сфере защиты информации 71
Глава 6. Государственная система защиты информации 77
6.1. Главные направления работ по защите информации 77
6.2. Структура государственной системы защиты информации 78
6.3. Организация защиты информации в системах и средствах информатизации и связи 81
6.4. Контроль состояния защиты информации 83
6.5. Финансирование мероприятий по защите информации 84

Р а з д е л II. Обеспечение безопасности автоматизированных систем 85
Глава 7. Организационная структура системы обеспечения безопасности автоматизированных систем 85
7.1. Технология управления безопасностью информации и ресурсов в автоматизированной системе 85
7.2. Институт ответственных за обеспечение информационной безопасности 87
7.3. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы 90
7.4. Политика безопасности организации 91
7.5. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты 93
7.6. Распределение функций по обеспечению безопасности автоматизированных систем 95
7.7. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем 96
Глава 8. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях 98
8.1. Проблема человеческого фактора 99
8.2. Общие правила обеспечения безопасности 99
8.3. Обязанности ответственного за обеспечение безопасности информации в подразделении 100
8.4. Ответственность за нарушения требований обеспечения безопасности 101
8.5. Порядок работы с носителями ключевой информации 102

Глава 9. Регламентация работ по обеспечению безопасности автоматизированных систем 106
9.1. Регламентация правил парольной и антивирусной защиты 107
9.2. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы 110
9.3. Регламентация порядка изменения конфигурации аппаратно-программных средств автоматизированной системы 112
9.4. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач 117
Глава 10. Категорирование и документирование защищаемых ресурсов 121
10.1. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов 121
10.2. Категорирование защищаемых ресурсов 123
10.3. Проведение информационных обследований и документирование защищаемых ресурсов 126
Глава 11. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем автоматизированной системы 128
11.1. Концепция информационной безопасности организации 129
11.2. План защиты информации 130
11.3. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы 131

Раздел III. Средства защиты информации от несанкционированного доступа 138
Глава 12. Назначение и возможности средств защиты информации от несанкционированного доступа 138
12.1. Основные механизмы защиты автоматизированных систем 138
12.2. Защита периметра компьютерных сетей и управление механизмами защиты 151
12.3. Страхование информационных рисков 153
Глава 13. Аппаратно-программные средства защиты информации от несанкционированного доступа 156
13.1. Рекомендации по выбору средств защиты информации от несанкционированного доступа 156
13.2. Обзор существующих на рынке средств защиты информации от несанкционированного доступа 159
13.3. Средства аппаратной поддержки 166
13.4. Способы аутентификации 167
Глава 14. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа 176
14.1. Стратегия безопасности Microsoft 177
14.2. Защита от вмешательства в процесс нормального функционирования автоматизированной системы 177

14.3. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы 179
14.4. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа 185
14.5. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования 187

Раздел IV. Обеспечение безопасности компьютерных сетей 189
Глава 15. Проблемы обеспечения безопасности в компьютерных сетях 189
15.1. Типовая корпоративная сеть 189
15.2. Уровни информационной инфраструктуры корпоративной сети 190
15.3. Уязвимости и их классификация 190
15.4. Классификация атак 198
15.5. Средства защиты сетей 203
Глава 16. Защита периметра корпоративной сети 204
16.1. Угрозы, связанные с периметром корпоративной сети 205
16.2. Составляющие защиты периметра 206
16.3. Межсетевые экраны 207
16.4. Анализ содержимого почтового и веб-трафика 215
16.5. Виртуальные частные сети 216
Глава 17. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности 219
17.1. Управление уязвимостями 219
17.2. Архитектура систем управления уязвимостями 220
17.3. Особенности сетевых агентов сканирования 221
17.4. Средства анализа защищенности системного уровня 223
Глава 18. Мониторинг событий безопасности 224
18.1. Введение в управление журналами событий 224
18.2. Категории журналов событий 225
18.3. Инфраструктура управления журналами событий 225
18.4. Введение в технологию обнаружения атак 227
18.5. Классификация систем обнаружения атак 228
Глоссарий 230
Литература 237
Приложение. Нормативно-правовое обеспечение информационной безопасности 239

Учебное издание

Бондарев Валерий Васильевич

Введение в информационную безопасность автоматизированных систем

Редактор *Л.В. Честная*
Технический редактор *Э.А. Кулакова*
Художник *Я.М. Ильина*
Корректор *Ю.Н. Морозова*
Компьютерная графика *Т.Ю. Кутузовой*
Компьютерная верстка *Е.В. Ляшкевич*

В оформлении использованы шрифты
Студии Артемия Лебедева.

Оригинал-макет подготовлен
в Издательстве МГТУ им. Н.Э. Баумана.

Подписано в печать 12.05.2016. Формат 70×100/16.
Усл. печ. л. 15,75. Тираж 50 экз. Изд. № 523-2015. Заказ

Издательство МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская ул., д. 5, стр. 1.
press@bmstu.ru
www.baumanpress.ru

Отпечатано в типографии МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская ул., д. 5, стр. 1.
baumanprint@gmail.com