Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина
Институт радиоэлектроники и информационных технологий — РТФ

Е. В. ВОСТРЕЦОВА

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Министерство науки и высшего образования
Российской Федерации
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина

Е. В. Вострецова

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Рекомендовано методическим советом
Уральского федерального университета
для студентов вуза, обучающихся
по укрупненной группе направлений
бакалавриата и специалитета
10.00.00 «Информационная безопасность»

Екатеринбург
Издательство Уральского университета
2019

УДК 004.056.5(075.8)
ББК 32.972.53я73
В78

Рецензенты:
канд. пед. наук, доц. Е. Н. Полякова, завкафедрой «Безопасность информационных и автоматизированных систем» ФГБОУ ВО «Курганский государственный университет»;
канд. техн. наук, доц. Т. Ю. Зырянова, завкафедрой «Информационные технологии и защита информации» ФГБОУ ВО «Уральский государственный университет путей сообщения»

На обложке изображение с сайта https://www.itsecurityguru.org/2017/01/26/despite-rise-breaches-companies-still-prioritising-network-endpoint-solutions-encryption/

Вострецова, Е. В.
В78 Основы информационной безопасности : учебное пособие для студентов вузов / Е. В. Вострецова. — Екатеринбург : Изд-во Урал. ун-та, 2019. — 204 с.

ISBN 978-5-7996-2677-8

Учебное пособие по курсу «Основы информационной безопасности» предназначено для студентов укрупненной группы направлений и специальностей 10.00.00 «Информационная безопасность» уровней бакалавриат и специалитет.

В пособии рассмотрены свойства информации как объекта защиты, определены закономерности создания защищённых информационных систем, раскрыты принципы обеспечения информационной безопасности государства, уделено внимание информационным войнам и информационному противоборству. Дан краткий анализ моделей и политики безопасности (разграничения доступа), а также международных стандартов в области информационной безопасности.

Пособие может использоваться студентами других специальностей при изучении курсов, связанных с защитой информации.

УДК 004.056.5(075.8)
ББК 32.972.53я73

ISBN 978-5-7996-2677-8

Оглавление

Предисловие

Учебное пособие «Основы информационной безопасности» предназначено для студентов укрупненной группы направлений подготовки и специальностей 10.00.00 «Информационная безопасность». Пособие может также использоваться студентами других направлений и специальностей при изучении вопросов, связанных с защитой информации.

В пособии рассмотрены свойства информации как объекта защиты, определены закономерности создания защищённых информационных систем, раскрыты принципы обеспечения информационной безопасности государства, уделено внимание информационным войнам и информационному противоборству. Дан краткий анализ моделей и политик безопасности (разграничения доступа), а также международных стандартов в области информационной безопасности.

В учебном пособии определены как теоретические, так и практические основы создания защищённых информационных систем.

Понимание научного подхода в построении защищенных систем необходимо для изучения программно-аппаратных, организационно-правовых, технических методов обеспечения информационной безопасности.

Знание основ теории информационной безопасности будет способствовать умелым действиям в решении практических вопросов защиты информации в профессиональной деятельности.

1. Основные понятия теории информационной безопасности

❖ История становления теории информационной безопасности ❖ Предметная область теории информационной безопасности ❖ Систематизация понятий в области защиты информации ❖ Основные термины и определения в области информационных отношений и защиты информации ❖ Понятия предметной области «Защита информации» ❖ Основные принципы построения систем защиты ❖

1.1. История становления теории информационной безопасности

Методы и средства защиты информации в каждую историческую эпоху тесно связаны с уровнем развития науки и техники. Категории защищаемой информации определялись экономическими, политическими и военными интересами государства.

Элементы защиты информации использовались с древнейших времён: известно, что тайнопись применяли ещё в Древнем Египте и Древнем Риме. По свидетельству Геродота, уже в V в. до н. э. применялось кодирование информации. Классическим примером одного из первых применений криптографии является так называемый «шифр Цезаря» [1, 2].

Проследим связь между развитием политической и экономической структуры России и деятельностью по защите информации (табл. 1, 2) [2, 3].

Выводы по таблице 1:

- Обусловленность системы защиты информации историческим развитием;
- Распределение компетенций, регламентация прав и ответственности между департаментами и отделами;

Таблица 1

Защита информации в России

Период	Факторы влияния	Деятельность по защите	Органы защиты
XVII в.	Образование российского централизованного государства, формирование органов государственного управления, развитие международных связей	Использование дезинформации; введение ограничений на въезд; шифрование переписки; введение ответственности за разглашение информации. Ответственность за шпионаж и государственную измену. Ответственность за хищение и подделку документов и печатей. Вопросы защиты информации в Судебниках 1497 и 1550 гг.	Оружейный, Казённый, Посольский приказы. Gриказ тайных дел
XVIII в.	Развитие торгово-промышленной деятельности, появление акционерных компаний, кредитные отношения, биржевая деятельность	Расширение состава защищаемой информации	Преображенский Приказ, Верховный тайный совет. Военная Коллегия. Коллегия иностранных дел. Тайная розыскных дел Канцелярия. Тайная экспедиция
XIX в.	Новые формы акционерных обществ, промышленная революция	Ограничение на публикацию сведений, полученных по служебным каналам. Защита коммерческой тайны (тайны торговых, купеческих книг). Законодательство в области патентного и авторского права. Цензурные уставы	Государственный Совет. 1-й и 3-й отдел Собственной Его императорского величества канцелярии. Главное управление по делам печати. Особый отдел Департамента полиции. Технический комитет
Начало XX в.	Первая мировая война	Закон «О государственной измене путём шпионажа». Создание «закрытых» зон. Расширение состава защищаемой информации. Военно-промышленная тайна. Защита информации в процессе радиотелеграфных переговоров	Министерство внутренних дел, Департамент полиции, Военное министерство, Комитет для защиты промышленной собственности

Таблица 2

Защита информации в СССР (1917–1995)

Период	Факторы влияния	Деятельность по защите	Органы защиты
1917–1945	Изменение политического и экономического строя	Отмена коммерческой тайны. Увеличение объёма сведений, составляющих гостайну. Активизация иностранных спецслужб по добыванию информации о политическом, экономическом и военном положении СССР. Централизация управления защитой госсекретов. Усиление ответственности за разглашение гостайны, утрату секретных документов и халатное обращение с ними	Спец. органы защиты информации (спец. отдел ВЧК-ГПУ, далее — 7-й отдел НКВД)
1945–1975	Холодная война	Введение должности заместителя начальника объекта по режиму. Расширение объёма и тематики защищаемой информации и категорирование её по степени секретности. Ужесточение режима секретности. «Перечень сведений, составляющих гостайну» (1948). «Инструкция по обеспечению сохранения гостайны в учреждениях и на предприятиях СССР» (1948)	Министерство государственной безопасности (1946). Комитет государственной безопасности при Совете министров СССР (1954)
1975–1995	Появление информационных войн и противоборства	Появление новых носителей информации, автоматизированных систем и распределенных систем обработки данных. Широкомасштабное применение средств технической разведки. Разработка теоретических моделей безопасности	Государственная техническая комиссия по противодействию иностранным техническим разведкам (1973)

- Отсутствие специальных органов защиты информации;
- Отсутствие научной проработки вопроса;
- Опыт защиты информации в Российской империи был использован при организации зашиты информации в СССР.

Выводы по таблице 2:

- На проблему защиты информации большое влияние оказывали внутренние и внешние политические причины.
- Враждебное для СССР окружение выдвинуло на первое место вопросы обеспечения секретности информации.

На современном этапе развития общества информация выступает как форма собственности, и следовательно, имеет определенную ценность. Чтобы подчеркнуть роль информации в обществе, говорят об «информационном обществе», в отличие от предыдущей фазы развития общества — «индустриальном обществе».

Начиная с 90-х гг. XX в. исследованиями в области информационной безопасности активно занимаются российские ученые [3].

В. А. Герасименко разработал системно-концептуальный подход к обеспечению информационной безопасности автоматизированных систем обработки данных. А. А. Грушо и Е. Е. Тимонина представили доказательный подход к проблеме гарантированности защиты информации в компьютерной системе. А. А. Грушо в сферу исследований были введены новые виды скрытых каналов утечки информации, основывающихся на использовании статистических характеристик работы системы. С. П. Расторгуев и А. Ю. Щербаков разработали теорию разрушающих программных воздействий. А. Ю. Щербаковым также была разработана субъектно-объектная модель системы, на базе которой сформированы понятия информационных потоков и доступов в компьютерной системе.

Большой вклад в исследование теоретических основ информационной безопасности внесли представители Санкт-

Петербургской научной школы во главе с П. Д. Зегждой. Ими разработана таксонометрия брешей и изъянов в системах защиты компьютерных систем, представлен ряд технических решений по созданию защищенных компьютерных систем, в частности, организационно-иерархическая система разграничения доступа.

Представителями школы Института криптографии, связи и информатики (ИКСИ) Академии ФСБ России во главе с Б. А. Погореловым (П. Н. Девянин, Д. И. Правиков, А. Ю. Щербаков, С. Н. Смирнов, Г. В. Фоменков и др.) были проведены исследования в области криптографической защиты информации, а также подготовлена целая серия учебных изданий, что позволило сформировать методическую базу подготовки специалистов в сфере информационной безопасности.

При рассмотрении вопросов информационной безопасности в настоящее время можно выделить два подхода [3]:

Неформальный, или описательный. При этом комплекс вопросов построения защищённых систем делится на основные направления, соответствующие угрозам, разрабатывается комплекс мер и механизмов защиты по каждому направлению.

Формальный. Основан на понятии политики безопасности и определении способов гарантирования выполнения её положений.

Как естественно-научная дисциплина теория информационной безопасности развивается в направлении формализации и математизации основных положений, выработки комплексных подходов к решению задач защиты информации.

Теория информационной безопасности постоянно развивается т. к. в связи с развитием технологий обработки и передачи информации постоянно возникают новые задачи по обеспечению информационной безопасности.

Необходимо отметить, что в настоящее время это одна из самых развивающихся естественных наук. Постоянно появляют-

ся новые перспективные направления исследований, а уже имеющиеся получают еще более глубокую научную проработку.

К числу перспективных направлений следует отнести следующие:

- Формализация положений теории информационной безопасности;
- Разработка моделей безопасности, более точно отражающих существующий уровень развития компьютерной техники и информационных технологий и более удобных для практического использования и анализа защищенности реальных АС;
- Разработка средств и методов противодействия угрозам информационной войны;
- Вопросы обеспечения безопасности в глобальных информационных сетях, например Internet;
- Безопасность систем электронной коммерции;
- Вопросы безопасности обработки информации мобильными пользователями.

Особую роль в развитии теории информационной безопасности как науки и отрасли промышленности играют так называемые центры информационной безопасности. К ним относятся государственные, общественные и коммерческие организации, а также неформальные объединения, основные направления деятельности которых — координация усилий, направленных на актуализацию проблем защиты информации, проведение теоретических исследований и разработка конкретных практических решений в области безопасности, аналитическая деятельность и прогнозирование.

В Российской Федерации известными центрами информационной безопасности являются такие учреждения, как Федеральная служба технического и экспортного контроля (ФСТЭК), Институт криптографии, связи и информатики Академии федеральной службы безопасности (ИКСИ) и Академия криптографии Российской Федерации (АК РФ).

Зарубежные центры информационной безопасности широко представлены в сети Internet. По приоритетным для них направлениям деятельности среди таких центров выделяются [3]:

- *Информационно-аналитические*. В основном занимаются сбором и распространением информации об известных уязвимых местах систем, атаках и вторжениях, программных и аппаратных средствах профилактики и защиты. Регулярно публикуются и рассылаются аналитические обзоры, проводятся интернет-конференции, посвященные защите информации.
- *Оперативного реагирования*. Для этих центров ключевым аспектом деятельности является оказание практической помощи тем, чьим интересам был нанесен ущерб в результате нарушения информационной безопасности.
- *Консультационные*. Преимущественно занимаются оказанием консалтинговых услуг организациям, испытывающим трудности с выбором или внедрением программных, аппаратных или комплексных мер защиты, разработкой политики безопасности или использованием нормативно-правовой базы, регламентирующей вопросы применения мер защиты.
- *Научно-исследовательские*. Как правило, функционируют на базе факультетов крупных учебных заведений или подразделений государственных организаций и сосредоточены на изучении и совершенствовании теоретических основ информационной безопасности, исследовании и разработке моделей безопасных систем, синтезе и анализе защитных механизмов, совершенствовании законодательной базы.
- *Центры сертификации*. Реализуют программы тестирования, сравнения и сертификации средств защиты, а также разрабатывают подходы к сертификации и методики тестирования. Существуют государственные и независимые центры сертификации.

Роль таких центров в целом выражена в том, что они определяют направления дальнейшего развития.

1.2. Предметная область теории информационной безопасности

Теория информационной безопасности наука сравнительно молодая. Свое развитие она получила в связи с бурным развитием информационных технологий, радиоэлектроники и связи и необходимостью сохранения информационных ресурсов. Как и любая другая наука, информационная безопасность имеет свой понятийный аппарат, который способен наиболее точно охарактеризовать все аспекты защиты информации. Многие понятия по своему содержанию соответствуют зарубежным аналогам. В то же время некоторые термины не являются устоявшимися и не всегда точно и полно характеризуют какой- либо процесс, свойство или предмет.

Предметной областью информационной безопасности являются:

- информация и ее свойства;
- угрозы безопасности информации и ее собственникам;
- политика безопасности и модели безопасности;
- способы, методы и средства защиты информации;
- классификация систем защиты;
- требования к защищенности информационных систем;
- методология оценки защищенности информационных систем и проектирования защиты.
- конкретные системы защиты информации, применяемые в различных органах управления, учреждениях и на предприятиях различных форм собственности.

Первый документ, устанавливающий основные термины и определения в области защиты информации в России был из-

дан в 1992 году Гостехкомиссией РФ под названием «Термины и определения в области защиты от НСД к информации. Руководящий документ Гостехкомиссии России». В 1996 году основные термины и определения были стандартизированы Госстандартом. Выпущен ГОСТ Р 50922–96 Защита информации. Основные термины и определения.

1.3. Систематизация понятий в области защиты информации

Базовыми в теории защиты информации являются термины: «информационная безопасность», «безопасность информации», «защита информации». Их сущность определяет в конечном итоге политику и деятельность в области защиты информации.

Информационная безопасность — состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам).

Безопасность информации — защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Из определений «информационная безопасность» и «безопасность информации» вытекает, что защита информации направлена на обеспечение безопасности информации, безопасность информации обеспечивается с помощью ее защиты.

Нарушение безопасности информации в конечном итоге наносит ущерб ее собственнику. Поэтому для того чтобы установить, что защищать, в чьих интересах защищать, как и чем

защищать, введена система понятий в области защиты информации, включающая в себя:

- понятия, связанные с определением информации, ее правового режима, правами собственности и доступа к защищаемой информации (правовые понятия в области информационных отношений);
- понятия, связанные непосредственно с предметной областью защиты информации.

Понятия первой группы используются в правовых документах, понятия второй — в нормативных.

Основные правовые документы:

- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.06 № 149-ФЗ;
- Федеральный закон «О государственной тайне» от 21.09.93 № 182;
- «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 № 230-ФЗ. Глава 70. Авторское право;
- Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. N 683;
- Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. Утверждена Указом Президента Российской Федерации от 09.05.2017 № 203.

Основные нормативные документы:

- ГОСТ Р 50922–96. Защита информации. Основные термины и определения.
- ГОСТ Р 50.1.053–2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.

- ГОСТ Р ИСО/МЭК 15408–1–2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
- ГОСТ Р ИСО/МЭК 15408–2–2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
- ГОСТ Р ИСО/МЭК 15408–3–2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
- ГОСТ Р ИСО/МЭК 15408 — Общие критерии оценки безопасности информационных технологий.
- ГОСТ Р ИСО/МЭК 27002 — Информационные технологии. Практические правила управления информационной безопасностью.
- ГОСТ Р ИСО/МЭК 27001 — Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования.
- Руководящие документы Гостехкомиссии России.

1.4. Основные термины и определения правовых понятий в области информационных отношений и защиты информации

Основные термины и определения правовых понятий в изучаемой области установлены в Федеральном законе «Об информации, информационных технологиях и о защите информации». В нем сформулировано понятие информации и информационных технологий, определены субъекты информационных отношений и защиты.

Информация — сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. В соответствии с ГОСТ 33707–2016 (ISO/IEC 2382:2015) Информационные технологии. Словарь, информационная система — это система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

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.

Также к правовым понятиям следует отнести понятие прав доступа к защищаемой информации. Ограничения доступа устанавливаются к сведениям, составляющим государственную тайну и иные виды тайны. В качестве собственников информации рассматриваются государство, организации и граждане (юридические и физические лица).

Доступ к информации — возможность получения информации и ее использования.

Предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

1.5. Понятия предметной области «Защита информации»

Основные понятия предметной области «Защита информации» установлены стандартом ГОСТ Р 50922–96, а также в Руководящих документах Гостехкомиссии России.

Условно вся предметная область может быть разделена на две подгруппы. Первая — это основные понятия в области защиты информации. Вторая подгруппа — это понятия, связанные с организацией защиты информации.

Основные понятия в области защиты информации (термины и определения)

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

Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации — принятие правовых, организационных и технических мер, направленных:

1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Защита информации от утечки — деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Защита информации от несанкционированного воздействия — деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия — деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения — деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа — деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может быть: государство; юридическое лицо; группа физических

лиц, в том числе общественная организация; отдельное физическое лицо.

Защита информации от разведки — деятельность, направленная на предотвращение получения защищаемой информации разведкой.

Примечание. Получение защищаемой информации может быть осуществлено как иностранной, так и отечественной разведкой.

Защита информации от технической разведки — деятельность, направленная на предотвращение получения защищаемой информации разведкой с помощью технических средств.

Защита информации от агентурной разведки — деятельность, направленная на предотвращение получения защищаемой информации агентурной разведкой.

Цель защиты информации — заранее намеченный результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Замысел защиты информации — основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Эффективность защиты информации — степень соответствия результатов защиты информации поставленной цели.

Показатель эффективности защиты информации — мера или характеристика для оценки эффективности защиты информации.

Нормы эффективности защиты информации — значения показателей эффективности защиты информации, установленные нормативными документами.

Понятия, связанные с организацией защиты информации

Организация защиты информации — содержание и порядок действий, направленных на обеспечение защиты информации.

Система защиты информации — совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Мероприятие по защите информации — совокупность действий, направленных на разработку и (или) практическое применение способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации — совокупность действий, направленных на разработку и (или) практическое применение способов и средств контроля эффективности защиты информации.

Техника защиты информации — средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

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

Способ защиты информации — порядок и правила применения определенных принципов и средств защиты информации.

Категорирование защищаемой информации (объекта защиты) — установление градации важности защищаемой информации (объекта защиты).

Контроль состояния защиты информации — проверка соответствия организации и эффективности защиты информации установленным требованиям и (или) нормам зашиты информации.

Все рассмотренные понятия являются общеметодологическими и применимы в целом для теории информационной безопасности.

Основные понятия, связанные с защитой информации в информационных системах, определены также в Руководящем документе Гостехкомиссии «Термины и определения в области защиты от НСД к информации».

Установленные термины обязательны для применения во всех видах документации. Для каждого понятия установлен один термин. Применение его синонимов не допускается.

1.6. Основные принципы построения систем защиты

Для защиты информации в информационных системах могут быть сформулированы следующие принципы [1, 6]:

1. *Законность и обоснованность защиты*.

Принцип законности и обоснованности предусматривает то, что защищаемая информация по своему правовому статусу относится к информации, которой требуется защита в соответствии с законодательством.

2. *Системность*.

Системный подход к защите информационной системы предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

- при всех видах информационной деятельности и информационного проявления;
- во всех структурных элементах;
- при всех режимах функционирования;
- на всех этапах жизненного цикла;

- с учетом взаимодействия объекта защиты с внешней средой.

При обеспечении безопасности информационной системы необходимо учитывать все слабые, наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и пути несанкционированного доступа к информации. Система защиты должна строиться не только с учетом всех известных каналов проникновения, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

3. *Комплексность*.

Комплексное использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

4. *Непрерывность защиты*.

Защита информации — это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы, начиная с самых ранних стадий проектирования. Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы.

5. *Разумная достаточность*.

Создать абсолютно непреодолимую систему защиты принципиально невозможно: при достаточных времени и средствах можно преодолеть любую защиту. Следовательно, возможно достижение лишь некоторого приемлемого уровня безопасности. Высокоэффективная система защиты требует больших ре-

сурсов (финансовых, материальных, вычислительных, временных) и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

6. *Гибкость*.

Внешние условия и требования с течением времени меняются. Принятые меры и установленные средства защиты могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровня защищенности средства защиты должны обладать определенной гибкостью.

7. *Открытость алгоритмов и механизмов защиты*.

Суть принципа открытости механизмов и алгоритмов защиты состоит в том, что знание алгоритмов работы системы защиты не должно давать возможности ее преодоления даже разработчику защиты. Однако это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна, необходимо обеспечивать защиту от угрозы раскрытия параметров системы.

8. *Простота применения средств защиты*.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения малопонятных ему операций.

1.7. Концепция комплексной защиты информации

Эффективное обеспечение защиты информации возможно только на основе комплексного использования всех известных методов и подходов к решению данной проблемы. К концепции комплексной защиты предъявляется ряд требований [5]:

1. Разработка и доведение до уровня регулярного использования всех необходимых механизмов гарантированного обеспечения требуемого уровня защищенности информации;

2. Существование механизмов практической реализации требуемого уровня защищенности;

3. Наличие средств рациональной реализации всех необходимых мероприятий по защите информации на базе достигнутого уровня развития науки и техники;

4. Разработка способов оптимальной организации и обеспечения проведения всех мероприятий по защите в процессе обработки информации.

В целях построения концепции, удовлетворяющей всей совокупности требований, в последнее время активно разрабатывается теория защиты информации, включающая понятия задачи защиты, средств защиты, системы защиты.

Функция защиты — совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в информационной системе различными средствами и методами в целях создания, поддержания и обеспечения условий, объективно необходимых для надежной защиты информации.

Полное множество функций защиты:

- предупреждение возникновения условий, благоприятствующих появлению дестабилизирующих факторов;
- предупреждение непосредственного проявления дестабилизирующих факторов;
- обнаружение проявившихся дестабилизирующих факторов;

- предупреждение воздействия на защищаемую информацию проявившихся дестабилизирующих факторов;
- обнаружение воздействия дестабилизирующих факторов;
- локализация воздействия дестабилизирующих факторов;
- ликвидация последствий локализованного воздействия дестабилизирующих факторов.

Полнота множества функций защиты имеет значение для оптимизации систем защиты информации. Осуществление функций защиты связано с расходованием ресурсов. Обозначим количество ресурсов (например, стоимость), расходуемых на осуществление i-го мероприятия по защите, как C_i. Вероятность успешного осуществления этого мероприятия P_i зависит от затраченных ресурсов

$$P_i = P_i\,(C_i).$$

Если требуется обеспечить определенный уровень (вероятность) защищенности информации $P_{з0}$, то следует выбирать такие мероприятия, которые обеспечат уровень защищенности не менее заданного:

$$P_з > P_{з0}.$$

С учетом этого задачу защиты информации можно сформулировать как оптимизационную: определить перечень мероприятий, при которых заданный уровень защиты обеспечивается при минимальных затратах. Возможна и другая постановка: достичь максимально возможного уровня защищенности информации при определенном уровне затрат на защиту.

Осуществление функций защиты достигается решением задач защиты.

1.8. Задачи защиты информации

Все задачи, необходимые для осуществления функций обеспечения защиты, могут быть объединены в классы:

- введение избыточности элементов системы;
- резервирование элементов системы;
- регулирование доступа к элементам системы;
- регулирование использования элементов системы;
- маскировка информации;
- контроль элементов системы;
- регистрация сведений;
- уничтожение информации;
- сигнализация;
- реагирование.

До сих пор не решена проблема оценки эффективности реализации функций защиты путем решения определенной задачи защиты.

1.9. Средства реализации комплексной защиты информации

Рассмотрим основные средства, используемые для создания механизмов защиты.

Все средства защиты делятся на *формальные* (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и *неформальные* (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические.

Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Из наиболее известных аппаратных средств можно отметить

схемы контроля информации по четности, схемы защиты полей памяти — по ключу и т. п.

Физические средства реализуются в виде автономных устройств и систем. Это могут быть, например замки на дверях помещений, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Указанные выше средства и составляли основу механизмов защиты на первой фазе развития технологии обеспечения безопасности связи в каналах телекоммуникаций. При этом считалось, что основными средствами защиты являются программные. Первоначально программные механизмы защиты включались, как правило, в состав ОС, управляющих ЭВМ, или систем управления базами данных. Практика показала, что надежность подобных механизмов защиты является явно недостаточной. Особенно слабым звеном оказалась защита по паролю. Поэтому в дальнейшем механизмы защиты становились все более сложными, с привлечением других средств обеспечения безопасности.

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы системы на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в данной стране или обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета и престижа человека.

Итак, информационная безопасность является важной составляющей национальной безопасности России. Политика государства в этой сфере деятельности направлена в первую очередь на организацию защиты государственной тайны и развитие правовых основ защиты информации. Правовая защита информации выступает как один из наиболее важных способов и методов защиты информации.

ВЫВОДЫ

- Знание основ теории информационной безопасности будет способствовать компетентному решению практических вопросов защиты информации, явится основой для профессиональной деятельности специалиста по информационной безопасности;
- Проблема защиты информации формулировалась поразному в разные исторические эпохи и связана политикой, экономикой, технологиями.
- Проблема защиты информации в автоматизированных (информационных) системах была сформулирована в середине 70-х годов XX века и с тех пор претерпела существенные изменения, связанные с уровнем развития систем;
- Перспективным является путь комплексного обеспечения информационной безопасности, сочетающий формальный и неформальный подход к решению проблемы;
- Однозначное определение базовых понятий в области ин-

формационной безопасности необходимо в интересах как производителей, так и потребителей информационных систем, а также для полного и непротиворечивого описания процесса защиты информации.

Вопросы для самоконтроля

1. Какие методы защиты информации, использовавшиеся в древнее время и в Средние века Вам известны?
2. Покажите связь между уровнем развития общества и технологиями защиты информации.
3. В каких направлениях идет развитие теории информационной безопасности в настоящее время?
4. Каков вклад российских ученых в теорию информационной безопасности?
5. С чем связан возросший интерес к проблемам защиты информации?
6. Каковы отличия формального и неформального подходов к проблемам защиты информации?
7. В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?
8. Что такое информационная система? Телекоммуникационная система? Автоматизированная система?
9. Каковы правовые понятия в области защиты информации?
10. Что такое защита информации? Информационная безопасность?
11. Охарактеризуйте понятия, связанные с организацией защиты информации.
12. Каковы основные принципы построения систем защиты информации?
13. Что такое комплексный подход к обеспечению информационной безопасности?

14. Каковы основные задачи защиты информации?
15. Докажите, что приведенное множество функций защиты является полным.
16. Какова взаимосвязь различных средств защиты информации? Есть ли среди них приоритетные?
17. Каковы основные средства реализации комплексной системы защиты информации?
18. Что такое морально-этические средства защиты информации?
19. Докажите необходимость сочетания различных средств защиты информации.
20. Приведите примеры формальных и неформальных средств защиты?
21. Что такое центры информационной безопасности и какова их роль в развитии теории и практики защиты информации?

2. Информация как объект защиты

❖ Понятие об информации как объекте защиты ❖ Уровни представления информации ❖ Основные свойства защищаемой информации ❖ Виды и формы представления информации. Информационные ресурсы ❖ Структура и шкала ценности информации. Классификация информационных ресурсов ❖ Правовой режим информационных ресурсов ❖

2.1. Понятие об информации как объекте защиты

В общем случае информация — это знания в широком значении этого слова. Не только образовательные или научные знания, а сведения и данные, которые присутствуют в любом объекте и необходимы для функционирования любых информационных систем (живых существ или созданных человеком).

Информация как объект познания имеет ряд особенностей:

- нематериальна по своей природе, отображается в виде символов на носителях;
- после записи на носитель информация приобретает определённые параметры и может быть измерена в объеме;
- информация, записанная на материальный носитель, может храниться, обрабатываться, передаваться по различным каналам связи;
- перемещаясь по линиям связи, информация создает физические поля, которые отражают ее содержание.

При обработке, хранении, передаче информация циркулирует в информационной системе. Простейшая информационная система состоит из источника информации, канала связи и получателя информации (рис. 2.1). Из этого следует, что нельзя поставить знак равенства между защитой информации и защитой информационной системы.

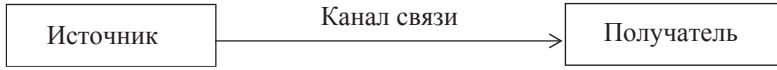


Рис. 2.1. Простейшая информационная система

2.2. Уровни представления информации

Можно выделить несколько уровней представления информации:

- уровень носителей;
- уровень средств взаимодействия с носителем;
- логический уровень;
- синтаксический уровень;
- семантический уровень.

Охарактеризуем каждый из них.

1) *Уровень носителей информации*

По своей природе информация не материальна и в чистом виде человеку не доступна. Для того чтобы человек воспринял информацию, должен быть материальный носитель: другой человек, вещество (вещественный носитель), энергия (энергетический носитель). Информация, являясь предметом защиты, требует защищенности тех объектов, в которых она присутствует в той или иной материальной форме.

Все носители имеют две категории информации:

- признаковая информация: информация носителя «о себе», о видовых признаках: форма, размер, структура, химические и физические свойства, энергетические параметры;
- семантическая информация: то, что не зависит от вида носителя, продукт абстрактного мышления на языке символов.

Роль **человека** по отношению к информации многообразна: человек может быть не только носителем информации, но и ге-

нератором новой информации, источником информации, владельцем, пользователем. По отношению к вопросам защиты человек может выступать и как нарушитель, и как защитник.

Как носитель человек нуждается не только в физической защите. Человека следует защищать от информации избыточной, бесполезной, от дезинформации, от разрушающей информации (информационно-психологическое оружие). Многие механизмы защиты работают у человека на биологическом уровне: при поступлении ненужной или избыточной информации снижается внимание, ухудшается запоминание, замедляется реакция. Так как часто на основе имеющейся информации принимаются решения, то важным является достаточная информированность человека. В этом случае опасна как неинформированность (возможно принятие неверных решений на основе неполной информации), так и сверхинформированность (сложности в определении приоритетов и основных факторов).

Вещественные носители разнообразны по своим качествам, среди них есть такие, которые используются уже тысячелетиями, есть созданные в последние годы. К наиболее распространённым в настоящее время относятся: бумага, электронные носители информации. Особенности вещественных носителей:

- придают информации свойство статичности (постоянства во времени), в связи с этим обычно используются для хранения информации;
- информация фиксируется прочно, её трудно уничтожить, не повредив носителя;
- со временем вещественные носители разрушаются и стареют, при этом информация гибнет вместе с носителем;
- запись информации связана с изменением физических и химических свойств носителей.

Вещественные носители, как и любой материальный объект, следует защищать от повреждения, преждевременного износа, хищения, утери. Необходима также защита при копировании информации. Копирование — процесс переноса информации

на аналогичный или иной носитель без изменения количества и качества. Копирование легко обеспечивается при помощи современных технологий. Для документов на бумажном носителе копирование осуществляется при помощи ксерокса, сканера, фотоаппарата. Для электронных носителей операция копирования предусмотрена стандартным программным обеспечением. В результате копирования одна и та же информация размещается в разных точках пространства на разных носителях, следовательно, нужна охрана всех носителей во всех местах дислокации.

Энергетические носители — это электромагнитное и акустическое поля.

Особенности энергетических носителей:

- используются в основном для передачи информации;
- не стареют;
- бесконтрольно распространяются в пространстве;
- способны к взаимному преобразованию;
- запись информации связана с изменением параметров поля (различные виды модуляции).

Основные способы защиты информации на энергетическом носителе: обеспечение помехоустойчивости при выборе кодирования (модуляции), обеспечение требуемой энергетики сигнала, защита от утечки, в том числе через побочные электромагнитные излучения и наводки (ПЭМИН), защита от перехвата в основном канале.

2) *Уровень средств взаимодействия с носителем*

Непосредственное взаимодействие с носителем не всегда возможно и часто осуществляется через сложные технические устройства. Для защиты на этом уровне нужно следить за исправностью устройств считывания информации, за отсутствием технических средств несанкционированного доступа к информации (так называемых «закладок»), задачей которых является перехват или перенаправление потока считываемой информации.

3) *Логический уровень*

На логическом уровне в информационной системе информация может быть представлена в виде логических дисков, каталогов, файлов, ..., секторов, кластеров. В современных операционных системах уровни отдельных байтов, кластеров, секторов не видны, поэтому часто забываются. Следует помнить, что удаление информации на высоком логическом уровне (например, на уровне файла) не приводит к удалению информации на нижних уровнях, откуда она может быть считана.

4) *Синтаксический уровень*

Синтаксический уровень представления информации связан с кодированием. Информация записывается и передаётся при помощи символов. Символ — это некоторый знак, которому придаётся определённый смысл. Линейный набор символов образует алфавит. В процессе кодирования один алфавит может быть преобразован в другой.

В зависимости от целей различаются следующие виды кодирования:

- с целью устранения избыточности — архивирование, линейное кодирование;
- с целью устранения ошибок — помехоустойчивое кодирование;
- с целью недоступности информации — криптографическое кодирование.

5) *Семантический уровень*

Семантический уровень связан со смыслом передаваемой информации. Одинаковые лексические конструкции могут иметь различный смысл в разном контексте. Использование профессионализмов, многозначных слов и слов, значение которых изменилось с течением времени, может исказить смысл информации.

2.3. Основные свойства защищаемой информации

Информация как объект познания и объект защиты обладает множеством свойств. Перечислим важнейшие из них.

Ценность. Как предмет собственности информация имеет определенную ценность. Именно потому, что информация имеет ценность, ее необходимо защищать.

Секретность (*конфиденциальность*) информации — субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации. Эта характеристика обеспечивается способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

Целостность информации — свойство информации существовать в неискаженном виде. Обычно интересует обеспечение более широкого свойства — достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, то есть ее неискаженности. Вопросы обеспечения адекватности отображения выходят за рамки проблемы обеспечения информационной безопасности.

Доступность информации — свойство системы, в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Концентрация. Суммарное количество информации может оказаться секретным, сводные данные обычно секретнее, чем одиночные.

Рассеяние. Ценная информация может быть разделена на части и перемешана с менее ценной с целью маскировки самого факта наличия информации. Примеры использования этого свойства — компьютерная стеганография.

Сжатие. Возможно сжатие без потери информации, например архивирование. Для уменьшения объема информации или увеличения пропускной способности канала передачи информации применяется сжатие с частичной потерей (например, сжатие в графических форматах типа jpg). Используется также необратимое сжатие (например, алгоритм электронно-цифровой подписи (ЭЦП), одностороннее ХЭШ-преобразование).

Прагматические свойства:

- важность;
- полнота (степень уменьшения априорной неопределенности);
- достоверность;
- своевременность;
- целесообразность;
- соотносимость с фактами, явлениями.

Для удовлетворения законных прав и интересов владельцев информации необходимо прежде всего постоянно поддерживать секретность, целостность и доступность информации. При нарушении хотя бы одного из этих свойств ценность информации снижается либо теряется вообще:

- если ценность теряется при ее раскрытии, то говорят, что имеется опасность нарушения секретности информации;
- если ценность информации теряется при изменении или уничтожении информации, то говорят, что имеется опасность для целостности информации;
- если ценность информации теряется при ее неоперативном использовании, то говорят, что имеется опасность нарушения доступности информации.

Ценность информации изменяется во времени. К изменению ценности информации приводят распространение ин-

формации и ее использование. Характер изменения ценности во времени зависит от вида информации. Для большинства видов можно представить общую схему жизненного цикла информации (рис. 2.2).

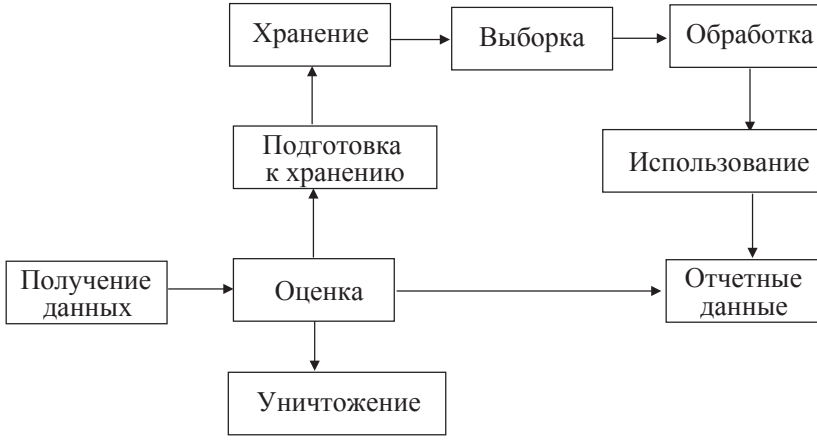


Рис. 2.2. Жизненный цикл информации

Ценность большинства видов информации, циркулирующей в информационной системе, со временем уменьшается — информация стареет. Старение информации $C_и$ в первом приближении можно аппроксимировать выражением вида

$$C_0(t) = C_0 \exp(-2{,}3t/t_{ж.ц}),$$

где C_0 — ценность информации в момент ее возникновения (создания); t — время от момента возникновения информации до момента ее использования; $t_{ж.ц}$ — продолжительность жизненного цикла информации (от момента возникновения до момента устаревания).

В соответствии с этим выражением за время жизненного цикла ценность информации уменьшается в 10 раз.

2.4. Виды и формы представления информации. Информационные ресурсы

В соответствии с законодательством вводится понятие информационных ресурсов. *Информационные ресурсы* предприятия, организации, учреждения, компании и других государственных и негосударственных структур включают в себя отдельные документы и отдельные массивы документов (дела), документы и комплексы документов в информационных системах (библиотеках, архивах, фондах, банках данных электронно-информационных систем) на любых носителях, в том числе обеспечивающих работу вычислительной и организационной техники. Информационные ресурсы являются объектами отношений физических и юридических лиц между собой и с государством. В совокупности они составляют информационные ресурсы России и защищаются наравне с другими видами ресурсов. Обязательным условием для включения в информационные ресурсы является документирование информации.

Любая документированная информация имеет следующие реквизиты:

- наименование документа;
- гриф секретности или конфиденциальности (если таковые имеются);
- регистрационный номер;
- дату создания и регистрации;
- автора и (или) исполнителя;
- срок действия грифа секретности или конфиденциальности, если таковые имеются;
- атрибуты учреждения.

Кроме того, в реквизитах могут указываться адреса рассылки (пользователей).

Документированная информация может быть представлена в виде справок, решений, приказов, распоряжений, заданий,

отчетов, ведомостей, инструкций, комментариев, писем и записок, телеграмм, чеков, статей и др. Все эти виды документов могут отличаться по форме. Обычно в служебном и секретном делопроизводстве эти формы стандартизованы. В различных ведомствах они могут быть неодинаковыми. В информационных системах документированная информация представлена в виде файлов, папок, массивов, баз данных, программ.

Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

2.5. Структура и шкала ценности информации. Классификация информационных ресурсов

Ценность информации может быть стоимостной категорией и характеризовать конкретный размер прибыли при ее исполь-

зовании или размер убытков при ее утрате. Степень ценности информации и необходимая надежность ее защиты находятся в прямой зависимости.

Информация часто становится ценной ввиду ее правового значения для фирмы или развития бизнеса, например учредительные документы, программы и планы, договоры с партнерами и посредниками и т. д. Ценность может проявляться в ее перспективном научном, техническом или технологическом значении.

Следует учитывать, что документ может быть не только управленческим (деловым), имеющим в большинстве случаев текстовую, табличную или анкетную форму. Большие объемы наиболее ценных документов представлены в изобразительной форме: конструкторские документы, картографические, научно-технические, документы на фотографических, магнитных и иных носителях. В соответствии с этим обычно выделяются два вида интеллектуально ценной информации [7]:

- техническая, технологическая: методы изготовления продукции, программное обеспечение, производственные показатели, химические формулы, рецептуры, результаты испытаний опытных образцов, данные контроля качества и т. п.;
- деловая: стоимостные показатели, результаты исследования рынка, списки клиентов, экономические прогнозы и т. п.

По принадлежности к виду собственности информационные ресурсы могут быть государственными или негосударственными, находиться в собственности граждан, органов государственной власти, исполнительных органов, органов местного самоуправления, государственных учреждений, организаций и предприятий, общественных организаций.

Защите подлежит любая официальная документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному

лицу. Таким образом, наличие права собственности на информацию как результат интеллектуальной деятельности определяет правовую целесообразность защиты информационных ресурсов. Существует также экономическая целесообразность защиты информационных ресурсов, основанная на потребительских свойствах информации, прежде всего на ее стоимости.

В соответствии с интересами обеспечения национальной безопасности и степенью ценности для государства, а также правовыми, экономическими и другими интересами информационные ресурсы могут быть *открытыми*, то есть общедоступными (используемыми в работе без специального разрешения, публикуемыми в средствах массовой информации, оглашаемыми в выступлениях и т. п.), и *ограниченного доступа* и использования, то есть содержащими сведения, составляющие тот или иной вид тайны и подлежащие защите, охране, наблюдению (рис. 2.3) [7].

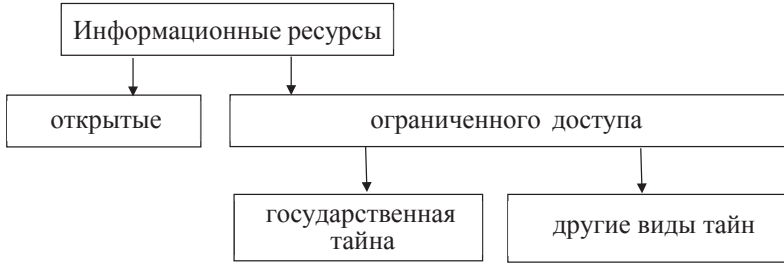


Рис. 2.3. Классификация информационных ресурсов

Запрещается относить к информации ограниченного доступа:

- законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, исполнительных органов, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

- документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
- документы, содержащие информацию о деятельности органов государственной власти, исполнительных органов и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии и потребностях населения, за исключением сведений, относящихся к государственной тайне;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, исполнительных органов, органов местного самоуправления, организаций, общественных объединений, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Ценная информация охраняется нормами права (патентного, авторского, смежных прав и др.), товарным знаком или защищается включением ее в категорию информации, составляющей определенный вид тайны.

Для информационных ресурсов ограниченного доступа вид тайны является определяющим основанием их классификации. Тайна — это нечто неизвестное, неведомое, неразгаданное, еще не познанное, нечто скрываемое от других, известное не всем. Выделяются две глобальные предметные сферы тайны:

- тайны природы, то есть объективные тайны: тайна Вселенной, тайны рождения и смерти и множество других тайн;
- тайны людей, то есть субъективные тайны: тайны личности, тайны производства, тайны искусства и т. п.

В понятие *тайны* включается не только документированная информация, а также базы данных, продукция, изделия, технологии, излучения, физические поля. Многообразие форм и субъектов собственности закрепляет за собственником право считать ту или иную ценную информацию тайной.

Состав видов тайны в современном российском законодательстве постоянно расширяется. В настоящее время основными видами тайны являются: государственная, служебная, профессиональная, коммерческая и личная. Каждый из этих видов имеет несколько подвидов.

Государственная тайна — защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Основы защиты государственной тайны регламентируются законом РФ от 21.07.1993 N 5485–1 «О государственной тайне».

Другие виды тайны являются негосударственными. Отнесение информации к информации ограниченного доступа осуществляется в порядке, установленном законодательством РФ, в соответствии с Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06.03.1997 г. № 188.

Служебная тайна содержит информацию ограниченного распространения, к которой относятся несекретные сведения, касающиеся деятельности организации, ограничения на распространение которых диктуются служебной необходимостью. К служебной информации относятся сведения, не подлежащие опубликованию в средствах массовой информации, использованию в открытых документах, оглашению на конференциях, переговорах и выставках, например черновики и варианты готовящихся документов, служебные инструкции, тактика ведения переговоров, персональные данные работников и т. д. Разновидностями служебной тайны можно назвать судебно-следствен-

ную тайну, тайну государственных банков, производственную тайну (до ее патентования) в некоммерческой сфере и др.

Профессиональная тайна — инструмент защиты персональных данных о гражданах и личной тайны граждан. Имеется в виду, что эти сведения переданы их собственником или находятся в распоряжении той или иной организации и необходимы ей для выполнения профессиональной деятельности: врачебная тайна, тайна страхования, тайна завещания, тайна голосования, тайна предприятий связи, тайна налоговых органов и др. Профессиональная тайна может быть также тайной мастерства, тайной профессионального умения, например тайна творчества, тайна рационализатора и др.

Коммерческая тайна — сведения, имеющие действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, когда к ним нет свободного доступа на законном основании и обладатель этих сведений принимает меры к охране их конфиденциальности. Учитывая, что коммерческая тайна как таковая отражает в значительной степени торговые секреты, иногда в рамках этого же определения используется термин «предпринимательская тайна». В зарубежной практике обычно используются термины, разделяющие предпринимательскую тайну на две части — производственную и коммерческую. Коммерческая тайна рассматривается как обязательное условие добросовестной конкуренции предприятий на рынке товаров или услуг. В России коммерческая тайна охватывает негосударственную сферу или коммерческие направления производственной деятельности и включает производственную, финансовую, научную и другие подвиды тайны. В рамках этого вида тайны выделяется коммерческая тайна банка (банковская тайна), тайна фирмы. К коммерческой тайне относятся секреты предприятий, с которыми сотрудничает фирма, секреты клиентов, покупателей, поставщиков и т. п.

Личная тайна граждан определена в Конституции Российской Федерации, где указано, что каждый имеет право

на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Не допускается сбор, хранение, использование и распространение информации о частной жизни граждан без их согласия. Семейную тайну можно считать разновидностью личной тайны. Она представляет собой тайну нескольких лиц, связанных родством, например: имущественное положение, взгляды и убеждения, отношения в семье, тайна факта усыновления.

Процесс выявления и регламентации реального состава информации ограниченного доступа важен для эффективной работы системы защиты информации.

Например, информация ограниченного доступа формируется в следующих направлениях деятельности предприятия:

- прогнозирование и планирование деятельности (расширение или свертывание производства, программы развития, планы инвестиций);
- управление предприятием (сведения о подготовке и принятии решений, применяемые методы управления);
- финансовая деятельность (баланс, сведения о состоянии счетов и уровне доходности, информация о получении кредитов);
- торговая деятельность (информация о рыночной стратегии, об эффективности коммерческой деятельности);
- производственная деятельность (производственные мощности, тип используемого оборудования, запасы сырья и готовой продукции);
- переговоры и совещания по направлениям деятельности предприятия (информация о подготовке и результатах проведения переговоров);
- формирование ценовой политики на продукцию и услуги (информация о структуре цен, методах расчета, размерах скидок);

- формирование состава партнеров, поставщиков и потребителей;
- изучение состава конкурентов;
- участие в торгах и аукционах;
- научная и исследовательская деятельность по созданию новой техники и технологий;
- использование новых технологий;
- подбор и управление персоналом;
- организация безопасности предприятия.

При определении состава информации ограниченного доступа следует выделять ключевые элементы информации, являющиеся основными носителями секрета. Информация может быть отнесена к коммерческой тайне при соблюдении следующих условий:

- информация не должна отражать негативные стороны деятельности предприятия;
- информация не должна быть общедоступной или общеизвестной;
- возникновение или получение информации должно быть законным и связано с расходованием материального, финансового или интеллектуального потенциала предприятия;
- персонал должен знать о ценности такой информации и обучен правилам работы с ней;
- должны быть выполнены реальные действия по защите этой информации (наличие системы защиты, нормативно-методического и технического обеспечения этой системы).

В соответствии с постановлением Правительства РФ «О перечне сведений, которые не могут составлять коммерческую тайну» от 5 декабря 1991 г. к конфиденциальной информации нельзя относить:

- учредительные документы, уставы предпринимательских структур;

- документы, дающие право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии, патенты);
- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РФ;
- документы о платежеспособности;
- сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;
- документы об уплате налогов и обязательных платежей;
- сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РФ и размерах причиненного при этом ущерба;
- сведения об участии должностных лиц предприятия в кооперативных, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

Состав ценной конфиденциальной информации, подлежащей защите, определяется ее собственником или владельцем. Предприятия однотипного профиля могут руководствоваться примерным составом защищаемых сведений.

При определении ценности информации следует определить возможный ущерб от реализации угроз безопасности. Определяя ущерб, важно оценить его в стоимостном выражении: стоимость продукции, которая не будет произведена или реализована, затраты на научные исследования и т. п.

В практической деятельности состав защищаемых сведений фиксируется в специальном Перечне конфиденциальных сведений. Определяется также перечень документов, не содержащих

конфиденциальные сведения, но представляющих ценность для предприятия и подлежащих охране (например, устав, контракт и т. п.). (Перечень ценных и конфиденциальных документов).

Таким образом, ценная информация включается в документы, входящие в состав информационных ресурсов ограниченного доступа к ним персонала. В соответствии с тем, к какому виду тайны относятся ресурсы, документы делятся на секретные и несекретные. Обязательным признаком секретного документа является наличие в нем сведений, составляющих государственную тайну. Несекретные документы, включающие сведения, относимые к негосударственной тайне или содержащие персональные данные, называются конфиденциальными. Обязательным признаком конфиденциального документа является наличие в нем информации, подлежащей защите.

К документам ограниченного доступа относятся:

- в государственных структурах: документы, проекты документов и сопутствующие материалы, относимые к служебной инфомации ограниченного распространения (документы «для служебного пользования»), содержащие сведения, отнесенные к служебной тайне, имеющие рабочий характер и не подлежащие опубликованию в открытой печати;
- в предпринимательских структурах — документы, содержащие сведения, которые собственник или владелец в соответствии с законодательством имеет право отнести к коммерческой (предпринимательской) тайне, тайне мастерства;
- независимо от принадлежности — документы и базы данных, фиксирующие любые персональные (личные) данные о гражданах, а также содержащие профессиональную тайну, технические и технологические новшества (до их патентования), тайну предприятий связи, сферы обслуживания и т. п.

Называть документы ограниченного доступа секретными или ставить на них гриф секретности не допускается.

Ограничение доступа к документам имеет значительный разброс по срокам ограничения свободного доступа к ним персонала (от нескольких часов до значительного числа лет). Следует учитывать, что основная масса конфиденциальных документов после окончания их исполнения или работы с ними теряет свою ценность и конфиденциальность. Например, переписка до заключения контракта может иметь гриф конфиденциальности, но после его подписания этот гриф снимается. Оставшиеся конфиденциальными исполненные документы, сохраняющие ценность для деятельности фирмы, формируются в дела в соответствии с номенклатурой дел.

Период ограничения доступа к документам может быть кратковременным или долговременным в зависимости от ценности информации, содержащейся в документах. Период ограничения доступа определяется по указанному выше перечню конфиденциальных сведений и зависит от специфики деятельности фирмы. Например, производственные, научно-исследовательские фирмы обладают более ценными документами, чем торговые, посреднические и др.

Документы долговременного периода ограничения доступа (программы и планы развития бизнеса, технологическая документация ноу-хау, изобретения и др.) имеют усложненный вариант обработки и хранения, обеспечивающий безопасность информации и ее носителя.

Документы кратковременного периода ограничения доступа, имеющие оперативное значение для деятельности фирмы, обрабатываются и хранятся по упрощенной схеме и могут не выделяться из технологической системы обработки открытых документов при наличии в этой системе минимальных защитных, контрольных и аналитических элементов.

Режим ограничения доступа к персональным данным снимается в случаях обезличивания этих данных или по истечении 75 лет срока их хранения, если иное не определено законом.

2.6. Правовой режим информационных ресурсов

Правовой режим информационных ресурсов определяется нормами, устанавливающими:

- порядок документирования информации;
- право собственности на отдельные документы и их массивы;
- категорию информации по уровню доступа к ней;
- порядок правовой защиты информации.

Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне.

Собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти.

Государственные информационные ресурсы РФ являются открытыми и общедоступными, исключение составляет документированная информация, отнесенная законом к категориям ограниченного доступа.

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне и конфиденциальную.

Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, — уполномоченными органами на основании закона РФ «О государственной тайне» от 21.09.93 № 182-ФЗ;
- в отношении конфиденциальной информации — собственником информационных ресурсов или уполномоченным лицом на основании Федерального закона «Об информации, информационных технологиях и защите информации от 27.07.2006 № 149-ФЗ;

- в отношении персональных данных — Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.

Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, разрабатывающие и применяющие информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности Законодательством РФ.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных ресурсов, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляется органами государственной власти.

Собственник информационных ресурсов имеет право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

Риск, связанный с использованием несертифицированных систем и средств, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

Персональные данные относятся к категории конфиденциальной информации, однако перечни этих данных должны быть закреплены на уровне федерального закона. В связи с этим деятельность негосударственных организаций и частных лиц, связанная с обработкой и представлением пользователям персональных данных, подлежит обязательному лицензированию. Все информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации.

Автоматизированные системы органов государственной власти, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации

Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности.

Закон предусматривает з*ащиту прав на доступ к информации*. Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

Во всех случаях лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба.

Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.

ВЫВОДЫ

- Характеристика понятия «информация», выделение основных свойств информации являются ключевыми моментами при определении того, что же подлежит защите.
- Выделены три основных свойства информации (конфиденциальность, целостность и доступность), защита которых обеспечивает сохранение ценности информации.
- Информация является объектом права собственности и информационные отношения регулируются соответствующими законодательными и нормативными актами.
- Информационные ресурсы классифицируются в зависимости от вида отражаемой ими тайны.

Вопросы для самоконтроля

1. Что такое информация и каковы уровни ее представления?
2. Перечислите основные носители информации, особенности их использования и защиты.
3. Какими свойствами определяется ценность информации?
4. Какие критерии оценки ценности информации Вы можете предложить?
5. Приведите примеры различной зависимости ценности информации от времени.
6. Что понимается под информационными ресурсами?
7. Что не разрешается относить к информации ограниченного доступа?
8. Что понимается под конфиденциальной информацией?
9. Какие существуют виды тайны?
10. Какое назначение имеет перечень конфиденциальных сведений предприятия?

3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности

❖ Информационная безопасность и ее место в системе национальной безопасности Российской Федерации ❖ Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность ❖

Информация, являясь продуктом деятельности, выступает как собственность государства, предприятий, учреждений, организаций, граждан и как объект собственности требует защищенности. Однако проблема защиты информации не сводится только к защите прав ее собственников, но и содержит в себе такой важный аспект, как защита прав граждан на свободный доступ к сведениям, гарантированный конституцией. Основы защиты информации разрабатываются органами государственной власти исходя из условий обеспечения информационной безопасности в частности и национальной безопасности России в целом.

3.1. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации

Необходимым условием нормального существования и развития каждого общества является защищенность от внешних и внутренних угроз, устойчивость к попыткам

внешнего давления, способность как парировать подобные попытки и нейтрализовать возникающие угрозы, так и обеспечивать такие внутренние и внешние условия существования страны, которые гарантируют возможность стабильного и всестороннего прогресса общества и его граждан. Для характеристики этого состояния используется понятие национальной безопасности.

Под *национальной безопасностью* понимается состояние защищенности жизненно важных национальных интересов от внутренних и внешних угроз, при котором обеспечивается реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности.

Поэтому в содержании понятия «национальная безопасность» можно выделить различные структурные элементы (компоненты), одним из которых является Информационная безопасность.

Информационная безопасность Российской Федерации (далее в данном разделе — информационная безопасность) — состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Поскольку в условиях информатизации страны, развития информационных технологий информационные ресурсы формируются во всех сферах деятельности, и в первую очередь в политической, военной, экономической, научно-технической, информационную безопасность следует рассматривать как комплексный показатель национальной безопасности. Этим определяется ее важное место и одна из ведущих ролей в системе национальной безопасности страны в современных условиях.

Обеспечение информационной безопасности осуществляется в рамках обеспечения национальной безопасности.

Национальная безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического и иного характера, адекватных угрозам жизненно важных интересов личности, общества и государства.

Политика России в области национальной безопасности строится на основе *«Стратегии национальной безопасности Российской Федерации»,* утвержденной Указом Президента Российской Федерации 31.12.2015 № 683.

«Стратегия национальной безопасности Российской Федерации» — официально признанная система стратегических приоритетов, целей и мер в области внутренней и внешней политики, определяющих состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу.

Стратегия является базовым документом по планированию развития системы обеспечения национальной безопасности Российской Федерации, в котором излагаются порядок действий и меры по обеспечению национальной безопасности.

Состояние национальной безопасности напрямую зависит от степени реализации стратегических национальных приоритетов и эффективности функционирования системы обеспечения национальной безопасности.

На основе Стратегии разработана «*Доктрина информационной безопасности Российской Федерации*», введенная в действие Указом Президента РФ от 05.12.2016 N 646.

Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. В Доктрине определены национальные интересы в информационной сфере, введены основные информационные угрозы и состояние информационной безопасности, сформулированы стратегические цели и основные направления обеспечения информационной безопасности, описаны организационные основы обеспечения информационной безопасности.

Законодательную основу обеспечения безопасности составляют:

- Конституция РФ;
- законы и другие нормативные акты РФ, регулирующие отношения в области безопасности;
- конституции, законы, нормативные акты республик;
- нормативные акты органов власти и управления краев, областей, принятые в пределах их компетенции;
- международные договоры и соглашения, заключенные или признанные РФ;
- основные законы в области защиты информации, прав субъектов, участвующих в информационных процессах и информатизации;
- федеральный закон «О безопасности» № 390-ФЗ от 28.12.2010;
- федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- федеральный закон от 21.09.93 г. № 182 «О государственной тайне»;
- федеральный закон от 27.07.06 г. № 152-ФЗ «О персональных данных»;

- федеральный закон от 27.12.91 г. «О средствах массовой информации»;
- федеральный закон от 6.04.11 г. № 63-ФЗ «Об электронной подписи»;
- Гражданский кодекс РФ (ч. 1, 2. 4);
- Уголовный кодекс РФ.

Помимо правовых документов, в Российской Федерации действуют нормативно-методические документы:

- методические документы государственных органов России: Доктрина информационной безопасности РФ, Руководящие документы ФСТЭК (Гостехкомиссии России), ведомственные приказы;
- стандарты информационной безопасности: международные стандарты, Государственные стандарты РФ, рекомендации по стандартизации, методические указания.

В целом развитие законодательной базы в области информационной безопасности идет по четырем основным направлениям:

- защита сведений, составляющих государственную тайну;
- защита конфиденциальной информации;
- защита авторского права в сфере информатизации;
- защита права на доступ к информации.

Систему *национальной безопасности* Российской Федерации образуют:

- органы законодательной, исполнительной и судебной властей;
- государственные, общественные и иные организации и объединения;
- граждане, принимающие участие в обеспечении безопасности в соответствии с законом;
- законодательство, регламентирующее отношения в сфере безопасности.

Силы обеспечения безопасности включают в себя:

- Вооруженные силы (ВС РФ);
- федеральные органы безопасности (ФСБ РФ);
- органы внутренних дел (МВД РФ);
- органы внешней разведки (СВР РФ);
- органы обеспечения безопасности органов законодательной, исполнительной, судебной властей и их высших должностных лиц;
- налоговую службу;
- службы ликвидации последствий чрезвычайных ситуаций (МЧС РФ);
- формирования гражданской обороны;
- пограничные войска;
- внутренние войска;
- органы, обеспечивающие безопасное ведение работ в промышленности, энергетике, на транспорте и в сельском хозяйстве;
- таможни, природоохранительные органы, органы охраны здоровья населения и другие государственные органы обеспечения безопасности.

Для рассмотрения вопросов внутренней и внешней политики РФ в области обеспечения безопасности, стабильности и правопорядка создан Совет безопасности РФ при Президенте. Он ответственен за состояние защищенности национальных интересов от внешних и внутренних угроз.

Совет безопасности РФ в соответствии с основными задачами его деятельности образует постоянные межведомственные комиссии, которые могут создаваться на функциональной или региональной основе. В частности, Межведомственная комиссия по защите государственной тайны разрабатывает и координирует федеральные программы по защите информации, составляющей государственную тайну.

Обеспечение информационной безопасности осуществляется в рамках обеспечения национальной безопасности России.

Оно предусматривает наличие государственной системы защиты информации и законодательства в этой области.

3.2. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность

Органы обеспечения информационной безопасности в совокупности с законодательством образуют государственную систему информационной безопасности и защиты информации.

Государственная система защиты информации включает:

- органы законодательной, исполнительной и судебной властей;
- законодательство, регулирующее отношения в области защиты информации и информационных ресурсов;
- нормативную правовую базу по защите информации;
- службы (органы) защиты информации предприятий, организаций, учреждений.

Структура государственной системы защиты информации представлена на рис. 3.1.

Органы законодательной власти (Государственная дума) издают законы, регулирующие отношения в области защиты информации. Их перечень рассмотрен в предыдущем разделе.

Нормативная база формируется на основе нормативных правовых актов в области защиты информации, издаваемых органами различных ветвей власти, министерствами, ведомствами. Основу нормативной базы составляют руководящие документы и стандарты, издаваемые Госстандартом.

Органы исполнительной власти (правительство) контролируют исполнение этих законов. Правительство принимает соответствующие постановления в области защиты информации и издает распоряжения, являющиеся подзаконными нормативными правовыми актами.

Рис. 3.1. Государственная система защиты информации

Министерства и ведомства в соответствии со своим предназначением разрабатывают и принимают постановления и реше-

ния, являющиеся нормативными правовыми актами. Кроме того, они разрабатывают и утверждают такие нормативные акты, как положения, руководства, инструкции, правила, методические рекомендации. К нормативным актам этого уровня относятся также приказы и письма руководителей ведомств и министерств.

К основным ведомствам, регулирующим отношения в области защиты информации, относятся:

- Межведомственная комиссия по защите государственной тайны;
- Федеральная служба технического и экспортного контроля (ФСТЭК);
- Госстандарт России;
- Федеральная служба безопасности (ФСБ РФ).

Кроме этого, в обеспечении информационной безопасности принимают участие Служба внешней разведки России и Федеральная пограничная служба.

Основным органом управления государственной системы защиты информации является ФСТЭК. В соответствии со своими функциями она осуществляет:

- координацию деятельности органов и организаций в области защиты информации, обрабатываемой техническими средствами;
- обеспечения защиты информации при помощи технических средств;
- организационно-методическое руководство деятельностью по защите информации;
- разработку и финансирование научно-технических программ по защите информации;
- утверждение нормативно-технической документации;
- функции государственного органа по сертификации продукции по требованиям безопасности информации;
- лицензирование деятельности предприятий по оказанию услуг в области защиты информации.

Для организации и осуществления защиты информации ФСТЭК издает соответствующие нормативные документы.

Госстандарт разрабатывает стандарты в области защиты информации.

Органы ФСБ РФ выполняют свои функции:

- при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;
- при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в России и её учреждениях, находящихся за пределами России;
- лицензирования и сертификации отдельных видов деятельности, предусматривающих допуск к государственной тайне Российской Федерации.

Органы МВД ведут борьбу с правонарушителями в информационной сфере и компьютерными преступлениями. Для этого в структуре МВД создано специальное управление «Р» для предотвращения и раскрытия компьютерных преступлений.

Органы Государственного таможенного комитета (ГТК) обязаны предупреждать незаконный ввоз и вывоз из России «пиратской» продукции, обеспечивая тем самым защиту авторских и патентных прав.

Руководители предприятий, организаций, учреждений в соответствии со своими должностными обязанностями при деятельности, связанной с информацией, которая составляет государственную или иную тайну, создают службу (подразделение) по защите информации. Для организации соответствующей деятельности они издают нормативные правовые акты (приказы, распоряжения), а также утверждают руководства, инструкции, положения, правила, методические рекомендации, касающиеся защиты информации и деятельности служб защиты информа-

ции. Для деятельности, связанной с государственной тайной, предприятие должно иметь лицензию на этот вид деятельности, в его структуру вводится специальный отдел ФСБ; все средства защиты должны быть сертифицированы.

Судебная власть осуществляет надзор и привлечение к ответственности за нарушения законодательства в информационной сфере. В своей деятельности суды руководствуются соответствующими статьями УК РФ, ГК РФ, КОАП.

Итак, информационная безопасность является важной составляющей национальной безопасности России. Политика государства в этой сфере деятельности направлена в первую очередь на организацию защиты государственной тайны и развитие правовых основ защиты информации. Правовая защита информации выступает как один из наиболее важных способов и методов защиты информации.

Вопросы для самоконтроля

1. Каково место информационной безопасности в системе национальной безопасности Российской Федерации?
2. Сформулируйте основные положения Доктрины информационной безопасности РФ.
3. Каковы основные цели защиты информации?
4. Каковы основные задачи в области информационной безопасности?
5. Какова структура государственной системы защиты информации?
6. Кто несет ответственность за нарушение режима защиты информации?
7. Каковы функции руководителей предприятий при организации защиты информации?
8. Каковы основные функции ФСТЭК?
9. Покажите роль различных министерств и ведомств в вопросах защиты информации.

4. Угрозы информационной безопасности

❖ Анализ уязвимостей системы ❖ Классификация угроз информационной безопасности ❖ Основные направления и методы реализации угроз ❖ Неформальная модель нарушителя ❖ Оценка уязвимости системы ❖

4.1. Анализ уязвимостей системы

При построении системы защиты информации обязательно нужно определить, что следует защищать и от кого (или чего) следует строить защиту. Определение информации, подлежащей защите, было дано выше. Защищаться следует от множества угроз, которые проявляются через действия нарушителя. Угрозы возникают в случае наличия в системе уязвимостей, то есть таких свойств информационной системы, которые могут привести к нарушению информационной безопасности.

Определение перечня угроз и построение модели нарушителя являются обязательным этапом проектирования системы защиты. Для каждой системы перечень наиболее вероятных угроз безопасности, а также характеристика наиболее вероятного нарушителя индивидуальны, поэтому перечень и модель должны носить неформальный характер. Защищенность информации обеспечивается только при соответствии предполагаемых угроз и качеств нарушителя реальной обстановке.

При наличии в системе уязвимости потенциальная угроза безопасности может реализоваться в виде атаки. Атаки принято классифицировать в зависимости от целей, мотивов, используемого механизма, места в архитектуре системы и местонахождения нарушителя.

Для предупреждения успешных атак необходим поиск и анализ уязвимостей системы. Уязвимости различаются в зависимости от источника возникновения, степени риска, распространенности, места в жизненном цикле системы, соотношения с подсистемами защиты. Анализ уязвимостей — обязательная процедура при аттестации объекта информатизации. В связи с возможностью появления новых уязвимостей необходим их периодический анализ на уже аттестованном объекте.

4.2. Классификация угроз информационной безопасности

Угроза — это фактор, стремящийся нарушить работу системы.

В настоящее время рассматривается достаточно обширный перечень угроз информационной безопасности, насчитывающий сотни пунктов.

Кроме выявления возможных угроз, должен быть проведен анализ этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из требований к системе защиты. При этом угрозы, соответствующие каждому признаку классификации, позволяют уточнить требования.

Для защищаемой системы составляют не полный перечень угроз, а перечень классов угроз, определяемых по ряду базовых признаков [3]. Это связано с тем, что описать полное множество угроз невозможно из-за большого количества факторов, влияющих на информацию.

Например, можно предложить классифицировать угрозы по следующим признакам:

1. Природа возникновения: естественные угрозы (связанные с природными процессами) и искусственные (вызванные деятельностью человека).

2. Степень преднамеренности проявления: случайные или преднамеренные.

3. Источник угроз: природная среда, человек, санкционированные программно-аппаратные средства, несанкционированные программно-аппаратные средства.

4. Положение источника угроз: в пределах или вне контролируемой зоны.

5. Зависимость от активности системы: проявляются только в процессе обработки данных или в любое время.

6. Степень воздействия на систему: пассивные, активные (вносят изменения в структуру и содержание системы).

7. Этап доступа к ресурсам: на этапе доступа, после получения доступа.

8. Способ доступа к ресурсам: стандартный, нестандартный.

9. Место расположения информации: внешние носители, оперативная помять, линии связи, устройства ввода-вывода.

Вне зависимости от конкретных видов угроз было признано целесообразным связать угрозы с основными свойствами защищаемой информации.

Соответственно для информационных систем было предложено рассматривать три основных вида угроз:

- *Угроза нарушения конфиденциальности* реализуется в том случае, если информация становится известной лицу, не располагающему полномочиями доступа к ней. Угроза нарушения конфиденциальности имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в информационной системе или передаваемой от одной системы к другой. Иногда в связи с угрозой нарушения конфиденциальности используется термин «утечка».
- *Угроза нарушения целостности* реализуется при несанкционированном изменении информации, хранящейся в информационной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно

изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

- *Угроза нарушения доступности* (отказа служб) реализуется, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Блокирование может быть постоянным — запрашиваемый ресурс никогда не будет получен, или может вызывать только задержку запрашиваемого ресурса.

Данные виды угроз можно считать первичными, или непосредственными, т. к. если рассматривать понятие угрозы как некоторой потенциальной опасности, реализация которой наносит ущерб информационной системе, то реализация вышеперечисленных угроз приведет к непосредственному воздействию на защищаемую информацию. В то же время непосредственное воздействие на информацию возможно для атакующей стороны в том случае, если система, в которой циркулирует информация, для нее «прозрачна», т. е. не существует никаких систем защиты или других препятствий. Описанные выше угрозы были сформулированы в 1960-х гг. применительно к открытым UNIX-подобным системам, для которых не предусматривались меры по защите информации.

На современном этапе развития информационных технологий подсистемы или функции защиты являются неотъемлемой частью комплексов по обработке информации. Информация не представляется «в чистом виде», на пути к ней имеется хотя бы какая-нибудь система защиты, и поэтому, чтобы угро-

жать, атакующая сторона должна преодолеть эту систему. Поскольку преодоление защиты также представляет собой угрозу, для защищенных систем будем рассматривать ее четвертый вид — *угрозу раскрытия параметров системы, включающей в себя систему защиты*. На практике любое проводимое мероприятие предваряется этапом разведки, в ходе которой определяются основные параметры системы, ее характеристики и т. п. Результатом разведки является уточнение поставленной задачи, а также выбор наиболее оптимального технического средства. Угрозу раскрытия параметров системы можно рассматривать как опосредованную. Последствия ее реализации не причиняют какой-либо ущерб обрабатываемой информации, но дают возможность реализоваться первичным, или непосредственным, угрозам, перечисленным выше. Введение данного вида угроз позволяет описывать с отличия защищенных информационных систем от открытых. Для последних угроза разведки параметров системы считается реализованной.

4.3. Основные направления и методы реализации угроз

К **основным направлениям** реализации злоумышленником информационных угроз относятся [3]:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая реализовать угрозы информационной безопасности;
- внедрение в технические средства программных или технических механизмов, нарушающих предполагаемую структуру и функции системы.

К числу **основных методов** реализации угроз информационной безопасности относятся [3, 5]:

- определение злоумышленником типа и параметров носителей информации;
- получение злоумышленником информации о программно-аппаратной среде, типе и параметрах средств вычислительной техники, типе и версии операционной системы, составе прикладного программного обеспечения;
- получение злоумышленником детальной информации о функциях, выполняемых системой;
- получение злоумышленником данных о применяемых системах защиты;
- определение способа представления информации;
- определение злоумышленником содержания данных, обрабатываемых в системе, на качественном уровне (применяется для мониторинга и для дешифрования сообщений);
- хищение (копирование) машинных носителей информации, содержащих конфиденциальные данные;
- использование специальных технических средств для перехвата побочных электромагнитных излучений и наводок (ПЭМИН);
- уничтожение средств вычислительной техники и носителей информации;
- несанкционированный доступ пользователя к ресурсам системы в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;
- несанкционированное превышение пользователем своих полномочий;
- несанкционированное копирование программного обеспечения;
- перехват данных, передаваемых по каналам связи;
- визуальное наблюдение;
- раскрытие представления информации (дешифрование данных);

- раскрытие содержания информации на семантическом уровне;
- уничтожение носителей информации;
- внесение пользователем несанкционированных изменений в программно-аппаратные компоненты системы и обрабатываемые данные;
- установка и использование нештатного аппаратного и/или программного обеспечения;
- заражение программными вирусами;
- внесение искажений в представление данных, уничтожение данных на уровне представления, искажение информации при передаче по линиям связи;
- внедрение дезинформации;
- выведение из строя носителей информации без уничтожения;
- проявление ошибок проектирования и разработки аппаратных и программных компонентов;
- искажение соответствия синтаксических и семантических конструкций языка;
- запрет на использование информации.

Перечисленные методы реализации угроз охватывают все уровни представления информации.

4.4. Неформальная модель нарушителя

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, с целью самоутверждения и т. п.) и использующее для этого различные возможности, методы и средства.

Злоумышленник — нарушитель, намеренно идущий на нарушение из корыстных побуждений.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т. п. Исследовав причины нарушений, можно либо повлиять на сами эти причины, либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

В каждом конкретном случае исходя из конкретной технологии обработки информации может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной системы.

Неформальная модель нарушителя разрабатывается при проектировании системы защиты и оценке защищенности информации.

При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителей.

По отношению к системе нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Практика показывает, что на долю внутренних нарушителей приходится более 2/3 от общего числа нарушений.

Внутренним нарушителем может быть лицо из следующих категорий персонала:

- руководители различных уровней должностной иерархии.
- пользователи системы;

- сотрудники отделов разработки и сопровождения программного обеспечения;
- персонал, обслуживающий технические средства;
- технический персонал, обслуживающий здания (уборщики, электрики, сантехники и др.);
- сотрудники службы безопасности.

Посторонние лица, которые могут быть нарушителями:

- посетители;
- клиенты;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т. п.);
- представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность);
- любые лица за пределами контролируемой территории.

Можно выделить три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Классификация нарушителей

По уровню знаний о системе:

1) знание функциональных особенностей, основных закономерностей формирования в системе массивов данных и потоков запросов к ним, умение пользоваться штатными средствами;

2) обладание высоким уровнем знаний и опытом работы с техническими средствами системы, а также опытом их обслуживания;
3) обладание высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации автоматизированных информационных систем;
4) знание структуры, функций и механизмов действия средств защиты, их сильные и слабые стороны.

По уровню возможностей:

Первый уровень определяет самый низкий уровень возможностей ведения диалога: запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяет возможность создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяет возможность управления функционированием системы, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяет весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств системы, вплоть до включения в состав собственных технических средств с новыми функциями по обработке информации.

Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

В своем уровне нарушитель является специалистом высшей квалификации, знает все о информационной системе, в частности, о системе и средствах ее защиты.

Классификация по уровню возможностей приводится в руководящем документе Гостехкомиссии «Концепция защиты

средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» в разделе «Модель нарушителя в автоматизированной системе».

По времени действия:

- в процессе функционирования (во время работы компонентов системы);
- в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т. п.);
- как в процессе функционирования, так и в период неактивности компонентов системы.

По месту действия:

- без доступа на контролируемую территорию организации;
- с контролируемой территории без доступа в здания и сооружения;
- внутри помещений, но без доступа к техническим средствам;
- с рабочих мест конечных пользователей (операторов);
- с доступом в зону данных (баз данных, архивов и т. п.);
- с доступом в зону управления средствами обеспечения безопасности.

Определение конкретных характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть определен с помощью характеристик, приведенных выше.

4.5. Оценка уязвимости системы

При решении практических задач защиты информации большое значение имеет количественная оценка ее уязвимости.

Ряд специалистов в области информационной безопасности разделяют методы и средства защиты от случайных и от преднамеренных угроз [6].

Для защиты от случайных угроз используются средства повышения надежности функционирования автоматизированных систем, средства повышения достоверности и резервирования информации.

При проектировании защиты от преднамеренных угроз определяются перечень и классификация по характеру, размещению, важности и времени жизни данных, подлежащих защите в заданной информационной системе. В соответствии с характером и важностью этих данных выбираются ожидаемая квалификация и модель поведения потенциального нарушителя. Рассмотрим ситуацию, когда угроза реализуется путем несанкционированного доступа к информации.

В соответствии с моделью нарушителя в проектируемой системе выявляются виды и количество возможных каналов несанкционированного доступа к защищаемым данным. Данные каналы делятся на технически контролируемые и неконтролируемые. Например, вход в систему со стороны клавиатуры может контролироваться специальной программой, а каналы связи территориально-распределенной системы — не всегда. На основе анализа каналов выбираются готовые или создаются новые средства защиты с целью перекрытия этих каналов.

Для создания единого постоянно действующего механизма защиты средства защиты с помощью специально выделенных средств централизованного управления объединяются в одну автоматизированную систему безопасности информации, которая путем анализа ее состава и принципов построения про-

веряется на предмет наличия возможных путей ее обхода. Если таковые обнаруживаются, то они перекрываются соответствующими средствами, которые также включаются в состав защитной оболочки. В результате будет построена замкнутая виртуальная оболочка защиты информации [6].

Степень защиты определяется полнотой перекрытия каналов утечки информации и возможных путей обхода средств защиты, а также прочностью защиты. Согласно принятой модели поведения нарушителя прочность защитной оболочки определяется средством защиты с наименьшим значением прочности из числа средств, составляющих эту оболочку.

Под *прочностью защиты* (преграды) понимается величина вероятности ее непреодоления нарушителем.

Прочность защитной преграды является достаточной, если ожидаемое время преодоления ее нарушителем больше времени жизни предмета защиты или больше времени обнаружения и блокировки доступа при отсутствии путей обхода этой преграды.

Защитная оболочка должна состоять из средств защиты, построенных по одному принципу (контроля или предупреждения несанкционированного доступа) и размещаемых на каналах доступа одного типа (технически контролируемых или неконтролируемых). На контролируемых каналах нарушитель рискует быть пойманным, а на неконтролируемых он может работать в комфортных условиях, не ограниченных временем и средствами. Прочность защиты во втором случае должна быть значительно выше. Поэтому целесообразно в информационной системе иметь отдельные виртуальные защитные оболочки: контролируемую и превентивную.

Кроме того, необходимо учитывать применение организационных мероприятий, которые в совокупности могут образовать свою защитную оболочку.

Стратегия и тактика защиты от преднамеренного несанкционированного доступа заключается в применении на возможных

каналах доступа к информации средств контроля, блокировки и предупреждения событий. Средства контроля и блокировки устанавливаются на возможных каналах доступа, где это возможно технически или организационно, а средства предупреждения (превентивные средства) применяются там, где такие возможности отсутствуют.

При расчете прочности средства защиты учитывается временной фактор, позволяющий получить количественную оценку его прочности — ожидаемую величину вероятности непреодоления его потенциальным нарушителем.

Рассмотрим варианты построения защитной оболочки и оценку ее прочности [6].

В простейшем случае предмет защиты помещен в замкнутую однородную защитную оболочку (рис. 4.1).

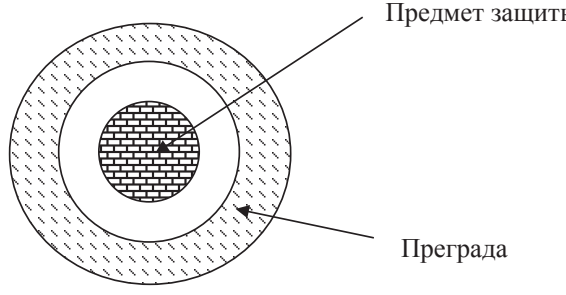


Рис. 4.1. Модель однозвенной защиты

Прочность защиты зависит от свойств преграды. Считается, что прочность созданной преграды достаточна, если стоимость ожидаемых затрат на ее преодоление потенциальным нарушителем превышает стоимость защищаемой информации.

Если обозначить вероятность непреодоления преграды нарушителем через $P_{н}$, вероятность преодоления преграды нарушителем через $P_{п}$, то согласно теории вероятности

$$P_{н} + P_{п} = 1.$$

В реальном случае у преграды могут быть пути ее обхода. Обозначим вероятность обхода преграды нарушителем через $P_о$. Нарушитель, действующий в одиночку, выберет один из путей: преодоление преграды или обходной вариант. Тогда, учитывая несовместность событий, формальное выражение прочности преграды можно представить в виде

$$P_н = \min \{(1 — P_п), (1 — P_о)\}.$$

Рассмотрим наиболее опасную ситуацию, когда нарушитель знает и выберет путь с наибольшей вероятностью преодоления преграды. В таком случае можно предположить, что прочность преграды определяется вероятностью ее преодоления или обхода потенциальным нарушителем по пути с наибольшим значением этой вероятности. То есть в случае действий единственного нарушителя прочность защиты определяется ее слабейшим звеном.

У преграды может быть несколько путей обхода. Тогда последнее выражение примет вид

$$P_н = \min \{(1 — P_п), (1 — P_{о1}), (1 — P_{о2}), (1 — P_{о3}), \ldots (1 — P_{оk})\},$$

где k — количество путей обхода.

Для случая, когда нарушителей более одного и они действуют одновременно (организованная группа) по каждому пути, это выражение с учетом совместности действий будет выглядеть так:

$$P_н = (1 — P_п)\,(1 — P_{о1})\,(1 — P_{о2})\,(1 — P_{о3}) \ldots (1 — P_{оk}).$$

Данная формула применима для неконтролируемой преграды.

Рассмотрим особенности расчета соотношений для контролируемой преграды. Когда к предмету защиты, имеющему постоянную ценность, необходимо и технически возможно обеспечить контроль доступа, обычно применяется постоянно действующая преграда, обладающая свойствами обнаруже-

ния и блокировки доступа нарушителя к предмету или объекту защиты.

Для анализа ситуации рассмотрим временную диаграмму процесса контроля и обнаружения несанкционированного доступа, приведенную на рис. 3.4.

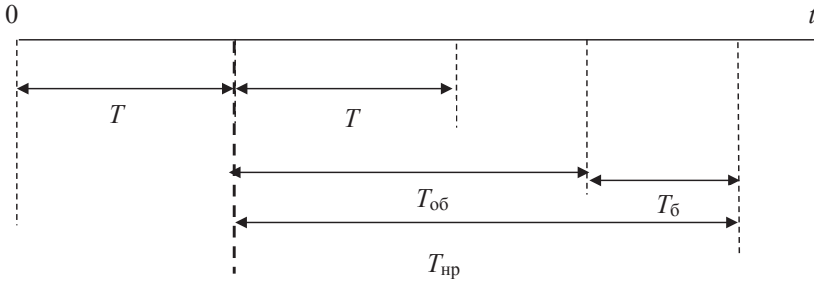


Рис. 4.2. Временная диаграмма процесса контроля и обнаружения НСД:

T — период опроса датчиков; $T_{об}$ — время передачи сигнала и обнаружения НСД; $T_б$ — время блокировки доступа; $T_{нр}$ — время нарушения

Из рис. 3.2 следует, что нарушитель может быть не обнаружен в двух случаях:

а) когда время нарушения меньше периода опроса датчиков: $T_{нр} < T$;

б) когда $T < T_{нр} < T_{об} + T_б$.

В случае а) требуется дополнительное условие — попадание интервала времени t в интервал T, т. е. необходима синхронизация действий нарушителя с частотой опроса датчиков обнаружения.

Формально эту задачу можно представить следующим образом. Есть последовательное множество событий в виде контрольных импульсов с расстоянием T между ними и есть определенное множество элементарных событий в виде отрезка длиной $T_{нр}$, который случайным образом накладывается на первое множество. Задача состоит в определении вероятности попадания отрезка $T_{нр}$ на контрольный импульс, если $T_{нр} < T$.

Если обозначить вероятность попадания отрезка на контрольный импульс, то есть вероятность обнаружения нарушения, через P_1, то

$$P_1 = \begin{cases} \dfrac{T_{\text{нр}}}{T}, T_{\text{нр}} < T, \\ 1, T_{\text{нр}} \geq T. \end{cases}$$

В случае б), когда $T < T_{\text{нр}} < T_{\text{об}} + T$, несанкционированный доступ фиксируется наверняка и вероятность обнаружения действий нарушителя будет определяться соотношением между $T_{\text{нр}}$ и $(T_{\text{об}} + T_{\text{б}})$.

Величина ожидаемого $T_{\text{нр}}$ зависит от многих факторов:

- характера поставленной задачи нарушения,
- метода и способа нарушения,
- технических возможностей и квалификации нарушителя,
- технических возможностей автоматизированной системы.

Поэтому можно говорить о вероятностном характере величины $T_{\text{нр.}}$ Если обозначить вероятность обнаружения и блокировки доступа через P_2, то

$$P_2 = \frac{T_{\text{нр}}}{T_{\text{об}} + T_{\text{б}}}.$$

Для более полного формального представления прочности преграды в виде системы обнаружения и блокировки несанкционированного доступа необходимо учитывать надежность ее функционирования и пути возможного обхода ее нарушителем.

Вероятность отказа системы определяется по формуле

$$P_{\text{отк}}(t) = e^{-\lambda t},$$

где λ — интенсивность отказов группы технических средств, составляющих систему обнаружения и блокировки; t — рассматриваемый интервал времени функционирования системы обнаружения и блокировки.

Исходя из наиболее опасной ситуации, считаем, что отказ системы контроля и НСД могут быть совместными событиями. Поэтому, с учетом этой ситуации формула прочности контролируемой преграды примет вид

$$P_{н} = \min\{P_2(1 - P_{отк}), (1 - P_{о1}), (1 - P_{о2}), (1 - P_{о3}), \ldots (1 - P_{ok})\},$$

где $P_{о}$ и количество путей обхода k определяются экспертным путем на основе анализа принципов построения конкретной системы контроля и блокировки несанкционированного доступа.

В случае, если ценность информации падает с течением времени, за условие достаточности защиты можно принять превышение затрат времени на преодоление преграды нарушителем над временем жизни информации. В качестве такой защиты может быть использовано криптографическое преобразование информации. Возможными путями обхода криптографической преграды могут быть криптоанализ исходного текста зашифрованного сообщения или доступ к действительным значениям ключей шифрования при хранении и передаче.

На практике в большинстве случаев защитный контур (оболочка) состоит из нескольких соединенных между собой преград с различной прочностью (рис. 4.3).

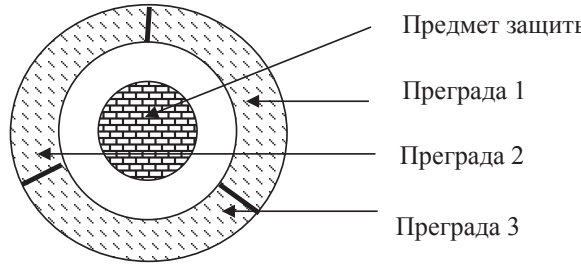


Рис. 4.3. Модель многозвенной защиты

Примером такого вида защиты может служить помещение, в котором хранится аппаратура. В качестве преград с различ-

ной прочностью здесь могут служить стены, потолок, пол, окна и замок на двери.

Формальное описание прочности многозвенной оболочки защиты почти полностью совпадает с однозвенной, т. к. наличие нескольких путей обхода одной преграды, не удовлетворяющих заданным требованиям, потребует их перекрытия другими преградами, которые в конечном итоге образуют многозвенную оболочку защиты.

Прочность многозвенной защиты из неконтролируемых преград, построенной для противостояния одному нарушителю, определяется по формуле

$$P_{\text{зи}} = \min\{P_{\text{сзи1}}, P_{\text{сзи2}}, P_{\text{сзи}i}, (1 - P_{\text{о1}}), (1 - P_{\text{о2}}), (1 - P_{\text{оз}}), \ldots (1 - P_{ok})\},$$

где $P_{\text{сзи}i}$ — прочность i-й преграды; P_{ok} — вероятность обхода преграды по k-му пути.

Прочность многозвенной защитной оболочки от одного нарушителя равна прочности ее слабейшего звена. Это правило справедливо и для защиты от неорганизованной группы нарушителей, действующих самостоятельно.

Прочность многозвенной защиты, построенной из неконтролируемых преград для защиты от организованной группы квалифицированных нарушителей, рассчитывается следующим образом:

$$P_{\text{зи0}} = P_{\text{сзи1}} \cdot P_{\text{сзи2}} \cdot \ldots P_{\text{сзи}i} (1 - P_{\text{о1}}) (1 - P_{\text{о2}}) (1 - P_{\text{оз}}) \ldots (1 - P_{ok}).$$

Прочность многозвенной защиты от организованной группы нарушителей равна произведению вероятностей непреодоления потенциальным нарушителем каждого из звеньев, составляющих эту защиту.

Расчет прочности многозвенной защиты с контролируемыми преградами аналогичен.

Расчеты итоговых прочностей защиты для неконтролируемых и контролируемых преград должны быть раздельными, по-

скольку исходные данные для них различны и, следовательно, на разные задачи должны быть разные решения — две разные оболочки защиты одного уровня.

Если прочность слабейшего звена защиты удовлетворяет предъявленным требованиям оболочки защиты в целом, возникает вопрос об избыточности прочности на остальных звеньях данной оболочки. Отсюда следует, что экономически целесообразно применять в многозвенной оболочке защиты равнопрочные преграды.

Если звено защиты не удовлетворяет предъявленным требованиям, преграду в этом звене следует заменить на более прочную или данная преграда дублируется еще одной преградой, а иногда двумя и более. Дополнительные преграды должны перекрывать то же количество или более возможных каналов несанкционированного доступа, что и первая.

В этом случае, если обозначить прочность дублирующих друг друга преград соответственно через $P_{д1}$, $P_{д2}$, $P_{д3}$, ..., $P_{дi}$, то вероятность преодоления каждой из них определяется как вероятность противоположного события: $(1 - P_{д1})$, $(1 - P_{д2})$, $(1 - P_{д3})$, ... $(1 - P_{дi})$.

Считаем, что факты преодоления этих преград нарушителем — события совместные. Это позволяет вероятность преодоления суммарной преграды нарушителем представить в виде

$$P_{п} = (1 - P_{д1})\,(1 - P_{д2})\,(1 - P_{д3}) \ldots (1 - P_{дi}).$$

В ответственных случаях при повышенных требованиях к защите применяется многоуровневая защита, модель которой представлена на рис. 4.4.

При расчете суммарной прочности многоуровневой защиты суммируются прочности отдельных уровней.

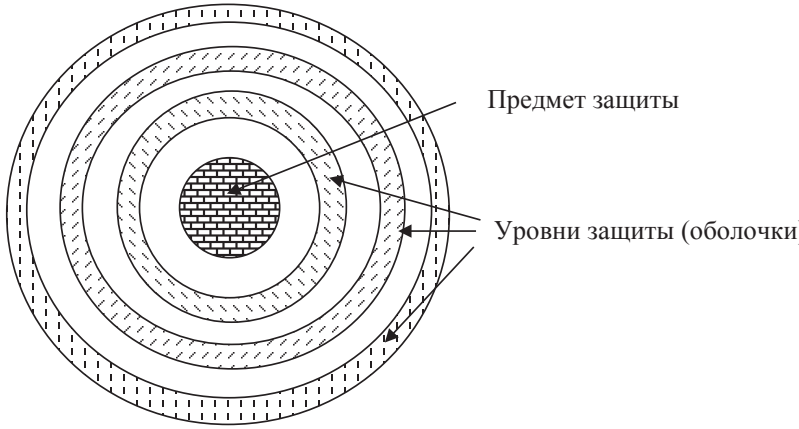


Рис. 4.4. Модель многоуровневой защиты

ВЫВОДЫ

- Система защиты информации должна предусматривать защиту от всех видов случайных и преднамеренных 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 путей и методов доступа к данным и вмешательства в процессы обработки и обмена информацией. Анализ всех уязвимостей системы, оценка возможного ущерба позволят верно определить мероприятия по защите информации. Расчет эффективности защитных мероприятий можно производить различными методами в зависимости от свойств защищаемой информации и модели нарушителя.
- Правильно построенная (адекватная реальности) модель нарушителя, в которой отражаются его практические и теоретические возможности, априорные знания, время и место действия и другие характеристики, явля-

ется важной составляющей успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

Вопросы для самоконтроля

1. На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности).
2. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
3. Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
4. В каких системах на первом месте стоит обеспечение доступности информации?
5. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
6. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
7. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.
8. Выведите формулу для расчета прочности трехуровневой защитной оболочки.
9. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.

5. Построение систем защиты от угрозы нарушения конфиденциальности

❖ Определение и основные способы несанкционированного доступа ❖ Методы защиты от НСД ❖ Организационные методы защиты от НСД ❖ Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам ❖ Идентификация и аутентификации ❖ Основные направления и цели использования криптографических методов ❖ Защита от угрозы нарушения конфиденциальности на уровне содержания информации ❖

5.1. Определение и основные способы несанкционированного доступа

В соответствии с определением несанкционированный доступ является одним из видов утечки информации.

Как уже было сказано выше, несанкционированным доступом к информации (НСД), согласно руководящим документам Гостехкомиссии, является доступ к информации, нарушающий установленные правила разграничения доступа. НСД может носить случайный или преднамеренный характер.

В результате НСД чаще всего реализуется угроза конфиденциальности информации, однако целью злоумышленника может быть и реализация других видов угроз (целостности информации, раскрытия параметров системы).

Для преднамеренного НСД используются как общедоступные, так и скрытые способы и средства.

Такими способами являются [3]:

- инициативное сотрудничество (предательство);
- склонение к сотрудничеству (подкуп, шантаж);
- подслушивание переговоров самыми различными путями;

- негласное ознакомление со сведениями, составляющими тайну;
- хищение, копирование, подделка, уничтожение;
- незаконное подключение к каналам и линиям связи и передачи данных;
- перехват (акустический или радиоперехват, в том числе и за счет побочных электромагнитных излучений и наводок);
- визуальное наблюдение, фотографирование;
- сбор и аналитическая обработка детальной информации или производственных отходов.

К основным способам НСД в информационных системах относятся [3]:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая осуществить НСД;
- внедрение в технические средства информационной системы программных или технических механизмов, нарушающих предполагаемую структуру и функции системы и позволяющих осуществить НСД.

Зная совокупность источников информации, возможные каналы утечки охраняемых сведений и многообразие способов несанкционированного доступа к источникам, можно приступать к выработке мероприятий по защите.

5.2. Методы защиты от НСД

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

- организационные (в т. ч. административные);
- технологические (или инженерно-технические);
- правовые;
- финансовые;
- морально-этические (или социально-психологические).

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников.

Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например, систем идентификации и аутентификации или охранной сигнализации.

Третья категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации.

Финансовые методы защиты предполагают введение специальных доплат при работе с защищаемой информацией, а также систему вычетов и штрафов за нарушение режимных требований.

Морально-этические методы не носят обязательного характера, однако являются достаточно эффективными при борьбе с внутренними нарушителями.

Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

5.3. Организационные методы защиты от НСД

Эффективная защита информации возможна при обязательном выполнении ряда условий:

- единство в решении производственных, коммерческих, финансовых и режимных вопросов;
- координация мер безопасности между всеми заинтересованными подразделениями предприятия;
- научная оценка информации и объектов, подлежащих классификации (защите); разработка режимных мер до начала проведения режимных работ;
- персональная ответственность (в том числе и материальная) руководителей всех уровней, исполнителей, участвующих в закрытых работах, за обеспечение сохранности тайны и поддержание на должном уровне режима охраны проводимых работ;
- включение основных обязанностей рабочих, специалистов и администрации по соблюдению конкретных требований режима в коллективный договор, контракт, трудовое соглашение, правила трудового распорядка;
- организация специального делопроизводства, порядка хранения, перевозки носителей тайны; введение соответствующей маркировки документов и других носителей закрытых сведений;
- формирование списка лиц, уполномоченных руководителем предприятия классифицировать информацию и объекты, содержащие конфиденциальные сведения;
- оптимальное ограничение числа лиц, допускаемых к защищаемой информации;
- наличие единого порядка доступа и оформления пропусков;
- выполнение требований по обеспечению сохранения защищаемой информации при проектировании и размещении специальных помещений, в процессе опытно-кон-

структорской разработки, испытаний и производства изделий, сбыта, рекламы, подписания контрактов, при проведении особо важных совещаний, в ходе использования технических средств обработки, хранения и передачи информации и т. п.;

- организация взаимодействия с государственными органами власти, имеющими полномочия по контролю определенных видов деятельности предприятий и фирм;
- наличие охраны, пропускного и внутриобъектового режимов;
- плановость разработки и осуществления мер по защите информации, систематический контроль за эффективностью принимаемых мер;
- создание системы обучения исполнителей правилам обеспечения сохранности информации.

5.4. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам

Нарушение конфиденциальности происходит в результате утечки информации. Защита информации от утечки — это деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Основными причинами утечки информации являются [3]:

- несоблюдение персоналом норм, требований, правил эксплуатации;
- ошибки в проектировании системы и систем защиты;
- ведение противостоящей стороной технической и агентурной разведок.

Причины утечки информации достаточно тесно связаны с видами утечки информации.

В соответствии с ГОСТ Р 50922–96 рассматриваются три вида утечки информации:

- разглашение;
- несанкционированный доступ к информации;
- получение защищаемой информации разведками (как отечественными, так и иностранными).

Канал утечки информации — совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может быть в пределах контролируемой зоны или вне ее.

При выявлении каналов утечки информации необходимо рассматривать всю совокупность элементов системы, включающую основное оборудование технических средств обработки информации, оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей информации, необходимо учитывать и вспомогательные технические средства и системы, такие как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др.

В качестве каналов утечки большой интерес представляют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещения с установленными в них основными и вспомогательными техническими средствами, металлические трубы систем ото-

пления, водоснабжения и другие токопроводящие металлоконструкции.

Следует помнить о внутренних каналах утечки информации, связанных с действиями администрации и обслуживающего персонала, с качеством организации режима работы, тем более что обычно им не придают должного внимания. Из них в первую очередь можно отметить такие каналы утечки, как хищение носителей информации, использование производственных и технологических отходов, визуальный съем информации с монитора и принтера, несанкционированное копирование и т. п.

Каналы утечки информации *по физическим принципам* можно разделить на следующие группы:

- акустические (включая и акустопреобразовательные). Связаны с распространением звуковых волн в воздухе или упругих колебаний в других средах;
- электромагнитные (в том числе магнитные и электрические);
- визуально-оптические (наблюдение, фотографирование). В качестве средства выделения информации в данном случае могут рассматриваться фото-, видеокамеры и т. п.;
- материально-вещественные (бумага, фото, магнитные носители, отходы и т. п.);
- информационные. Связаны с доступом к элементам системы, носителям информации, самой вводимой и выводимой информации, к программному обеспечению, а также с подключением к линиям связи.

На практике применяется также деление каналов утечки на технические (к ним относятся акустические, визуально-оптические и электромагнитные) и информационные.

При оценке степени опасности технических каналов утечки следует иметь в виду, что не всегда наличие носителя (акустического или электромагнитного поля) является фактором, достаточным для съема информации. Например, при низкой

разборчивости речи невозможно восстановить ее смысл. Побочные электромагнитные излучения электронной аппаратуры могут не нести информативного сигнала (например, излучение, возникшее вследствие генерации тактовых импульсов средств вычислительной техники). Для объективной оценки проводят специальные исследования оборудования и специальные проверки рабочих помещений. Такого рода исследования и проверки выполняются организациями, имеющими лицензии на соответствующий вид деятельности. При выявлении технических каналов утечки информации применяются меры по их перекрытию.

5.5. Идентификация и аутентификация

К категории технологических методов защиты от НСД относятся идентификация и аутентификация.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать гарантированность того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя. В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы. Различают три группы методов аутентификации, основанных на наличии у пользователей:

- индивидуального объекта заданного типа;
- индивидуальных биометрических характеристик;
- знаний некоторой известной только пользователю и проверяющей стороне информации.

К первой группе относятся методы аутентификации, предполагающие использование удостоверений, пропуска, магнит-

ных карт и других носимых устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.

Во вторую группу входят методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем «подделать» биометрические параметры практически невозможно.

Последнюю группу составляют методы аутентификации, при которых используются пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией. Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны. Третью сторону называют сервером аутентификации или арбитром.

Выбирая тот или иной протокол аутентификации, необходимо определить, какая именно аутентификация требуется — односторонняя или взаимная, нужно ли использовать доверенное третье лицо и если да, то какая из сторон — претендент или верификатор — будет с ним взаимодействовать. Протоколы бездиалоговой аутентификации часто осуществляют еще и контроль целостности данных.

5.6. Основные направления и цели использования криптографических методов

При построении защищенных систем роль криптографических методов для решения различных задач информационной безопасности трудно переоценить. Криптографические методы в настоящее время являются базовыми для обеспечения надежной аутентификации сторон информационного обмена, защиты информации в транспортной подсистеме, подтверждения целостности объектов информационной системы и т. д.

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

Криптография занимается поиском и исследованием математических методов преобразования информации. Криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

Сфера интересов криптоанализа — исследование возможности расшифровывания информации без знания ключей.

Основные направления и цели использования криптографических методов:

- передача конфиденциальной информации по каналам связи (например, электронная почта);
- обеспечение достоверности и целостности информации;
- установление подлинности передаваемых сообщений;
- хранение информации (документов, баз данных) на носителях в зашифрованном виде;
- выработка информации, используемой для идентификации и аутентификации субъектов, пользователей и устройств;

- выработка информации, используемой для защиты аутентифицирующих элементов защищенной системы.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите.

Алфавит — конечное множество используемых для кодирования информации знаков.

Текст — упорядоченный набор из элементов алфавита.

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

- алфавит Z33–32 буквы русского алфавита и пробел;
- алфавит Z256 — символы, входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит — Z2 = {0,1};
- восьмеричный алфавит или шестнадцатеричный алфавит;

Шифрование — преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом (рис. 5.1).

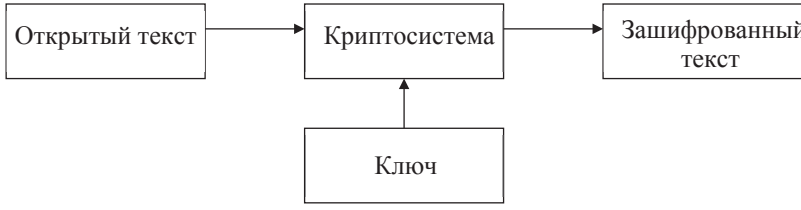


Рис. 5.1. Шифрование

Дешифрование — обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный (рис. 5.2).

Ключ — информация, необходимая для беспрепятственного шифрования и дешифрования текстов. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на симметричные и ассиметричные (с открытым ключом).

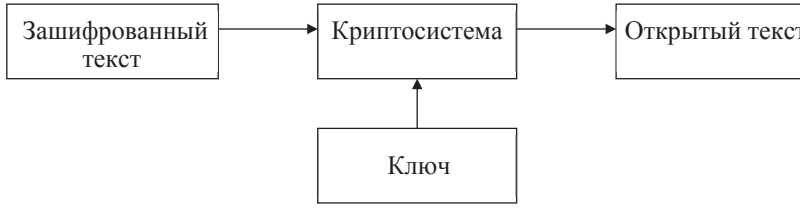


Рис. 5.2. Дешифрование

В *симметричных криптосистемах* и для шифрования, и для дешифрования используется один и тот же ключ: источник зашифровывает открытый текст на секретном ключе K, а приемник расшифровывает шифртекст на секретном ключе K*. Обычно K = K*.

В *ассиметричных системах (системах с открытым ключом)* используются два ключа — открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения или наоборот.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т. е. криптоанализу).

В зависимости от исхода криптоанализа все алгоритмы шифрования можно разделить на три группы.

К первой группе относятся совершенные шифры, заведомо не поддающиеся дешифрованию (при правильном использовании). Примером такого шифра является шифр гаммирования случайной равновероятной гаммой.

Во вторую группу входят шифры, допускающие неоднозначное дешифрование. Например, такая ситуация возникает, если зашифровать с помощью шифра простой замены очень короткое сообщение.

Основная масса используемых шифров относится к третьей группе и может быть в принципе однозначно дешифрована.

Сложность дешифрования шифра из этой группы будет определяться трудоемкостью используемого алгоритма дешифрования. Следовательно, для оценки стойкости такого шифра необходимо рассмотреть все известные алгоритмы дешифрования и выбрать из них имеющий минимальную трудоемкость, т. е. тот, который работает в данном случае быстрее всех остальных. Трудоемкость этого алгоритма и будет характеризовать стойкость исследуемого шифра.

Удобнее всего измерять трудоемкость алгоритма дешифрования в элементарных операциях, но более наглядным параметром является время, необходимое для вскрытия шифра (при этом необходимо указывать технические средства, которые доступны криптоаналитику). Не следует забывать, что вполне возможно существование неизвестного на данный момент алгоритма, который может значительно снизить вычисленную стойкость шифра. К большому сожалению разработчиков шифросистем, строго доказать с помощью математических методов невозможность существования простых алгоритмов дешифрования удается чрезвычайно редко. Очень хорошим результатом в криптографии является доказательство того, что сложность решения задачи дешифрования исследуемого шифра эквивалентна сложности решения какой-нибудь известной математической задачи. Такой вывод хотя и не дает 100 % гарантии, но позволяет надеяться, что существенно понизить оценку стойкости шифра в этом случае будет очень непросто.

К средствам криптографической защиты информации (СКЗИ) относятся:

- аппаратные;
- программно-аппаратные;
- программные средства.

Предполагается, что СКЗИ используются в некоторой информационной системе совместно с механизмами реализации и гарантирования политики безопасности.

Можно говорить о том, что СКЗИ производят защиту объектов на семантическом уровне. В то же время объекты-параметры криптографического преобразования являются полноценными объектами информационной системы и могут быть объектами некоторой политики безопасности (например, ключи шифрования могут и должны быть защищены от НСД, открытые ключи для проверки цифровой подписи — от изменений и т. д.).

Основные причины нарушения безопасности информации при ее обработке СКЗИ:

1. Утечка информации по техническим каналам.
2. Неисправности в элементах СКЗИ.
3. Работа совместно с другими программами: непреднамеренное и преднамеренное влияние (криптовирусы).
4. Воздействие человека.

В связи с этим помимо встроенного контроля за пользователем, необходимо отслеживание правильности разработки и использования средств защиты с применением организационных мер.

Процесс синтеза и анализа СКЗИ отличается высокой сложностью и трудоемкостью, поскольку необходим всесторонний учет влияния перечисленных выше угроз на надежность реализации СКЗИ. В связи с этим практически во всех странах, обладающих развитыми криптографическими технологиями, разработка СКЗИ относится к сфере государственного регулирования. Государственное регулирование включает, как правило, лицензирование деятельности, связанной с разработкой и эксплуатацией криптографических средств, сертификацию СКЗИ и стандартизацию алгоритмов криптографических преобразований.

В России в настоящее время организационно-правовые и научно-технические проблемы синтеза и анализа СКЗИ находятся в компетенции ФСБ.

Правовая сторона разработки и использования СКЗИ регламентируется в основном указом Президента Российской Феде-

рации от 03.04.95 № 334 с учетом принятых ранее законодательных и нормативных актов РФ.

Дополнительно учитываемой законодательной базой являются законы «О федеральных органах правительственной связи и информации», «О государственной тайне», «Об информации, информационных технологиях и о защите информации», «О сертификации продукции и услуг».

В настоящее время шифрование является единственным надежным средством защиты при передаче информации.

5.7. Защита от угрозы нарушения конфиденциальности на уровне содержания информации

Существуют различные методы защиты конфиденциальности информации на уровне содержания.

Рассмотрим ситуацию, когда злоумышленнику удалось получить доступ к синтаксическому представлению конфиденциальной информации, т. е. он имеет перед собой последовательность знаков некоторого языка, удовлетворяющую формальным правилам нотации. Данная ситуация может возникнуть, например, тогда, когда удалось дешифровать файл данных и получить текст, который может рассматриваться как осмысленный. В этом случае для сокрытия истинного содержания сообщения могут применяться различные приемы, суть которых сводится к тому, что в соответствие одной последовательности знаков или слов одного языка ставятся знаки или слова другого.

В качестве примера можно привести шифр «Аве Мария», в кодовом варианте которого каждому слову, а порой и фразе ставятся в соответствие несколько слов явной религиозной тематики, в результате чего сообщение выглядит как специфический текст духовного содержания. Обычный жаргон также мо-

жет иллюстрировать применяемые в повседневной практике подходы к сокрытию истинного смысла сообщений.

Другим направлением защиты является использование стеганографии. Слово «стеганография» в переводе с греческого буквально означает «тайнопись». К ней относится огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков (применяемое в сигнальной агентурной связи), цифровые подписи, тайные каналы и средства связи на плавающих частотах.

Вот какое определение предлагает Маркус Кун: «Стеганография — это искусство и наука организации связи таким способом, который скрывает собственно наличие связи. В отличие от криптографии, где неприятель имеет возможность обнаруживать, перехватывать и декодировать сообщения — при том, что ему противостоят определенные меры безопасности, гарантированные той или иной криптосистемой, — методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы нельзя было даже подозревать существования подтекста» [3].

Применительно к компьютерным технологиям можно сказать, что стеганография использует методы размещения файла-сообщения в файле- «контейнере», изменяя файл-«контейнер» таким образом, чтобы сделанные изменения были практически незаметны. Большинство из компьютерных стеганографических приемов объединяет методология изменения наименьшего значимого бита (Least Significant Bits-LSB), который считается «шумящим», т. е. имеющим случайный характер в отдельных байтах файла-«контейнера».

На практике в большинстве случаев открытый контейнер не содержит бесполезных данных, которые могут быть использованы для модификации. Вместо этого контейнерные файлы естественно содержат различные уровни шума, который при ближайшем рассмотрении, за исключением остальной части байта, может являться произвольной величиной. Звуковой

(.WAV) файл, например, содержит по большей части неслышный шум фона на уровне LSB; 24-битовый графический образ будет содержать изменения цвета, которые почти незаметны человеческому глазу.

ВЫВОДЫ

- Эффективная защита от НСД возможна только при сочетании различных методов: организационных, технических, нормативно-правовых.
- Для перекрытия каналов несанкционированного доступа к информации большое значение имеет построение систем идентификации и аутентификации, позволяющих ограничить доступ к защищаемой информации. Подобные системы используются как при контроле физического доступа (биометрическая аутентификация, аутентификация с использованием определенного объекта), так и при контроле доступа к ресурсам и данным (парольные системы).
- В настоящее время криптографические методы защиты информации от несанкционированного доступа являются единственным надежным средством защиты при передаче информации по каналам связи. Целесообразно использовать криптографическую защиту при хранении информации, что позволит в сочетании с мерами по ограничению доступа предотвратить несанкционированный доступ к информации.

Вопросы для самоконтроля

1. В чем отличие терминов «НСД» и «Нарушение конфиденциальности информации»?
2. Что понимается под утечкой информации?
3. Каким образом классифицируются каналы утечки информации?

4. Каким образом следует выбирать меры защиты конфиденциальности информации?
5. Дайте определение идентификации и аутентификации пользователя. В чем разница между этими понятиями?
6. Перечислите основные способы аутентификации. Какой, на Ваш взгляд, является наиболее эффективным?
7. Какие основные методы контроля доступа используются в известных вам информационных системах? В чем их достоинства и недостатки?
8. Почему аутентификация с использованием пароля считается в настоящее время ненадежной?
9. Каковы методы аутентификации с использованием предметов заданного типа? Назовите те, которые получили распространение в последнее время.
10. Дайте определение шифра и сформулируйте основные требования к нему.
11. Поясните, что понимается под совершенным шифром.
12. Почему большинство современных шифрограмм могут быть однозначно дешифрованы?
13. Каким образом государство регулирует использование средств крипозащиты?

6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа

❖ Защита целостности информации при хранении ❖ Защита целостности информации при обработке ❖ Защита целостности информации при транспортировке ❖ Защита от угрозы нарушения целостности информации на уровне содержания ❖ Построение систем защиты от угрозы отказа доступа к информации ❖ Защита семантического анализа и актуальности информации ❖

Понятие целостности данных в научной литературе имеет несколько определений. В одной из наиболее распространенных трактовок под целостностью данных подразумевается отсутствие ненадлежащих изменений. Смысл понятия «ненадлежащее изменение» раскрывается Д. Кларком и Д. Вилсоном: ни одному пользователю автоматизированной системы, в том числе и авторизованному, не должны быть разрешены такие изменения данных, которые повлекут за собой их разрушение или потерю [3].

Нарушение целостности информации происходит либо при несанкционированном доступе к информации, либо без него.

Угроза целостности существует на всех этапах жизни информации:

- при хранении;
- обработке;
- транспортировке.

6.1. Защита целостности информации при хранении

В информационной системе основное место хранения информации — электронные носители, поэтому рассмотрим меры защиты применительно к этому классу носителей.

Определяя порядок хранения информации на электронных носителях, следует иметь в виду, что от состояния носителей зависит качество программ и защищаемых данных. Электронные носители являются утройствами, подвергаюшимися интенсивному износу. Кроме того, в электронные носители могут быть внедрены закладки, поэтому используемые методы записи, хранения и считывания нельзя считать защищенными.

Организационно-технологические меры защиты целостности информации на электронных носителях можно разделить на две основные группы:

- организационные меры по поддержке целостности информации;
- технологические меры контроля целостности битовых последовательностей.

Организационные меры

Организационные меры защиты направлены на предупреждение хищения или утраты носителей, а вместе с ними и информации. Организационные меры излагаются в документах, описывающих режим хранения конфиденциальной информации.

Организационные меры разделяются на две группы:

- создание резервных копий информации, хранимой на электронных носителях;
- обеспечение правильных условий хранения и эксплуатации носителей.

Создание резервных копий

Создание резервных копий информации, хранимой в информационной системе, должно быть обязательной регулярной процедурой, периодичность которой зависит от важности информации и технологии ее обработки, в частности от объема вводимых данных, возможности повторного ввода и т. д. Для создания резервных копий могут использоваться как стандартные утилиты, так и специализированные системы резервного

копирования, адаптированные к конкретной системе. В последнем случае можно применять собственные методы «разностного» архивирования, когда на вспомогательный носитель записывается, а только та часть информации, которая была введена с момента последнего сохранения.

В качестве вспомогательных носителей для хранения архивных данных выбирают, как правило, те, которые оптимальны по цене единицы хранимой информации.

При ведении резервных копий необходимо регулярно проверять сохранность и целостность находящейся в них информации.

Обеспечение правильных условий хранения и эксплуатации

Обеспечение правильных условий хранения и эксплуатации определяется конкретным типом носителя.

Регистрация и учет носителей производятся независимо от того, есть ли на них конфиденциальная информация или нет. Служебные носители должны иметь ясную, хорошо видимую этикетку, на которой проставлены гриф, номер, дата регистрации. Гриф секретности носителя может изменяться только в большую сторону, т. к. информация не может быть гарантированно удалена. Учет носителей по журналу ведется в течение всей «жизни» носителя. В помещении не должно быть личных носителей. Не допускается работа с непроверенными носителями. Должна проводиться систематическая комиссионная проверка наличия носителей и информации.

Хранение электронных носителей такое же, как обычных документов такого же уровня конфиденциальности. Основное требование при хранении — исключение НСД. Передача между подразделениями должна осуществляться под расписку и учитываться в журнале. Вынос за пределы помещения возможен только с разрешения уполномоченных лиц.

Жесткий диск регистрируется с грифом, соответствующим категории компьютера, независимо от целей его использования. На корпусе жесткого диска должна быть соответствующая

этикетка. При передаче компьютера в ремонт необходимо либо изъять жесткий диск, либо гарантированно удалить с него информацию, либо присутствовать при ремонте.

Копирование файлов с зарегистрированных электронных носителей допускается только на компьютерах, категория которых не ниже грифа секретности носителя. Каждое копирование должно учитываться в обычном или электронном журнале.

Следует уделять особое внимание удалению информации с носителей. Обычные способы удаления файлов не приводят к удалению области данных, происходит стирание только на логическом уровне. Кроме того, при удалении следует учесть, что в современных средствах обработки информация существует в нескольких экземплярах, под разными именами.

Технологические меры

Рассмотрим теперь технологические меры контроля целостности битовых последовательностей, хранящихся на электронных носителях. Целостность информации в областях данных проверяется с помощью контрольного кода, контрольные числа которого записываются после соответствующих областей, причем в контролируемую область включаются соответствующие маркеры.

Для обеспечения контроля целостности информации чаще всего применяют циклический контрольный код. Этот метод, дающий хорошие результаты при защите от воздействия случайных факторов (помех, сбоев и отказов), совсем не обладает имитостойкостью, т. е. не обеспечивает защиту от целенаправленных воздействий нарушителя, приводящих к навязыванию ложных данных.

Для контроля целостности можно использовать методы имитозащиты, основанные на криптографических преобразованиях. Они обеспечивают надежный контроль данных, хранящихся в системе, но в то же время реализуются в виде объемных программ и требуют значительных вычислительных ресурсов.

6.2. Защита целостности информации при обработке

При рассмотрении вопроса целостности данных при обработке используется интегрированный подход, основанный на ряде работ Д. Кларка и Д. Вилсона, а также их последователей и оппонентов и включающий в себя девять теоретических принципов [3]:

- корректность транзакций;
- аутентификация пользователей;
- минимизация привилегий;
- разграничение функциональных обязанностей;
- аудит произошедших событий;
- объективный контроль;
- управление передачей привилегий;
- обеспечение непрерывной работоспособности;
- простота использования защитных механизмов.

Понятие *корректности транзакций* определяется следующим образом. Пользователь не должен модифицировать данные произвольно, а только определенными способами, т. е. так, чтобы сохранялась целостность данных. Другими словами, данные можно изменять только путем корректных транзакций и нельзя произвольными средствами. Кроме того, предполагается, что «корректность» каждой из таких транзакций может быть некоторым способом доказана.

Второй принцип гласит, что изменение данных может осуществляться только специально *аутентифицированными* для этой цели пользователями. Данный принцип работает совместно с последующими четырьмя, с которыми тесно связана его роль в общей схеме обеспечения целостности.

Идея *минимизации привилегий* появилась еще на ранних этапах развития информационной безопасности в форме ограничения, накладываемого на возможности выполняющихся в системе процессов и подразумевающего то, что процессы

должны быть наделены теми и только теми привилегиями, которые естественно и минимально необходимы для выполнения процессов. Принцип минимизации привилегий распространяется и на программы, и на пользователей. Пользователи имеют, как правило, несколько больше привилегий, чем им необходимо для выполнения конкретного действия в данный момент времени. А это открывает возможности для злоупотреблений.

Разграничение функциональных обязанностей подразумевает организацию работы с данными таким образом, что в каждой из ключевых стадий, составляющих единый критически важный, с точки зрения целостности, процесс, необходимо участие различных пользователей. Это гарантирует невозможность выполнения одним пользователем всего процесса целиком (или даже двух его стадий) с тем, чтобы нарушить целостность данных. В обычной жизни примером воплощения данного принципа служит передача одной половины пароля для доступа к программе управления ядерным реактором первому системному администратору, а другой — второму.

Аудит произошедших событий, включая возможность восстановления полной картины происшедшего, является превентивной мерой в отношении потенциальных нарушителей.

Принцип *объективного контроля* также является одним из краеугольных камней политики контроля целостности. Суть данного принципа заключается в том, что контроль целостности данных имеет смысл лишь тогда, когда эти данные отражают реальное положение вещей. В связи с этим Кларк и Вилсон указывают на необходимость регулярных проверок, имеющих целью выявление возможных несоответствий между защищаемыми данными и объективной реальностью, которую они отражают.

Управление передачей привилегий необходимо для эффективной работы всей политики безопасности. Если схема назначения привилегий неадекватно отражает организационную структуру предприятия или не позволяет администраторам без-

опасности гибко манипулировать ею для обеспечения эффективности производственной деятельности, защита становится обременительной и провоцирует попытки обойти ее.

Принцип *обеспечения непрерывной работы* включает защиту от сбоев, стихийных бедствий и других форс-мажорных обстоятельств.

Простота использования защитных механизмов необходима, в том числе для того, чтобы пользователи не стремились обойти их как мешающих «нормальной» работе. Кроме того, как правило, простые схемы являются более надежными. Простота использования защитных механизмов подразумевает, что самый безопасный путь эксплуатации системы будет также наиболее простым, и наоборот, самый простой — наиболее защищенным.

6.3. Защита целостности информации при транспортировке

Средства контроля целостности должны обеспечивать защиту от несанкционированного изменения информации нарушителем при ее передаче по каналам связи.

При транспортировке информации следует защищать как целостность, так и подлинность информации.

Схема контроля целостности данных подразумевает выполнение двумя сторонами — *источником* и *приемником* — некоторых (возможно, разных) криптографических преобразований данных. Источник преобразует исходные данные и передает их приемнику вместе с некоторым приложением, обеспечивающим избыточность шифрограммы.

Приемник обрабатывает полученное сообщение, отделяет приложение от основного текста и проверяет их взаимное соответствие, осуществляя таким образом контроль целостности.

Контроль целостности может выполняться с *восстановлением* или *без восстановления* исходных данных.

Целостность отдельного сообщения обеспечивается имитовставкой, ЭЦП или шифрованием, целостность потока сообщений — соответствующим механизмом целостности.

Имитовставка

Для обеспечения целостности в текст сообщения часто вводится некоторая дополнительная информация, которая легко вычисляется, если секретный ключ известен, и является трудновычислимой в противном случае. Если такая информация вырабатывается и проверяется с помощью одного и того же секретного ключа, то ее называют *имитовставкой* (в зарубежных источниках используется термин *код аутентификации сообщений* — Message Authentication Code (MAC) — поскольку помимо целостности может обеспечиваться еще и аутентификация объекта). Имитовставкой может служить значение хэш-функции, зависящей от секретного ключа, или выходные данные алгоритма шифрования в режиме сцепления блоков шифра.

Шифрование

Целостность данных можно обеспечить и с помощью их шифрования симметричным криптографическим алгоритмом при условии, что подлежащий защите текст обладает некоторой избыточностью. Последняя необходима для того, чтобы нарушитель, не зная ключа шифрования, не смог бы создать шифрограмму, которая после расшифрования успешно прошла бы проверку целостности.

Избыточности можно достигнуть многими способами. В одних случаях текст может обладать достаточной естественной избыточностью (например, в тексте, написанном на любом языке, разные буквы и буквосочетания встречаются с разной частотой). В других можно присоединить к тексту до шифрования некоторое контрольное значение, которое, в отличие от имитовставки

и цифровой подписи, не обязательно должно вырабатываться криптографическими алгоритмами, а может представлять собой просто последовательность заранее определенных символов.

Контроль целостности потока сообщений

Контроль целостности потока сообщений помогает обнаружить их повтор, задержку, переупорядочение или утрату. Предполагается, что целостность каждого отдельного сообщения обеспечивается шифрованием, имитовставкой или цифровой подписью. Для контроля целостности потока сообщений можно, например:

- присвоить сообщению *порядковый номер целостности*;
- использовать в алгоритмах шифрования *сцепление* с предыдущим сообщением.

При использовании порядкового номера целостности, который может включать в себя порядковый номер сообщения и имя источника, приемник хранит последний номер принятого сообщения каждого источника. Для контроля целостности приемник проверяет, например, что порядковый номер целостности текущего сообщения от данного источника на единицу больше номера предыдущего сообщения. Если в качестве порядкового номера целостности используется время отправки сообщения, то проверяется, действительно ли время отправки и время приема близки друг к другу с точностью до задержки сообщения в канале связи и разности хода часов источника и приемника.

Электронная подпись

Термин «электронная подпись» (ЭЦП) используется для методов, позволяющих устанавливать подлинность автора сообщения при возникновении спора относительно авторства этого сообщения. ЭЦП применяется в информационных системах, в которых отсутствует взаимное доверие сторон (финансовые системы, системы контроля за соблюдением международных договоров и др.).

Концепцию цифровой подписи для аутентификации информации предложили Диффи и Хеллман в 1976 г. Она заключа-

ется в том, что каждый абонент сети имеет личный секретный ключ, на котором он формирует подпись и известную всем другим абонентам сети проверочную комбинацию, необходимую для проверки подписи (эту проверочную комбинацию иногда называют открытым ключом). Цифровая подпись вычисляется на основе сообщения и секретного ключа отправителя. Любой получатель, имеющий соответствующую проверочную комбинацию, может аутентифицировать сообщение по подписи.

ЭЦП в цифровых документах играет ту же роль, что и подпись, поставленная от руки в документах, которые напечатаны на бумаге: это данные, присоединяемые к передаваемому сообщению и подтверждающие, что отправитель (владелец подписи) составил или заверил данное сообщение. Получатель сообщения или третья сторона с помощью цифровой подписи может проверить, что автором сообщения является именно владелец подписи (т. е. аутентифицировать источник данных) и что в процессе передачи не была нарушена целостность полученных данных.

Если пользователь ведет себя грамотно, с точки зрения соблюдения норм секретности (хранение секретных ключей подписи, работа с «чистым» программным продуктом, осуществляющим функции подписи), и тем самым исключает возможность похищения ключей или несанкционированного изменения данных и программ, то стойкость системы подписи определяется исключительно криптографическими качествами.

6.4. Защита от угрозы нарушения целостности информации на уровне содержания

Защита от угрозы нарушения целостности информации на уровне содержания в обычной практике рассматривается как защита от дезинформации. Пусть у злоумышленника нет возмож-

ности воздействовать на отдельные компоненты системы, находящиеся в пределах контролируемой зоны, но, если источники поступающей в нее информации находятся вне системы, всегда остается возможность взять их под контроль. При намеренной дезинформации применяют как заведомую ложь, так и полуправду, создающие искаженное представление о событиях.

Наиболее распространенные приемы дезинформации [3]:

- прямое сокрытие фактов;
- тенденциозный подбор данных;
- нарушение логических и временных связей между событиями;
- подача правды в таком контексте (добавлением ложного факта или намека), чтобы она воспринималась как ложь;
- изложение важнейших данных на ярком фоне отвлекающих внимание сведений;
- смешивание разнородных мнений и фактов;
- изложение данных словами, которые можно истолковывать по-разному;
- отсутствие упоминания ключевых деталей факта.

В процессе сбора и получения информации могут возникнуть искажения.

Основные причины искажений информации:

- передача только части сообщения;
- интерпретация услышанного в соответствии со своими знаниями и представлениями;
- пропуск фактуры через призму субъективно-личностных отношений.

Для успешности *борьбы с вероятной дезинформацией* следует:

- различать факты и мнения;
- применять дублирующие каналы информации;
- исключать все лишние промежуточные звенья и т. п.

В информационных системах необходимо предусматривать наличие подсистем, проводящих первичный смысловой анализ и в определенной степени контролирующих работу оператора. Наличие подобных подсистем позволяет защитить информацию не только от случайных, но и от преднамеренных ошибок.

6.5. Построение систем защиты от угрозы отказа доступа к информации

Поскольку одной из основных задач информационной системы является своевременное обеспечение пользователей системы необходимой информацией (сведениями, данными, управляющими воздействиями и т. п.), то угроза отказа доступа к информации может еще рассматриваться как угроза отказа в обслуживании или угроза отказа функционирования. Угроза отказа функционирования информационной системы может быть вызвана:

- целенаправленными действиями злоумышленников;
- ошибками в программном обеспечении;
- отказом аппаратуры.

Часто невозможно бывает разделить причины отказа. В связи с этим вводят понятие надежности.

Надежность — свойство объекта сохранять во времени значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонта, хранения и транспортировки.

Для оценки надежности функционирования информационной системы не важно, вызваны ли отказы действиями злоумышленника или связаны с ошибками разработки, важно, как и в каком объеме произойдет их парирование.

Целесообразно проводить отдельно оценку надежности аппаратуры и программного обеспечения, так как подход к определению надежности здесь различен.

Оценка *надежности оборудования* основана на следующем подходе.

Элементная надежность любого устройства или системы в целом оценивается как произведение вероятности безотказной работы $P'(t)$ на коэффициент готовности K_r:

$$P_0(t) = P'(t)K_r.$$

Если надежность выступает в качестве одной из мер эффективности системы, то оптимальным ее значением является такое, при котором стоимость эксплуатации является минимальной. Оптимальное значение показателя надежности может быть оценено графически (рис. 6.1).

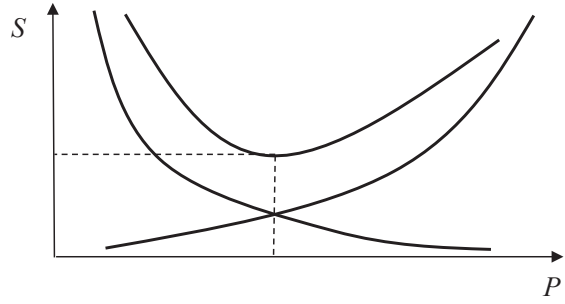


Рис. 6.1. Зависимость затрат от надежности:
$S_э$ — эксплуатационные затраты; $S_р$ — затраты на разработку

В некоторых случаях решается задача достижения максимальной надежности при фиксированных затратах или других закрепленных условиях.

Для определения надежности существуют как теоретические методы расчета, так и рабочие методики. Именно на основе таких расчетов вырабатываются практические мероприятия

по повышению надежности работы как отдельных элементов, так и систем в целом.

На начальной стадии проектирования чаще всего используются рабочие методики, основанные на простых моделях, или элементарные методики расчета надежности, исходящие из предположения о самостоятельности отдельных элементов. В теоретических методах расчета надежности наиболее широкое распространение получили методики расчета по элементам. При этом функциональные зависимости и параметры, характеризующие надежность работы отдельного элемента, могут быть выражены следующими формулами:

частота отказов

$$f(t) = dq(t)/dt = — dP(t)/dt;$$

интенсивность отказов

$$\lambda(t) = \frac{1}{P(t)} \frac{dq(t)}{dt} = -\frac{1}{P(t)} \frac{dP(t)}{dt};$$

среднее время безотказной работы

$$t_{\text{ср}} = \int_0^\infty t \cdot f(t) dt,$$

где P — вероятность безотказной работы элемента; q — вероятность отказа элемента.

Эти формулы применимы к системам с любым числом элементов и произвольным их отношением.

Вероятность безотказной работы системы является функцией вероятностей безотказной работы входящих в систему элементов

$$P_{\text{с}} = f_1 [P_1(t), P_2(t), \ldots, P_n(t)].$$

Взаимосвязь функций для отдельных элементов может быть разной. В частности, вероятность безотказной работы или функция надежности системы, состоящей из n произвольно соединенных элементов, может быть выражена в виде полинома

$$P_{\text{с}} = \sum_{i=1}^{k} a_i P_i.$$

В случае независимого влияния отдельных элементов на работоспособность установки, если отказ каждого из элементов приводит к отказу всей системы, схема структурных надежных отношений представляется в виде последовательного соединения элементов. В этом случае вероятность безотказной работы системы определяется произведением вероятностей безотказной работы элементов

$$P_{\text{с}}(t) = \prod_{i=1}^{n} P_i(t).$$

Если же элементы влияют друг на друга, то схема структурных надежных отношений будет параллельной или смешанной. Если отказ элемента не приводит к отказу системы, то в схеме структурных надежных отношений этот элемент включается параллельно, а при вычислении надежности системы перемножаются вероятности отказов параллельных элементов и полученное произведение вычитается из единицы:

$$P_{\text{с}}(t) = 1 - \prod_{j=1}^{n} (1 - P_j(t)).$$

Надежность работы элементов не всегда удобно характеризовать вероятностью безотказной работы, так как для малых периодов времени работы элементов значения $P_i(t)$ будут близкими к единице. В этом случае лучше использовать интенсивность отказов, которая характеризует плотность вероятности появления отказа отдельно взятого элемента. Она определяется количеством отказов n_i в единицу времени Δt, отнесенных к количеству исправно работающих в данный момент однотипных элементов N, то есть

$$\lambda = \frac{n_i}{N \Delta t}.$$

Вероятность безотказной работы связана с интенсивностью отказов следующим соотношением:

$$P(t) = \exp(-\int_0^{\infty} \lambda(t)dt).$$

Функция $\lambda(t)$ имеет вид, изображенный на рис. 6.2.

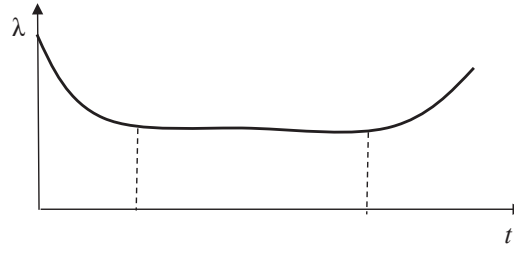


Рис. 6.2. Изменение интенсивности отказов системы в течение срока службы

Первый участок повышенной интенсивности отказов характеризует период, отказы в котором возникают главным образом в результате скрытых неисправностей, допущенных при проектировании, нарушении технологии изготовления системы или связанных с трудностями освоения эксплуатации. Наиболее длительное время система эксплуатируется в нормальных условиях (участок II). Именно этот период работы системы принимается во внимание при расчете надежности в процессе проектирования. Участок III характеризует период увеличения интенсивности отказов вследствие износа оборудования и его старения.

Анализ работы многочисленных технических устройств показал: чем они проще, тем более надежны.

При обеспечении защиты информационной системы от угрозы отказа функционирования обычно считается, что надежность аппаратных компонентов достаточно высока и данной состав-

ляющей в общей надежности можно пренебречь. Это связано с тем, что темпы морального старения вычислительной техники значительно опережают темпы ее физического старения и замена вычислительной техники, как правило, происходит до ее выхода из строя.

Таким образом, на надежность функционирования информационной системы во многом влияет *надежность функционирования программного обеспечения,* входящего в ее состав.

Несмотря на явное сходство в определениях надежности для аппаратных средств и программного обеспечения, фактически последнее имеет принципиальные отличия:

- программа в большинстве случаев не может отказать случайно;
- ошибки в программном обеспечении, допущенные при его создании, зависят от технологии разработки, организации работ и квалификации исполнителей;
- ошибки не являются функцией времени;
- причиной отказов является набор входных данных, сложившихся к моменту отказа.

Существует два основных подхода к обеспечению защиты программного обеспечения от угрозы отказа функционирования [3]:

- обеспечение отказоустойчивости программного обеспечения;
- предотвращение неисправностей.

Отказоустойчивость предусматривает, что оставшиеся ошибки программного обеспечения обнаруживаются во время выполнения программы и парируются за счет использования программной, информационной и временной избыточности. Предотвращение неисправностей связано с анализом природы ошибок, возникающих на разных фазах создания программного обеспечения, и причин их возникновения.

6.6. Защита семантического анализа и актуальности информации

На уровне представления информации защиту от угрозы отказа доступа к информации (защиту семантического уровня) можно рассматривать как противодействие сопоставлению используемым синтаксическим конструкциям (словам некоторого алфавита, символам и т. п.) определенного смыслового содержания. В большей степени эта задача относится к области лингвистики, рассматривающей изменение значения слов с течением времени, переводу с иностранного языка и другим аналогичным научным и прикладным областям знаний.

Применительно к информационным системам защита содержания информации от угрозы блокировки доступа (отказа функционирования) означает юридическую обоснованность обработки и использования информации.

ВЫВОДЫ

- Эффективность методов контроля целостности определяется в основном характеристиками используемых криптографических средств шифрования — цифровой подписи, хэш-функций.
- Вопросы обеспечения своевременного беспрепятственного доступа к информации приобретают все большее значение с развитием распределенных систем обработки. Усложнение топологии систем, применяемого оборудования и используемого программного обеспечения, а также задача сопряжения всех элементов требуют повышенного внимания к обеспечению работоспособности системы и доступности циркулирующей в ней информации.
- Отдельное направление защиты — обеспечение секретности параметров информационной системы, в которой циркулирует конфиденциальная информация. Методы

защиты параметров такой системы аналогичны общим методам, применяемым для защиты конфиденциальности информации.

Вопросы для самоконтроля

1. Каковы способы контроля целостности потока сообщений?
2. Какие существуют способы контроля целостности сообщений при взаимном доверии сторон?
3. Как контролировать целостность сообщений при высоком уровне помех в каналах связи?
4. Как организован обмен документами, заверенными цифровой подписью?
5. В чем отличие и сходство обычной и цифровой подписей?
6. Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?
7. Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?
8. Что означает контроль целостности данных на уровне содержания? Приведите примеры.
9. Как обеспечить целостность данных при их хранении?
10. Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?
11. Следует ли различать защиту от случайных угроз и от действий злоумышленника при обеспечении беспрепятственного доступа к информации? Обоснуйте свой ответ.
12. Как защитить программное обеспечение от изучения логики его работы?
13. Предложите меры по обеспечению более надежной работы ЛВС университета.
14. Как изменяется надежность аппаратуры с течением времени?
15. Каковы способы повышения надежности аппаратуры и линий связи?

7. Политика и модели безопасности

❖ Политика безопасности ❖ Субъектно-объектные модели разграничения доступа ❖ Аксиомы политики безопасности ❖ Политика и модели дискреционного доступа ❖ Парольные системы разграничения доступа ❖ Политика и модели мандатного доступа ❖ Теоретико-информационные модели ❖ Политика и модели тематического разграничения доступа❖ Ролевая модель безопасности ❖

7.1. Политика безопасности

Технология защиты информационных систем начала развиваться относительно недавно, но уже сегодня существует значительное число теоретических моделей, позволяющих описывать различные аспекты безопасности и обеспечивать средства защиты с формальной стороны.

Под *политикой безопасности* понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое условие безопасности системы. Формальное выражение политики безопасности называют *моделью безопасности*.

Основная цель создания политики безопасности — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений.

Кроме того, модели безопасности позволяют решить еще целый ряд задач, возникающих в ходе проектирования, разработки и сертификации защищенных систем, поэтому их используют не только теоретики информационной безопасности, но и другие категории специалистов, участвующих в процессе создания и эксплуатации защищенных информационных систем.

Модели безопасности обеспечивают системотехнический подход, включающий решение следующих задач [7]:

- выбор и обоснование базовых принципов архитектуры защищенных систем, определяющих механизмы реализации средств и методов защиты информации;
- подтверждение свойства защищенности разрабатываемых систем путем формального доказательства соблюдения политики безопасности;
- составление формальной спецификации политики безопасности как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных систем.

Производители защищенных информационных систем используют модели безопасности в следующих случаях:

- при составлении формальной спецификации политики безопасности разрабатываемой системы;
- при выборе и обосновании базовых принципов архитектуры защищенной системы, определяющих механизмы реализации средств защиты;
- в процессе анализа безопасности системы, при этом модель используется в качестве эталонной модели;
- при подтверждении свойств разрабатываемой системы путем формального доказательства соблюдения политики безопасности.

Потребители путем составления формальных моделей безопасности получают возможность довести до сведения производителей свои требования, а также оценить соответствие защищенных систем своим потребностям.

Эксперты в ходе анализа адекватности реализации политики безопасности в защищенных системах используют модели безопасности в качестве эталонов.

По сути, модели безопасности являются связующим элементом между производителями, потребителями и экспертами.

7.2. Субъектно-объектные модели разграничения доступа

Основы моделирования процессов защиты информации рассмотрены, например, в работах В. А. Герасименко, одного из наиболее известных отечественных исследователей теоретических и практических аспектов защиты информации в автоматизированных системах, автора системно-концептуального подхода к информационной безопасности. В. А. Герасименко представил общую модель процессов защиты информации, структурировав ее на взаимосвязанные компоненты и выделив в отдельный блок модели систем разграничения доступа к ресурсам.

Разграничение доступа к информации — разделение информации, циркулирующей в информационной системе, на части, элементы, компоненты, объекты и т. д. и организация системы работы с информацией, предполагающей доступ пользователей к той части (к тем компонентам) информации, которая им необходима для выполнения функциональных обязанностей.

Разграничение доступа непосредственно обеспечивает конфиденциальность информации, а также снижает вероятность реализации угроз целостности и доступности. Разграничение доступа можно рассматривать среди других методов обеспечения информационной безопасности как комплексный программно-технический метод защиты информации. Разграничение доступа является также необходимым условием обеспечения информационной безопасности.

Большинство моделей разграничения доступа основывается на представлении системы как совокупности субъектов и объектов доступа.

Рассмотрим основные положения наиболее распространенных политик безопасности, основанных на контроле доступа субъектов к объектам и моделирующих поведение системы с помощью пространства состояний, одни из которых являются

безопасными, а другие — нет [7]. Все рассматриваемые модели безопасности основаны на следующих базовых представлениях:

1. В системе действует дискретное время.

2. В каждый фиксированный момент времени система представляет собой конечное множество элементов, разделяемых на два подмножества:

- подмножество субъектов доступа S;
- подмножество объектов доступа O.

Субъект доступа — активная сущность, которая может изменять состояние системы через порождение процессов над объектами, в том числе порождать новые объекты и инициализировать порождение новых субъектов.

Объект доступа — пассивная сущность, процессы над которой могут в определенных случаях быть источником порождения новых субъектов.

При таком представлении системы безопасность обработки информации обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с заданным набором правил и ограничений, которые образуют политику безопасности. Общим подходом для всех моделей является именно разделение множества сущностей, составляющих систему, на множества субъектов и объектов, хотя сами определения понятий «объект» и «субъект» в разных моделях могут различаться.

В модели предполагается наличие механизма различения субъектов и объектов по свойству активности. Кроме того, предполагается также, что в любой момент времени t_k, в том числе и в начальный, множество субъектов доступа не пусто.

3. Пользователи представлены одним или некоторой совокупностью субъектов доступа, действующих от имени конкретного пользователя.

Пользователь — лицо, внешний фактор, аутентифицируемый некоторой информацией и управляющий одним или несколькими субъектами, воспринимающий объекты и получающий

информацию о состоянии системы через субъекты, которыми он управляет.

Таким образом, в субъектно-объектной модели понятия субъектов доступа и пользователей не тождественны. Предполагается, что пользовательские управляющие воздействия не могут изменить свойств самих субъектов доступа, что не соответствует реальным системам, в которых пользователи могут изменять свойства субъектов через изменение программ. Однако подобная идеализация позволяет построить четкую схему процессов и механизмов доступа.

4. Субъекты могут быть порождены из объектов только активной сущностью (другим субъектом).

Объект o_i называется *источником* для субъекта s_m, если существует субъект s_j, в результате воздействия которого на объект o_i возникает субъект s_m. Субъект s_j является *активизирующим* для субъекта s_m.

Для описания процессов порождения субъектов доступа вводится следующая команда:

Create $(s_j, o_i) \rightarrow s_m$ — из объекта o_i порожден субъект s_m, при активизирующем воздействии субъекта s_j.

Create называют операцией порождения субъектов. Ввиду того, что в системе действует дискретное время, под воздействием активизирующего субъекта в момент времени t_k новый субъект порождается в момент времени t_{k+1}.

Результат операции *Create* зависит как от свойств активизирующего субъекта, так и от свойств объекта-источника.

Активная сущность субъектов доступа заключается в их способности осуществлять определенные действия над объектами, что приводит к возникновению потоков информации.

5. Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов отношений определяется в виде набора операций, которые субъекты могут производить над объектами.

6. Все процессы в системе описываются доступом субъектов к объектам, вызывающим потоки информации.

Потоком информации между объектом o_i и объектом o_j называется произвольная операция над объектом o_j, реализуемая в субъекте s_m и зависящая от объекта o_i.

Поток может осуществляться в виде различных операций над объектами: чтение, изменение, удаление, создание и т. д. Объекты, участвующие в потоке, могут быть как источниками, так и приемниками информации, как ассоциированными с субъектом, так и неассоциированными, а также могут быть пустыми объектами (например, при создании или удалении файлов). Потоки информации могут быть только между объектами, а не между субъектом и объектом.

Доступом субъекта s_m к объекту o_j называется порождение субъектом s_m потока информации между объектом o_j и некоторым объектом o_i.

Формальное определение понятия доступа дает возможность средствами субъектно-объектной модели перейти непосредственно к описанию процессов безопасности информации в защищенных системах. С этой целью вводится множество потоков P для всей совокупности фиксированных декомпозиций системы на субъекты и объекты во все моменты времени (множество P является объединением потоков по всем моментам времени функционирования системы).

Правила разграничения доступа субъектов к объектам есть формально описанные потоки, принадлежащие множеству P.

7. Политика безопасности задается в виде правил, в соответствии с которыми должны осуществляться все взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.

8. Все операции контролируются монитором безопасности и либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.

9. Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет *состояние* системы. Каждое состояние системы является либо *безопасным,* либо *небезопасным* в соответствии с предложенным в модели критерием безопасности.

10. Основной элемент модели безопасности — это доказательство утверждения (теоремы) о том, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

7.3. Аксиомы политики безопасности

Анализ опыта защиты информации, а также основных положений субъектно-объектной модели позволяет сформулировать несколько аксиом, касающихся построения политик безопасности [10].

Аксиома 1. В защищенной информационной системе в любой момент времени любой субъект и объект должны быть идентифицированы и аутентифицированы.

Данная аксиома определяется самой природой и содержанием процессов коллективного доступа пользователей к ресурсам. Иначе субъекты имеют возможность выдать себя за других субъектов или подменить одни объекты доступа на другие.

Аксиома 2. В защищенной системе должна присутствовать активная компонента (субъект, процесс и т. д.) с соответствующим объектом-источником, которая осуществляет управление доступом и контроль доступа субъектов к объектам, — монитор или ядро безопасности.

Монитор безопасности — механизм реализации политики безопасности в информационной системе, совокупность аппаратных, программных и специальных компонентов систе-

мы, реализующих функции защиты и обеспечения безопасности (общепринятое сокращение — ТСВ — Trusted Computing Base).

В большинстве информационных систем можно выделить ядро (ядро ОС, машина данных СУБД), в свою очередь разделяемое на компоненту представления информации (файловая система ОС, модель данных СУБД), компоненту доступа к данным (система ввода–вывода ОС, процессор запросов СУБД) и надстройку (утилиты, сервис, интерфейсные компоненты) (рис. 7.1).

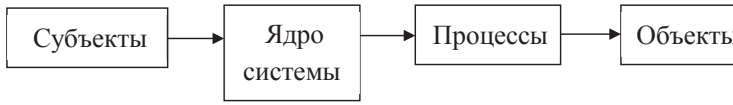


Рис. 7.1. Незащищенная система

В защищенной системе появляется дополнительный компонент, обеспечивающий процессы защиты информации, прежде всего процедуры идентификации/аутентификации, а также управление доступом на основе той или иной политики безопасности (разграничения доступа) (рис. 7.2).

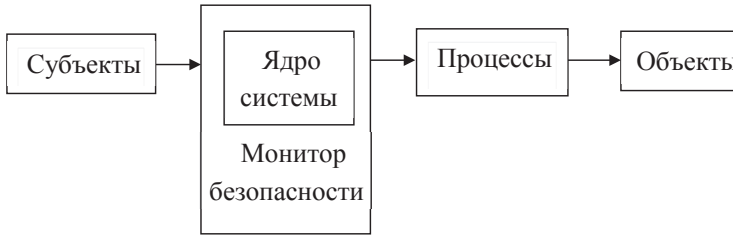


Рис. 7.2. Защищенная система

С учетом нормативных требований по сертификации защищенных систем к реализации монитора безопасности предъявляются следующие обязательные требования:

1. Полнота. Монитор безопасности должен вызываться при каждом обращении за доступом любого субъекта к любому объекту, и не должно быть никаких способов его обхода.

2. Изолированность. Монитор безопасности должен быть защищен от отслеживания и перехвата работы.

3. Верифицируемость. Монитор безопасности должен быть проверяемым (само- или внешнетестируемым) на предмет выполнения своих функций.

4. Непрерывность. Монитор безопасности должен функционировать при любых, в том числе и аварийных ситуациях.

Монитор безопасности в защищенной системе является субъектом осуществления принятой политики безопасности, реализуя через алгоритмы своей работы соответствующие модели безопасности.

Аксиома 3. Для реализации принятой политики безопасности, управления и контроля доступа субъектов к объектам необходима информация и объект, ее содержащий.

Следствие 3.1. В защищенной системе существует особая категория активных сущностей, которые не инициализируют и которыми не управляют пользователи системы, — системные процессы (субъекты), присутствующие в системе изначально.

Следствие 3.2. Ассоциированный с монитором безопасности объект, содержащий информацию о системе разграничения доступа, является наиболее критическим с точки зрения безопасности информационным ресурсом в защищенной информационной системе.

Следствие 3.3. В защищенной системе может существовать доверенный пользователь (администратор системы), субъекты которого имеют доступ к ассоциированному с монитором безопасности объекту — данным для управления политикой разграничения доступа.

Принципы, способы представления и реализация ассоциированных с монитором безопасности объектов определяют-

ся типом политики безопасности и особенностями конкретной системы.

К настоящему времени разработано большое количество различных моделей безопасности, все они выражают несколько исходных политик безопасности. При этом имеет значение критерий безопасности доступов субъектов к объектам, т. е. правило разделения информационных потоков, порождаемых доступом субъектов к объектам, на безопасные и небезопасные.

Система безопасна тогда и только тогда, когда субъекты не имеют возможностей нарушать (обходить) установленную в системе политику безопасности.

Субъектом обеспечения политики безопасности выступает монитор безопасности. Его наличие в структуре системы соответственно является *необходимым* условием безопасности. Что касается условий *достаточности,* то они заключены в безопасности самого монитора безопасности.

7.4. Политика и модели дискреционного доступа

Политика дискреционного (избирательного) доступа реализована в большинстве защищенных систем и исторически является первой проработанной в теоретическом и практическом плане.

Первые описания моделей дискреционного доступа к информации появились еще в 1960-х гг. и подробно представлены в литературе. Наиболее известны модель АДЕПТ-50 (конец 1960-х гг.), пятимерное пространство Хартсона (начало 1970-х гг.), модель Хариссона — Руззо-Ульмана (середина 1970-х гг.), модель Take-Grant (1976 г.). Авторами и исследователями этих моделей был внесен значительный вклад в теорию безопасности информационных систем, а их работы заложили основу для последующего создания и развития защищенных информационных систем.

Модели дискреционного доступа непосредственно основываются на субъектно-объектной модели и развивают ее как совокупность некоторых множеств взаимодействующих элементов (субъектов, объектов и т. д.). Множество (область) безопасных доступов в моделях дискреционного доступа определяется дискретным набором троек «пользователь (субъект) — поток (операция) — объект».

В модели, исходя из способа представления области безопасного доступа и механизма разрешений на доступ, анализируется и доказывается, что за конечное число переходов система останется в безопасном состоянии.

Модели на основе матрицы доступа

На практике наибольшее применение получили дискреционные модели, основанные на матрице доступа. В данных моделях область безопасного доступа строится как прямоугольная матрица (таблица), строки которой соответствуют субъектам доступа, столбцы — объектам доступа, а в ячейках записываются разрешенные операции (права) субъекта над объектом (рис. 7.3). В матрице используются следующие обозначения: *w* — «писать», *r* — «читать», *e* — «исполнять».

Объекты доступа

Субъекты доступа	o_1	o_2	…	o_j	…	o_n
1						
2	*r*					
	r, *w*		*e*	*r*		
i						
	w	*e*		*r*		
m					*w*	*w*

Рис. 7.3. Матрица доступа

Права доступа в ячейках матрицы в виде разрешенных операций над объектами определяют виды безопасного доступа субъекта к объекту. Для выражения типов разрешенных операций используются специальные обозначения, составляющие основу (алфавит) некоторого языка описания политики разграничения доступа. Таким образом, в рамках дискреционной политики каждая ячейка содержит некоторое подмножество троек «субъект — операция — объект».

Матрица доступа представляет собой ассоциированный с монитором безопасности объект, содержащий информацию о политике разграничения доступа в конкретной системе. Структура матрицы, ее создание и изменение определяются конкретными моделями и конкретными программно-техническими решениями систем, в которых они реализуются.

Принцип организации матрицы доступа в реальных системах определяет использование двух подходов — централизованного и распределенного.

При *централизованном* подходе матрица доступа создается как отдельный самостоятельный объект с особым порядком размещения и доступа к нему. Количество объектов и субъектов доступа в реальных системах может быть велико. Для уменьшения количества столбцов матрицы объекты доступа могут делиться на две группы — группу объектов, доступ к которым не ограничен, и группу объектов дискреционного доступа. В матрице доступа представляются права пользователей только к объектам второй группы. Наиболее известным примером такого подхода являются «биты доступа» в UNIX-системах.

При *распределенном* подходе матрица доступа как отдельный объект не создается, а представляется или *«списками доступа»,* распределенными по объектам системы, или *«списками возможностей»,* распределенными по субъектам доступа [10]. В первом случае каждый объект системы, помимо идентифицирующих характеристик, наделяется еще своеобразным списком, непосредственно связанным с самим объектом и представляющим,

по сути, соответствующий столбец матрицы доступа. Во втором случае список с перечнем разрешенных для доступа объектов (строку матрицы доступа) получает каждый субъект при своей инициализации.

И централизованный, и распределенный принципы организации матрицы доступа имеют свои преимущества и недостатки, присущие в целом централизованному и децентрализованному принципам организации и управления.

Согласно *принципу управления доступом* выделяются два подхода:

- принудительное управление доступом;
- добровольное управление доступом.

В случае принудительного управления право создания и изменения матрицы доступа имеют только субъекты администратора системы, который при регистрации для работы в системе нового пользователя создает с соответствующим заполнением новую строку матрицы доступа, а при возникновении нового объекта, подлежащего избирательному доступу, образует новый столбец матрицы доступа. Подобный подход наиболее широко представлен в базах данных.

Принцип *добровольного управления доступом* основывается на принципе владения объектами. Владельцем объекта доступа называется пользователь, инициализировавший поток, в результате чего объект возник в системе, или определивший его иным образом. Права доступа к объекту определяют их владельцы.

Заполнение и изменение ячеек матрицы доступа осуществляют субъекты пользователей-владельцев соответствующих объектов. Подобный подход обеспечивает управление доступом в тех системах, в которых количество объектов доступа является значительным или неопределенным. Такая ситуация типична для операционных систем.

Все дискреционные модели уязвимы для атак с помощью «троянских» программ, поскольку в них контролируются только

операции доступа субъектов к объектам, а не потоки информации между ними. Поэтому, когда «троянская» программа переносит информацию из доступного этому пользователю объекта в объект, доступный нарушителю, то формально никакое правило дискреционной политики безопасности не нарушается, но утечка информации происходит.

7.5. Парольные системы разграничения доступа

В документальных информационных системах, в системах автоматизации документооборота широкое распространение получили так называемые парольные системы разграничения доступа, представляющие отдельную разновидность механизмов реализации дискреционного принципа разграничения доступа [7].

Основные положения парольных систем можно сформулировать следующим образом.

1. Система представляется следующим набором сущностей:
- множеством информационных объектов (документов) $O(o_1, ..., o_m)$;
- множеством пользователей $S(s_1, ..., s_n)$;
- множеством паролей доступа к объектам $K(k_1, ..., k_p)$.

2. В системе устанавливается отображение множества O на множество K, задаваемое следующей функцией:

$$f_{ko} : O \to K.$$

Значением функции $f_{ko}(o) = k_o$ является пароль k_o доступа к документу o.

3. Область безопасного доступа задается множеством троек (s, k, o), каждый элемент которого соответствует владению пользователем паролем доступа к объекту. В результате устанавливается отображение множества S на множество K:

$$f_{ks} : S \to K.$$

Значением $f_{ks}(s) = K_s$ является набор паролей доступа к документам системы, известных пользователю s.

4. Процессы доступа пользователей к объектам системы организуются в две фазы:

- фаза открытия документа;
- фаза закрытия (сохранения) документа.

При открытии документа o пользователь s предъявляет (вводит, передает) монитору безопасности АС пароль k_{s0} доступа к данному документу.

Запрос в доступе удовлетворяется, если

$$k_{s0} = f_{k0}(o).$$

В случае успешного открытия пользователю предоставляются права работы по фиксированному набору операций с объектом.

Возможны два подхода, соответствующие добровольному и принудительному способам управления доступом.

При использовании принудительного способа назначение паролей доступа к документам, их изменение осуществляет только выделенный пользователь — администратор системы. При необходимости шифрования измененного объекта или при появлении в системе нового объекта, подлежащего дискреционному доступу к нему, администратор системы на основе специальной процедуры генерирует пароль доступа к новому объекту, зашифровывает документ на ключе, созданном на основе пароля, и фиксирует новый документ в зашифрованном состоянии в системе. Администратор сообщает пароль доступа к данному документу тем пользователям, которым он необходим. Тем самым формируется подмножество троек доступа $\{(s_1, k, o), (s_2, k, o), ...\}$ к документу o.

При добровольном управлении доступом описанную выше процедуру формирования подмножества троек доступа к новому документу производят владельцы объекта.

Преимуществом парольных систем по сравнению с системами дискреционного разграничения доступа, основанными на матрице доступа, является то, что в них отсутствует ассоциированный с монитором безопасности объект, хранящий информацию о разграничении доступа к конкретным объектам. Данный объект является наиболее критичным с точки зрения безопасности объектом системы.

Кроме того, в парольных системах обеспечивается безопасность и в том случае, когда не ограничен или технически возможен доступ посторонних лиц к носителям, на которых фиксируются и хранятся зашифрованные объекты.

Эти преимущества парольных систем разграничения доступа обусловливают их чрезвычайно широкое применение в документальных информационных системах.

Несмотря на то, что дискреционные модели разработаны почти 40 лет назад, и то, что многочисленные исследования показали их ограниченные защитные свойства, данные модели широко применяются на практике. Основные их достоинства — это простота и максимальная детальность в организации доступа.

7.6. Политика и модели мандатного доступа

Политика мандатного доступа является примером использования технологий, наработанных во внекомпьютерной сфере, в частности принципов организации секретного делопроизводства и документооборота, применяемых в государственных структурах большинства стран.

Основным положением политики мандатного доступа является назначение всем участникам процесса обработки защищаемой информации и документам, в которых она содержит-

ся, специальной метки, например *секретно, сов. секретно* и т. д., получившей название уровня безопасности. Все уровни безопасности упорядочиваются с помощью установленного отношения доминирования, например, уровень *сов. секретно* считается более высоким, чем уровень *секретно*. Контроль доступа осуществляется в зависимости от уровней безопасности взаимодействующих сторон на основании двух правил:

1. *No read up (NRU)* — нет чтения вверх: субъект имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности.

2. *No write down (NWD)* — нет записи вниз: субъект имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности.

Первое правило обеспечивает защиту информации, обрабатываемой более доверенными (высокоуровневыми) лицами, от доступа со стороны менее доверенных (низкоуровневых). Второе правило предотвращает утечку информации (сознательную или несознательную) от высокоуровневых участников процесса обработки информации к низкоуровневым.

Формализация механизмов разграничения доступа в секретном делопроизводстве применительно к субъектно-объектной модели показала необходимость решения следующих задач:

- разработки процедур формализации правила NRU, а в особенности правила NWD;
- построения формального математического объекта и процедур, адекватно отражающих систему уровней безопасности (систему допусков и грифов секретности).

При представлении служащих, работающих с секретными документами, в качестве субъектов доступа, а секретных документов в качестве объектов доступа буквальное следование правилу NWD приводит к включению в механизмы обеспечения безопасности субъективного фактора в лице субъекта-пользователя, который при внесении информации должен оценить

соответствие вносимой информации уровню безопасности документа. Задача исключения данного субъективного фактора может решаться различными способами, самым простым из которых является полный запрет изменения субъектами объектов с уровнем безопасности более низким, чем уровень безопасности соответствующих субъектов. При этом существенно снижается функциональность системы.

Таким образом, если в дискреционных моделях управление доступом происходит путем наделения пользователей полномочиями осуществлять определенные операции над определенными объектами, то мандатные модели управляют доступом неявным образом — с помощью назначения всем сущностям системы уровней безопасности, которые определяют все допустимые взаимодействия между ними. Следовательно, мандатное управление доступом не различает сущностей, которым присвоен одинаковый уровень безопасности, и на их взаимодействия ограничения отсутствуют. Любой объект определенного уровня безопасности доступен любому субъекту соответствующего уровня безопасности (с учетом правил NRU и NWD). Мандатный подход к разграничению доступа, основанный лишь на понятии уровня безопасности, без учета специфики других характеристик субъектов и объектов приводит в большинстве случаев к избыточности прав доступа конкретных субъектов в пределах соответствующих классов безопасности. Для устранения данного недостатка мандатный принцип разграничения доступа дополняется дискреционным внутри соответствующих классов безопасности. В теоретических моделях для этого вводят *матрицу доступа,* разграничивающую разрешенный по мандатному принципу доступ к объектам одного уровня безопасности.

7.7. Теоретико-информационные модели

Одной из самых труднорешаемых проблем безопасности в информационных системах, в том числе и основанных на моделях мандатного доступа, является проблема скрытых каналов утечки информации.

Скрытым каналом утечки информации называется механизм, посредством которого в системе может осуществляться информационный поток (передача информации) между сущностями в обход политики разграничения доступа.

Например, к скрытым каналам утечки информации относятся рассмотренные ранее потоки, возникающие за счет «троянских» программ, и неявные информационные потоки в системах на основе дискреционных моделей.

Скрытым каналом утечки информации в системах мандатного доступа является механизм, посредством которого может осуществляться передача информации от сущностей с высоким уровнем безопасности к сущностям с низким уровнем безопасности без нарушения правил NRU и NWD. В определенных случаях информацию можно получить или передать и без непосредственного осуществления операций *read/write* к объектам, в частности на основе анализа определенных процессов и параметров системы. Например, если по правилу NRU нельзя читать секретный файл, но можно «видеть» его объем, то высокоуровневый субъект, меняя по определенному правилу объем секретного файла, может таким кодированным образом передавать секретную информацию низкоуровневому объекту. От высокоуровневых субъектов может передаваться информация о количестве создаваемых или удаляемых секретных файлов, получить доступ по чтению к которым низкоуровневые субъекты не могут, но «видеть» их наличие и соответственно определять их количество могут.

Другие возможности «тайной» передачи информации могут основываться на анализе временных параметров протекания процессов.

Скрытые каналы утечки информации можно разделить на три вида:

- скрытые каналы по памяти (на основе анализа объема и других статических параметров объектов системы);
- скрытые каналы по времени (на основе анализа временных параметров протекания процессов системы);
- скрытые статистические каналы (на основе анализа статистических параметров процессов системы).

Требования по перекрытию и исключению скрытых каналов впервые были включены в спецификацию уровней защиты автоматизированных систем, предназначенных для обработки сведений, составляющих государственную тайну в США (Оранжевая книга).

Теоретические основы подходов к решению проблемы скрытых каналов разработаны Д. Денингом, исследовавшим принципы анализа потоков данных в программном обеспечении и принципы контроля совместно используемых ресурсов. Основываясь на идеях Денинга, Дж. Гоген и Дж. Мезигер предложили теоретико-информационный подход на основе понятий *информационной невыводимости* и *информационного невмешательства*.

Сущность данного подхода [7, 8] заключается в отказе от рассмотрения процесса функционирования информационной системы как детерминированного процесса. При рассмотрении моделей конечных состояний (HRU, TAKE-GRANT, Белла — ЛаПадулы) предполагалось, что функция перехода в зависимости от запроса субъекта и текущего состояния системы однозначно определяет следующее состояние системы. В системах коллективного доступа (много пользователей, много объектов) переходы, следовательно, и состояния системы обусловливаются большим количеством самых разнообразных, в том числе и случайных, факторов, что предполагает использование аппарата теории вероятностей для описания системы.

При таком подходе политика безопасности требует определенной модификации и, в частности, теоретико-вероятностной трактовки процессов функционирования систем и опасных информационных потоков:

1. Информационная система рассматривается как совокупность двух непересекающихся множеств сущностей:

- множества высокоуровневых объектов H;
- множества низкоуровневых объектов L.

Информационная система представляется мандатной системой с решеткой, состоящей всего из двух уровней безопасности — высокого и низкого и соответственно определяющей невозможность обычных (*read*/*write*) информационных потоков «сверху вниз».

2. Состояние любого объекта является случайным. Понятие информационной невыводимости основывается на определении «опасных» потоков: в системе присутствует информационный поток от высокоуровневых объектов к низкоуровневым, если некое возможное значение переменной в некотором состоянии низкоуровневого объекта невозможно одновременно с определенными возможными значениями переменных состояний высокоуровневых объектов.

3. Формулируется следующий критерий информационной невыводимости: система безопасна в смысле информационной невыводимости, если в ней отсутствуют информационные потоки вида, задаваемого в п. 2.

Анализ критерия информационной невыводимости показывает, что его требования являются чрезвычайно жесткими и достижимы, в частности, при полной изоляции высокоуровневых объектов от низкоуровневых.

Требование отсутствия выводимости высокоуровневой информации на основе анализа состояний низкоуровневых объектов одновременно приводит и к обратному, т. е. отсутствию возможностей выводимости низкоуровневой информации из анализа состояний высокоуровневых объектов. Данное

свойство является избыточным и противоречит основным положениям мандатной политики, а именно — неопасности и допустимости потоков «снизу вверх» от низкоуровневых сущностей к сущностям с более высокими уровнями безопасности.

Другой подход основывается на идее *информационного невмешательства*. Понятие опасных потоков имеет здесь следующий смысл: в системе присутствует информационный поток от высокоуровневых объектов к низкоуровневым, если информация (состояние) низкоуровневых объектов зависит от информации высокоуровневых объектов. Это значит, что на состояние высокоуровневых объектов в текущий момент времени не влияет состояние низкоуровневых объектов в предшествующий момент времени и наоборот. Разноуровневые объекты не имеют возможности влиять на последующие состояния объектов другого уровня. Анализ процессов функционирования информационной системы показывает, что такие требования являются чрезвычайно жесткими, фактически совпадающими с требованиями полной изоляции разноуровневых сущностей.

Несмотря на то, что понятия информационной невыводимости и информационного невмешательства непосредственно не применимы для разграничения доступа, они послужили основой широко применяемых в современных информационных системах *технологий представлений и разрешенных процедур*. Эти технологии исторически возникли как политика разграничения доступа в СУБД.

Представлением информации в информационной системе называется процедура формирования и представления пользователю (после его входа в систему и аутентификации) необходимого подмножества информационных объектов, в том числе с возможным их количественным и структурным видоизменением исходя из задач разграничения доступа к информации.

В технологиях представлений пользователи, входя и работая в системе, оперируют не с реальной, а с виртуальной системой, формируемой индивидуально для каждого. В результате зада-

ча разграничения доступа решается автоматически. Проблемы безопасности при этом сводятся к скрытым каналам утечки информации, рассмотрение и нейтрализация которых осуществляется на основе анализа условий и процедур, обеспечивающих выполнение критериев безопасности.

Технология представлений решает проблему скрытых каналов утечки первого вида. Часть каналов второго и третьего вида перекрывается техникой разрешенных процедур. Системой разрешенных процедур называется разновидность интерфейса системы, когда при входе в систему аутентифицированным пользователям предоставляется только возможность запуска и исполнения конечного набора логико-технологических процедур обработки информации без возможности применения элементарных методов доступа (read, write, create и т.п.) к информационным объектам системы. Следовательно, в системах с интерфейсом разрешенных процедур пользователи не видят информационные объекты, а выполняют операции на уровне логических процедур. Автоматизированная система при этом для пользователей превращается в дискретный автомат, получающий команды на входе и выдающий обработанную информацию на выходе.

Впервые подобный подход к представлению информационной системы был рассмотрен Гогеном (J. Goguen) и Мезигером (J. Meseguer), предложившими *автоматную модель информационного невлияния* (невмешательства) — GM-модель.

7.8. Политика и модели тематического разграничения доступа

Политика тематического разграничения доступа близка к политике мандатного доступа [7].

Общей основой является введение специальной процедуры классификации сущностей системы (субъектов и объектов до-

ступа) по какому-либо критерию. Выше рассматривалось, что основой классификации сущностей АС в моделях мандатного доступа является линейная решетка на упорядоченном множестве уровней безопасности. При этом использование аппарата решеток является принципиальным, так как посредством механизмов наименьшей верхней и наибольшей нижней границ обеспечивается возможность анализа опасности/неопасности потоков между любой парой сущностей системы.

В ряде случаев основанием для классификации информации и субъектов доступа к ней выступают не конфиденциальность данных и доверие к субъектам доступа, как в мандатных моделях, а тематическая структура предметной области информационной системы. Стремление расширить мандатную модель для отражения тематического принципа разграничения доступа, применяемого в государственных организациях многих стран, привело к использованию более сложных структур, чем линейная решетка уровней безопасности, именуемых MLS-решетками. MLS-решетка является произведением линейной решетки уровней безопасности и решетки подмножеств множества категорий (тематик).

Еще одним фактором, обусловливающим необходимость построения специальных моделей тематического разграничения доступа, является то, что в большинстве случаев на классификационном множестве в документальных информационных системах устанавливается не линейный порядок (как на множестве уровней безопасности в мандатных моделях), а частичный порядок, задаваемый определенного вида корневыми деревьями (иерархические и фасетные рубрикаторы).

Важным аспектом, присутствующим в практике разграничения доступа к «бумажным» ресурсам, является тематическая «окрашенность» информационных ресурсов предприятий, учреждений по организационно-технологическим процессам и профилям деятельности. Организация доступа сотрудников к информационным ресурсам (в библиотеках, архивах, доку-

ментальных хранилищах) осуществляется на основе *тематических классификаторов*. Все документы информационного хранилища тематически индексируются, т. е. соотносятся с теми или иными тематическими рубриками классификатора. Сотрудники предприятия согласно своим функциональным обязанностям или по другим основаниям получают права работы с документами определенной тематики. Данный подход в сочетании с дискреционным и мандатным доступом, обеспечивает более адекватную и гибкую настройку системы разграничения доступа на конкретные функционально-технологические процессы, предоставляет дополнительные средства контроля и управления доступом.

7.9. Ролевая модель безопасности

Ролевая модель безопасности представляет собой существенно усовершенствованную модель Харрисона–Руззо–Ульмана, однако ее нельзя отнести ни к дискреционным, ни к мандатным, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов. Поэтому ролевая модель представляет собой совершенно особый тип политики, которая основана на компромиссе между гибкостью управления доступом, характерной для дискреционных моделей, и жесткостью правил контроля доступа, присущей мандатным моделям.

В ролевой модели классическое понятие «субъект» замещается понятиями «пользователь» и «роль» [5, 7]. Пользователь — это человек, работающий с системой и выполняющий определенные служебные обязанности. Роль — это активно действующая в системе абстрактная сущность, с которой связан набор полномочий, необходимых для осуществления определенной

деятельности. Самым распространенным примером роли является присутствующий почти в каждой системе административный бюджет (например, root для UNIX и Administrator для Windows NT), который обладает специальными полномочиями и может использоваться несколькими пользователями.

Ролевая политика распространена очень широко, потому что она, в отличие от других более строгих и формальных политик, очень близка к реальной жизни. Ведь на самом деле работающие в системе пользователи действуют не от своего личного имени, они всегда осуществляют определенные служебные обязанности, т. е. выполняют некоторые роли, которые никак не связаны с их личностью.

Поэтому вполне логично осуществлять управление доступом и назначать полномочия не реальным пользователям, а абстрактным (неперсонифицированным) ролям, представляющим участников определенного процесса обработки информации. Такой подход к политике безопасности позволяет учесть разделение обязанностей и полномочий между участниками прикладного информационного процесса, т. к. с точки зрения ролевой политики имеет значение не личность пользователя, осуществляющего доступ к информации, а то, какие полномочия ему необходимы для выполнения его служебных обязанностей.

В такой ситуации ролевая политика позволяет распределить полномочия между этими ролями в соответствии с их служебными обязанностями: роли администратора назначаются специальные полномочия, позволяющие ему контролировать работу системы и управлять ее конфигурацией, роль менеджера баз данных позволяет осуществлять управление сервером баз данных, а права простых пользователей ограничиваются минимумом, необходимым для запуска прикладных программ. Кроме того, количество ролей в системе может не соответствовать количеству реальных пользователей: один пользователь, если на нем лежит множество обязанностей, требующих различных

полномочий, может выполнять (одновременно или последовательно) несколько ролей, а несколько пользователей могут выполнять одну и ту же роль, если они производят одинаковую работу.

При использовании ролевой политики управление доступом осуществляется в две стадии: во-первых, для каждой роли указывается набор полномочий, представляющий набор прав доступа к объектам, во-вторых — каждому пользователю назначается список доступных ему ролей. Полномочия назначаются ролям в соответствии с принципом наименьших привилегий, из которого следует, что каждый пользователь должен обладать только минимально необходимым для выполнения своей работы набором полномочий.

В отличие от других политик, ролевая политика практически не гарантирует безопасность с помощью формального доказательства, а только определяет характер ограничений, соблюдение которых и служит критерием безопасности системы. Такой подход позволяет получать простые и понятные правила контроля доступа, которые легко могут быть применены на практике, но лишает систему теоретической доказательной базы. В некоторых ситуациях это обстоятельство затрудняет использование ролевой политики, однако в любом случае оперировать ролями гораздо удобнее, чем субъектами, поскольку это более соответствует распространенным технологиям обработки информации, предусматривающим разделение обязанностей и сфер ответственности между пользователями. Кроме того, ролевая политика может использоваться одновременно с другими политиками безопасности, когда полномочия ролей, назначаемых пользователям, контролируются дискреционной или мандатной политикой, что позволяет строить многоуровневые схемы контроля доступа.

ВЫВОДЫ

Определение политики безопасности и модели этой политики позволяют теоретически обосновать безопасность системы при корректном определении модели системы и ограничений в ее использовании. Обеспечение информационной безопасности предполагает повышение защищенности информации за счет разграничения доступа. В последнее десятилетие как в нашей стране, так и за рубежом активно проводятся исследования по развитию моделей разграничения доступа. Дальнейшими направлениями исследований в этой сфере могут быть поиски решений разграничения доступа в гипертекстовых информационно-поисковых системах, развитие концепции мультиролей в системах ролевого доступа, развитие моделей комплексной оценки защищенности системы.

Вопросы для самоконтроля

1. Что такое политика безопасности, кто ее разрабатывает и где она применяется?
2. Приведите классификацию моделей разграничения доступа. Какова их роль в теории информационной безопасности?
3. Каковы основные достоинства и недостатки дискреционных моделей?
4. Приведите примеры использования дискреционных моделей разграничения доступа.
5. Составьте матрицу доступа и граф доступа для организации документооборота факультета (объекты доступа: экзаменационные ведомости, персональные данные студентов, рабочие программы дисциплин; субъекты доступа: студенты, преподаватели, декан).
6. Что такое монитор безопасности и какие требования к нему предъявляются?

7. Перечислите основные положения субъектно-объектного подхода к разграничению доступа? В чем достоинства и недостатки такого подхода?
8. В чем суть мандатной политики разграничения доступа?
9. Каковы основные достоинства и недостатки мандатной политики?
10. Что такое скрытые каналы утечки информации и как их обнаружить?
11. Почему ролевая политика получила большое распространение?
12. В чем суть моделей группового доступа?
13. Что такое информационная невыводимость и информационное невмешательство?
14. Как и зачем строятся многоуровненвые схемы разграничения доступа. Приведите пример.

8. Обзор международных стандартов информационной безопасности

❖ Роль стандартов информационной безопасности ❖ Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC ❖ Европейские критерии безопасности информационных технологий (ITSEC) ❖ Федеральные критерии безопасности информационных технологий США ❖ Единые критерии безопасности информационных технологий ❖ Группа международных стандартов 270000 ❖

8.1. Роль стандартов информационной безопасности

С развитием информационных технологий появилась необходимость стандартизации требований в области защиты информации. Главная задача стандартов информационной безопасности — создать основу для взаимодействия между производителями, потребителями и специалистам по сертификации. Каждая из этих групп имеет свои интересы и свои взгляды на проблему информационной безопасности.

Производители нуждаются в стандартах как средстве сравнения возможностей своих продуктов, и в применении процедуры сертификации как механизме оценки их свойств, а также в стандартизации определенного набора требований безопасности, который мог бы ограничить фантазию заказчика конкретного продукта и заставить его выбирать требования из этого набора.

Потребители заинтересованы в методике, позволяющей обоснованно выбрать продукт, отвечающий их нуждам и решающий их проблемы, для чего им необходима шкала оценки безопасности и инструмент, с помощью которого они могли бы формулировать свои требования производителям.

Специалисты по сертификации рассматривают стандарты как инструмент, позволяющий им оценить уровень безопас-

ности, обеспечиваемый системой, и предоставить потребителям возможность сделать обоснованный выбор. Специалисты по сертификации заинтересованы в четких и простых критериях, так как они должны дать обоснованный ответ пользователям — удовлетворяет продукт их нужды, или нет. В конечном счете именно они принимают на себя ответственность за безопасность продукта, получившего квалификацию уровня безопасности и прошедшего сертификацию.

Таким образом, перед стандартами информационной безопасности стоит непростая задача создать эффективный механизм взаимодействия всех сторон.

8.2. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC

«Критерии безопасности компьютерных систем» (Trusted Computer System Evaluation Criteria), получившие неформальное название Оранжевая книга, были разработаны Министерством обороны США в 1983 году с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем, и выработки соответствующей методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах военного назначения.

В данном документе были впервые нормативно определены такие понятия, как «политика безопасности», «ядро безопасности» (TCB) и т. д. [3, 4].

Предложенные в этом документе концепции защиты и набор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности.

Классификация требований и критериев Оранжевой книги

В Оранжевой книге предложены три категории требований безопасности — политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних — на качество самих средств защиты. Рассмотрим эти требования подробнее.

1. *Политика безопасности*.

- Политика безопасности

Система должна поддерживать точно определённую политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основе их идентификации и набора правил управления доступом. Там, где необходимо, должна использоваться политика нормативного управления доступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации (информации, отмеченной грифом секретности: «секретно», «сов. секретно» и т.д.).

- Метки

С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа. Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту.

2. *Аудит*.

- Идентификация и аутентификация

Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентифика-

ции) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

- Регистрация и учет

Для определения степени ответственности пользователей за действия в системе все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективность его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

3. *Корректность*.

- Контроль корректности функционирования средств защиты

Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учёт, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

- Непрерывность защиты

Все средства защиты (в т. ч. и реализующие данное требование) должны быть защищены от несанкционированного вме-

шательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

Приведенные базовые требования к безопасности служат основой для критериев, образующих единую шкалу оценки безопасности компьютерных систем, определяющую семь классов безопасности.

Классы безопасности компьютерных систем

Оранжевая книга предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа A). Каждая группа включает один или несколько классов. Группы D и A содержат по одному классу (классы D и A соответственно), группа C — классы C1, C2, а группа B — Bl, B2, B3, характеризующиеся различными наборами требований безопасности. Уровень безопасности возрастает при движении от группы D к группе A, а внутри группы — с возрастанием номера класса.

Группа **D**. Минимальная защита.

Класс **D**. Минимальная защита. К этому классу относятся все системы, не удовлетворяющие требованиям других классов.

Группа **C**. Дискреционная защита.

Группа характеризуется произвольным управлением доступом и регистрацией действий субъектов.

Класс **C1.** Дискреционная защита. Системы этого класса удовлетворяют требованиям обеспечения разделения пользователей и информации и включают средства контроля и управления доступом, позволяющие задавать ограничения для инди-

видуальных пользователей, что дает им возможность защищать свою приватную информацию от других пользователей. Класс C1 рассчитан на многопользовательские системы, в которых осуществляется совместная обработка данных одного уровня секретности.

Класс **C2.** Управление доступом. Системы этого класса осуществляют более избирательное управление доступом, чем системы класса C1, с помощью применения средств индивидуального контроля за действиями пользователей, регистрацией, учетом событий и выделением ресурсов.

Группа **B**. Мандатная защита.

Основные требования этой группы — нормативное управление доступом с использованием меток безопасности, поддержка модели и политики безопасности, а также наличие спецификаций на функции ТСв. Для систем этой группы монитор взаимодействий должен контролировать все события в системе.

Класс **B1.** Защита с применением меток безопасности. Системы класса B1 должны соответствовать всем требованиям, предъявляемым к системам класса C2, и, кроме того, должны поддерживать определенную неформально модель безопасности, маркировку данных и нормативное управление доступом. При экспорте из системы информация должна подвергаться маркировке. Обнаруженные в процессе тестирования недостатки должны быть устранены.

Класс **B2.** Структурированная защита. Для соответствия классу B2 ТСВ системы должна поддерживать формально определенную и четко документированную модель безопасности, предусматривающую произвольное и нормативное управление доступом, которое распространяется по сравнению с системами класса B1 на все субъекты. Кроме того, должен осуществляться контроль скрытых каналов утечки информации. В структуре ТСВ должны быть выделены элементы, критичные с точки зрения безопасности. Интерфейс ТСВ должен быть четко определен, а ее архитектура и реализация выполнены с учетом

возможности проведения тестовых испытаний. По сравнению с классом B1 должны быть усилены средства аутентификации. Управление безопасностью осуществляется администраторами системы. Должны быть предусмотрены средства управления конфигурацией.

Класс **B3.** Домены безопасности. Для соответствия этому классу ТСВ системы должна поддерживать монитор взаимодействий, который контролирует все типы доступа субъектов к объектам, который невозможно обойти. Кроме того, ТСВ должна быть структурирована с целью исключения из нее подсистем, не отвечающих за реализацию функций защиты, и достаточно компактна для эффективного тестирования и анализа. В ходе разработки и реализации ТСВ необходимо применение методов и средств, направленных на минимизацию ее сложности. Средства аудита должны включать механизмы оповещения администратора при возникновении событий, имеющих значение для безопасности системы. Требуется наличие средств восстановления работоспособности системы.

Группа **A**. Верифицированная защита.

Данная группа характеризуется применением формальных методов верификации корректности работы механизмов управления доступом (произвольного и нормативного). Требуется дополнительная документация, демонстрирующая, что архитектура и реализация ТСВ отвечают требованиям безопасности.

Класс **A1.** Формальная верификация. Системы класса A1 функционально эквивалентны системам класса B3, и к ним не предъявляется никаких дополнительных функциональных требований. В отличие от систем класса B3 в ходе разработки должны применяться формальные методы верификации, что позволяет с высокой уверенностью получить корректную реализацию функций защиты. Процесс доказательства адекватности реализации начинается на ранней стадии разработки с построения формальной модели политики безопасности и спецификаций высокого уровня. Для обеспечения методов ве-

рификации системы класса A1 должны содержать более мощные средства управления конфигурацией и защищенную процедуру дистрибуции.

Высший класс безопасности, требующий осуществления верификации средств защиты, построен на доказательстве соответствия программного обеспечения его спецификациям с помощью специальных методик, однако это доказательство (очень дорогостоящее, трудоемкое и практически неосуществимое для реальных операционных систем) не подтверждает адекватность реализации политики безопасности.

Согласно «Оранжевой книге» безопасная компьютерная система — это система, поддерживающая управление доступом к обрабатываемой в ней информации таким образом, что только соответствующие авторизованные пользователи или процессы, действующие от их имени, получают возможность читать, писать, создавать и удалять информацию.

Приведенные классы безопасности надолго определили основные концепции безопасности и ход развития средств защиты.

Устаревание ряда положений Оранжевой книги обусловлено прежде всего интенсивным развитием компьютерных технологий. Именно для того, чтобы исключить возникшую в связи с изменением аппаратной платформы некорректность некоторых положений Оранжевой книги, адаптировать их к современным условиям и сделать адекватными нуждам разработчиков и пользователей программного обеспечения, и была проделана огромная работа по развитию положений этого стандарта. В результате возник целый ряд сопутствующих Оранжевой книге документов, многие их которых стали ее неотъемлемой частью.

Круг специфических вопросов по обеспечению безопасности компьютерных сетей и систем управления базами данных нашел отражение в отдельных документах, изданных Национальным центром компьютерной безопасности США в виде дополнений к Оранжевой книге.

Итак, «Критерии безопасности компьютерных систем» Министерства обороны США представляют собой первую попытку создать единый стандарт безопасности, рассчитанный на разработчиков, потребителей и специалистов по сертификации компьютерных систем. В свое время этот документ явился настоящим прорывом в области безопасности информационных технологий и послужил отправной точкой для многочисленных исследований и разработок. Основной отличительной чертой этого документа является его ориентация на системы военного применения, причем в основном на операционные системы. Это предопределило доминирование требований, направленных на обеспечение секретности обрабатываемой информации и исключение возможностей ее разглашения. Большое внимание уделено меткам (грифам секретности) и правилам экспорта секретной информации.

Оранжевая книга послужила основой для разработчиков всех остальных стандартов информационной безопасности и до сих пор используется в США в качестве руководящего документа при сертификации компьютерных систем обработки информации.

8.3. Европейские критерии безопасности информационных технологий (ITSEC)

Обзор основывается на версии 1.2 этих критериев, опубликованной в июне 1991 года от имени четырех стран: Франции, Германии, Нидерландов и Великобритании.

Европейские критерии рассматривают следующие задачи средств информационной безопасности:

- защита информации от несанкционированного доступа с целью обеспечение конфиденциальности;
- обеспечение целостности информации посредством защиты от ее несанкционированной модификации или уничтожения;

- обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

В «Европейских критериях» проводится различие между системами и продуктами.

Система — это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.

Продукт — это аппаратно-программный «пакет», который можно купить и по своему усмотрению встроить в ту или иную систему.

Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях. Угрозы безопасности системы носят вполне конкретный и реальный характер. Относительно угроз продукту можно лишь строить предположения. Разработчик может специфицировать условия, пригодные для функционирования продукта; дело покупателя обеспечить выполнение этих условий.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем — облегчить и удешевить оценку системы, составленной из ранее сертифицированных продуктов. В этой связи для систем и продуктов вводится единый термин — *объект оценки*. В соответствующих местах делаются оговорки, какие требования относятся исключительно к системам, а какие — только к продуктам.

Для того чтобы удовлетворить требованиям конфиденциальности, целостности и работоспособности, необходимо реализовать соответствующий набор функций безопасности, таких как идентификация и аутентификация, управление доступом, восстановление после сбоев и т. д. Чтобы средства защиты можно было признать эффективными, требуется определенная степень уверенности в правильности их выбора и надежности функционирования. Для решения этой проблемы в «Европейских кри-

териях» впервые вводится понятие адекватности (assurance) средств защиты.

Общая оценка уровня безопасности системы складывается из функциональной мощности средств защиты и уровня адекватности их реализации.

Большинство требований безопасности совпадает с аналогичными требованиями Оранжевой книги.

В «Европейских критериях» определено десять классов безопасности. Классы **F-C1, F-C2, F-B1, F-B2, F-B3** соответствуют классам безопасности Оранжевой книги с аналогичными обозначениями.

Класс **F-IN** предназначен для систем с высокими потребностями в обеспечении целостности, что типично для систем управления базами данных.

Его описание основано на концепции «ролей», соответствующих видам деятельности пользователей, и предоставлении доступа к определённым объектам только посредством доверенных процессов. Должны различаться следующие виды доступа: чтение, запись, добавление, удаление, создание, переименование и выполнение объектов.

Класс **F-AV** характеризуется повышенными требованиями к обеспечению работоспособности. Это существенно, например для систем управления технологическими процессами.

В требованиях этого класса указывается, что система должна восстанавливаться после отказа отдельного аппаратного компонента таким образом, чтобы все критически важные функции постоянно оставались доступными. В таком же режиме должна происходить и замена компонентов системы. Независимо от уровня загрузки должно гарантироваться определенное время реакции системы на внешние события.

Класс **F-DI** ориентирован на распределенные системы обработки информации.

Перед началом обмена и при получении данных стороны должны иметь возможность провести идентификацию участников вза-

имодействия и проверить ее подлинность. Должны использоваться средства контроля и исправления ошибок. В частности, при пересылке данных должны обнаруживаться все случайные или намеренные искажения адресной и пользовательской информации. Знание алгоритма обнаружения искажений не должно позволять злоумышленнику производить нелегальную модификацию передаваемых данных. Необходимо обнаруживать попытки повторной передачи ранее переданных сообщений.

Класс **F-DC** уделяет особое внимание требованиями к конфиденциальности передаваемой информации.

Информация по каналам связи должна передаваться в зашифрованном виде. Ключи шифрования защищают от несанкционированного доступа.

Класс **F-DX** предъявляет повышенные требования и к целостности и к конфиденциальности информации.

Его можно рассматривать как объединение классов F-DI и F-DC с дополнительными возможностями шифрования и защиты от анализа трафика. Следует ограничить доступ к ранее переданной информации, которая в принципе может способствовать проведению криптоанализа.

Критерии адекватности

Адекватность включает в себя два аспекта: эффективность, отражающую соответствие средств безопасности решаемым задачам, и корректность, характеризующую процесс их разработки и функционирования.

Эффективность — соответствие между задачами, поставленными перед средствами безопасности, и реализованным набором функций защиты — их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками слабых мест защиты.

Корректность — правильность и надежность реализации функций безопасности.

Европейские критерии уделяют адекватности средств защиты значительно больше внимания, чем функциональным требованиям. Как уже говорилось, адекватность складывается из двух компонентов — эффективности и корректности работы средств защиты.

Европейские критерии определяют семь уровней адекватности — от E0 до E6. При проверке адекватности анализируется весь жизненный цикл системы — от начальной фазы проектирования до эксплуатации и сопровождения. Уровни адекватности от E1 до E6 выстроены по нарастанию требований тщательности контроля. Так, на уровне E1 анализируется лишь общая архитектура системы, а адекватность средств защиты подтверждается функциональным тестированием. На уровне E3 к анализу привлекаются исходные тексты программ и схемы аппаратного обеспечения. На уровне E6 требуется формальное описание функций безопасности, общей архитектуры, а также политики безопасности.

В Европейских критериях определены три уровня безопасности — базовый, средний и высокий. Степень безопасности системы определяется самым слабым из критически важных механизмов защиты.

Безопасность считается базовой, если средства защиты способны противостоять отдельным случайным атакам.

Безопасность считается средней, если средства защиты способны противостоять злоумышленникам, обладающим ограниченными ресурсами и возможностями.

Наконец, безопасность можно считать высокой, если есть уверенность, что средства защиты могут быть преодолены только злоумышленником с высокой квалификацией, набор возможностей и ресурсов которого выходит за рамки возможного.

Итак, Европейские критерии безопасности информационных технологий, появившиеся вслед за Оранжевой книгой, оказали существенное влияние на стандарты безопасности и методику сертификации.

Главное достижение этого документа — введение понятия адекватности средств защиты и определение отдельной шкалы для критериев адекватности. Как уже упоминалось, Европейские критерии придают адекватность средств защиты даже большее значение, чем их функциональности. Этот подход используется во многих появившихся позднее стандартах информационной безопасности.

8.4. Федеральные критерии безопасности информационных технологий США

Федеральные критерии безопасности информационных технологий (Federal Criteria for Information Technology Security) разрабатывались как одна из составляющих Американского федерального стандарта по обработке информации (Federal Information Processing Standard), призванного заменить Оранжевую книгу. Разработчиками стандарта выступили Национальный институт стандартов и технологий США (Nationa Institute of Standards and Technology) и Агентство национальной безопасности США (National Security Agency). Данный обзор основан на версии 1.0 этого документа, опубликованной в декабре 1992 года.

Этот документ разработан на основе результатов многочисленных исследований в области обеспечения безопасности информационных технологий 1980-х — начала 1990-х гг., а также на основе анализа опыта использования Оранжевой книги.

Федеральные критерии безопасности информационных технологий (далее, просто Федеральные критерии) охватывают практически полный спектр проблем, связанных с защитой и обеспечением безопасности, т. к. включают все аспекты обеспечения конфиденциальности, целостности и работоспособности.

Основными объектами применения требований безопасности Федеральных критериев являются

- продукты информационных технологий (Information Technology Products);
- системы обработки информации (Information Technology Systems).

Под *продуктом информационных технологий* (далее просто ИТ-продукт) понимается совокупность аппаратных и/или программных средств, которая представляет собой поставляемое конечному потребителю готовое к использованию средство обработки информации.

Как правило, ИТ-продукт эксплуатируется не автономно, а интегрируется в систему обработки информации, представляющую собой совокупность ИТ-продуктов, объединенных в функционально полный комплекс, предназначенный для решения прикладных задач. В ряде случаев система обработки информации может состоять только из одного ИТ-продукта, обеспечивающего решение всех стоящих перед системой задач и удовлетворяющего требованиям безопасности. С точки зрения безопасности принципиальное различие между ИТ-продуктом и системой обработки информации определяется средой их эксплуатации. Продукт информационных технологий обычно разрабатывается в расчете на то, что он будет использован во многих системах обработки информации, и, следовательно, разработчик должен ориентироваться только на самые общие предположения о среде эксплуатации своего продукта, включающие условия применения и общие угрозы. Напротив, система обработки информации разрабатывается для решения прикладных задач в расчете на требования конечных потребителей, что позволяет в полной мере учитывать специфику воздействий со стороны конкретной среды эксплуатации.

Федеральные критерии содержат положения, относящиеся к отдельным продуктам информационных технологий. Вопросы построения систем обработки информации из набора

ИТ-продуктов не являются предметом рассмотрения этого документа.

Положения Федеральных критериев касаются собственных средств обеспечения безопасности ИТ-продуктов, т. е. механизмов защиты, встроенных непосредственно в эти продукты в виде соответствующих программных, аппаратных или специальных средств. Для повышения их эффективности могут дополнительно применяться внешние системы защиты и средства обеспечения безопасности, к которым относятся как технические средства, так и организационные меры, правовые и юридические нормы. В конечном счете, безопасность ИТ-продукта определяется совокупностью собственных средств обеспечения безопасности и внешних средств.

Ключевым понятием концепции информационной безопасности Федеральных критериев является понятие *Профиль защиты* (Protection Profile). Профиль защиты — это нормативный документ, который регламентирует все аспекты безопасности ИТ-продукта в виде требований к его проектированию, технологии разработки и квалификационному анализу. Как правило, один Профиль защиты описывает несколько близких по структуре и назначению ИТ-продуктов. Основное внимание в Профиле защиты уделяется требованиям к составу средств защиты и качеству и реализации, а также их адекватности предполагаемым угрозам безопасности.

Федеральные критерии представляют процесс разработки систем обработки информации, начинающийся с формулирования требований потребителями и заканчивающийся введением в эксплуатацию, в виде следующих основных этапов:

1. Разработка и анализ Профиля защиты. Требования, изложенные в Профиле защиты, определяют функциональные возможности ИТ-продуктов по обеспечению безопасности и условия эксплуатации, при соблюдении которых гарантируется соответствие предъявляемым требованиям. Кроме требований безопасности, Профиль защиты содержит требования по со-

блюдению технологической дисциплины в процессе разработки, тестирования и квалификационного анализа ИТ-продукта. Профиль безопасности анализируется на полноту, непротиворечивость и техническую корректность.

2. Разработка и квалификационный анализ ИТ-продуктов. Разработанные ИТ-продукты подвергаются независимому анализу, целью которого является определение степени соответствия характеристик продукта сформулированным в Профиле защиты требованиям и спецификациям.

3. Компоновка и сертификация системы обработки информации в целом. Успешно прошедшие квалификацию уровня безопасности ИТ-продукты интегрируются в систему обработки информации. Полученная в результате система должна удовлетворять заявленным в Профиле защиты требованиям при соблюдении указанных в нем условий эксплуатации.

Федеральные критерии регламентируют только первый этап этой схемы — разработку и анализ Профиля защиты, процесс создания ИТ-продуктов и компоновка систем обработки информации остаются вне рамок этого стандарта.

Профиль защиты

1) Описание.

Информация для его идентификации в специальной картотеке (характеристика проблемы обеспечения безопасности).

2) Обоснование.

Описание среды эксплуатации, предполагаемых угроз и методов использования ИТ-продукта; перечень задач по обеспечению безопасности, решаемых с помощью данного профиля.

3) Функциональные требования к ИТ-продукту.

Определение условий, в которых обеспечивается безопасность в виде перечня парируемых угроз.

4) Требования к технологии разработки ИТ-продукта.

Требования к самому процессу разработки, к условиям, в которых она проводится, к используемым технологическим средствам, к документированию процесса.

5)Требования к процессу сертификации

Порядок сертификации в виде типовой методики тестирования и анализа

Этапы разработки профиля защиты.

1) Анализ среды применения ИТ-продукта с точки зрения безопасности.

2) Выбор профиля-прототипа.

3) Синтез требований.

Выбор наиболее существенных функций защиты, их ранжирование по степени важности с точки зрения обеспечения качества защиты.

После разработки профиль защиты проверяется для подтверждения полноты, корректности, непротиворечивости и реализуемости.

Классы функциональных требований к ИТ-продукту.

1) Политика безопасности.

2) Мониторинг взаимодействий.

3) Логическая защита ТСв.

- требования корректности внешних субъектов относительно субъектов ТСВ;
- требования к интерфейсам взаимодействия.

4) Физическая защита ТСв.

5) Самоконтроль ТСв.

6) Инициализация и восстановление ТСв.

7) Ограничение привилегий при работе с ТСв.

8) Простота использования ТСв.

Классификация функциональных требований.

1. Широта сферы применения.

Пользователи системы, субъекты и объекты доступа; функции ТСВ и интерфейс взаимодействия; аппаратные, программные и специальные компоненты; параметры конфигурации.

2. Степень детализации.

Определяется множеством атрибутов сущностей, к которым применяются данные требования.

3. Функциональный состав средств защиты.

Определяется множеством функций, включённых в ТСВ для реализации группы требований.

4. Обеспечиваемый уровень безопасности.

Определяется условиями, в которых компоненты системы способны противостоять заданному множеству угроз.

Итак, Федеральные критерии безопасности информационных технологий — первый стандарт информационной безопасности, в котором определяются три независимые группы требований: функциональные требования к средствам защиты, требования к технологии разработки и к процессу квалификационного анализа. Авторами этого стандарта впервые предложена концепция Профиля защиты — документа, содержащего описание всех требований безопасности как к самому ИТ-продукту, так и к процессу его проектирования, разработки, тестирования и квалификационного анализа.

Функциональные требования безопасности хорошо структурированы и описывают все аспекты функционирования ТСв. Требования к технологии разработки, впервые появившиеся в этом документе, побуждают производителей использовать современные технологии программирования как основу для подтверждения безопасности своего продукта.

Требования к процессу квалификационного анализа носят общий характер и не содержат конкретных методик тестирования и исследования безопасности ИТ-продуктов.

Разработчики Федеральных критериев отказались от используемого в Оранжевой книге подхода к оценки уровня безопасности ИТ-продукта на основании обобщенной универсальной шкалы классов безопасности. Вместо этого предлагается независимое ранжирование требований каждой группы, т. е.

вместо единой шкалы используется множество частных шкал-критериев, характеризующих обеспечиваемый уровень безопасности. Данный подход позволяет разработчикам и пользователям ИТ-продукта выбрать наиболее приемлемое решение и точно определить необходимый и достаточный набор требований для каждого конкретного ИТ-продукта и среды его эксплуатации.

Стандарт рассматривает устранение недостатков существующих средств безопасности как одну из задач защиты наряду с противодействием угрозам безопасности и реализацией модели безопасности.

Данный стандарт ознаменовал появление нового поколения руководящих документов в области информационной безопасности, а его основные положения послужили базой для разработки Канадских критериев безопасности компьютерных систем и Единых критериев безопасности информационных технологий.

8.5. Единые критерии безопасности информационных технологий

Единые критерии безопасности информационных технологий (Common Criteria for Information Technology Security Evaluation, далее — Единые критерии) являются результатом совместных усилий авторов Европейских критериев безопасности информационных технологий, Федеральных критериев безопасности информационных технологий и Канадских критериев безопасности компьютерных систем, направленных на объединение основных положений этих документов и создание Единого международного стандарта безопасности информационных технологий. Работа над этим самым масштабным в истории стандарте информационной безопасности проектом

началась в июне 1993 года с целью преодоления концептуальных и технических различий между указанными документами, их согласования и создания единого международного стандарта. Версия 2.1 этого стандарта утверждена Международной организацией по стандартизации (ISO) в 1999 г. в качестве Международного стандарта информационной безопасности ISO/IEC 15408. В Российской федерации стандарт действует под номером ГОСТ Р ИСО/МЭК 15408.

Единые критерии сохраняют совместимость с существующими стандартами и развивают их путем введения новых концепций, соответствующих современному уровню развития информационных технологий и интеграции национальных информационных систем в единое мировое информационное пространство. Этот документ разработан на основе достижений многочисленных исследований в области безопасности информационных технологий 1990-х гг. и на результатах анализа опыта применения положенных в его основу стандартов. Единые критерии оперируют уже знакомым по Федеральным критериям понятием *продукт информационных технологий*, или ИТ-продукт, и используют предложенную в них концепцию Профиля защиты.

Единые критерии разрабатывались в расчете на то, чтобы удовлетворить запросы трех групп специалистов, в равной степени являющихся пользователями этого документа: производителей и потребителей продуктов информационных технологий, а также экспертов по квалификации уровня их безопасности. Заинтересованные стороны могут задать функциональные возможности безопасности продукта с использованием стандартных профилей защиты и самостоятельно выбрать оценочный уровень уверенности в безопасности из совокупности семи возрастающих оценочных уровней уверенности в безопасности от 1 до 7.

Потребители рассматривают квалификацию уровня безопасности ИТ-продукта как метод определения соответствия ИТ-продукта их запросам. Обычно эти запросы составляются на основании результатов проведенного анализа рисков и выбранной

политики безопасности. Единые критерии играют существенную роль в процессе формирования запросов потребителей, так как содержат механизмы, позволяющие сформулировать эти запросы в виде стандартизованных требований. Это позволяет потребителям принять обоснованное решение о возможности использования тех или иных продуктов. Наконец, Единые критерии предоставляют потребителям механизм Профилей защиты, с помощью которого они могут выразить специфичные для них требования, не заботясь о механизмах их реализации.

Производители должны использовать Единые критерии в ходе проектирования и разработки ИТ-продуктов, а также для подготовки к квалификационному анализу и сертификации. Этот документ дает возможность производителям на основании анализа запросов потребителей определить набор требований, которым должен удовлетворять разрабатываемый ими продукт. Производители используют предлагаемую Едиными критериями технологию для обоснования своих претензий на то, что поставляемый ими ИТ-продукт успешно противостоит угрозам безопасности, на основании того, что он удовлетворяет выдвинутым функциональным требованиям и их реализация осуществлена с достаточным уровнем адекватности. Для осуществления этой технологии Единые критерии предлагают производителям специальный механизм, названный Проект защиты, дополняющий Профиль защиты и позволяющий соединить описания требований, на которые ориентировался разработчик, спецификации механизмов реализации этих требований.

Кроме того, производители могут использовать Единые критерии для определения границ своей ответственности, а также условий, которые необходимо выполнить для успешного прохождения квалификационного анализа и сертификации созданного ими продукта.

Эксперты по квалификации используют этот документ в качестве основных критериев определения соответствия средств защиты ИТ-продукта требованиям, предъявляемым к нему по-

требителями, и угрозам, действующим в среде его эксплуатации. Единые критерии описывают только общую схему проведения квалификационного анализа и сертификации, но не регламентируют процедуру их осуществления. Вопросам методологии квалификационного анализа и сертификации посвящен отдельный документ — «Общая методология оценки безопасности информационных технологий».

Таким образом, Единые критерии обеспечивают нормативную поддержку процесса выбора ИТ-продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

Единые критерии рассматривают информационную безопасность как совокупность конфиденциальности и целостности информации, обрабатываемой ИТ-продуктом, а также доступности ресурсов ВС, ставят перед средствами защиты задачу противодействия угрозам, актуальным для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации.

Единые критерии регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ-продуктов, используя схему из Федеральных критериев. Единые критерии предлагают достаточно сложный процесс разработки и квалификационного анализа ИТ-продуктов, требующий от потребителей и производителей составления и оформления весьма объемных и подробных нормативных документов.

Задачи защиты — базовое понятие Единых критериев, выражающее потребность потребителей ИТ-продукта в противостоянии заданному множеству угроз безопасности или в необходимости реализации политики безопасности.

Профиль защиты — специальный нормативный документ, представляющий собой совокупность Задач защиты, функци-

ональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ-продукта при создании Проекта защиты.

Проект защиты — специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования.

Каталог функциональных классов:

- аудит,
- связь (подтверждение приёма/передачи информации),
- криптографическая поддержка,
- защита данных пользователя (конфиденциальность, целостность, доступность),
- идентификация и аутентификация,
- управление безопасностью,
- приватность (конфиденциальность работы в системе),
- надёжность средств защиты,
- контроль за использованием ресурсов,
- контроль доступа к объекту оценки,
- доверенный маршрут/канал (прямое взаимодействие).

Требования уверенности в безопасности (адекватности)

- управление проектом,
- дистрибуция,
- разработка,
- документация,
- процесс разработки,
- тестирование,
- анализ защиты.

«Единые критерии» содержат совокупность предопределённых оценочных уровней уверенности в безопасности, составленных из компонентов семейств требований уверенности в безопасности. Эти уровни предназначены:

- для достижения совместимости с исходными критериями;

- для обеспечения потребителя пакетами компонентов общего назначения.

Для достижения конкретных целей уровень может быть усилен дополнительными компонентами.

ОУБ1 — функциональное тестирование (соответствует американскому TCSEC — D, европейскому ITSEC — E1).

ОУБ2 — структурное тестирование (C1, E2).

ОУБ3 — методическое тестирование и проверка (C2, E3).

ОУБ4 — методическое проектирование, тестирование и просмотр (B1, E4).

ОУБ5 — полуформальное проектирование и тестирование (B2, E5).

ОУБ6 — полуформальная верификация проекта и тестирование (B3, E6).

ОУБ7 –формальная верификация проекта и тестирование (A1, E7).

Эквивалентность указана в целом, точного соответствия не существует, т. к. различаются подходы.

Согласно Единым критериям, безопасность информационных технологий может быть достигнута посредством применения предложенной технологии разработки, сертификации и эксплуатации ИТ-продуктов.

Единые критерии определяют множество типовых требований, которые в совокупности с механизмом Профилей защиты позволяют потребителям создавать частные наборы требований, отвечающие их нуждам. Разработчики могут использовать Профиль защиты как основу для создания спецификаций своих продуктов. Профиль защиты и спецификации средств защиты составляют Проект защиты, который и представляет ИТ-продукт в ходе квалификационного анализа.

Квалификационный анализ может осуществляться как параллельно с разработкой ИТ-продукта, так и после ее завершения. Для проведения квалификационного анализа разработчик продукта должен представить следующие материалы:

- профиль защиты, описывающий назначение ИТ-продукта и характеризующий среду его эксплуатации, а также устанавливающий Задачи защиты и требования, которым должен отвечать продукт;
- проект защиты, включающий спецификации средств защиты, также обоснование соответствия ИТ-продукта задачам защиты из Профиля защиты и указанным в нем требованиям Единых критериев;
- различные обоснования и подтверждения свойств и возможностей ИТ-продукта, полученные разработчиком;
- сам ИТ-продукт;
- дополнительные сведения, полученные путем проведения различных независимых экспертиз.

Процесс квалификационного анализа включает три стадии:

1. Анализ Профиля защиты на предмет его полноты, непротиворечивости, реализуемости и возможности использования в качестве набора требований для анализируемого продукта.

2. Анализ Проекта защиты на предмет его соответствия требованиям Профиля защиты, а также полноты, непротиворечивости, реализуемости и возможности использования в качестве эталона при анализе ИТ-продукта.

3. Анализ ИТ-продукта на предмет соответствия Проекту защиты. Результатом квалификационного анализа является заключение о том, что проанализированный ИТ-продукт соответствует представленному Проекту защиты. Заключение состоит из нескольких отчетов, отличающихся уровнем детализации и содержащих мнение экспертов по квалификации об ИТ-продукте на основании критериев квалификации Единых критериев.

Применение квалификационного анализа и сертификации приводит к повышению качества работы производителей в процессе проектирования и разработки ИТ-продуктов. В продуктах, прошедших квалификацию уровня безопасности, вероятность появления ошибок и изъянов защиты и уязвимостей существенно меньше, чем в обычных продуктах. Все это позво-

ляет говорить о том, что применение Единых критериев оказывают положительное и конструктивное влияние на процесс формирование требований, разработку ИТ-продукта, сам продукт и его эксплуатацию.

Таким образом, Единые критерии безопасности информационных технологий представляют собой результат обобщения всех достижений последних лет в области информационной безопасности. Впервые документ такого уровня содержит разделы, адресованные потребителям, производителям и экспертам по квалификации ИТ-продуктов.

Разработчики Единых критериев продолжили работу над Федеральными критериями, направленными на отказ от единой шкалы безопасности, усилив гибкость предложенных в них решений путем введения частично упорядоченных шкал, благодаря чему потребители и производители получили дополнительные возможности по выбору требований и их адаптации к своим прикладным задачам.

Особое внимание этот стандарт уделяет адекватности реализации функциональных требований, которая обеспечивается как независимым тестированием и анализом ИТ-продукта, так и применением соответствующих технологий на всех этапах его проектирования и реализации.

Таким образом, требования Единых критериев охватывают практически все аспекты безопасности ИТ-продуктов и технологии их создания, а также содержат все исходные материалы, необходимые потребителям и разработчикам для формирования Профилей и Проектов защиты.

Кроме того, требования Единых критериев являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника по безопасности информационных технологий.

Данный стандарт ознаменовал собой новый уровень стандартизации информационных технологий, подняв его на межгосударственный уровень. За этим проглядывается реальная

перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что предоставит возможности для интеграции национальных информационных систем.

8.6. Группа международных стандартов 270000

Основное назначение международных стандартов — это создание на межгосударственном уровне единой основы для разработки новых и совершенствования действующих систем качества. Сотрудничество в области стандартизации направлено на приведение в соответствие национальной системы стандартизации с международной. Международные стандарты не имеют статуса обязательных для всех стран-участниц. Любая страна мира вправе применять или не применять их. Решение вопроса о применении международного стандарта связано в основном со степенью участия страны в международном разделении труда.

Международные стандарты принимаются Международной организацией по стандартизации — ИСО (International Organization for Standardization, ISO).

ИСО учреждена в 1946 г. представителями двадцати пяти индустриально развитых стран и обладает полномочиями по координации на международном уровне разработки различных промышленных стандартов и осуществляет процедуру принятия их в качестве международных стандартов.

Сфера деятельности ИСО касается стандартизации во всех областях, кроме электротехники и электроники, относящихся к компетенции Международной электротехнической комиссии (МЭК, IEC). Некоторые виды работ выполняются этими организациями совместно. В этом случае в наименовании стандарта появляется аббревиатура ИСО/МЭК.

В системе международных стандартов в 2008 г. выделена отдельная группа, связанная с информационной безопасностью, имеющая наименование ISO/IEC 27000. Эти стандарты опубликованы совместно Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC).

Серия содержит лучшие практики и рекомендации в области информационной безопасности для создания, развития и поддержания Системы менеджмента информационной безопасности.

В настоящее время серия содержит более 30 стандартов, большинство из которых действуют на территории Российской Федерации с аналогичным номером ГОСТ. В первую десятку группы входят:

ГОСТ Р ИСО/МЭК 27000–2012— «СМИБ. Общий обзор и терминология».

ГОСТ Р ИСО/МЭК 27001–2006— «СМИБ. Требования» ГОСТ Р ИСО/МЭК 27002–2012— «СМИБ. Свод норм и правил менеджмента информационной безопасности».

ГОСТ Р ИСО/МЭК 27003–2012—»СМИБ. Руководство по реализации системы менеджмента информационной безопасности».

ГОСТ Р ИСО/МЭК 27004–2011— «СМИБ. Измерения».

ГОСТ Р ИСО/МЭК 27005–2010 — «СМИБ. Менеджмент риска информационной безопасности».

ГОСТ Р ИСО/МЭК 27006–2008— «СМИБ. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».

ГОСТ Р ИСО/МЭК 27007–2014 — «СМИБ. Руководства по аудиту систем менеджмента информационной безопасности».

Итак, главная задача стандартов информационной безопасности — согласовать позиции и цели производителей, потребителей и аналитиков-классификаторов в процессе созда-

ния и эксплуатации продуктов информационных технологий. Первые версии стандартов создавались в основном исходя из нужд обороны и были нацелены на обеспечение секретности информации. С развитием средств вычислительной техники и телекоммуникаций возникла потребность создания новых стандартов, отражающих особенности современного уровня информационных технологий. Применяемые международные стандарты не содержат сквозных шкал и перечней требований безопасности, они ориентированы на применение профилей защиты, представляющих собой перечень функциональных требований для систем определённого назначения.

Вопросы для самоконтроля

1. Цели применения стандартов информационной безопасности.
2. Охарактеризуйте основные положения Оранжевой книги.
3. Почему в современных стандартах отказываются от единых шкал, характеризующих уровень безопасности?
4. Каковы основные положения Европейских критериев безопасности информационных технологий?
5. Чем отличаются «информационная система» и «продукт информационных технологий»?
6. Для чего вводятся критерии адекватности?
7. Что такое Профиль защиты?
8. В чем особенности Канадских критериев безопасности компьютерных систем?
9. Опишите структуру Общих критериев безопасности информационных технологий.
10. Опишите технологию применения Общих критериев безопасности информационных технологий.
11. Каковы тенденции развития международной нормативной базы в области информационной безопасности?

9. Информационные войны и информационное противоборство

❖ Определение и основные виды информационных войн ❖ Информационно-техническая война ❖ Информационно-психологическая война ❖

В настоящее время промышленно развитые страны переживают новый исторический этап развития, связанный с возрастанием роли информации в обществе. Информационная зависимость всех сфер жизнедеятельности общества и государства чрезвычайно велика. Так, по оценкам американских экспертов, нарушение работы компьютерных сетей, используемых в системах управления государственными и банковскими структурами США способно нанести экономике страны серьезный ущерб, сравнимый с ущербом от применения против США ядерного оружия [4].

Следовательно, развитие информационных технологий ведет к появлению качественно новых форм борьбы, получивших название «информационная война», «информационное противоборство», «информационное воздействие».

9.1. Определение и основные виды информационных войн

Информационная война — открытые или скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной, военной, политической или идеологической сферах [10].

Впервые термин «информационная война» появился в США в середине 70-х гг. XX в., его появление было обусловлено скач-

ком в развитии компьютерных технологий и средств связи. Информационное оружие не менее опасно, чем оружие традиционное. Информационная борьба может быть как самостоятельным видом противоборства (без вооруженного конфликта), так и дополнением традиционных военных действий.

В зависимости от масштабов информационные войны делятся:

- на персональные,
- корпоративные,
- глобальные.

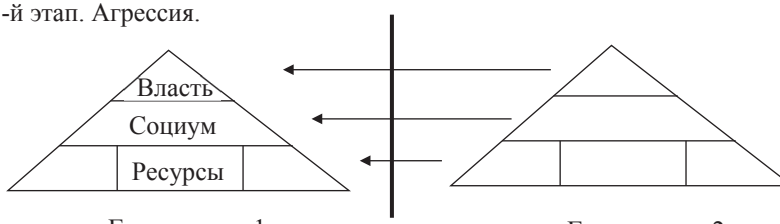
Персональные информационные войны чаще всего связаны с нарушением личной информационной неприкосновенности. Корпоративные информационные войны возникают вследствие соперничества между корпорациями и нацелены на получение информации о деятельности конкурента или его ликвидацию. Во время глобальной информационной войны наносится ущерб информационным ресурсам противника при одновременной защите своих на уровне государства. При глобальной информационной войне можно выделить три основных направления ведения войны:

- воздействие на индивидуальное, групповое и массовое сознание с использованием СМИ;
- воздействие на системы принятия решений в политической, экономической, военной, научно-технической, социальной сферах;
- воздействие на информационные системы с целью управления, блокирования, съема обрабатываемой информации.

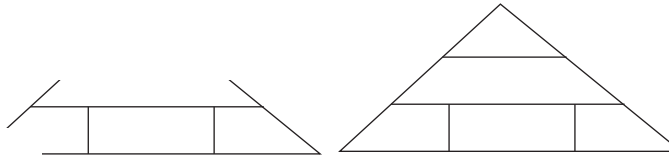
Рассмотрим отличия традиционной и информационной межгосударственных войн. Если схематично представить государство в виде пирамиды, на вершине которой находится аппарат государственной власти, основание составляют ресурсы (материальные, человеческие, энергетические), а между ними

расположен социум (общество), то отличие информационной и традиционной войны можно проиллюстрировать рис. 9.1, 9.2.

1-й этап. Агрессия.



2-й этап. Разрушение надстройки и части ресурсов.



3-й этап. Встраивание ресурсов в государство-победитель.

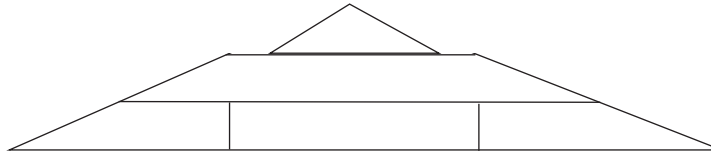


Рис. 9.1. Схема ведения традиционной войны

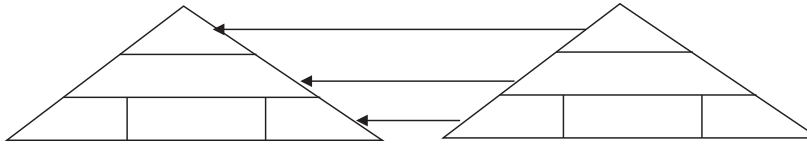


Рис. 9.2. Схема ведения информационной войны

Считается, что цель войны — получение ресурсов. При ведении традиционной войны разрушается надстройка побежденного государства, гибнет часть ресурсов; определенный ущерб наносится и государству-победителю. Последствия традиционной войны в современном мире могут быть неприемлемы для победителя (например, в случае ядерного конфликта). При информационной войне нет явной границы противоборства (фронта), однако в результате успешной информационной войны под контроль победителя попадают все уровни, включая власть, ресурсы, территорию.

По направленности воздействий информационная борьба подразделяется на два основных вида [10]:

- информационно-техническую,
- информационно-психологическую.

Они отличаются объектами защиты и воздействия.

Основные объекты воздействия информационно-психологической войны:

- психика человека,
- система принятия политических решений,
- система общественного сознания,
- система формирования общественного мнения.

Основные объекты воздействия информационно-технической войны:

- радиоэлектронная борьба,
- линии связи и телекоммуникации.

Выделяется четыре сферы ведения информационной войны:

1. Политическая.

К этой сфере относятся:

- борьба за ноосферу. Объекты этой битвы — государственные идеи, духовные и национальные ценности, системы вероисповеданий, т. е. духовная сфера жизнедеятельности людей;

- интеллектуальная борьба элит (инновации, рефлексивное управление). Исследования показывают, что воздействие на информационный ресурс государства может стать одним из источников угроз для национальной безопасности. Наиболее сложная форма воздействия — рефлексивное управление процессом принятия решения в государственных структурах посредством формирования выгодной для воздействующего информации или дезинформации.
- информационное противоборство в ходе избирательных процессов.

2. Финансово-экономическая.

В настоящее время мировая финансовая система стала главной ареной информационно-психологического противоборства между ведущими государствами мира. Одним из теоретиков и практиков информационно-психологического противоборства в финансовой сфере является Д. Сорос. Первой информационно-психологической битвой в финансовой сфере между ведущими странами мира можно считать мировые финансовые кризисы 1997–1998 гг. В будущем информационные войны будут в основном вестись именно в финансовой, а не в военной сфере. В условиях создания единого общемирового информационного пространства развернется геостратегическое противоборство между ведущими мировыми державами за доминирование в информационной среде мировой финансовой системы. Для того чтобы стать экономически процветающей державой, Россия должна научиться защищать свои национальные интересы в мировой информационной среде и противодействовать информационной экспансии других стран в мировой финансовой системе.

3. Дипломатическая.

4. Военная.

Отдельно можно выделить противоборство в Интернете.

Информационная революция способствовала появлению новых форм и способов ведения информационно-психологического противоборства в мировом информационном пространстве. Во многом это связано с созданием сети Интернет, данную тенденцию необходимо учитывать при разработке теории информационно-психологического обеспечения национальной безопасности России.

9.2. Информационно-техническая война

В информационно-технической борьбе главными объектами нападения и защиты являются системы управления и связи, телекоммуникационные системы, различные радиоэлектронные средства. Понятие «информационное оружие», получившее широкое распространение после завершения военной операции против Ирака в 1991 г., сформировалось как раз в результате появления средств ведения информационно-технической борьбы. Решающий вклад в поражение Ирака внесло комплексное применение средств разведки, управления, связи, навигации и радиоэлектронной борьбы, совокупность которых и была определена как информационное оружие театра военных действий. Опыт локальных войн конца XX в. свидетельствует о том, что обязательным атрибутом победы в современном бою является завоевание превосходства в информационной сфере. В военное время ведение информационной войны предполагается на стратегическом, оперативном и тактическом уровнях. Но информационное оружие необходимо задействовать еще до начала боевых действий, а в полной мере применять уже в ходе сражений. Еще в мирное время объектами и целями этой борьбы являются информационные ресурсы государства, в которые включается прежде всего информация, существующая на ма-

териальных носителях или в любой другой форме. Особое значение информационных ресурсов обусловлено тем ключевым положением, которое они в силу особой роли информации как системообразующего фактора занимают по отношению к любым другим ресурсам государства — экономическим, научно-техническим и собственно военным.

В первую очередь информационное оружие направлено против вооруженных сил, предприятий оборонного комплекса, структур безопасности. При атаках удары наносят по телекоммуникациям или транспортным системам. Универсальность, скрытность, многовариантность форм программно-аппаратной реализации, радикальность воздействия, достаточный выбор места и времени применения, экономичность делают информационное оружие чрезвычайно опасным. Оно позволяет вести наступательные действия анонимно, без объявления войны. Классификация Мартина Либицки [10] рассматривает методы ведения этих действий в рамках следующих форм:

- командно-управленческой,
- разведывательной,
- электронной,
- экономической,
- кибер-войны,
- хакерской войны.

1. Командно-управленческая информационная война.

Разрушить структуру управления войсками противника можно, направив удар на лидера армии или штаб командования — «голову» или сеть коммуникаций, соединяющих командование с основной массой войск, — «шею». Удар по «голове» — это испытанный прием всех военных операций с древности. Во время войны в Заливе успешность военных действий американцев во многом была обеспечена предварительным разрушением структуры командования и управления войсками противника. Им удалось добиться, таким образом, дезориентации ирак-

ских войск и неэффективности их военных действий. Штабы командования противника легко распознать по большому количеству коммуникаций, которые их окружают, постоянному движению больших потоков информации. Современные информационные технологии дают возможность использовать этот метод по-новому. Теперь коммуникации противника можно разрушить не только при помощи бомб, или физической атаки, а через компьютерную систему, например перекрыв подачу электричества, глуша радиоволны, внедрив вирусы в компьютерную сеть. Удар по «шее», разрыв связи между командованием и основной армией позволит отделить «голову» от «туловища», тем самым противник потеряет дееспособность. Для того чтобы использовать этот способ, нужно точно знать, каким образом происходит коммуникация противника, насколько важно командованию врага постоянно поддерживать связь с армией. Каждому действию в информационной войне должна предшествовать тщательная исследовательская и разведывательная работа, чтобы оно принесло необходимый результат. Например, во время войны во Вьетнаме разрушение связи между армией и командованием не имело ожидаемого эффекта, поскольку стратеги в США не учли особенности вьетнамских традиций в ведении войны. Оказалось, что во Вьетнаме, в отличие от США, отдельные подразделения армии обладают большой независимостью и они способны самостоятельно планировать военные действия, организовывать сопротивление без верховного командования в течение длительного времени. Таким образом, удары по «голове» и «шее» не дали никаких положительных результатов. Кроме того, уничтожение лидера или командования может привести к такому неприятному эффекту, как распространение неконтролируемой партизанской войны.

2. Разведывательная война.

Традиционно командование армии получает от разведки информацию о месторасположении противника, его качествен-

ных и количественных характеристиках. Это необходимо, чтобы планировать дальнейшую военную деятельность. Современная разведка благодаря развитию информационных технологий может обеспечивать командование достаточным количеством информации о противнике. Основная работа разведчика сегодня состоит в адекватном анализе полученной информации, способствующем принятию эффективных действий. Оборонительная составляющая этого типа войны включает работу по «обману» источников развединформации, когда они не уничтожаются, но нарушаются так, чтобы передавать неверную информацию.

3. Радиоэлектронная война.

Это особый вид информационной борьбы, призванный нарушать или затруднять функционирование электронных средств противника путем излучения, отражения электромагнитных сигналов, акустических и инфракрасных сигналов. Эта борьба осуществляется наземными, корабельными и авиационными системами постановки помех. Сюда входят способы по глушению радиосигналов противника, радиоперехваты, нарушение правильной работы радаров посредством введения ошибок в компьютерную сеть. К средствам ведения радиоэлектронной войны относятся электромагнитные бомбы и электромагнитные пушки. Мощный электромагнитный импульс (до десятков гигаватт), излучаемый этими устройствами, выводит из строя все электронное оборудование.

4. Хакерская война (компьютерные войны).

Целью нападения может быть полное разрушение компьютерной системы, ее временный выход из строя, программирование на выдачу ошибочной информации, кража информации или услуг. Нападение на военные информационные системы может осуществляться как во время конфликта, так и в мирное время. Атакующее информационное оружие этого типа широко

распространено и многообразно. По мнению С. П. Расторгуева [10], информационным оружием следует называть средства уничтожения, хищения, искажения информационных массивов, средства дезорганизации работы технических устройств, компьютерных систем.

Вредоносные программы способны разрушать программное обеспечение компьютерных систем. Они могут размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления.

Кроме того, сюда относятся различные средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления, различного рода ошибки, сознательно вводимые лазутчиком в программное обеспечение объекта.

5. Экономическая война.

Выделяется две ее разновидности. Первая — это информационная блокада, когда страна-агрессор перекрывает потоки информации из внешнего мира, необходимые для процветания государства. Вторая разновидность — формационный империализм — преобладание информационных продуктов одной страны, экспансия своих ценностей и культуры в различных проявлениях. Наиболее ярким примером являются процессы «американизации» современного мира.

6. Кибер-война.

Этот тип информационной войны пока не существует, но предполагается, что к нему должно привести дальнейшее развитие информационных технологий.

Среди вариантов кибер-войн сейчас наиболее понятны для осмысления семантические атаки и симуляционные войны. Отличие семантических атак от обычного хакерства в том, что система не выводится из строя, не разрушается, она продолжает

нормально функционировать, но настраивается таким образом, чтобы выдавать пользователю неверные ответы, неправильно решает поставленные задачи. Симуляционные войны ведутся только в виртуальном пространстве, причем победивший в них признается победителем и в реальном мире.

9.3. Информационно-психологическая война

В информационно-психологической борьбе главными объектами нападения и защиты являются психика личного состава вооруженных силовых структур, населения противостоящих сторон, системы формирования общественного мнения и принятия решений. Такая борьба ведется методами и средствами информационно-психологического воздействия, ориентированного на войска и население по обе стороны «фронта».

Под *информационно-психологическими воздействиями* понимаются информационные воздействия на психику, в первую очередь на сознание человека и сообществ людей, проявляющиеся в изменении восприятия ими реальной действительности, коррекции своего поведения и принятия решений, а также, в некоторых случаях — в изменении физиологического состояния организма человека. Так, информационно-психологические воздействия в политической сфере понимаются как использование дипломатических, военно-демонстрационных, экономических, политических, информационных приемов для прямого или косвенного воздействия на мнение, настроения, чувства и, в итоге, на поведение другой стороны с целью подавить волю, заставить действовать под диктовку.

Информационно-психологические методы и средства психотехнологий подразделяются на открытые и скрытые, положительные и негативные и деструктивные, преследующие яв-

ные и скрытые цели. Открытые психотехнологии реализуются с помощью честных «чистых» и обманных «грязных» методов и приемов. Информационно-психологические воздействия скрытого типа направлены на прямую манипуляцию сознанием человека через его подсознание путем применения скрытых психотехнологий, когда объект воздействия не осознает самого факта воздействия. Указанные скрытые воздействия включают психотропные (техногенные) средства, а также суггестивные (внушение, массовый гипноз) и психотропные (фармакологические) воздействия. Психофизические воздействия имеют скрытую насильственную направленность на психику и подсознание человека с целью безусловной модификации сознания, поведения и здоровья в нужном для воздействующей стороны направлении. Стремление скрыто воздействовать через подсознание человека осуществляется современными психотехнологиями, в том числе с применением сверхслабых энергоинформационных взаимодействий. В данный момент многие аналитики обращают внимание на нарастающее со стремительной скоростью совершенствование старых и на появление новых информационных психотехнологий, составляющих реальное оружие и опасность для интеллекта отдельной личности и народа в целом, его армии, силовых структур, руководящих органов власти.

До последнего времени главным объектом воздействия утверждалось сознание человека. Считалось непреложной истиной, что осязаемые эффекты могут быть восприняты нашим сознанием тогда и только тогда, когда они критически осмыслены нашим сознанием, пройдут через фильтр нашей оперативной памяти, а лишь потом отложаться в хранилище памяти — в нашем подсознании, прямой доступ к которому категорически закрыт. Подсознание рассматривается скорее как нечто мифическое, эфемерное как нечто спящее, неактивное, не способное влиять на «здравые» мысли и поступки личности. Новейшие исследования убедительно доказали, что наша

оперативная память, формирующая наш здравый смысл, — это всего лишь малая часть от нашей суммарной памяти, которой обладает человек. Главный ее резерв и хранилище — наше подсознание. В подсознании содержится от 70 до 99 процентов объема нашей памяти (всех знаний). Отсюда огромный интерес к раскрытию резервных возможностей человека путем прямого воздействия на его подсознание. Попытка «раскопать» глубинные залежи нашего мозга направлена на активное задействование подсознания в оперативный процесс мышления, когда реализуются феноменальные возможности человека по запоминанию информации, по фантастической скорости счета, по раскрытию его парапсихических способностей. С другой стороны, за этим стоит желание научиться прямо воздействовать на подсознание людей, программировать их на определенные мысли и поступки. Подобные действия влекут за собой не только фундаментальные сдвиги в подсознании и психике людей, но и изменение их мировоззренческих позиций.

Стремление воздействовать на человека напрямую через его подсознание выражено в разработке самых различных методов, при использовании которых объект воздействия не осознает ни цель, ни даже сам факт воздействия. Их коренное отличие от информационных воздействий открытого типа заключается в том, что они скрытно, то есть без ведома объекта воздействия, лишают его права самостоятельного выбора логически обоснованных решений, свободы выбора своего поведения, исполнения желаний, выражения эмоций и даже психофизиологического состояния организма (настроения, здоровья). Это достигается либо предварительным введением объекта воздействия в измененное состояние сознания, либо внедрением манипулирующей информации на фоне отвлекающих сообщений прямо в подсознание, минуя этап критического восприятия ее сознанием человека. В востребованное время эта информация по условному сигналу (паролю) с уровня подсознания всплыва-

ет в сознании и воспринимается человеком как его собственные мысли и убеждения. В соответствии с заложенной программой человек — объект воздействия — организует свое поведение, принимая решения. В предельном варианте этот человек в результате информационно-психологического воздействия скрытого типа превращается в зомби, который безотказно выполняет волю своего повелителя. Человек, подвергшийся «программированию», внешне ведет себя так же, как обычный человек, и не подозревает о том, что он «запрограммирован». Он среагирует только на ключевую команду, переданную ему в нужное время. После выполнения задания человек-зомби даже не осознает, что он сделал по этой команде, — программой ему «приказали» забыть этот факт. В подсознание такого человека можно заложить и несколько спецпрограмм.

Использование психотропных средств возможно и в военных целях, что позволяет говорить о психотропном оружии, которое может применяться как отдельно, так и в сочетании с другими средствами воздействия.

Итак, по мере повышения роли информации и информационных технологий в жизнедеятельности человека противоборство между государствами, политическими партиями, транснациональными корпорациями и международными террористическими организациями стало приобретать новые формы. В настоящее время ученые из разных стран в основном проанализировали систему закономерностей информационной борьбы. Они связывают воедино явления и процессы, протекающие в различных сферах: экономической, политической, духовной, военной. Закономерности информационной борьбы выступают как отношения не только между материальными факторами, но и между активно действующими в ней духовными силами.

Если до конца 40-х гг. XX в. информационная борьба между государствами в основном велась в период боевых действий

и подчинялась военной стратегии, то сегодня она ведется практически постоянно и повсеместно. Необходимо пристальное внимание политиков и международной общественности, чтобы своевременно увидеть и по возможности предотвратить угрозу перехода от информационной борьбы к более агрессивным и разрушительным формам.

Возрастает необходимость создать условия для заключения многосторонних международных соглашений о запрещении применения средств технологического воздействия на национальные информационные ресурсы, определить принципы контроля использования информационных систем и сформировать основные приоритеты в проводимой международными организациями политике интеграции национальных сегментов информационных систем в единую мировую информационную инфраструктуру. Традиционно для разрешения задач внешней политики используются экономические, дипломатические, идеологические, культурные и другие «невоенные» средства. Сегодня к этому перечню средств можно добавить информационные технологии.

Вопросы для самоконтроля

1. Чем отличаются понятия «информационная война» и «информационное противоборство»?
2. Чем отличается информационная война от обычного вооруженного конфликта?
3. Какие виды информационных войн Вы можете выделить?
4. Приведите пример межкорпоративной информационной войны.
5. Можно ли рассматривать рекламу как средство ведения информационной борьбы?
6. Какие приемы ведения информационной войны используются во время предвыборных кампаний, приведите примеры.

7. Что такое информационное оружие? Какие виды оружия применяются в ходе ведения информационной войны?
8. Каковы цели информационной войны?
9. Каковы средства и методы защиты от информационно-технического оружия?
10. Каковы особенности информационно-психологической войны?

Библиографический список

1. Васильков А. В. Безопасность и управление доступом в информационных системах / А. В. Васильков, И. А. Васильков. — Москва : ФОРУМ: ИНФРА-М, 2013. — 368 с.
2. Жигулин Г. П. Организационное и правовое обеспечение информационной безопасности / Г. П. Жигулин. — Санкт-Петербург : СПбНИУИТМО, 2014. — 173 с.
3. Теоретические основы компьютерной безопасности / П. Н. Девянин [и др.]. — Москва : Радио и связь, 2000. — 192 с.
4. Бардаев Э. А. Документоведение : учебник для студ. высш. учеб. заведений / Э. А. Бардаев, В. Б. Кравченко. — Москва : Издательский центр «Академия», 2008. — 304 с.
5. Малюк А. А. Введение в защиту информации в автоматизированных системах / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. — Москва : Горячая линия — Телеком, 2001. — 148 с.
6. Мельников В. В. Безопасность информации в автоматизированных системах / В. В. Мельников. — Москва : Финансы и статистика, 2003. — 368 с.
7. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах / Н. А. Гайдамакин. — Екатеринбург : Изд-во Урал. ун-та, 2003. — 328 с.
8. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. — Москва : Горячая линяя — Телеком, 2000. — 452 с.
9. Барсуков В. С. Безопасность: технологии, средства, услуги / В. С. Барсуков. — Москва : КУДИЦ-ОБРАЗ, 2001–496 с.
10. Расторгуев С. П. Информационные войны / С. П. Расторгуев. — Москва : «Финансы и статистика», 1998. — 415 с.

Учебное издание

Вострецова Елена Владимировна

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Редактор О. С. Сергеева
Верстка О. П. Игнатьевой

Подписано в печать 23.05.2019. Формат 60×84/16.
Бумага офсетная. Цифровая печать. Усл. печ. л. 11,9.
Уч.-изд. л. 10,2. Тираж 40 экз. Заказ 126.

Издательство Уральского университета
Редакционно-издательский отдел ИПЦ УрФУ
620049, Екатеринбург, ул. С. Ковалевской, 5
Тел.: +7 (343) 375-48-25, 375-46-85, 374-19-41
E-mail: rio@urfu.ru

Отпечатано в Издательско-полиграфическом центре УрФУ
620083, Екатеринбург, ул. Тургенева, 4
Тел.: +7 (343) 358-93-06, 350-58-20, 350-90-13
Факс: +7 (343) 358-93-06
http://print.urfu.ru

ВОСТРЕЦОВА ЕЛЕНА ВЛАДИМИРОВНА

Доцент, кандидат технических наук. Опыт преподавания дисциплины «Основы информационной безопасности» составляет более 20 лет.

Область научных интересов — технические средства защиты информации, анализ и обработка сигналов; методики и технологии современного высшего образования.

Автор более 100 научных и учебно-методических трудов.