ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
Государственное образовательное учреждение высшего профессионального образования
УЛЬЯНОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

А. А. Гладких, В. Е. Дементьев

БАЗОВЫЕ ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Учебное пособие
для студентов, обучающихся по специальностям

08050565, 21040665, 22050165, 23040165

Ульяновск
2009

УДК 002:34+004.056.5
ББК 67.401+32.973.2-018.2
Г15

Рецензенты:
Кафедра «Телекоммуникационных технологий и сетей» Ульяновского государственного университета зав. кафедрой д-р техн. наук, профессор А.А. Смагин;
Ульяновский ФГУП «Центр-Информ» ФНС РФ, директор В.А. Терентьев

Утверждено редакционно-издательским советом университета в качестве учебного пособия

Гладких А.А.
Базовые принципы информационной безопасности вычислительных сетей : учебное пособие для студентов, обучающихся по специальностям 08050565, 21040665, 22050165, 23040165 / А.А. Гладких, В.Е. Дементьев;- Ульяновск : УлГТУ, 2009.- 156 с.

ISBN 5-89146-344-X

Излагаются основные принципы обеспечения информационной безопасности в ходе эксплуатации элементов вычислительных сетей, необходимые специалистам различных специальностей.
Пособие предназначено для студентов изучающих теоретические основы сетевых технологий и средств телекоммуникации (специальности 08050565 «Управление персоналом», 21040665 «Управление качеством», 22050165 «Сети связи и системы коммутации», 23040165 «Прикладная математика»), и преподавателей, ведущих указанные дисциплины. Учебное пособие может использоваться также студентами других специальностей, связанных с обработкой информации.

УДК 002:34+004.056.5
ББК 67.401+32.973.2-018.2

ISBN 5-89146-344-X

СПИСОК СОКРАЩЕНИЙ

АС – автоматизированная система
ВС – вычислительная сеть
ВТ – вычислительные технологии
ВТСС – вспомогательные технические средства и системы
ГМД – гибкий магнитный диск
ИБ – информационная безопасность
ИРК – информационно-расчетный комплекс
ИТР – инженерно-технический работник
ЗИ – защита информации
КЗ – класс защиты
ЛВС – локальные вычислительные сети
МЭ – межсетевой экран
НДВ – недекларируемые возможности
НСД – несанкционированный доступ
ПК – персональный компьютер
ПЗУ – постоянное запоминающее устройство
ОБС – обманная система
ОС – операционная система
ПЗУ – постоянное запоминающее устройство
ПО – программное обеспечение
СА – системы автоматизации
САЗ – система активной защиты
СВР – служба внешней разведки
СЗИ – система защиты информации
СУБД – система управления базами данных
СУРБД – система управления распределенными базами данных
ОТСС – основные технические средства и системы
ТСОИ – технические средства обработки информации
УЦ – удостоверяющий центр
ФСБ – Федеральная служба безопасности
ФСТЭК – Федеральная служба по техническому и экспортному контролю
ЭД – электронный документ
ЭЦП – электронно-цифровая подпись
MBR – master boot record (главная загрузочная запись)
PKI – public key infrastructure (инфраструктура открытых ключей)

ВВЕДЕНИЕ

Главная тенденция развития современного общества тесно связана с ростом информационной составляющей (информационные ресурсы, информационные технологии и т.п.) и, как следствие, информационной безопасности. Вопросы информационной безопасности на современном этапе рассматриваются как приоритетные в государственных структурах, в научных учреждениях и в коммерческих фирмах. Информационные системы специального назначения (банковские системы, силовые ведомства и т.п.), являясь приоритетными в структуре государства, не могут оставаться в вопросах обеспечения информационной безопасности только на уровне традиционных средств: криптографическая защита, совершенствование систем разделения доступа, реализация специальных требований для абонентского трафика, проведение организационных мероприятий по усилению режима.

Нет смысла перечислять все преимущества, которые получает организация, подключившись к глобальной сети Интернет. Однако при этом необходимо учитывать и отрицательные стороны такой акции. В общедоступной сети – это возможные атаки на подключенные к ней локальные сети и компьютеры. Общепризнанно, что ежегодные убытки из-за недостаточно защищенных корпоративных информационных систем исчисляются десятками миллионов долларов. Видя свои преимущества от использования сетевых технологий, первоначально пользователи часто не придают значения выбору средств защиты информации, реально ставя под угрозу свое финансовое положение, репутацию и конкурентоспособность.

Защита информации – это лишь одна составляющая задачи обеспечения информационной безопасности. Другая ее часть – это обеспечение бесперебойной работы оборудования. Выход из строя того или иного узла в результате хакерской атаки приводит как к затратам на его восстановление, когда требуется обновить или заменить программное обеспечение, так и к потере части клиентуры. Можно представить, во сколько обойдется один день

простоя сайта крупного Интернет-магазина. Поэтому при включении компьютера в сеть, при интеграции корпоративной информационной системы в сеть необходимо в первую очередь продумать вопросы обеспечения защиты этой системы.

Существующие на сегодняшний день методы и средства защиты информации в автоматизированных системах достаточно разнообразны, что, несомненно, отражает многообразие способов и средств возможных несанкционированных действий. Главным недостатком существующих методов и средств защиты информации, включая современные средства поиска уязвимостей автоматизированных систем и обнаружения несанкционированных действий, является то, что они, в подавляющем большинстве случаев, позволяют организовать защиту информации лишь от постфактум выявленных угроз, что отражает определенную степень пассивности обороны.

Адекватный уровень информационной безопасности в состоянии обеспечить только комплексный подход, предполагающий целенаправленное использование традиционных организационных и программно-технических правил обеспечения безопасности на единой концептуальной основе с одновременным поиском и глубоким изучением новых приемов и средств защиты.

Настоящее пособие не является инструкцией по применению тех или иных приемов защиты, его главная цель повышение общей культуры пользователя в вопросах информационной безопасности, т.е. предполагается определенное знание им основ современных сетевых и телекоммуникационных технологий. Имея базовый уровень подготовки в рассматриваемой предметной области, каждый специалист должен квалифицированно учитывать требования конкретных руководящих документов по обеспечению информационной безопасности, регламентирующих его деятельность на рабочем месте.

1. АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

1.1. Вычислительная сеть – как объект исследования

Современные системы управления различных структур относятся к классу организационно-технических (человеко-машинных) систем. Они рассматриваются как совокупность взаимосвязанных и согласованных между собой технических элементов (средств, комплексов связи и автоматизации), представляющих иерархическую метрику должностных лиц, совершающих согласованные действия [3,6,21].

Таким системам присущи специфические особенности, важнейшие из которых могут быть сформулированы следующим образом:

– любые вычислительные сети (ВС) по своей сути предназначены для функционирования в потенциально конфликтных ситуациях, и игнорирование этого условия приводит к нежелательным последствиям, наиболее тяжелым из которых является экономический фактор;

– современные и перспективные информационно-расчетные комплексы (ИРК) строятся по принципу распределенных приложений в соответствии с конкретной технологией;

– технологии разрабатываются конкретными авторскими коллективами, имеющими собственные представления о степени сбалансированности целевого назначения программного продукта и безопасности его применения, поэтому многие технологии обладают рядом типовых угроз и уязвимостей;

– построение перспективных механизмов обеспечения безопасности связывается не с защитой от выявленных уязвимостей, а с возможностью предотвращать новые, неизвестные методы проведения атак.

Объединяемые в сеть, средства обработки данных могут располагаться с различным удалением друг от друга. Каждому пользователю сети обеспечивается доступ ко многим ресурсам: аппаратным, программным и

информационным, что дает основание считать сетевую концепцию наиболее приемлемой для построения системы автоматизации (СА) и автоматизированного управления (АУ) в целом.

Концепция вычислительной сети предполагает использование пакетов общесистемного и прикладного программного обеспечения (ПО), разработанных специально для сетевой технологии работы. К таковым относятся, в частности, системы управления распределенными базами данных (СУРБД), сетевые системы управления базами данных (СУБД), системы электронной почты. Применение данного программного обеспечения позволяет существенно расширить возможности ВС как с точки зрения реализуемых функций, так и по эргономическим показателям.

Применение локально-вычислительных сетей (ЛВС) в системах управления предоставляет персоналу широкие возможности, основными из которых являются: обмен сообщениями; обмен файлами; совместное использование внешней памяти; коллективное использование печатающих устройств высокого качества (лазерных принтеров); выход в сети автоматических телефонных станций (АТС) по протоколу X.25, сети обмена данными (технологии FR и ATM) и другие вычислительные сети; обеспечение совместного функционирования совокупности ВС посредством организации мостов и/или шлюзов; разграничение доступа к информации по пользователям, содержанию, времени и машинным носителям.

Современные ЛВС различных структур являются типовыми и представляют собой высокоскоростные вычислительные сети на базе мощных персональных ЭВМ, которые взаимодействуют между собой по прямым каналам передачи данных или через информационную сеть общего пользования.

Увеличение роли информационных систем в современных структурах управления, по вполне понятным причинам, привлекает внимание специалистов и с точки зрения вскрытия возможностей таких систем с целью

отрицательного воздействия на них [1,2]. Это привело к образованию предметной области, рассматривающей информационное противоборство как одну из важных составляющих борьбы за целостность информационного потенциала.

Новые информационные технологии (электронные СМИ, Интернет, мобильная связь, глобальная навигация, волоконные и беспроводные сети передачи данных) расширили возможности негативного информационного воздействия на ИРК [8]. Обострение борьбы за обеспечение информационного превосходства открывает перспективы усиления контроля за ресурсами конфликтующей стороны. В этой связи защиту собственного информационного ресурса одной из сторон следует рассматривать как составную часть сохранения целостности системы.

1.2. Структура информационного противоборства

В условиях информационного конфликта одной из важных целей атакующей стороны является снижение показателей своевременности, достоверности и безопасности информационного обмена в противоборствующей системе до уровня, приводящего к срыву (потере) управления.

В соответствии с этим, содержание информационного противоборства включает две составные части, которыми охватывается вся совокупность действий, позволяющих достичь информационного превосходства над противником рис. 1.1. Первой составной частью служит противодействие информационному обеспечению управления противника (информационное противодействие). Оно включает мероприятия по нарушению конфиденциальности оперативной информации, внедрению дезинформации, блокированию добывания сведений, обработки и обмена информацией (включая физическое уничтожение носителей информации) и блокированию

фактов внедрения дезинформации на всех этапах информационного обеспечения управления противника. Информационное противодействие осуществляется путем проведения комплекса мероприятий, включающих техническую разведку систем связи и управления, перехват передаваемой по каналам связи оперативной информации.

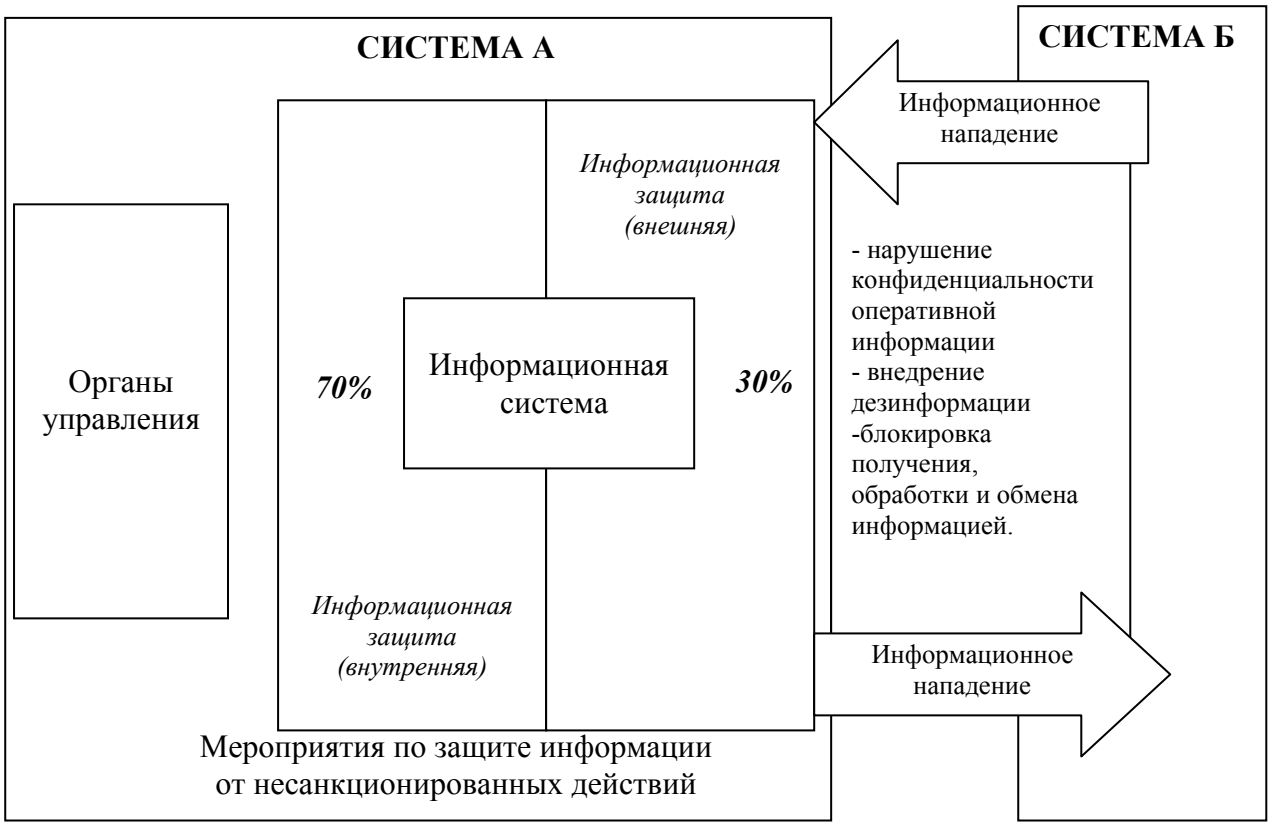


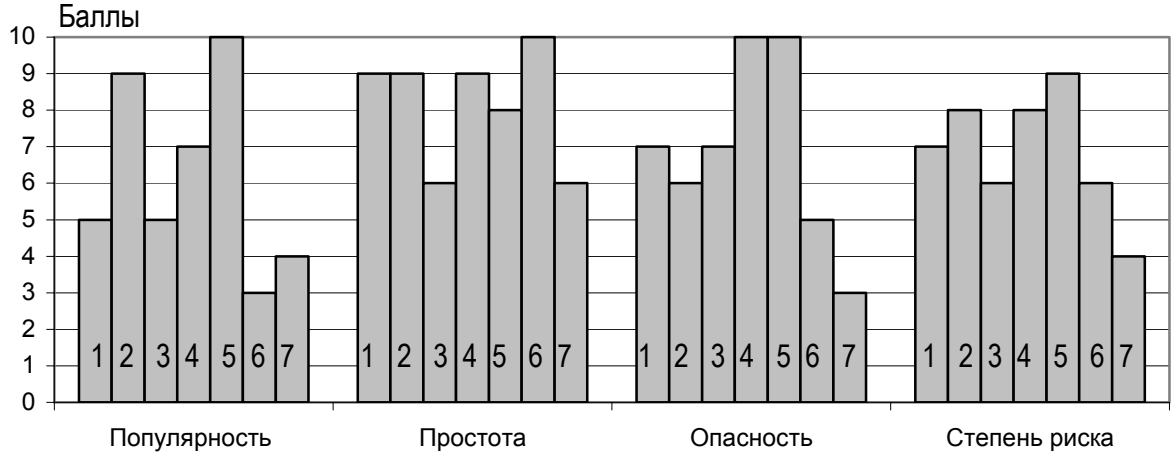
Рис. 1.1. Структура информационного противоборства

Вторую часть составляют мероприятия по защите информации, средств ее хранения, обработки, передачи и автоматизации этих процессов от воздействий противника (информационная защита), включающие действия по деблокированию информации (в том числе защиту носителей информации от физического уничтожения), необходимой для решения задач управления и блокированию дезинформации, распространяемой и внедряемой в систему управления.

Информационная защита не исключает мероприятий по разведке, защите от захвата элементов информационных систем, а также по радиоэлектронной

защите. Как известно, атаки могут производиться как из-за пределов сети (атаки по сети), так и по внутренним каналам (физические атаки). Поэтому информационная защита также делится на два вида: внешнюю и внутреннюю. Для достижения своих целей атакующая сторона будет пытаться использовать оба вида атак. Сценарий ее действий заключается в том, чтобы с помощью физических атак завладеть некоторой информацией о сети, а затем с помощью атак по сети осуществлять несанкционированный доступ (НСД) к компонентам всей сети системы. По данным статистики доля физических атак составляет 70 % от общего числа совершенных атак. На рис.1.2 дана оценка совершенных НСД в ходе физических атак на вычислительные сети, при этом для наглядности сравнительные данные по различным категориям нарушений приведены к десятибалльной шкале. Заметно, что 5 позиция во всех категориях является превалирующей.

Наиболее частым нарушениями по сети являются: сбор имен и паролей, подбор паролей, выполнение действий, приводящих к переполнению буферных устройств и т.п.



1 – рабочее место; 2 – разгребание мусора; 3 – поиск информации о сети; 4 – доступ к консоли; 5 – кража компьютеров; 6 – загрузка альтернативной ОС; 7 – взлом BIOS

Рис. 1.2. Оценка НСД в ходе физических атак на вычислительные сети по десятибалльной системе

Действительно, в случае получения доступа к офисной технике, рабочим столам сотрудников, компьютерным системам и сетевым устройствам, атакующая сторона резко повышает шансы на успех в целях изучения уязвимых мест в системе защиты и проведения эффективной атаки.

Поиск уязвимых мест в информационно-расчетном комплексе (ИРК) занимает определенный интервал времени $k\Delta T$, в то время как атака производится на интервале Δt. Здесь $k\Delta T >> \Delta t$, при этом Δt достаточно мало, а $k > 0$. Определим k как коэффициент защиты. Если $k \to \infty$, ИРК считается неуязвимым, при $1 > k > 0$ атакующая сторона использует априорную информацию для преодоления защиты и проведения атаки на систему. Будем считать, что система защиты носит пассивный характер при $k \le 1$, при $k >> 1$ ресурс системы повышается в k раз.

Значения параметра $k >> 1$ обеспечивается за счет своевременного изменения конфигурации защиты или подготовки вместо реальных параметров ИРК ложных, обманных. Подготовку таких параметров целесообразно выделить в самостоятельную область защиты, не связывая ее с рядом фоновых задач по обеспечению безопасности ИРК.

1.3. Анализ проблемы защиты ресурсов вычислительных сетей

Развитие средств, методов и форм автоматизации процессов обработки информации и массовое применение персональных компьютеров, обслуживаемых неподготовленными в специальном отношении пользователями, делают информационный процесс уязвимым по ряду показателей. Основными факторами, способствующими повышению информационной уязвимости, являются следующие:

– увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;

– сосредоточение в единых базах данных информации различного назначения и различной принадлежности;

– расширение круга пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней массивам данных;

– усложнение режимов работы технических средств вычислительных систем;

– автоматизация межмашинного обмена информацией, в том числе на больших расстояниях;

– слабая подготовка (недостаточная квалификация) персонала.

Динамика изменения вскрытых уязвимостей системных компонентов по годам представлена на рис. 1.3 (в предположении, что все уязвимости, зарегистрированные за рассматриваемый период принять за 100%).

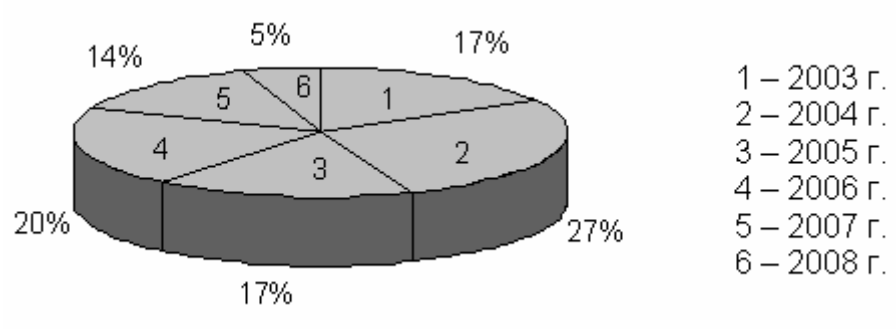


Рис. 1.3. Динамика изменения количества уязвимостей системных компонентов

Снижение количества выявленных уязвимостей в последнее время может быть объяснено тем, что повысился уровень квалификации персонала, были найдены и устранены лежащие на поверхности ошибки ОС. Новые ОС, как правило, имеют закрытые коды и труднодоступны злоумышленникам для детального изучения и поиска уязвимостей. С выходом новых ОС, очевидно, следует ожидать очередного скачка в количестве уязвимостей или, по крайней мере, сохранения тенденции на уровне прежних лет, при этом обходимо понимать, что процентный показатель оперирует относительными понятиями и если перевести это на количественный показатель, то более 70 уязвимостей в год это недопустимо много. Можно сделать предположение о подготовленных,

но не проведенных атаках, что представляет значительную потенциальную угрозу.

Данная позиция объясняется тем, что сложность программ постоянно возрастает, причем сложность архитектуры современного ПО так велика, что без повторного использования ранее созданного кода (программ) невозможно с приемлемой скоростью создавать новые программы, необходимые и востребованные на рынке. Сегодня практически никто не может себе позволить разрабатывать сложные программы с нуля, поэтому в них, как правило, повторно используется код с большой вероятностью содержащий еще не найденные ошибки, а вновь написанный код аккумулирует новые ошибки.

Классифицируя уязвимости, исходят из того, что атака – это вредоносное воздействие атакующей стороны на систему. Известные подходы к классификации рассматривают уязвимость как нечто статическое, уже случившееся, однако средства обеспечения безопасности, по сути, оперируют не уязвимостями, а атаками. Можно сказать, что атака – это реализация угрозы безопасности; действие, совершаемое злоумышленником.

Под угрозой понимается целенаправленное действие, которое повышает уязвимость накапливаемой, хранимой и обрабатываемой в системе информации и приводит к ее случайному или преднамеренному изменению или уничтожению.

Все угрозы безопасности информации можно классифицировать по следующим признакам: по цели воздействия; по характеру воздействия и по способу возникновения (рис. 1.4).

В зависимости от характера воздействия нарушителя могут быть выделены активные и пассивные угрозы безопасности информации.

При пассивном вторжении (перехвате информации) нарушитель только наблюдает за прохождением информации в ВС, не вторгаясь ни в информационный поток, ни в содержание передаваемой информации.

При активном вторжении нарушитель стремится изменить информацию, передаваемую в сообщении.

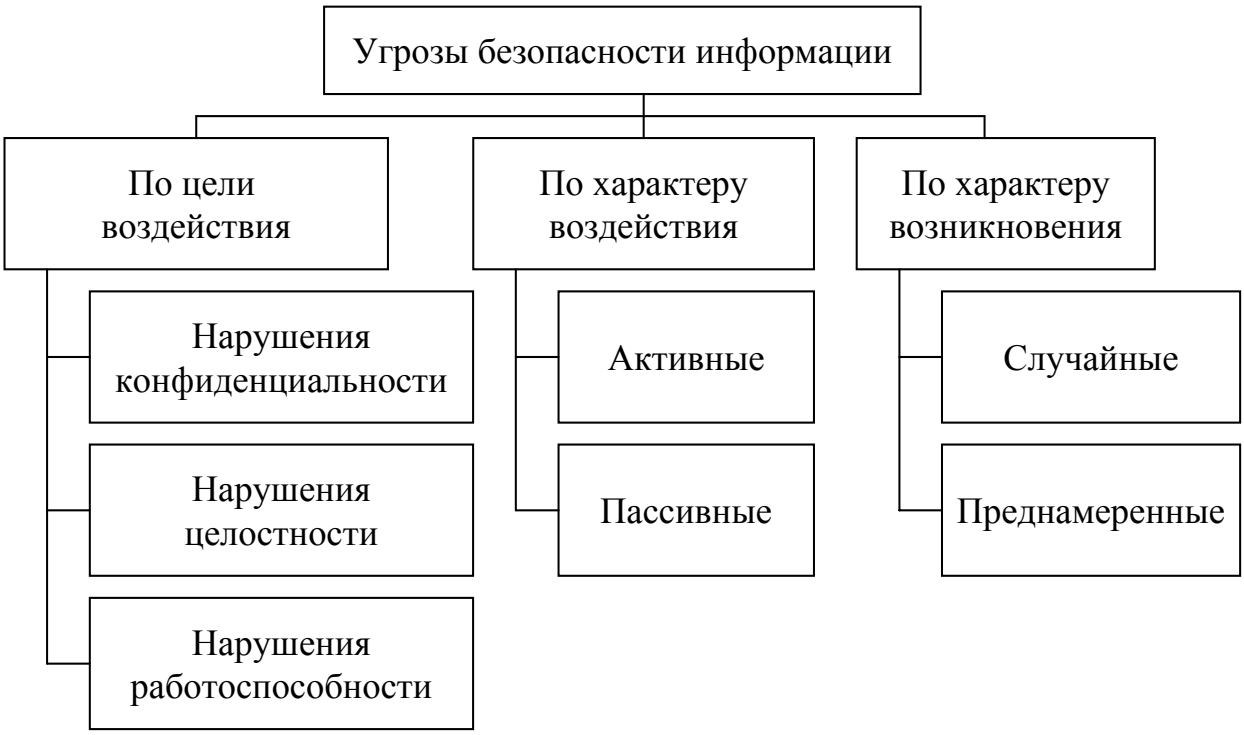


Рис. 1.4. Классификация угроз безопасности информации

Причинами случайных угроз могут быть:

– аварийные ситуации из-за стихийных бедствий и отключения электропитания;

– отказы и сбои аппаратуры;

– ошибки в программном обеспечении;

– ошибки в работе обслуживающего персонала и пользователей;

– помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. Действия нарушителя могут быть обусловлены разными мотивами: недовольством, взяткой, любопытством, конкуренцией и т. п.

Преднамеренные угрозы могут реализовать как внутренние для системы участники процесса обработки данных (персонал, сервисное звено и т. д.), так и люди, внешние по отношению к системе, так называемые «хакеры».

По частоте проявления преднамеренные угрозы можно выстроить в следующем порядке (рис 1.5):

- злоупотребления в Internet со стороны сотрудников;
- несанкционированный доступ со стороны сотрудников;
- отказ в обслуживании;
- атаки внешних злоумышленников;
- кража конфиденциальной информации;
- саботаж и финансовые мошенничества;
- мошенничества с телекоммуникационными устройствами.

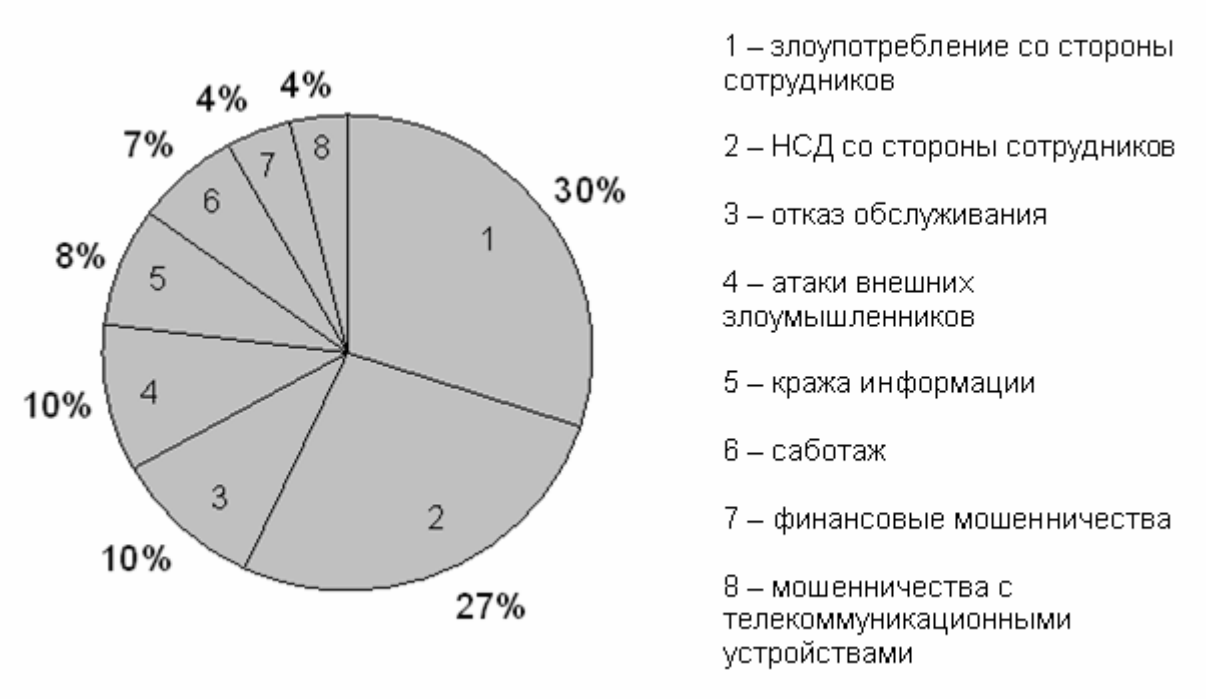


Рис.1.5. Частота обнаружения атак на вычислительные сети

В таблице 1.1 представлены способы воздействия на перечисленные объекты, реализующие основные угрозы безопасности информации.

Из таблицы видно, что рассмотренные способы воздействия на аппаратные средства и программное обеспечение могут быть осуществлены только непосредственно авторизованными пользователями (должностными лицами органов управления, обслуживающим персоналом). Кроме того, воздействия на ПО и данные могут осуществляться удаленно, используя

сетевые ресурсы. Исполнение угроз осуществляется посредством программных атак.

Таблица 1.1

Пути реализации угроз безопасности системы

Способы нанесения ущерба	**Объекты воздействий**			
	Оборудование	**Программы**	**Данные**	**Персонал**
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкциониро-ванное использование ресурсов	Несанкциониро-ванное копирование, перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, спец. вложения, изменение режимов работы, несанкциониро-ванное использование ресурсов	Внедрение «троянских коней» и «жучков»	Искажение, модификация	Вербовка персонала, «маскарад»
Нарушение работоспособности автоматизированной системы	Изменение режимов функциониро-вания, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование (воспроизведение) информации	Изготовление аналогов без лицензий	Использование незаконных копий	Публикация без ведома авторов	–

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ (НСД). Суть НСД состоит в получении нарушителем доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой политикой безопасности. НСД может быть осуществлен как штатными средствами системы, так и специально созданными аппаратными и программными средствами.

Интересна статистика ведущей аудиторской компании Ernst & Young, затронувшая более 1300 организаций с годовым оборотом более 100 млн долларов. В соответствии с проведенным исследованием, около половины компаний серьезно обеспокоены доступностью опытного и тренированного персонала, как в области ИТ (51 %), так и в сфере информационной безопасности (46 %). Эти причины возглавляют составленный аналитическим агентством Ernst & Young список основных факторов, сдерживающих развитие отрасли информационной безопасности в мире (см. рис. 1.6).

Рис. 1.6. Сдерживающие факторы индустрии информационной безопасности

В предыдущие годы пальма первенства принадлежала беспечности пользователей (2004) и бюджетным ограничениям (2003), а нехватка специалистов стояла только на третьем месте. В 2008 году третьей по

популярности причиной стало отсутствие финансирования (46 %), что также совершенно неудивительно. Денег, как известно, всегда не хватает, и отрасль информационной безопасности не является исключением.

Принципиально важным является набравший 42 % пункт «поддержка со стороны менеджмента». Ведь не секрет, что от нее очень сильно зависит успех любого (не обязательно информационной безопасности) проекта и пренебрегать ей нельзя ни в коем случае.

Как и любой другой молодой рынок, отрасль информационной безопасности испытывает некоторые проблемы с доступностью технологий, а также с наличием грамотных консультантов. Однако эти трудности никак нельзя назвать критическими или непреодолимыми. По большому счету, предложение на современном рынке имеется, причем оно весьма неплохо отвечает потребностям потенциальных пользователей.

Несколько лет назад ответ на вопрос о роли информационной безопасности в бизнесе современной организации был очевиден. Компании рассматривали ее как обычную страховку от всяческих проблем и неприятностей: заплатил деньги, внедрил решение и можешь спокойно сосредоточиться на основной деятельности.

Однако развитие рынка, рост количества угроз и средств обеспечения безопасности приводит к принципиально иному пониманию роли информационной безопасности. Сегодня ее нельзя воспринимать исключительно как защиту или страховку – она перерастает в нечто большее, а именно – в один из ключевых бизнес-активов современной организации. По мнению специалистов аналитического центра компании Perimetrix, внедрение технологий информационной безопасности может способствовать росту бизнеса напрямую, а не только с помощью минимизации рисков. И в будущем этот тренд будет только усиливаться.

По данным исследования Ernst & Young за 2007 г. (см. рис. 1.7), основным драйвером (причиной использования решений) современного рынка

информационной безопасности для 64 % респондентов является необходимость соответствия различным нормативным актам. Такое положение вещей можно назвать привычным – по оценкам Ernst & Young, этот пункт возглавляет список с 2005 года. Интересно, что до 2005 года среди факторов, стимулирующих развитие информационной безопасности, первое место занимали классические вирусы и сетевые черви.

Рис. 1.7. Драйверы рынка информационной безопасности

При этом большинство нормативных актов влияют на информационную безопасность опосредованно. Так, например, основная цель закона SOX – обеспечить прозрачность внутреннего контроля и корректность информации в отчетах, а задача норматива Basel II – побудить финансовые компании резервировать операционные риски. Ни тот, ни другой не затрагивают информационной безопасности напрямую, однако, оба оказывают на нее огромное влияние, причем, по данным исследования, оно носит преимущественно положительный характер.

По информации Ernst & Young на 2008 г. (см. рис. 1.8), в целом 80 % опрошенных полагают, что соответствие нормативным актам положительно влияет на информационную безопасность.

Специалисты аналитического центра компании Perimetrix считают данный вопрос чрезвычайно актуальным и для России в том числе. По данным различных исследований, большинство отечественных специалистов также положительно оценивают влияние, например, закона «О персональных данных», стандарта банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» и других нормативных актов на информационную безопасность.

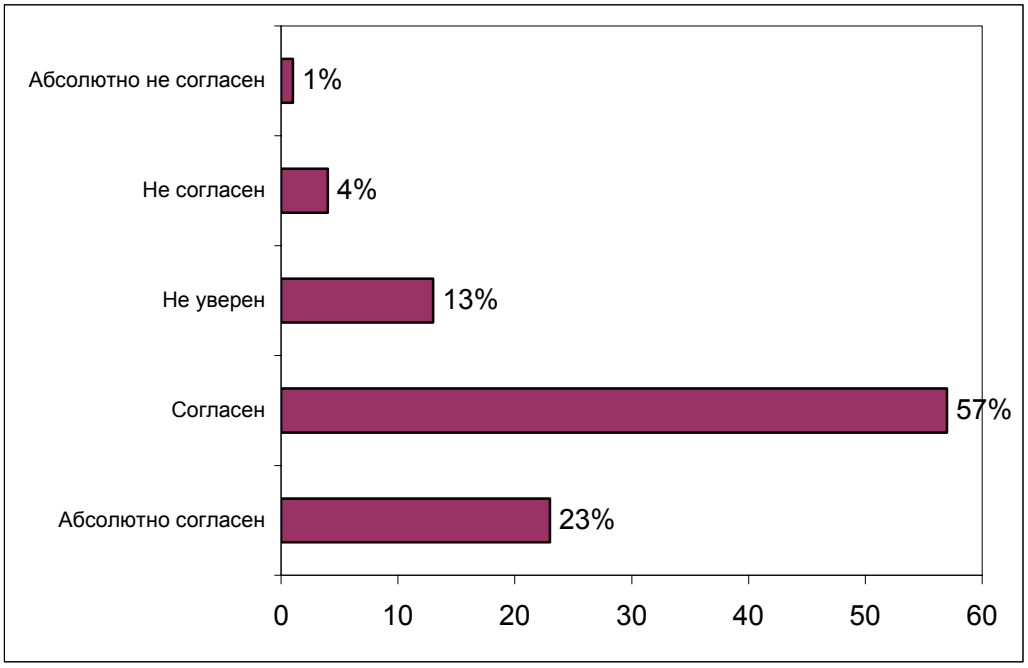


Рис. 1.8. Положительное влияние соответствия нормативным актам на безопасность компании

Таким образом, информационная безопасность перестает быть отдельным направлением деятельности организации и начинает определять ее бизнес в целом. Примерно 80 % респондентов Ernst & Young отметили, что решение задач информационной безопасности приводит к повышению эффективности ИТ-процессов. Приведем типичный пример. Большинство нормативных актов так или иначе требуют, чтобы конфиденциальная информация (сведения о

клиентах, интеллектуальная собственность и т. д.) была выделена и должным образом защищена. Но для этого важно провести сортировку данных, хранящихся в корпоративной сети организации. А правильная классификация прямым образом влияет на бизнес – сотрудники перестают тратить время на поиск нужных документов на файл-серверах, которые сегодня часто представляют собой обычную свалку информации.

Представленная информация описывает третий по счету драйвер рынка информационной безопасности, а именно – о достижении тех или иных бизнес-целей (45 %). А на втором месте «расположилась» защита конфиденциальных данных, которая, с одной стороны, тесно пересекается с остальными драйверами (прежде всего, с нормативными актами), но в то же время является отдельно стоящей темой. Отметим, что за последний год ее актуальность выросла почти в полтора раза – с 41 % до 58 %.

Специалисты компании Perimetrix предполагают, что организации не хотят допускать утечки, поскольку каждая из них сопровождается серьезными материальными потерями. По данным исследования Ponemon Institute «2007 Annual Study: The cost of data breach», средний ущерб от потери всего одной конфиденциальной записи (например, информации об одном клиенте) составляет почти 200 долларов, причем большая часть из этих средств приходится на репутационный урон. Хотелось бы отметить, что ущерб репутации оказался на пятом месте в перечне Ernst & Young.

Четвертым драйвером рынка, по мнению респондентов, является интеграция процессов обеспечения информационной безопасности в общую функцию компании по управлению рисками (см. рис. 1.9).

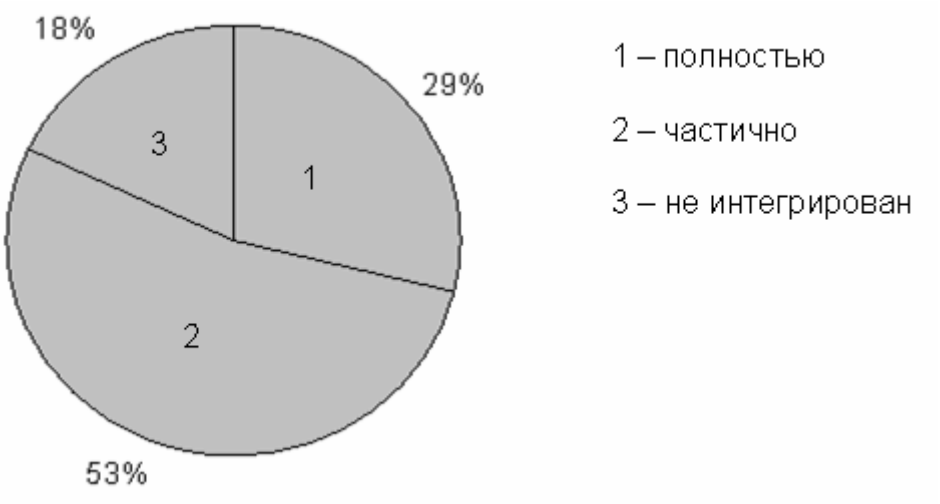


Рис. 1.9. Степень интеграции функций информационной безопасности и управления рисками

Данные исследования говорят о том, что степень интеграции постепенно растет, и это логично вытекает из общей канвы развития рынка. Мы уже говорили, что безопасность превращается из опосредованной функции в средство решения прикладных бизнес-задач, а управление рисками как раз и является одной из них.

Остальные драйверы можно считать малозначительными или специфичными для отдельно взятой отрасли/региона. Принципиально важно, что среди них находятся внешние риски (фишинг, вирусы, шпионское ПО), а также развитие технологий безопасности. Другими словами, и тот и другой фактор влияют на современную ИБ не слишком сильно, и это обстоятельство также следует иметь в виду.

Профиль угроз, с которыми борются решения по информационной безопасности, постоянно меняется. Как следствие, организации вынуждены искать способы оценить эффективность внедренных продуктов. С ростом количества и сложности защитных систем эта задача становится существенно труднее, и зачастую с ней нельзя справиться, привлекая только внутренние ресурсы. Среди основных способов, используемых для оценки собственной защищенности, организации называют внутренний и внешний аудит, внутреннюю самооценку и внешнюю оценку независимыми компаниями.

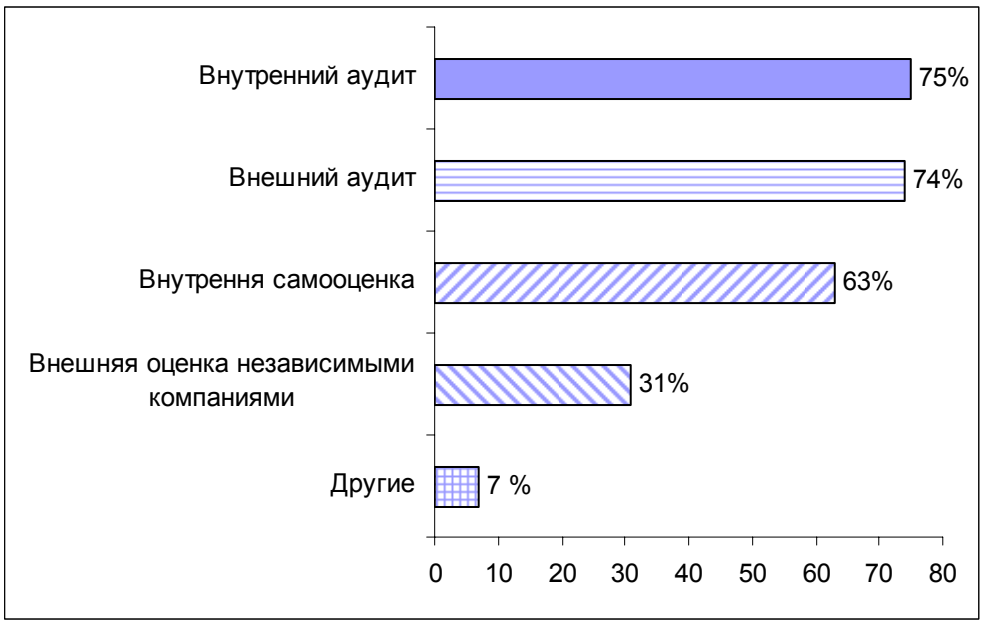


Рис. 1.10. Способы оценки эффективности системы информационной безопасности

Аналитики Ernst & Young рекомендуют применять все методики в комплексе. Причем делать это необходимо постоянно и объективно.

В противном случае вместо решения бизнес-задач системы информационной безопасности будут предназначены для вытягивания денег из корпоративного бюджета.

Не менее важной представляется и задача внешнего контроля. Дело в том, что огромная масса проблем по безопасности возникает на стадии передачи информации сторонним компаниям. По сведениям Ponemon Institute, до 40 % утечек информации происходят по вине «третьих» организаций. Исключить этот процесс решительно невозможно, а как-то бороться с проблемой необходимо. По данным Ernst & Young, в 2007 году 78 % организаций выдвигают требования по информационной безопасности своим партнерам. Подход крайне простой: хочешь работать с нами - будь добр соответствовать нашим запросам. Надо заметить, что в 2006 году этот показатель составлял 66 %. Таким образом, мы видим еще один яркий пример прямого влияния ИБ на бизнес различных организаций.

Среди рекомендаций Ernst & Young по улучшению системы безопасности необходимо отметить усиление взаимосвязи информационной безопасности и

бизнес-целей, интеграция информационной безопасности в систему управления рисками, обеспечение соответствия стандартам и использование нетрадиционных подходов для поиска специалистов.

1.4. Вероятностная модель несанкционированных действий на информационно-расчетный комплекс

При системном рассмотрении проблемы надежности системы обработки информации (в контексте безопасности информации), подвергающейся атакам, необходимо провести анализ поведения атакованной системы.

Допустим, множество НСД является конечным и насчитывает N компонент: $\mathbf{Y} = \{Y_1, Y_2, ..., Y_N\}$. Тогда при построении модели НСД на ИРК необходимо рассмотреть саму возможность атак каждого НСД из множества $\mathbf{Y} = \{Y_1, Y_2, ..., Y_N\}$ на каждый элемент. Результатом такого исследования должна быть таблица интенсивностей атак из **Y** на элементы ИРК (табл. 1.2):

Таблица 1.2

Интенсивность атак Y_i на элементы ИРК E_j

–	E_1	E_2	...	E_m	...	E_M
Y_1	$\mu_{11}(t)$	$\mu_{12}(t)$	...	$\mu_{1m}(t)$	...	$\mu_{1M}(t)$
Y_2	$\mu_{21}(t)$	$\mu_{22}(t)$	...	$\mu_{2m}(t)$	...	$\mu_{2M}(t)$
...	...	...	...	...	...	...
Y_n	$\mu_{n1}(t)$	$\mu_{n2}(t)$	...	$\mu_{nm}(t)$	...	$\mu_{nM}(t)$
...	...	...	...	...	...	...
Y_N	$\mu_{N1}(t)$	$\mu_{N2}(t)$	...	$\mu_{Nm}(t)$	...	$\mu_{NM}(t)$

В этой таблице $\mu_{nm}(t)$ – интенсивность потока атак n-го НСД на m-й элемент ИРК. Поток атак на ИРК описывается распределением вероятностей промежутков времени между соседними атаками, которое обозначается:

$A(t) = P$ (время между последовательными атаками $\le t$).

Поток атак Y_n на ИРК является простейшим.

На основе предельной теоремы для суммарного потока можно сделать вывод, что сумма потоков атак различных НСД на любой элемент будет сходиться к пуассоновскому потоку, для которого справедливо утверждение:
при сложении любого числа N независимых ординарных потоков будет получаться снова ординарный поток, интенсивность которого равна сумме интенсивностей складываемых потоков.

То есть для элемента программного обеспечения E_m интенсивность суммарного потока атак всех угроз из множества **Y** будет равна

$$\mu_m(t) = \sum_{n=1}^{N} \mu_{nm}(t), \tag{1.1}$$

а для интенсивности потока атак на ИРК в целом будет справедливо:

$$\mu(t) = \sum_{m=1}^{M} \mu_m(t) = \sum_{n=1}^{N} \sum_{m=1}^{M} \mu_{nm}(t). \tag{1.2}$$

Как показано в ряде работ, если параметр μ пуассоновского закона зависит от времени, т. е. поток возникновения атак неоднороден, то вероятность возникновения *a* атак на участке времени Δt описывается выражениями:

- для элемента m и НСД n:

$$P_{nm}(X(t, \Delta t)) = \frac{1}{a!}\left(\int_{t}^{t+\Delta t} \mu_{nm}(t)dt \right)^{a} \exp\left(- \int_{t}^{t+\Delta t} \mu_{nm}(t)dt \right); \tag{1.3}$$

- для элемента m и множества $\mathbf{Y} = \{Y_1, Y_2, ..., Y_N\}$:

$$P_{m}(X(t, \Delta t)) = \frac{1}{a!}\left(\int_{t}^{t+\Delta t} \mu_{m}(t)dt \right)^{a} \exp\left(- \int_{t}^{t+\Delta t} \mu_{m}(t)dt \right); \tag{1.4}$$

- для СОИ и множества НСД $\mathbf{Y} = \{Y_1, Y_2, ..., Y_N\}$:

$$P(X(t, \Delta t)) = \frac{1}{a!}\left(\int_{t}^{t+\Delta t} \mu(t)dt \right)^{a} \exp\left(- \int_{t}^{t+\Delta t} \mu(t)dt \right). \tag{1.5}$$

Интенсивности потоков атак на элементы ИРК E_m определяются из

таблицы 1.2 и соотношениями 1.1 и 1.2.

Зная, что число атак, попадающих на интервал Δt (где бы он ни находился), распределено по закону Пуассона, и полагая a=0, а также учитывая, что 0!=1, получим вероятность того, что за интервал времени Δt не произойдет ни одной атаки на ИРК

$$P_0(t, \Delta t) = \exp\left(- \int_t^{t+\Delta t} \mu(t) dt \right). \quad (1.6)$$

Событие, состоящее в том, что на ИРК будет произведена хотя бы одна атака на интервале τ, является противоположным событию ненападения на ИРК на том же участке времени. Тогда вероятность атаки на интервале τ будет определяться следующим выражением:

$$P(t, \Delta t) = 1 - P_0(t, \Delta t) = 1 - \exp\left(- \int_t^{t+\Delta t} \mu(t) dt \right). \quad (1.7)$$

Таким образом, для построения вероятностной модели воздействия множества атак **Y** на элементы ИРК необходимо:

– определить множество потенциальных НСД - **Y**;

– с каждым элементом ИРК E_m связать подмножество НСД $\mathbf{Y_m}$ относительно полного множества **Y**, которые могут воздействовать на этот элемент;

– составить таблицу интенсивностей 1.2;

– определить вероятностные характеристики потока атак на элемент E_m (соотношения 1.3 и 1.4);

– определить вероятностные характеристики (1.5, 1.6, 1.7) потока атак на ИРК.

На рисунке 1.11 представлен двухдольный граф для множества отношений элемент ИРК – множество атак. В левой части графа представлены возможные угрозы безопасности ИРК. При этом некоторые из них могут проявляться в неявном виде или вообще оказываются скрытыми от аналитика,

следовательно, от специалиста по безопасности требуется большая разносторонняя аналитическая работа по вскрытию именно таких угроз.

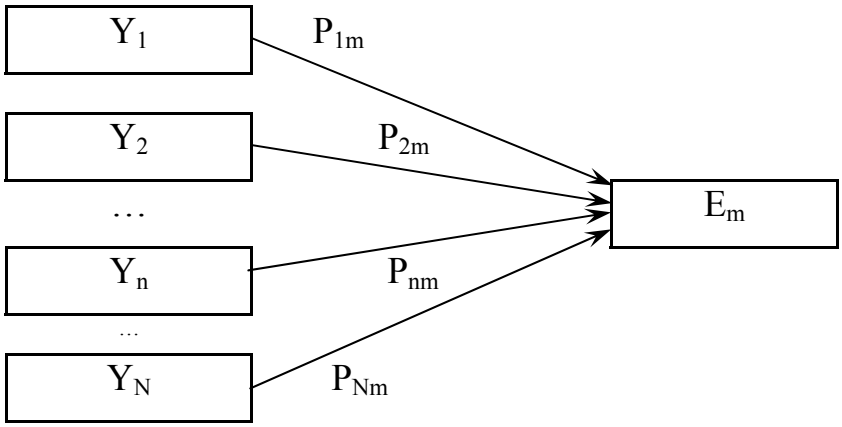


Рис. 1.11. Двухдольный граф для множества отношений элемент ИРК – множество атак

1.5. Существующие подходы к повышению уровня защищенности вычислительных сетей

Главным направлением в данной предметной области следует считать развитие рецепторных схем выявления несанкционированных действий, позволяющих использовать активные средства защиты в виде параметрической или структурной адаптации с целью увеличения параметра $k\Delta t$.

Системы обнаружения атак создаются, чтобы обеспечить дополнительный уровень защиты вычислительной сети, дополняя традиционные средства защиты: межсетевые экраны, криптомаршрутизаторы, серверы аутентификации и т. д. Очень часто противник в первую очередь атакует и пытается вывести из строя, имеющиеся защитные средства, обеспечивающие безопасность выбранной им цели.

Обнаруживать, блокировать и предотвращать нарушения политики безопасности можно несколькими путями. Первый и самый распространенный способ – это распознавание уже реализуемых атак. Это способ применяется в классических системах обнаружения атак. Однако недостаток средств данного класса в том, что атаки могут быть реализованы повторно. Поэтому было бы

правильнее предотвращать атаки еще до их осуществления. В этом и заключается суть второго способа. Реализуется он путем поиска уязвимостей, которые могут быть использованы для совершения атаки. И, наконец, третий путь – выявление уже совершенных атак и предотвращение их повторения в дальнейшем.

Таким образом, системы обнаружения нарушений политики безопасности можно классифицировать следующим образом (рис. 1.12)

Рис. 1.12. Классификация систем обнаружения атак по этапам осуществления атаки

Системы анализа защищенности проводят всесторонние исследования систем с целью обнаружения уязвимостей, которые могут привести к нарушениям политики безопасности. Результаты, полученные от средств анализа защищенности, представляют «мгновенный снимок» состояния защиты системы в данный момент времени. Несмотря на то, что эти системы не могут обнаруживать атаку в процессе ее развития, они могут определить возможность реализации атак.

Функционировать системы анализа защищенности могут на всех уровнях информационной инфраструктуры, т. е. на уровне сети, операционной системы, СУБД и прикладного программного обеспечения. Наибольшее распространение получили средства анализа защищенности сетевых сервисов и протоколов.

Связано это, в первую очередь, с универсальностью используемых протоколов. Изученность и повсеместное использование таких стеков протоколов, как TCP/IP, SMB/NetBIOS и т. п., позволяют с высокой степенью эффективности проверять защищенность информационной системы, работающей в данном сетевом окружении, независимо от того, какое программное обеспечение функционирует на более высоких уровнях. Вторыми по распространенности являются средства анализа защищенности операционных систем. Связано это также с универсальностью и распространенностью некоторых операционных систем (например, UNIX и Windows NT). Однако из-за того, что каждый производитель вносит в операционную систему свои изменения (ярким примером является множество разновидностей ОС UNIX), средства анализа защищенности ОС анализируют в первую очередь параметры, характерные для всего семейства одной ОС.

Контроль целостности позволяет реализовать стратегию эффективного мониторинга, сфокусированную на системах, в которых целостность данных и целостность процессов играет наиболее важную роль. Этот подход дает возможность контролировать конкретные файлы, системные объекты и атрибуты системных объектов на происходящие изменения, обращая особое внимание скорее на конечный результат атаки, а не на подробности развития атаки.

Аналогично системам анализа защищенности классические системы обнаружения атак также можно классифицировать по уровню информационной инфраструктуры, на котором обнаруживаются нарушения политики безопасности.

Обнаружение атак реализуется посредством анализа или журналов регистрации операционной системы и прикладного ПО, или сетевого трафика в реальном времени. Компоненты обнаружения атак, размещенные на узлах или сегментах сети, оценивают различные действия, в т. ч. и использующие известные уязвимости. Средства обнаружения атак функционируют сразу на

двух этапах – втором и третьем. На втором этапе эти средства дополняют традиционные механизмы новыми функциями, повышающими защищенность корпоративной сети. Например, при проникновении противника в сеть через межсетевой экран, система обнаружения атак сможет обнаружить и предотвратить действия, отличающиеся от нормального поведения пользователя, у которого украли пароль. Также эффективно системы обнаружения атак будут блокировать и враждебные действия привилегированных пользователей (администраторов). И, наконец, эти системы одинаково эффективно функционируют и для защиты периметра корпоративной сети, дополняя возможности межсетевых экранов, и для защиты внутренних сегментов сети.

Вторым, не менее важным подходом является использование модели адаптивной защиты информации от несанкционированного доступа в условиях информационного противоборства. С позиции адаптивной защиты ВС от НСД при ведении компьютерной войны основными аспектами оборонительной составляющей является защита информационных, программных, вычислительных и телекоммуникационных ресурсов, обнаружение и противодействие НСД.

Ключевым аспектом технологии адаптивной защиты является переход от принципа «обнаружения и ликвидация НСД» к принципу «анализ – прогнозирование – предупреждение – противодействие». Для вычислительных сетей реализация данного принципа является обязательной, так как целенаправленное воздействие противника является для них вполне очевидным и предсказуемым явлением.

Основу системы адаптивной защиты (САЗ) составляет подсистема идентификации безопасности состояний ВС, которая в основном и определяет способность системы защиты информации (СЗИ) оперативно обнаруживать и предупреждать НСД к ее ресурсам. Реализация данной подсистемы может быть основана на следующих частных методах динамической идентификации:

– обнаружение НСД на основе динамического анализа использования вычислительных ресурсов при выполнении прикладных программ;

– обнаружение злоупотреблений пользователей на основе анализа данных аудита.

Осуществляя контроль вызовов системных функций в процессе выполнения прикладных программ в многопрограммном режиме и статистический анализ использования ими ресурсов вычислительной системы, можно в режиме реального времени обнаруживать деструктивные изменения программного кода и блокировать их реализацию в вычислительной среде.

Второй из предлагаемых частных методов адаптивной защиты – метод обнаружения злоупотреблений пользователей основан на анализе данных различных регистрационных журналов узлов сети (например, журнала безопасности, журнала системных событий, журналов приложений и т. п.). Цель анализа – выявление неявных (скрытых) закономерностей и действий субъектов доступа – пользователей и инициируемых ими прикладных программ по отношению к объектам доступа – защищаемым информационным ресурсам.

Рассмотренные методы не позволяют в полном объеме решать проблему динамической идентификации состояний вычислительной сети, так как отражают лишь аспекты защиты от злоупотреблений пользователей и внедрения деструктивного кода. Однако их несомненным достоинством является возможность упреждения (предотвращения) НСД, что является основным принципом реализации технологии адаптивной защиты информации.

1.6. Механизм функционирования обманных систем в системе защиты информации в вычислительных сетях

В условиях информационного противоборства, когда цена информации весьма высока, становится очевидным, что для обеспечения успешного

противодействия атаке необходимо, чтобы нарушитель действовал в условиях априорной неопределенности ($1 \le k \le K$, где К достаточно велико).

Этого добиваются введением в контур защиты обманной системы (ОБС), целью которой является вовлечение нарушителя в своего рода «игру», тем самым увеличивается время, необходимое на обход СЗИ.

Работа обманных систем заключается в том, что они эмулируют те или иные известные уязвимости, которых в реальности не существует.

Исходя из названия видно, что обманные системы используют в качестве защитного механизма методы обмана. Естественно это требует ресурса аппаратных и программных средств, что на современном этапе развития вычислительной техники не представляет собой экзотической задачи, но теория вопроса разработана недостаточно и ждет своих исследователей.

Необходимо отметить, что обман, по указанной выше причине, очень редко используется в качестве защитного механизма. Существует множество различных вариантов использования обмана в благих целях. Вкратце перечислим некоторые механизмы обмана, основываясь на классификации Даннигана (Dunnigan) и Ноуфи (Nofi): сокрытие, камуфляж, дезинформация. К этому целесообразно добавить методы провокаций (подталкивания).

В области информационной безопасности наибольшее распространение получил первый метод – сокрытие. Ярким примером использования этого метода в целях обеспечения информационной безопасности можно назвать сокрытие сетевой топологии при помощи межсетевого экрана. Примером камуфляжа можно назвать использование Unix-подобного графического интерфейса в системе, функционирующей под управлением операционной системы Windows NT. Если злоумышленник случайно увидел такой интерфейс, то он будет пытаться реализовать атаки, характерные для ОС Unix, а не для ОС Windows NT. Это существенно увеличит время, необходимое для «успешной» реализации атаки.

Как правило, каждая операционная система обладает присущим только ей представлением механизма идентификации пользователя, отличающимся от

своих собратьев цветом и типом шрифта, которым выдается приглашение; текстом самого приглашения, местом его расположения и т.д. Камуфляж позволяет защититься от такого рода атак.

И, наконец, в качестве примера дезинформации можно назвать использование заголовков (banner), которые бы давали понять злоумышленнику, что атакуемая им система уязвима.

Использование средств (deception systems), реализующих камуфляж и дезинформацию, приводит к следующему:

– увеличение числа выполняемых нарушителем операций и действий. Чтобы заранее определить, является ли обнаруженная нарушителем уязвимость истинной или нет, злоумышленнику приходится выполнять определенный объем дополнительных операций. Например, попытка запустить программу подбора паролей (например, Crack для Unix или L0phtCrack для Windows) на сфальсифицированный и несуществующий в реальности файл, приведет к бесполезной трате времени без какого-либо видимого результата. Нападающий с определенной долей вероятности будет предполагать, что он не смог подобрать пароли, в то время как на самом деле программа «взлома» была просто обманута;

– получение возможности для идентификации нападающих. За тот период времени, когда нападающие пытаются проверить все обнаруженные уязвимости, в т.ч. и фиктивные, администраторы безопасности в состоянии проследить весь путь до нарушителя или нарушителей и предпринять соответствующие меры.

Обычно в информационной системе используются от 5 до 10 зарезервированных портов (с номерами от 1 до 1024). К ним можно отнести порты, отвечающие за функционирование сервисов HTTP, FTP, SMTP, NNTP, NetBIOS, Echo, Telnet и т. д. Если обманные системы (например, RealSecure компании ISS) эмулируют использование еще 100 и более портов, то работа нападающего увеличивается в сто раз. Теперь злоумышленник обнаружит не 5-

10, а 100 открытых портов. При этом мало обнаружить открытый порт, надо еще попытаться использовать уязвимости, связанные с этим портом. И даже если нападающий автоматизирует эту работу путем использования соответствующих программных средств (Nmap, SATAN и т. д.), то число выполняемых им операций все равно существенно увеличивается, что приводит к быстрому снижению производительности его работы. И при этом злоумышленник все время находится под присмотром администраторов безопасности.

Есть и другая особенность использования обманных систем. По умолчанию обращение ко всем неиспользуемым портам игнорируется. Тем самым попытки сканирования портов могли быть пропущены используемыми защитными средствами. В случае же использования обманных систем все эти действия будут сразу же обнаружены при первой попытке обращения к ним.

Обманная система может быть реализована двумя способами. Первый вариант представляет собой эмуляцию некоторых сервисов или уязвимостей только на том компьютере, на котором запущена обманная система (The Deception Toolkit; DTK). В этом случае никаких проблем с размещением обманной системы не возникает, так как она устанавливается на защищаемый узел.

Набор инструментальных обманных средств DTK является первым средством, предназначенным для реализации механизма обмана злоумышленников, пытающихся проникнуть в вычислительную сеть. Данное средство разработано с той целью, чтобы ввести в заблуждение автоматизированные средства анализа защищенности путем создания ложных уязвимостей, что позволит своевременно обнаружить попытки НСД и противопоставить им эффективные средства защиты и, возможно, обнаружить атакующего.

DTK представляет собой набор программ на языке C и Perl, реализующих описанные выше механизмы обмана злоумышленников. Эти

программы могут быть модифицированы под конкретные нужды пользователей. DTK может функционировать под управлением любой ОС, поддерживающей стек протоколов TCP/IP и имеющей реализацию транслятора с языка Perl. В частности под управлением большого числа различных Unix'ов.

А вот со вторым классом систем иногда может возникнуть некоторое недопонимание из-за того, что они эмулируют не отдельные сервисы, а сразу целые компьютеры и даже сегменты, содержащие виртуальные узлы (CyberCop Sting, ManTrap).

CyberCop Sting «создает» виртуальную сеть на выделенном узле, работающем под управлением Windows NT. Каждый из виртуальных узлов имеет один или несколько IP-адресов, на которые можно посылать сетевой трафик и получать вполне «реальный» ответ. В более сложных случаях виртуально созданных узел может выступать в роли ретранслятора пакетов на невидимый, но реальный компьютер, который и отвечает на все запросы злоумышленника.

Главное достоинство системы CyberCop Sting в том, что для моделирования «приманки» для нарушителя не требуется большого количества компьютеров и маршрутизаторов, все реализуется на единственном компьютере (рис. 1.13).

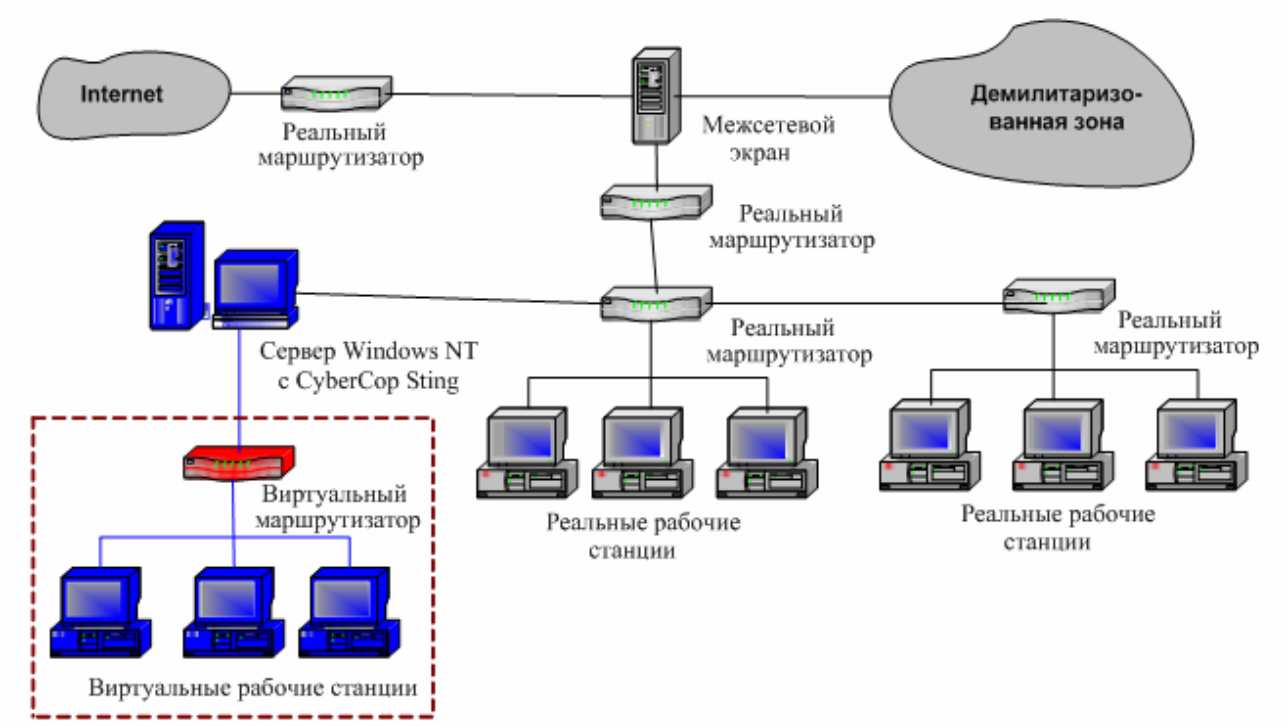


Рис. 1.13. Применение системы CyberCop Sting для создания виртуального сегмента сети

Для таких систем предложено два варианта их размещения.

Суть первого варианта заключается в том, что обманная система размещается в отдельном сегменте корпоративной сети.

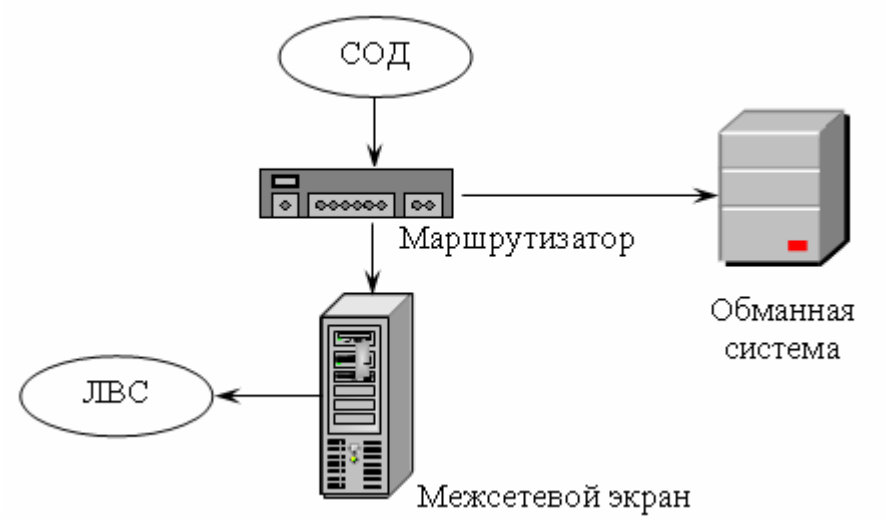


Рис. 1.14. Размещение обманной системы в сегменте корпоративной сети по первому варианту

Другим способом размещения ОБС является размещение такой системы в контролируемом сегменте сети. Узел с обманной системой подключается к

тому же коммутатору или концентратору, что и рабочие узлы сегмента, и имеет адрес, незначительно отличающийся от адресов рабочих узлов. Например, IP – адреса сервера баз данных, файлового сервера и контроллера доменов – 200.0.0.100, 200.0.0.254, и 200.0.0.1 соответственно, а 200.0.0.200 – адрес обманной системы. Злоумышленник, определяя цель атаки путем сканирования узлов, попадает в созданную ловушку, давая сигнал администратору безопасности. Помимо схожего с рабочими IP-адреса, обманная система может иметь и близкое по звучанию DNS-имя, вводящее в заблуждение нарушителя. Например, main.infosec.ru или fw.infosec.ru. При этом на одну обманную систему могут указывать несколько различных имен или IP-адресов, что реализуется путем использования псевдонимов (рис. 1.15).

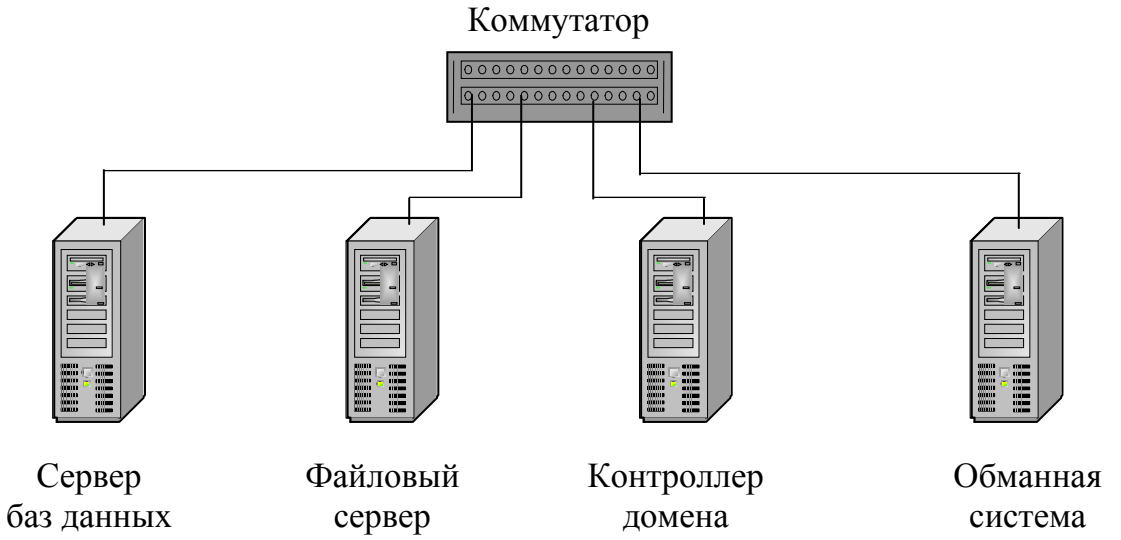


Рис. 1.15. Размещение обманной системы в сегменте корпоративной сети по второму варианту

Рассмотренные выше и другие существующие на сегодня ОБС работают с различными операционными системами, что наглядно демонстрирует таблица 1.3.

Таблица 1.3

Операционные системы, используемые обманными системами

Тип ОБС	*Операционная система*
The Deception Toolkit	Различные версии Unix (после доработки и под Windows NT)
CyberCop Sting	Windows NT, Solaris
Man Trap	Windows NT, Windows 2000, Windows 95/98, Solaris
RealSecure OS Sensor	Windows NT, Windows 2000, Solaris, HP UX, AIX
Facebo	Solaris, Linux, Windows
Iptrap	Unix, Linux
Honeyd	Free Dsd, Solaris, Linux

Для описания такой СЗИ предлагается вербальная модель, смысл которой поясняется схемой, представленной на рис. 1.16.

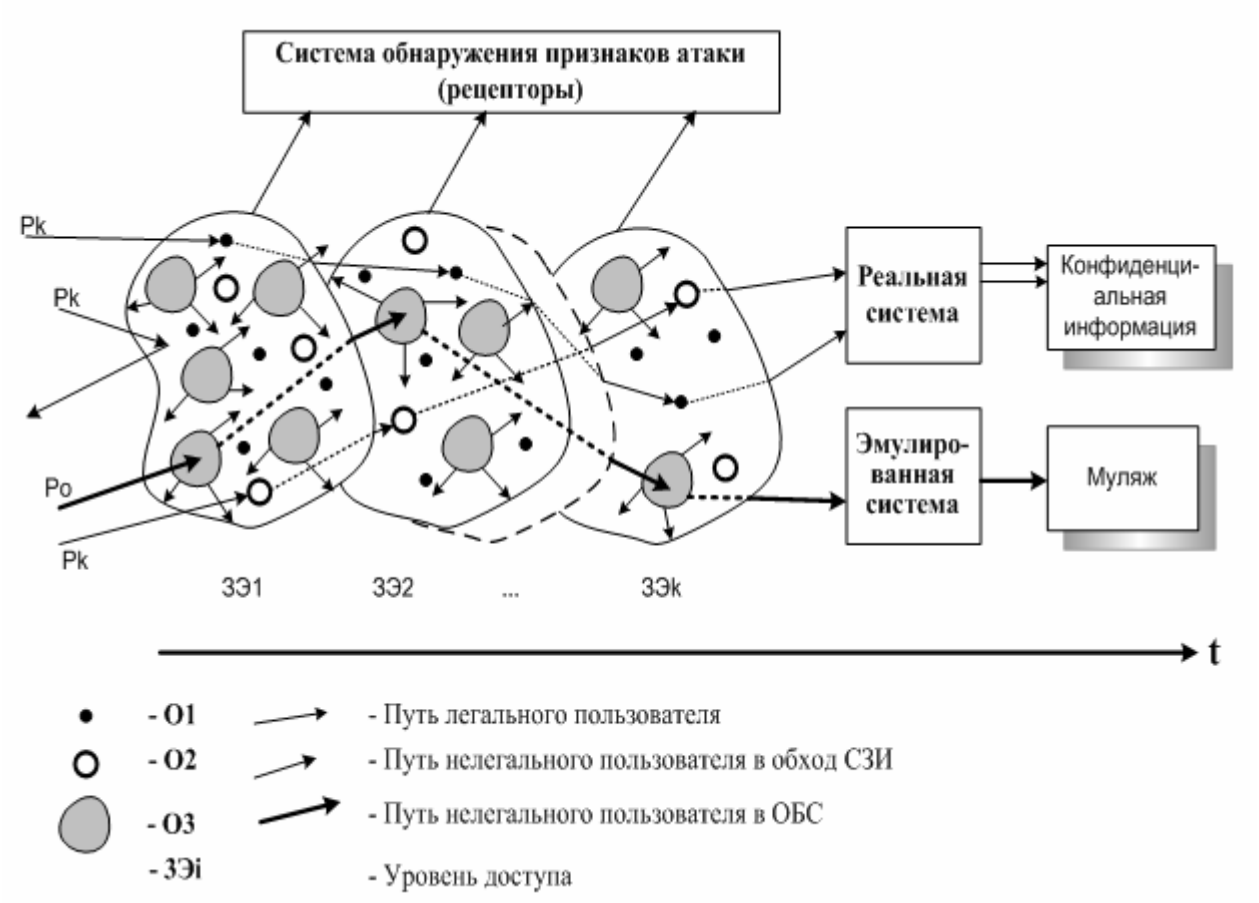


Рис. 1.16. Вербальная модель СЗИ с обманной системой

С помощью обманных систем против злоумышленников применяют их же оружие, и чаша весов склоняется уже не в пользу атакующих, которые раньше почти всегда были на шаг впереди специалистов по защите.

Выполняющий все инструкции пользователь преодолевает все области О1 с наименьшими временными затратами. Нарушитель, пытаясь определить уязвимые места в СЗИ, сканирует поверхность упругого экрана, в результате чего он либо отражается от защитного экрана, либо поглощается областями О2 или О3. Так как площади эмулированных уязвимостей О3 значительно больше, чем реально существующих, то нарушитель с большей вероятностью попадает именно в «муляж». При этом до некоторого момента времени нарушитель не подозревает, что работает с обманной системой. Пытаясь закрепиться в системе и найти слабое место в следующей ступени защиты, он проявляет себя.

В момент работы обманной системы, настоящая система продолжает функционировать и успешно решать возложенные на нее задачи, а система «предупреждения НСД» принимает меры по вычислению нарушителя и формирует стратегию и тактику предупреждения НСД.

С развитием информационных технологий и вовлечением в них все большего числа пользователей увеличивается число уязвимостей вычислительных сетей, что приводит к росту числа угроз, которым может быть подвергнута система.

Проведенный анализ проблемы защиты информации показывает, что с ростом числа угроз безопасности ИРК необходимо совершенствование механизмов защиты.

1. В условиях применения концепции вычислительных сетей для обеспечения, например, управления банковскими структурами, информация, обрабатываемая в них, становится первостепенным объектом воздействия со стороны противника, что подтверждается анализом последних десятилетий. При этом основная масса нарушений политики безопасности исходит от пользователей информационной системы.

2. Рост угроз приводит к необходимости совершенствования принятой политики безопасности, поиску технических (программных) средств защиты, не зависящих от квалификации персонала и повышения уровня трудозатрат администраторов безопасности. Существует реальная угроза несанкционированного изменения хода выполнения прикладных программ, защита от которой существующими средствами защиты информации не обеспечивается в полной мере.

3. Многие известные и широко распространенные способы защиты довольно статичны, они могут быть изучены за конечный интервал времени и успешно преодолены за конечный интервал времени, кроме того, квалифицированному нарушителю могут быть известны приемы оказания адекватного противодействия и обнаружения каналов НСД, что естественным образом ослабляет систему защиты.

4. Применение обманных систем не требует участия в ее работе легального пользователя и поэтому не усложняет правил его поведения в системе, не требуется специальная подготовка, повышение квалификации и т. п. Управление такой системой ведет узкий круг специалистов по политике безопасности.

5. Использование таких систем целесообразно основывать на разрешении игровых ситуаций, т. к. такая система не должна быть статичной, в случае необходимости желательно ее внезапное применение. Эти факторы носят негативный характер, они усложняют применение обманных систем в реальных СЗИ, но с учетом развития средств ВТ и определенному оживлению рынка такой продукции они вполне преодолимы.

6. Использование методов обмана позволяет в большей или меньшей мере ввести в заблуждение нарушителей и с некоторой долей вероятности отвести угрозу от реально работающей вычислительной сети.

Контрольные вопросы к главе 1

1. Раскройте суть информационного конфликта.
2. Какова структура информационного противоборства?
3. Покажите возможные пути информационного нападения на вычислительную сеть.
4. Какие вычислительные сети могут считаться неуязвимыми.
5. Какие факторы приводят к ослаблению защиты элементов вычислительных сетей?
6. Дайте классификацию угроз безопасности вычислительных сетей.
7. Укажите возможные пути реализации угроз безопасности для вычислительных сетей.
8. Раскройте суть аналитической модели несанкционированных действий, приводящих к вероятному снижению безопасности информационного процесса.
9. Каковы существующие подходы к обеспечению защиты вычислительных сетей?
10. Дайте классификацию систем обнаружения атак на вычислительную сеть.
11. Какова, по современным взглядам, классификация систем обнаружения атак?
12. В чем заключается суть применения обманных систем в информационной защите вычислительных сетей?
13. Каков, на ваш взгляд, самый слабый элемент в защите целостности информационной системы?

2. ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Антивирусные средства

Материальным носителем информационной безопасности являются конкретные программно-технические решения, которые объединяются в комплексы в зависимости от целей их применения. Организационные меры вторичны относительно имеющейся материальной основы обеспечения информационной безопасности, поэтому в данном разделе пособия основное внимание будет уделено принципам построения основных программно-технических решений и перспективам их развития.

Угрозой интересам субъектов информационных отношений обычно называют потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или другие компоненты ИРК может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

В силу особенностей современных ИРК, существует значительное число различных видов угроз безопасности субъектам информационных отношений.

Одним из распространенных видов угроз являются компьютерные вирусы. Они способны причинить значительный ущерб ИРК. Поэтому важное значение имеет не только защита сети или отдельных средств информационного обмена от вирусов, но и понимание пользователями принципов антивирусной защиты.

В нашей стране наиболее популярны антивирусные пакеты «Антивирус Касперского» и DrWeb. Существуют также другие программы, например «McAfee Virus Scan» и «Norton AntiVirus». Динамика изменения информации в данной предметной области высокая, поэтому дополнительную информацию по защите от вирусов можно найти в Internet, выполнив поиск по ключевым словам «защита от вирусов».

Известно, что нельзя добиться 100 %-й защиты ПК от компьютерных вирусов отдельными программными средствами. Поэтому для уменьшения потенциальной опасности внедрения компьютерных вирусов и их распространения по корпоративной сети необходим комплексный подход, сочетающий различные административные меры, программно-технические средства антивирусной защиты, а также средства резервирования и восстановления. Делая акцент на программно-технических средствах, можно выделить три основных уровня антивирусной защиты:

- поиск и уничтожение известных вирусов;
- поиск и уничтожение неизвестных вирусов;
- блокировка проявления вирусов [6].

Уровни и средства антивирусной защиты схематично представлены на рис. 2.1.

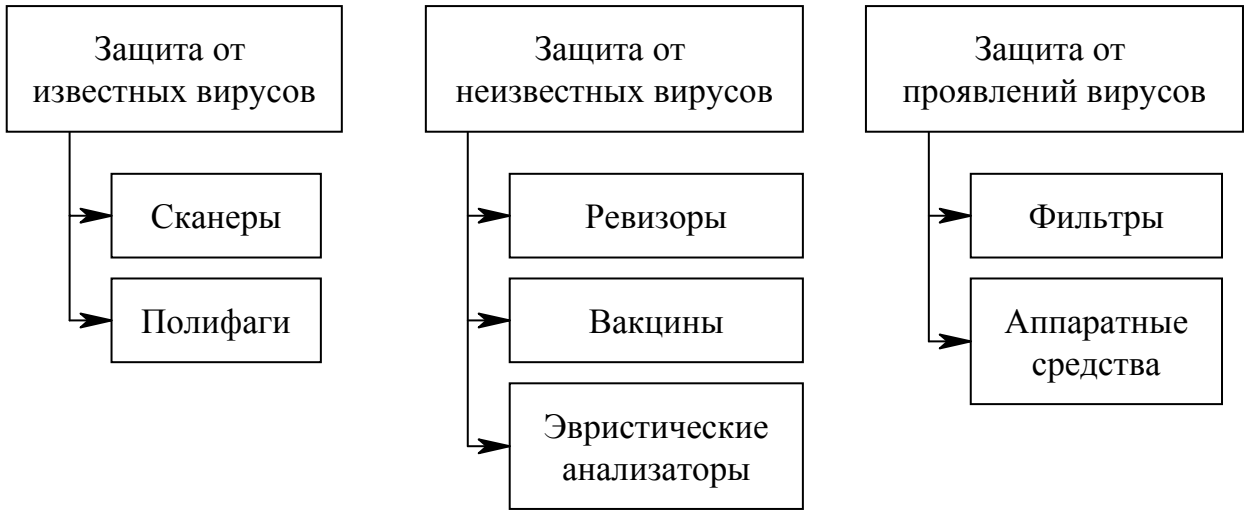


Рис. 2.1. Уровни и средства антивирусной защиты

2.1.1. Защита от известных вирусов

При поиске и уничтожении известных вирусов наиболее распространенным является метод сканирования. Указанный метод заключается в выявлении компьютерных вирусов по их уникальному фрагменту программного кода (сигнатуре, программному штамму). Для этого создается некоторая *база данных сканирования* с фрагментами кодов известных

компьютерных вирусов. Обнаружение вирусов осуществляется путем сравнения данных памяти компьютера с фиксированными кодами базы данных сканирования. В случае выявления и идентификации кода нового вируса, его сигнатура может быть введена в базу данных сканирования. В виду того, что сигнатура известна, существует возможность корректного восстановления (обеззараживания) зараженных файлов и областей. Следует добавить, что некоторые системы хранят не сами сигнатуры, а, например, контрольные суммы или имитоприставки сигнатур.

Антивирусные программы, выявляющие известные компьютерные вирусы, называются *сканерами* или детекторами. Программы, включающие функции восстановления зараженных файлов, называют *полифагами* (фагами), докторами или дезинфекторами. Принято разделять сканеры на следующие:

– транзитные, периодически запускаемые для выявления и ликвидации вирусов,

– резидентные (постоянно находящиеся в оперативной памяти), проверяющие заданные области памяти системы при возникновении связанных с ними событий (например, проверка файла при его копировании или переименовании).

К недостаткам сканеров следует отнести то, что они позволяют обнаружить только те вирусы, которые уже проникали в вычислительные системы, изучены и для них определена сигнатура. Для эффективной работы сканеров необходимо оперативно пополнять базу данных сканирования. Однако с увеличением объема базы данных сканирования и числа различных типов искомых вирусов снижается скорость антивирусной проверки. Само собой, если время сканирования будет приближаться ко времени восстановления, то необходимость в антивирусном контроле может стать не столь актуальной.

Некоторые вирусы (мутанты и полиморфные) кодируют или видоизменяют свой программный код. Это затрудняет или делает невозможным

выделить сигнатуру и, следовательно, обнаружить вирусы методом сканирования.

Для выявления указанных маскирующихся вирусов используются специальные методы. К ним можно отнести метод эмуляции процессора. Метод заключается в имитации выполнения процессором программы и подсовывания вирусу фиктивных управляющих ресурсов. Обманутый таким образом вирус, находящийся под контролем антивирусной программы, расшифровывает свой код. После этого, сканер сравнивает расшифрованный код с кодами из своей базы данных сканирования.

2.1.2. Защита от неизвестных вирусов

Выявление и ликвидация неизвестных вирусов необходимы для защиты от вирусов, пропущенных на первом уровне антивирусной защиты. Наиболее эффективным методом является контроль целостности системы (обнаружение изменений). Данный метод заключается в проверке и сравнении текущих параметров вычислительной системы с эталонными параметрами, соответствующими ее незараженному состоянию. Понятно, что контроль целостности не является прерогативой системы антивирусной защиты. Он обеспечивает защищенность информационного ресурса от несанкционированных модификации и удаления в результате различного рода нелегитимных воздействий, сбоев и отказов системы и среды.

Для реализации указанных функций используются программы, называемые *ревизорами*. Работа ревизора состоит из двух этапов: фиксирование эталонных характеристик вычислительной системы (в основном диска) и периодическое сравнение их с текущими характеристиками. Обычно контролируемыми характеристиками являются контрольная сумма, длина, время, атрибут «только для чтения» файлов, дерево каталогов, сбойные кластеры, загрузочные сектора дисков. В сетевых системах могут накапливаться среднестатистические параметры функционирования подсистем

(в частности исторический профиль сетевого трафика), которые сравниваются с текущими параметрами.

Ревизоры, как и сканеры, делятся на транзитные и резидентные. К недостаткам ревизоров, в первую очередь резидентных, относят создаваемые ими различные неудобства и трудности в работе пользователя. Например, многие изменения параметров системы вызваны не вирусами, а работой системных программ или действиями пользователя-программиста. По этой же причине ревизоры не используют для контроля зараженности текстовых файлов, которые постоянно меняются. Таким образом, необходимо соблюдение некоторого баланса между удобством работы и контролем целостности системы.

Ревизоры обеспечивают высокий уровень выявления неизвестных компьютерных вирусов, однако они не всегда обеспечивают корректное лечение зараженных файлов. Для лечения файлов, зараженных неизвестными вирусами, обычно используются эталонные характеристики файлов и предполагаемые способы их заражения.

Разновидностью контроля целостности системы является метод программного самоконтроля, именуемый вакцинацией. Идея метода состоит в присоединении к защищаемой программе модуля (*вакцины*), контролирующего характеристики программы, обычно ее контрольную сумму.

Помимо статистических методов контроля целостности, для выявления неизвестных и маскирующихся вирусов используются эвристические методы. Они позволяют выявить по известным признакам (определенным в базе знаний системы) некоторые маскирующиеся или новые модифицированные вирусы известных типов. В качестве примера признака вируса можно привести код, устанавливающий резидентный модуль в памяти, меняющий параметры таблицы прерываний и др. Программный модуль, реализующий эвристический метод обнаружения вирусов, называют *эвристическим анализатором*.

Примером сканера с эвристическим анализатором является программа Dr Web фирмы «Диалог-Наука».

К недостаткам эвристических анализаторов можно отнести ошибки 1-го и 2-го рода: ложные срабатывания и пропуск вирусов. Соотношение указанных ошибок зависит от уровня эвристики.

Понято, что если для обнаруженного эвристическим анализатором компьютерного вируса сигнатура отсутствует в базе данных сканирования, то лечение зараженных данных может быть некорректным.

2.1.3. Защита от проявлений вирусов

Блокировка проявления вирусов предназначена для защиты от деструктивных действий и размножения компьютерных вирусов, которым удалось преодолеть первые два уровня защиты. Методы основаны на перехвате характерных для вирусов функций. Известны два вида указанных антивирусных средств:

- программы-фильтры,
- аппаратные средства контроля.

Программы-фильтры, называемые также резидентными сторожами и мониторами, постоянно находятся в оперативной памяти и перехватывают заданные прерывания с целью контроля подозрительных действий. При этом они могут блокировать «опасные» действия или выдавать запрос пользователю.

Действия, подлежащие контролю, могут быть следующими: модификация главной загрузочной записи (MBR) и загрузочных записей логических дисков и ГМД, запись по абсолютному адресу, низкоуровневое форматирование диска, оставление в оперативной памяти резидентного модуля и др. Как и ревизоры, фильтры часто являются «навязчивыми» и создают определенные неудобства в работе пользователя.

Встроенные аппаратные средства ПК обеспечивают контроль модификации системного загрузчика и таблицы разделов жесткого диска,

находящихся в главной загрузочной записи диска (MBR). Включение указанных возможностей в ПК осуществляется с помощью программы Setup, расположенной в ПЗУ. Следует указать, что программу Setup можно обойти в случае замены загрузочных секторов путем непосредственного обращения к портам ввода-вывода контроллеров жесткого и гибкого дисков.

Наиболее полная защита от вирусов может быть обеспечена с помощью специальных контроллеров аппаратной защиты. Такой контроллер подключается к ISA-шине ПК и на аппаратном уровне контролирует все обращения к дисковой подсистеме компьютера. Это не позволяет вирусам маскировать себя. Контроллер может быть сконфигурирован так, чтобы контролировать отдельные файлы, логические разделы, «опасные» операции и т. д. Кроме того, контроллеры могут выполнять различные дополнительные функции защиты, например, обеспечивать разграничение доступа и шифрование.

К недостаткам указанных контроллеров, таких как ISA-плат, относят отсутствие системы автоконфигурирования, и, как следствие, возможность возникновения конфликтов с некоторыми системными программами, в том числе антивирусными.

При работе в глобальных сетях общего пользования, в частности в Internet, кроме традиционных способов антивирусной защиты данных компьютеров, становится актуальным антивирусный контроль всего проходящего трафика. Это может быть осуществлено путем реализации антивирусного прокси-сервера, либо интеграции антивирусной компоненты с межсетевым экраном. В последнем случае межсетевой экран передает антивирусной компоненте (или серверу) допустимый, например, SMTP, FTP и HTTP-трафик. Содержащиеся в нем файлы проверяются на предмет наличия вирусов и, затем, направляются пользователям. Можно сказать, мы имеем дело с новым уровнем антивирусной защиты – уровнем межсетевого экранирования.

2.1.4. Обзор возможностей антивирусных средств

В настоящее время наблюдается тенденция в интегрировании различных антивирусных средств с целью обеспечения надежной многоуровневой защиты. На российском рынке наиболее мощными являются антивирусный комплект DialogueScience's Anti-Virus kit (DSAV) АО «ДиалогНаука» и интегрированная антивирусная система AntiViral Toolkit Pro (AVP) ЗАО «Лаборатория Касперского». Указанные комплексы высоко зарекомендовали себя в нашей стране, особенно при обеспечении антивирусной защиты информационных систем малого и среднего офиса. Рассмотрим возможности средства «Лаборатория Касперского».

Указанный программный продукт декларирует: «Одной из главных задач специалистов «Лаборатории Касперского» при создании Антивируса Касперского являлась оптимальная настройка всех параметров приложения. Это дает возможность пользователю с любым уровнем компьютерной грамотности, не углубляясь в параметры, обеспечить безопасность компьютера сразу же после установки приложения». Окно-приглашение (главное окно) указанного антивирусного средства доступно для понимания пользователю любого уровня.

В случае необходимости пользователь может обратиться за помощью к справочной системе, нажав кнопку «? Справка» и получить ответ на интересующий его вопрос. Приведем без купюр содержание одного из информационных окон программного продукта.

Антивирус Касперского – это принципиально новый подход к защите информации. Главное в приложении – это объединение и заметное улучшение текущих функциональных возможностей всех продуктов компании в одно комплексное решение защиты. Приложение обеспечивает не только антивирусную защиту, но и защиту от неизвестных угроз. Больше не нужно устанавливать несколько продуктов на компьютер, чтобы обеспечить себе полноценную защиту. Достаточно просто установить Антивирус Касперского.

Комплексная защита обеспечивается на всех каналах поступления и передачи информации. Гибкая настройка любого компонента приложения позволяет максимально адаптировать Антивирус Касперского под нужды конкретного пользователя. Предусмотрена также единая настройка всех компонентов защиты.

Рассмотрим детально нововведения Антивируса Касперского.

Новое в защите

– Теперь Антивирус Касперского защищает не только от уже известных вредоносных программ, но и от тех, что еще не известны. Наличие компонента *проактивной защиты* – основное преимущество приложения. Его работа построена на анализе поведения приложений, установленных на вашем компьютере, на контроле изменений системного реестра, отслеживании выполнения макросов и борьбе со скрытыми угрозами. В работе компонента используется эвристический анализатор, позволяющий обнаруживать различные виды вредоносных программ. При этом ведется история вредоносной активности, на основе которой обеспечивается откат действий, совершенных вредоносной программой, и восстановление системы до состояния, предшествующего вредоносному воздействию.

– Изменилась технология защиты файлов на компьютере пользователя: теперь вы можете снизить нагрузку на центральный процессор и дисковые подсистемы и увеличить скорость проверки файлов. Это достигается за счет использования технологий iChecker и iSwift. Такой режим работы приложения исключает повторную проверку файлов.

– Процесс поиска вирусов теперь подстраивается под вашу работу на компьютере. Проверка может занимать достаточное количество времени и ресурсов системы, но пользователь может параллельно выполнять свою работу. Если выполнение какой-либо операции требует ресурсов системы, поиск вирусов будет приостановлен до момента завершения этой операции. Затем проверка продолжится с того места, на котором остановилась.

– Проверка критических областей компьютера, заражение которых может привести к серьезным последствиям, представлена отдельной задачей. Вы можете настроить автоматический запуск этой задачи каждый раз при старте системы.

– Значительно улучшена защита электронной корреспонденции на компьютере пользователя от вредоносных программ. Приложение проверяет на вирусы почтовый трафик на следующих протоколах:

* IMAP, SMTP, POP3, независимо от используемого вами почтового клиента;
* NNTP, независимо от почтового клиента;
* Независимо от типа протокола (в том числе MAPI, HTTP) в рамках работы плагинов, встроенных в почтовые программы Microsoft Office Outlook и The Bat!

– В таких широко известных почтовых клиентах как Microsoft Office Outlook, Microsoft Outlook Express и The Bat! встроены специальные модули расширения (плагины), позволяющие настраивать защиту почты непосредственно в почтовом клиенте.

– Расширена функция *оповещения пользователя* о возникновении в работе приложения определенных событий. Вы сами можете выбрать способ уведомления для каждого из типов событий: почтовое сообщение, звуковое оповещение, всплывающее сообщение, запись в журнал событий.

– Реализована проверка трафика, передаваемого через защищенное соединение по протоколу SSL.

– Добавлена технология самозащиты приложения, защиты от удаленного несанкционированного управления сервисом Антивируса, а также защиты доступа к параметрам приложения с помощью пароля. Это позволяет избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.

– Добавлена возможность создания диска аварийного восстановления системы. С помощью этого диска можно провести первоначальную загрузку операционной системы после вирусной атаки и выполнить проверку компьютера на наличие вредоносных объектов.

Достаточно популярной у ряда пользователей является программа Dr. Web. Основная направленность Dr. Web состоит в обнаружение полиморфных вирусов. В настоящее время Dr. Web реализует наиболее эффективный эвристический анализатор неизвестных вирусов в мире. По данным журнала Virus Bulletin, это обеспечивает обнаружение до 80 – 91% неизвестных вирусов, в т. ч. 99 % макро-вирусов! На международных конкурсах Dr. Web несколько раз входил в тройку самых лучших антивирусов для DOS. Продукт достаточно компактный, что позволяет запускать его с дискеты.

В заключении отметим, что администратор сети, пользователи ПК должны постоянно следить за обновлением антивирусных средств и своевременно осуществлять комплекс мер по защите программно-аппаратных средств сети от высоковероятного поражения их вирусами.

2.2. Криптографические методы защиты информации

2.2.1. Общие сведения о криптографии

Криптография – наука о шифрах. Долгое время сведения этой предметной области были строго засекречены, так как шифры применялись, в основном, для защиты государственных и военных секретов. В настоящее время методы и средства криптографии используются для обеспечения информационной безопасности не только государства, но и частных лиц и организаций. Дело здесь совсем не обязательно в секретах. Слишком много различных сведений «гуляет» по всему свету в цифровом виде. И над этими сведениями «висят» угрозы недружественного ознакомления, накопления, подмены, фальсификации и т. п. Наиболее надежные методы защиты от таких угроз дает именно

криптография. Но и она бессильна защитить информационное пространство пользователя, если он нарушает правила применения доступных ему шифров. Поэтому знание основ криптографических методов защиты информации является неотъемлемой составляющей культуры современного человека, сталкивающегося практически ежедневно с применением современных сетевых технологий при эксплуатации средств вычислительной техники.

Темпы развития информационных технологий таковы, что косвенно многим уже приходилось пользоваться некоторыми криптографическими средствами: шифрование электронной почты, электронной подписи, интеллектуальные банковские карточки и др. Естественно, что при этом основной вопрос для пользователя – обеспечивает ли данное криптографическое средство надежную защиту. Но даже правильно сформулировать этот элементарный вопрос непросто. От какого противника защищаемся? Какие возможности у этого противника? Какие цели он может преследовать? Как измерять надежность защиты? Список таких вопросов можно продолжить.

Для ответа на них пользователю необходимы знания основных понятий криптографии. Цель данного раздела дать представление об основных понятиях современной криптографии: шифр, ключ, стойкость, электронная цифровая подпись, криптографический протокол и др.

Как передать нужную информацию нужному адресату в тайне от других?

Размышляя над задачей передачи конфиденциальных сведений, нетрудно прийти к выводу, что для этого есть три возможности.

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.

2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.

3. Использовать общедоступный канал связи, но передавать по нему нужную информацию в таком преобразованном виде, чтобы восстановить ее мог только адресат.

Прокомментируем эти три возможности.

1. При современном уровне развития науки и техники сделать такой канал связи между удаленными абонентами для неоднократной передачи больших объемов информации практически нереально.

2. Разработкой средств и методов скрытия факта передачи сообщения занимается стеганография.

Первые следы стеганографических методов теряются в глубокой древности. Например, известен такой способ скрытия письменного сообщения: голову раба брили, на коже головы писали сообщение и после отрастания волос раба отправляли к адресату.

Из детективных произведений хорошо известны различные способы тайнописи между строк обычного, незащищаемого текста: от молока до сложных химических реактивов с последующей обработкой.

Также из детективов известен метод «микроточки»: сообщение записывается с помощью современной техники на очень маленький носитель (микроточку), который пересылается с обычным письмом, например, под маркой или где-нибудь в другом, заранее обусловленном месте.

В настоящее время в связи с широким распространением компьютеров известно много тонких методов маскировки защищаемой информации внутри больших объемов информации, хранящейся в компьютере. Следует отметить, что стеганография и криптография – совершенно различные направления в теории и практике защиты информации.

3. Разработкой методов преобразования (шифрования) информации с целью ее защиты от незаконных пользователей занимается криптография. Такие методы и способы преобразования информации называются шифрами.

Шифрование (зашифрование) – процесс применения шифра к защищаемой информации, т. е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, криптограмму) с помощью определенных правил, содержащихся в шифре.

Дешифрование – процесс, обратный шифрованию, т. е. преобразование шифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Криптография – прикладная наука, она использует самые последние достижения фундаментальных наук, в первую очередь, математики. С другой стороны, все конкретные задачи криптографии существенно зависят от уровня развития техники и технологии, от применяемых средств связи и способов передачи информации.

2.2.2. Предмет криптографии

Что же является предметом криптографии? Для ответа на этот вопрос вернемся к задаче конфиденциальной передачи информации от одного субъекта к другому, чтобы уточнить ситуацию и используемые понятия.

Прежде всего заметим, что эта задача возникает только для информации, которая нуждается в защите. Обычно в таких случаях говорят, что информация содержит тайну или является защищаемой, приватной, конфиденциальной, секретной. Для наиболее типичных, часто встречающихся ситуаций такого типа введены даже специальные понятия:

- государственная тайна;
- военная тайна;
- коммерческая тайна;
- юридическая тайна;
- врачебная тайна и т. д. [22]

Далее будем говорить о защищаемой информации, имея в виду следующие признаки такой информации:

- имеется какой-то определенный круг законных пользователей, которые имеют право владеть этой информацией;
- имеются незаконные пользователи, которые стремятся овладеть этой информацией с тем, чтобы обратить ее себе во благо, а законным пользователям во вред.

Для простоты мы вначале ограничимся рассмотрением только одной угрозы – угрозы разглашения информации, например, сведений о доходах. Существуют и другие угрозы для защищаемой информации со стороны незаконных пользователей: подмена, имитация и др. Такие угрозы целесообразно рассмотреть отдельно. Рассмотрим процесс передачи секретных сведений по общедоступной системе связи с использованием средств криптографической защиты (см. рис. 2.2).

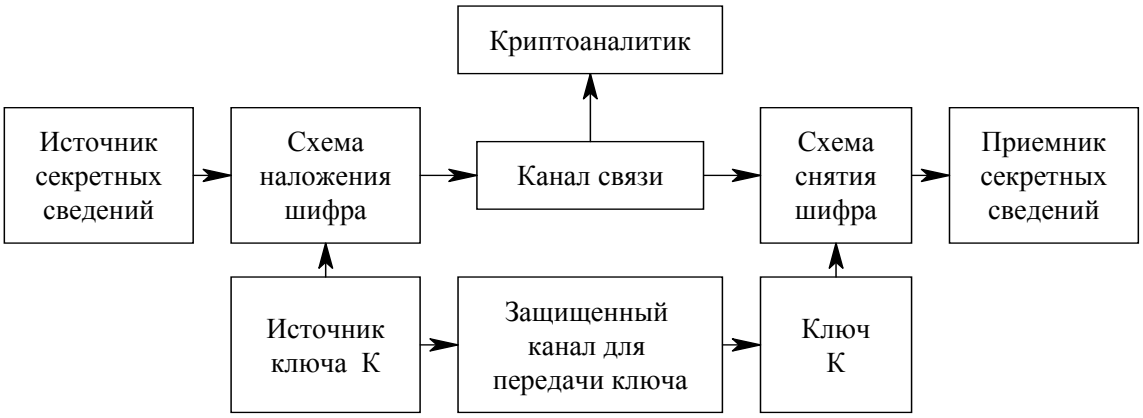


Рис. 2.2. Модель криптографической защиты

Здесь источник секретных сведений и их приемник – удаленные законные пользователи защищаемой информации: они хотят обмениваться информацией по общедоступному каналу связи. Криптоаналитик – незаконный пользователь (противник или злоумышленник), который может перехватывать передаваемые по каналу связи сообщения и пытаться извлечь из них интересующую его информацию. Особую роль в схеме играет источник ключа ***К***, который вырабатывает ключ и в простейшем случае по защищенному от посторонних лиц каналу связи передает его приемной стороне. Эту формальную схему можно считать моделью типичной ситуации, в которой применяются криптографические методы защиты информации [7].

Отметим, что исторически в криптографии закрепились некоторые военные термины (противник, атака на шифр и др.). Они наиболее точно отражают смысл соответствующих криптографических понятий. Вместе с тем широко известная военная терминология, основанная на понятии кода (военно-морские

коды, коды Генерального штаба, кодовые книги дипломатических представительств и миссий и т. п.), уже не применяется в теоретической криптографии. Дело в том, что за последние десятилетия сформировалась теория кодирования – большое научное направление, которое разрабатывает и изучает методы защиты информации от случайных искажений в каналах связи. И если ранее термины «кодирование» и «шифрование» употреблялись как синонимы, то теперь это недопустимо. Так, например, очень распространенное выражение «кодирование – разновидность шифрования» становится просто неправильным.

Информация в обыденном понимании этого термина имеет семантическую составляющую, например, объем доступных средств на кредитной карточке. Криптография занимается методами преобразования информации, которые бы не позволили злоумышленнику извлечь ее смысловое содержание из перехватываемых сообщений. При этом по каналу связи передается уже не сама защищаемая информация, а результат ее преобразования с помощью шифра, и для противника возникает сложная задача вскрытия шифра.

Вскрытие или взламывание шифра – процесс получения защищаемой информации из шифрованного сообщения без знания ключа $\boldsymbol{K}$ [16].

Однако помимо перехвата и вскрытия шифра противник может пытаться получить защищаемую информацию многими другими способами. Наиболее известным из таких способов является агентурный, когда противник каким-либо путем склоняет к сотрудничеству одного из законных пользователей и с помощью этого агента получает доступ к защищаемой информации. В такой ситуации криптография бессильна.

Противник может пытаться не получить, а уничтожить или модифицировать защищаемую информацию в процессе ее передачи. Это совсем другой тип угроз для информации, отличный от перехвата и вскрытия шифра. Для защиты от таких угроз разрабатываются свои специфические методы.

Таким образом, криптографические сценарии с точки зрения злоумышленника можно разделить на пассивное прослушивание канала связи (см. рис. 2.3) и активное нападение на систему обмена информацией с модификацией семантической составляющей в выгодном для себя (противника) варианте (см. рис. 2.4) [10].

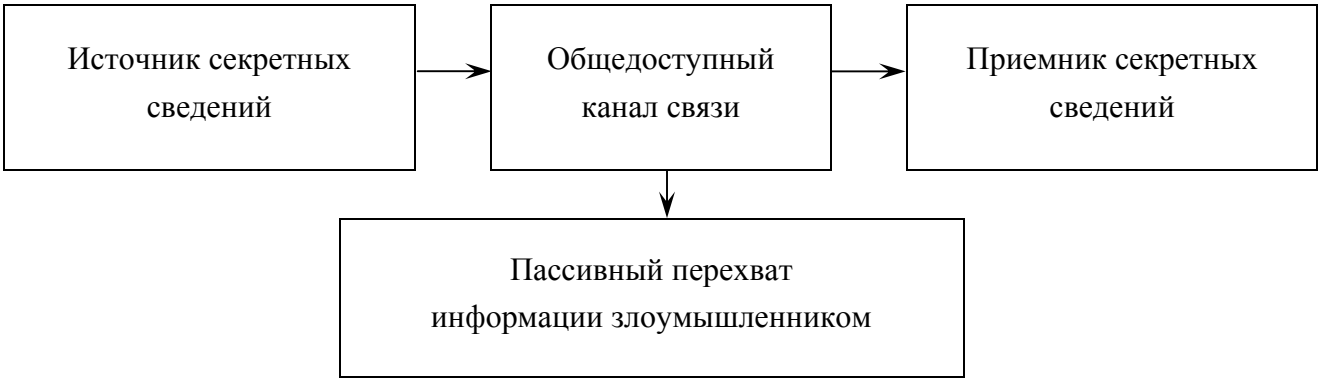


Рис. 2.3. Сценарий пассивного перехвата информации

Первая форма нападения на криптографический протокол относительно проста для большинства передающих сред, особенно для радиоканалов, где физическое соединение не требуется. При этом термин «пассивный перехват информации» означает, что противник до определенного момента времени пытается собрать некоторую информацию, не воздействуя на сам процесс передачи, т. е. поведение злоумышленника далеко не пассивно.

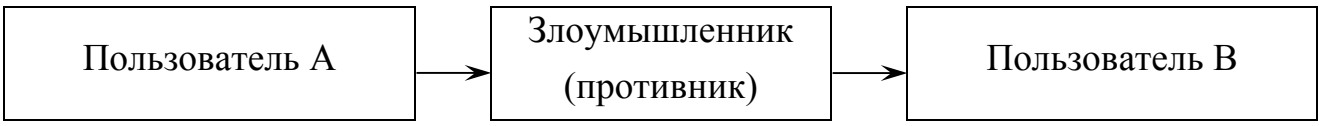


Рис. 2.4. Сценарий активной модификации информации

Возрастающее использование сетей пакетной коммутации, где данные обрабатываются в каждом маршрутизаторе, означает, что нападение с подстановкой также вполне возможно. Хорошим действующим примером

второго типа канала нападения (с перехватом сообщений) является брандмауэр (firewall) Internet – программно-аппаратное средство межсетевой защиты.

Осуществив получение по любому сценарию зашифрованного текста злоумышленник может совершить попытку взлома шифра, может собрать данные по ошибкам, допускаемым операторами в ходе обмена зашифрованной информацией, может собирать иную статистику для реализации взлома.

Наиболее грубой ошибкой пользователей является передача по общедоступному каналу одних и тех же сведений в открытом и зашифрованном виде. При этом наиболее уязвимой частью зашифрованного текста является адресная часть сообщения, которая с высокой вероятностью известна и по которой возможно осуществить вскрытие шифра.

По второму сценарию возможна модификация сообщения с расчетом внести в него ложные данные или путем имитации правдоподобного сообщения заставить пользователя сознательно выполнять неправильные действия.

При всех видах нападений следует предполагать, что сам алгоритм шифрования известен. Объясняется это тем, что в большинстве случаев шифр является коммерческим продуктом, который свободно продается на рынке.

Защита зависит только от ключа. Некоторые разработчики коммерческих программ шифрования в целях повышенной защиты пытаются сохранять свои алгоритмы в секрете. Однако реверсировать машинный код обратно в ассемблерный – относительно простая задача, и неблагоразумно предполагать, что такие шифры не попадут в плохие руки.

Следовательно, на пути от одного законного пользователя к другому информация должна защищаться разными способами, противостоящими различным угрозам. Возникает ситуация цепи из разнотипных звеньев, которая защищает информацию. Естественно, противник будет стремиться найти самое слабое звено, чтобы с наименьшими затратами добраться до информации.

А значит, и законные пользователи должны учитывать это обстоятельство в своей стратегии защиты: бессмысленно делать какое-то звено очень прочным, если есть заведомо более слабые звенья («принцип равнопрочности защиты»).

Не следует забывать и еще об одной важной проблеме: проблеме соотношения цены информации, затрат на ее защиту и затрат на ее добывание. При современном уровне развития техники сами средства связи, а также разработка средств перехвата информации из них и средств защиты информации требуют очень больших затрат. Прежде чем защищать информацию, следует оценить показатель экономической целесообразности применения криптосистемы. Следует решить альтернативную задачу: является ли защищаемая информация для противника более ценной, чем стоимость атаки и является ли она для пользователя более ценной, чем стоимость защиты. Именно перечисленные соображения и являются решающими при выборе подходящих средств защиты: физических, стеганографических, криптографических и др.

Говоря о системе шифрования, необходимо различать инициатора передачи информации, получателя сообщения и априори предполагать о наличии противника, пытающегося разыграть один из перечисленных криптографических сценариев.

Инициатор передачи организует зашифрованную связь, ему принадлежит ведущая роль в криптосистеме. Именно он определяет целесообразность закрытия информации теми или иными средствами, заказывает ключевую документацию и организует ее доставку надежным каналом к получателю сообщения. При одном получателе процедура доставки ключа в большинстве практических приложений не вызывает трудностей, но они возникают, если получателей сообщений достаточно много. Так как ключ имеет определенный срок действия, то организатор зашифрованной связи обязан предусмотреть схему смены ключей, выработать правило их использования и контролировать процедуру их применения.

Приемник сообщения обязан выполнять предусмотренные старшей инстанцией правила пользования ключевой документацией и обеспечивать доведение полученной информации до соответствующих исполнителей.

Действия противника могут только прогнозироваться инициатором передачи данных и их получателем, поскольку свои намерения злоумышленник не декларирует. О действии противника, как правило, становится известно только после выявления материального, финансового или иного вида ущерба.

Приведенные рассуждения носят качественный характер. Для получения некоторого представления о количественных характеристиках криптографической системы необходимо более детально рассмотреть свойства отдельных элементов системы, понять принцип их работы и взаимодействия.

2.2.3. Свойства источника сообщений

Источник секретных сведений (источник сообщений) передает информацию с использованием того или иного алфавита или системы счисления, если информация носит сугубо цифровой характер. Подлежащие передаче сведения формируются за счет усилий одного пользователя или группы лиц. Аналогичные сведения могут быть образованы и автоматическими устройствами, используемыми в информационном процессе.

Главной особенностью информации, представленной на естественном языке исполнителя, является наличие статистики в повторении букв алфавита того или иного языка, используемых для написания осмысленного текста. Указанная статистическая зависимость является неравномерной. В ней есть буквы, которые в текстах повторяются больше других, а есть буквы, которые повторяются довольно редко. Например, наиболее повторяемой буквой русского языка является буква «о». Для английского языка такой буквой является буква «е». Наименее повторяемой в осмысленном тексте русского языка является буква «ъ».

Естественно, указанная статистика проявляется на достаточно больших по объему текстах, но отмеченная закономерность используется злоумышленниками для взлома шифра без знания ключа.

Возьмем достаточно длинный осмысленный текст, написанный на русском языке, в котором содержится N букв. Решим рутинную задачу, определяя и суммируя появление каждой буквы в тексте. Пусть буква «а» в итоговом результате имеет значение накопленной суммы N_a, тогда частота ее появления для данного текста будет определяться отношением $\frac{N_a}{N}$. Подводя общий итог, можно заметить, что результатом эксперимента является цепочка неравенств вида

$$\frac{\mathrm{N_о}}{\mathrm{N}} > \frac{\mathrm{N_а}}{\mathrm{N}} > \ldots > \frac{\mathrm{N_ъ}}{\mathrm{N}}. \qquad (2.1)$$

Указанную закономерность можно представить в виде гистограммы (рис. 2.5).

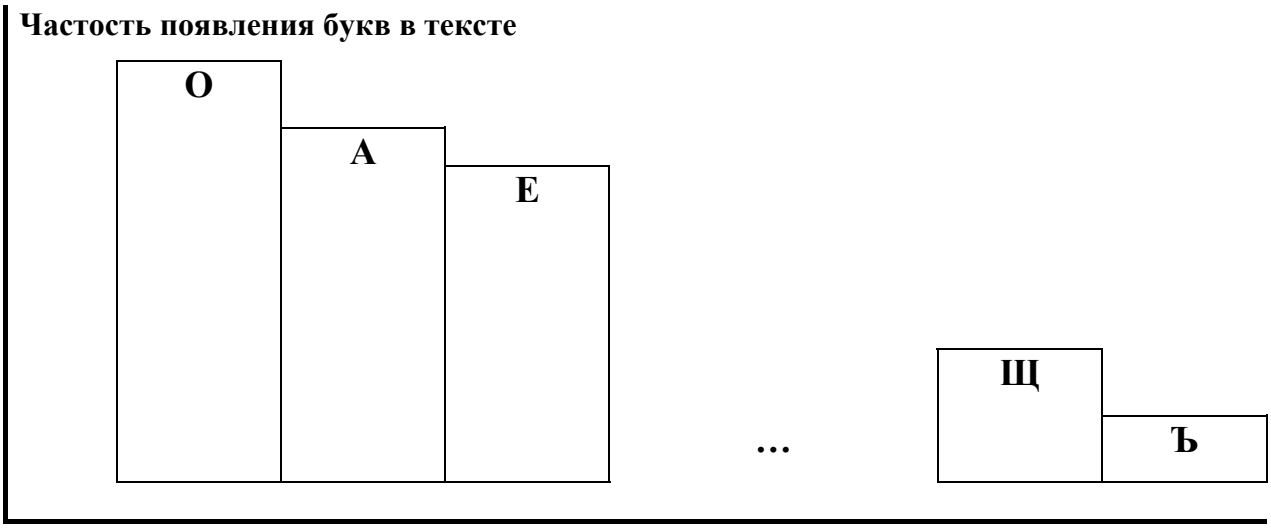


Рис. 2.5. Гистограмма появления букв в тексте русского языка

Анализ зашифрованного сообщения с использованием данной закономерности получил название частотного анализа.

Принцип частотного анализа использовался выдающимися писателями

А. Конан Дойлом в рассказе «Пляшущие человечки» и Э. По в рассказе «Золотой жук», когда главные герои этих произведений вскрывали содержание текстов, одинаковые буквы которых заменялись на некие условные знаки (другие буквы), всегда одинаковые для одних и тех же букв исходного текста. Правила замены были понятен только отправителю сообщения и его получателю. В общей классификации шифров подобное преобразование исходного текста получило название шифра замены.

Известно, что код Морзе, используемый в слуховой радиосвязи, является неравномерным кодом, адаптированным к английскому языку. Его приспособленность заключается в том, что наиболее употребляемая буква этого языка «е» передается самым коротким знаком азбуки Морзе – единственной точкой [14].

Из сказанного можно сделать вывод: замена одних и тех же букв алфавита в скрываемом тексте на другие знаки (буквы), но всегда одни и те же для данной буквы алфавита, однозначно взламывается злоумышленником, который в своих действиях использует статистику языка, на котором написано сообщение.

Другим важным выводом является то, что шифрование одного открытого осмысленного текста другим осмысленным текстом не приводит к существенному нарушению статистики языка и лишь не намного увеличивает время взлома первого и второго сообщения с использованием частотного анализа.

2.2.4. Свойства схемы наложения шифра

Применительно к ЭВМ каждый знак текста, набранный пользователем, представляется одним байтом. Предположим, что используется алфавит русского языка. Тогда для представления в двоичной форме 32 основных букв такого алфавита требуется всего 5 бит, т. к. $2^5=32$ [9]. Без потери общности рассуждений представим в виде таблицы 2.1 условное соответствие некоторых

букв кириллицы набору двоичных символов. Из таблицы исключены буквы Ё, Й и Ъ.

Таблица 2.1

Соответствие букв кириллицы набору двоичных символов

Буквы алфавита	Двоичный код	Буквы алфавита	Двоичный код	Буквы алфавита	Двоичный код
А	00001	Л	01011	Х	10101
Б	00010	М	01100	Ц	10110
В	00011	Н	01101	Ч	10111
Г	00100	О	01110	Ш	11000
Д	00101	П	01111	Щ	11001
Е	00110	Р	10000	Ы	11010
Ж	00111	С	10001	Ь	11011
З	01000	Т	10010	Э	11100
И	01001	У	10011	Ю	11101
К	01010	Ф	10100	Я	11110

Пусть источник информации сформировал сообщение, котором содержится слово …ПОБЕДА… и пусть для зашифрования этого слова источником ключа сформирована последовательность …КМЫХЬЮ…. В схеме наложения шифра буква «К» преобразует букву открытого текста «П» в другую. Преобразование, как правило, осуществляется по модулю некоторого числа. В ЭВМ такое преобразование осуществляется по модулю числа два.

Обычно схема сложения по модулю два представляется в терминах алгебры логики как схема неравнозначности, которая формально выполняет операцию вида $Y = X_1 \cdot \overline{X}_2 + \overline{X}_1 \cdot X_2$ (таблица 2.2).

Таблица 2.2

Таблица состояний схемы сложения по модулю два

X_1	X_2	Y
0	0	0
0	1	1
1	0	1
1	1	0

Заметно, что при сложении одинаковых значений X_i результирующее значение равно нулю. Представим исходный текст в виде таблицы соответствия между буквами алфавита и соответствующими наборами двоичного кода:

П	О	Б	Е	Д	А
01111	01110	00010	00110	00101	00001

Такую же таблицу получим для символов источника ключа.

К	М	Ы	Х	Ь	Ю
01010	01100	11010	10101	11011	11101

Результат работы схемы наложения шифра представляется таблицей 2.3, которая не требует особых комментариев. В результате по каналу связи будет передан зашифрованный текст … ДБШУЯЭ….

Таблица 2.3

Результат работы схемы наложения шифра

Символы открытого текста (ОТ)	П	О	Б	Е	Д	А
Символы ключа (К)	К	М	Ы	Х	Ь	Ю
Двоичное представление ОТ	01111	01110	00010	00110	00101	00001
Двоичное представление К	01010	01100	11010	10101	11011	11101
Двоичное представление криптограммы	00101	00010	11000	10011	11110	11100
Символы зашифрованного текста	Д	Б	Ш	У	Я	Э

Замечательным свойством схемы сложения по модулю два является то, что операция сложения символов равносильна операции вычитания. Это позволяет схему снятия шифра на приемной стороне построить по принципу схемы наложения шифра. Суть работа такой схемы представлена таблицей 2.4.

Таблица 2.4

Результат работы схемы снятия шифра

Символы зашифрованного текста	Д	Б	Ш	У	Я	Э
Двоичное представление криптограммы	00101	00010	11000	10011	11110	11100
Двоичное представление К	01010	01100	11010	10101	11011	11101
Двоичное представление ОТ	01111	01110	00010	00110	00101	00001
Символы ключа (К)	К	М	Ы	Х	Ь	Ю
Символы открытого текста (ОТ)	П	О	Б	Е	Д	А

Очевидно, что во всех представленных последовательностях должна соблюдаться строгая синхронизация между символами. Например, если в таблице 2.3 двоичное представление ключа или зашифрованного текста сместить всего на один символ, то рашифрование текста не произойдет. Получатель увидит набор знаков, лишенный какого-либо смысла. Схемы подобного типа находят применение в реальных системах защиты, т. е. проблемы снятия и наложения шифра принципиально решены.

2.2.5. Свойства источника ключа

Под ключом в криптографии понимают сменный элемент шифра, который применяется для шифрования конкретного сообщения. Безопасность защищаемой информации определяется в первую очередь именно этим элементом схемы шифрования. Сам шифр, шифрмашина или принцип шифрования стали считать известными противнику и доступными для предварительного изучения, но в них появился неизвестный для противника ключ, от которого существенно зависят применяемые преобразования информации. Теперь законные пользователи, прежде чем обмениваться шифрованными сообщениями, должны тайно от противника обменяться ключами или установить одинаковый ключ на обоих концах канала связи.

В общей схеме шифрования должен присутствовать недоступный противнику секретный канал связи для обмена ключами. Создать такой канал связи вполне реально, поскольку нагрузка на него при наличии малого числа пользователей, вообще говоря, небольшая. Подобные схемы получили название систем шифрования с частными ключами, а сами системы называются симметричными, т. к. обе связывающиеся стороны имеют один и тот же ключ.

Для противника появляется новая задача – определить ключ, после чего можно легко прочитать зашифрованные на этом ключе сообщения.

Отметим, что не существует единого шифра, подходящего для всех случаев. Выбор способа шифрования зависит от особенностей информации, ее ценности и возможностей владельцев по защите своей информации. Прежде всего, подчеркнем большое разнообразие видов защищаемой информации: документальная, телефонная, телевизионная, компьютерная и т. д. Каждый вид информации имеет свои специфические особенности, и эти особенности сильно влияют на выбор методов шифрования информации. Большое значение имеют объемы и требуемая скорость передачи шифрованной информации. Выбор вида шифра и его параметров существенно зависит от характера защищаемых секретов или тайны. Некоторые тайны (например, государственные, военные и др.) должны сохраняться десятилетиями, а некоторые (например, биржевые) – уже через несколько часов можно разгласить. Необходимо учитывать также и возможности того противника, от которого защищается данная информация. Одно дело – противостоять одиночке или даже банде уголовников, а другое дело – мощной государственной структуре.

Способность шифра противостоять всевозможным атакам на него называют *стойкостью шифра.*

Под *атакой на шифр* понимают попытку вскрытия этого шифра.

Понятие стойкости шифра является центральным для криптографии. Хотя качественно понять его довольно легко, но получение строгих доказуемых оценок стойкости для каждого конкретного шифра – проблема нерешенная. Это объясняется тем, что до сих пор нет необходимых для решения такой проблемы математических результатов. (Мы вернемся к обсуждению этого вопроса ниже.) Поэтому стойкость конкретного шифра оценивается только путем всевозможных попыток его вскрытия и зависит от квалификации *криптоаналитиков,* атакующих шифр. Такую процедуру иногда называют *проверкой стойкости* [16].

Важным подготовительным этапом для проверки стойкости шифра является продумывание различных предполагаемых возможностей, с помощью которых противник может атаковать шифр. Появление таких возможностей у противника обычно не зависит от криптографии, это является некоторой внешней подсказкой и существенно влияет на стойкость шифра. Поэтому оценки стойкости шифра всегда содержат те предположения о целях и возможностях противника, в условиях которых эти оценки получены.

Прежде всего, как это уже отмечалось выше, обычно считается, что противник знает сам шифр и имеет возможности для его предварительного изучения. Противник также знает некоторые характеристики открытых текстов, например, общую тематику сообщений, их стиль, некоторые стандарты, форматы и т. д.

Из более специфических приведем еще три примера возможностей противника:

– противник может перехватывать все шифрованные сообщения, но не имеет соответствующих им открытых текстов;

– противник может перехватывать все шифрованные сообщения и добывать соответствующие им открытые тексты;

– противник имеет доступ к шифру (но не к ключам!) и поэтому может зашифровывать и дешифровывать любую информацию.

В заключение данного раздела сделаем еще одно замечание – о терминологии. В последнее время наряду со словом «криптография» часто встречается и слово «криптология», но соотношение между ними не всегда понимается правильно. Сейчас происходит окончательное формирование этих научных дисциплин, уточняются их предмет и задачи.

Криптология – наука, состоящая из двух ветвей: криптографии и криптоанализа.

Криптография – наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей.

Криптоанализ – наука (и практика ее применения) о методах и способах вскрытия шифров.

Соотношение криптографии и криптоанализа очевидно: криптография - защита, т. е. разработка шифров. Криптоанализ - нападение, т. е. атака на шифры. Однако эти две дисциплины связаны друг с другом, и не бывает хороших криптографов, не владеющих методами криптоанализа.

В завершении отметим, что процедура шифрования исходного текста осуществляется на прикладном уровне эталонной модели взаимодействия открытых систем.

2.2.6. Примеры шифрования

Известны случаи, когда криптография считалась даже черной магией. Этот период развития криптографии как искусства длился с незапамятных времен до начала XX века, когда появились первые шифровальные машины. Понимание математического характера решаемых криптографией задач пришло только в середине XX века – после работ выдающегося американского ученого К. Шеннона.

Свой след в истории криптографии оставили многие хорошо известные исторические личности. Первые сведения об использовании шифров в военном

деле связаны с именем спартанского полководца Лисандра (шифр «Сцитала»). Цезарь использовал в переписке шифр, который вошел в историю как «шифр Цезаря». В древней Греции был изобретен вид шифра, который в дальнейшем стал называться «квадрат Полития». Одну из первых книг по криптографии написал аббат И. Трителий (1462 – 1516), живший в Германии. В 1566 году известный математик Д. Кардано опубликовал работу с описанием изобретенной им системы шифрования («решетка Кардано»). Франция XVI века оставила в истории криптографии шифры короля Генриха IV и Ришелье.

Рассмотрим более подробно примеры, отражающие логику развития представляемой предметной области.

Шифр «Сцитала». Этот шифр известен со времен войны Спарты против Афин в V веке до н. э. [7] Для его реализации использовалась сцитала – жезл, имеющий форму цилиндра. На сциталу виток к витку наматывалась узкая папирусная лента (без просветов и нахлестов), а затем на этой ленте вдоль оси сциталы записывался открытый текст. Лента разматывалась и получалось (для непосвященных), что поперек ленты в беспорядке написаны какие-то буквы. Затем лента отправлялась адресату. Адресат брал такую же сциталу, таким же образом наматывал на нее полученную ленту и читал сообщение вдоль оси сциталы.

Отметим, что в этом шифре преобразование открытого текста в шифрованный заключается в определенной перестановке букв открытого текста.

Поэтому класс шифров, к которым относится и шифр «Сцитала», называется *шифрами перестановки.*

Шифр подобного класса можно получить иным путем. Пусть необходимо зашифровать фразу: «Это слово будет зашифровано». В такой простой фразе просматривается закономерность относительно частости повторения отдельных букв языка (см. таблицу 2.5).

Таблица 2.5

Простой перестановочный шифр

Э	Т	О	С	Л	О
В	О	Б	У	Д	Е
Т	З	А	Ш	И	Ф
Р	О	В	А	Н	О

Передадим в канал связи криптограмму, разбив ее для удобства представления на пятизначные группы:

ЭВТРТ ОЗООБ АВСУШ АЛДИН ОЕФОФ.

Заметно, что криптограмма совершенно не стойкая относительно частного анализа. Данный шифр с позиций современной криптографии наивен. Шифр можно усилить за счет перестановки столбцов по ключевому слову.

Другим простым типом шифра является шифр замены (трансформационный шифр). Каждый символ в сообщении заменяется в зашифрованном тексте другим символом. Символы для зашифрованного текста обычно берутся из того же алфавита, что и для сообщения, но это не обязательно. Система называется *моноалфавитной* из-за того, что каждый символ сообщения всегда преобразуется в один и тот же символ зашифрованного текста (статистика языка сохраняется) [17].

Рассмотрим шифр Цезаря. Этот шифр реализует следующее преобразование открытого текста: каждая буква открытого текста заменяется третьей после нее буквой в алфавите, который считается написанным по кругу, т. е. после буквы «я» следует буква «а». Отметим, что Цезарь заменял букву третьей после нее буквой, но можно заменять и какой-нибудь другой. Главное, чтобы тот, кому посылается шифрованное сообщение, знал эту величину сдвига. Класс шифров, к которым относится и шифр Цезаря, называется *шифрами замены*.

Для иллюстрации такого шифра создадим таблицу замены, получившей название таблицы Веженера. Таблица приведена в Приложении. Поступим по правилу Цезаря и зашифруем ранее приведенную фразу. Для этого в первом столбце будем брать буквы открытого текста, а в качестве ключа возьмем букву «Г». Получим криптограмму вида

АХСФО СЕСДЦ ЗИХЛГ ЬМЧУС ЕГРСД.

В этой криптограмме подозрительно часто употребляется буква «С», т. е. сохраняется признак открытого текста, исходя из частости повторения букв. Вскрыть такой шифр способен даже не опытный в вопросах криптоанализа человек. Покажем это на примере. Выпишем в одну строку криптограмму и разворачивая столбцы вниз под каждой буквой напишем продолжение алфавита таким образом, чтобы в столбце оказались буквы всего алфавита с некоторым циклическим сдвигом.

В выделенной строке таблицы криптоанализа появляется сообщение, которое среди других строк таблицы имеет выраженную семантику. Более безопасной (но лишь незначительно) является произвольная подстановка, когда изменяется *порядок* подстановочных символов. Однако, хотя такая система имеет больше возможных ключей (30! вместо 30 возможных в системе Цезаря, один из которых тривиален), проблема со всеми шифрами замены состоит в том, что их очень просто атаковать с использованием частотного анализа.

Например, избыточность, свойственная английскому языку, такова, что только около 25 символов зашифрованного текста требуются для того, чтобы дешифровать сообщение. Если в зашифрованном тексте остаются пробелы, расшифровка его даже упрощается. Через эти прорехи может просачиваться и другая информация сообщения.

Применяя в качестве ключа не одну букву, а несколько, например, в виде слова, можно получить более стойкую криптограмму. Читателю представляется

возможность самостоятельно изучить данную проблему, применяя в качестве ключа двухбуквенный ключ, трехбуквенный и т. д. Ключ в форме кодового слова легко запомнить, но шифр очень беден. Одним из способов преодоления атаки частотного анализа является использование *разных* алфавитов преобразования, зависящих от позиции символа в сообщении (рис. 2.6).

А	**Х**	**С**	**Ф**	**О**	**С**	**Е**	**С**	**Д**	**Ц**	**З**	**И**	**Х**	**Л**	**Г**	**Ь**	**М**	**Ч**	**У**	**С**	**Е**	**Г**	**Р**	**С**	**Д**
Б	**Ц**	**Т**	**Х**	**П**	**Т**	**Ж**	**Т**					**Ц**							**Т**				**Т**	
В	**Ч**	**У**	**Ц**	**Р**	**У**	**З**	**У**					**Ч**							**У**				**У**	
Г	**Ш**	**Ф**	**Ч**	**С**	**Ф**	**И**	**Ф**					**Ш**							**Ф**				**Ф**	
Д	**Щ**	**Х**	**Ш**	**Т**	**Х**	**К**	**Х**					**Щ**							**Х**				**Х**	
Е	**Ы**	**Ц**	**Щ**	**У**	**Ц**	**Л**	**Ц**					**Ы**							**Ц**				**Ц**	
Ж	**Ь**	**Ч**	**Ы**	**Ф**	**Ч**	**М**	**Ч**					**Ь**							**Ч**				**Ч**	
З	**Э**	**Ш**	**Ь**	**Х**	**Ш**	**Н**	**Ш**					**Э**							**Ш**				**Ш**	
И	**Ю**	**Щ**	**Э**	**Ц**	**Щ**	**О**	**Щ**					**Ю**							**Щ**				**Щ**	
К	**Я**	**Ы**	**Ю**	**Ч**	**Ы**	**П**	**Ы**					**Я**							**Ы**				**Ы**	
Л	А	**Ь**	**Я**	**Ш**	**Ь**	**Р**	**Ь**					А							**Ь**				**Ь**	
М	**Б**	**Э**	А	**Щ**	**Э**	**С**	**Э**					**Б**							**Э**				**Э**	
Н	**В**	**Ю**	**Б**	**Ы**	**Ю**	**Т**	**Ю**					**В**							**Ю**				**Ю**	
О	**Г**	**Я**	**В**	**Ь**	**Я**	**У**	**Я**					**Г**							**Я**				**Я**	
П	**Д**	А	**Г**	**Э**	А	**Ф**	А					**Д**							А				А	
Р	**Е**	**Б**	**Д**	**Ю**	**Б**	**Х**	**Б**					**Е**							**Б**				**Б**	
С	**Ж**	**В**	**Е**	**Я**	**В**	**Ц**	**В**					**Ж**							**В**				**В**	
Т	**З**	**Г**	**Ж**	А	**Г**	**Ч**	**Г**					**З**							**Г**				**Г**	
У	**И**	**Д**	**З**	**Б**	**Д**	**Ш**	**Д**					**И**							**Д**				**Д**	
Ф	**К**	**Е**	**И**	**В**	**Е**	**Щ**	**Е**					**К**							**Е**				**Е**	
Х	**Л**	**Ж**	**К**	**Г**	**Ж**	**Ы**	**Ж**					**Л**							**Ж**				**Ж**	
Ц	**М**	**З**	**Л**	**Д**	**З**	**Ь**	**З**					**М**							**З**				**З**	
Ч	**Н**	**И**	**М**	**Е**	**И**	**Э**	**И**					**Н**							**И**				**И**	
Ш	**О**	**К**	**Н**	**Ж**	**К**	**Ю**	**К**					**О**							**К**				**К**	
Щ	**П**	**Л**	**О**	**З**	**Л**	**Я**	**Л**					**П**							**Л**				**Л**	
Ы	**Р**	**М**	**П**	**И**	**М**	А	**М**					**Р**							**М**				**М**	
Ь	**С**	**Н**	**Р**	**К**	**Н**	**Б**	**Н**					**С**							**Н**				**Н**	
Э	**Т**	**О**	**С**	**Л**	**О**	**В**	**О**	.	.	.	.	**Т**	.	.	.	.	.	.	**О**	.	.	.	**О**	.
Ю	**У**	**П**	**Т**	**М**	**П**	**Г**	**П**					**У**							**П**				**П**	
Я	**Ф**	**Р**	**У**	**Н**	**Р**	**Д**	**Р**					**Ф**							**Р**				**Р**	

Рис. 2.6. Пример взлома шифра Цезаря без знания ключа

Такие полиалфавитные шифры лучше, чем моноалфавитные, но они все еще уязвимы для нападения, использующего частотный анализ, когда

нападающий вычисляет длину повторения кодового слова и может затем выполнить частотный анализ для каждого алфавита индивидуально.

Важнейшим для развития криптографии был вывод К. Шеннона о существовании и единственности абсолютно стойкого шифра. Единственным таким шифром является какая-нибудь форма так называемой «*ленты однократного использования»,* в которой открытый текст «объединяется» с полностью случайным ключом такой же длины. Этот результат был доказан К. Шенноном с помощью разработанного им теоретико-информационного метода исследования шифров.

Подчеркнем, что для абсолютной стойкости существенным является каждое из следующих требований к «ленте однократного использования»:

1) полная случайность (равновероятность) ключа (это, в частности, означает, что ключ нельзя вырабатывать с помощью какого-либо детерминированного устройства);

2) равенство длины ключа и длины открытого текста;

3) однократность использования ключа.

В случае нарушения хотя бы одного из этих условий шифр, перестает быть абсолютно стойким, и появляются принципиальные возможности для его вскрытия (хотя они могут быть трудно реализуемыми).

Но, оказывается, именно эти условия и делают абсолютно стойкий шифр очень дорогим и непрактичным. Прежде чем пользоваться таким шифром, необходимо обеспечить всех абонентов достаточным запасом случайных ключей и исключить возможность их повторного применения. А это сделать необычайно трудно и дорого.

В силу указанных причин, абсолютно стойкие шифры применяются только в сетях связи с небольшим объемом передаваемой информации, обычно это сети для передачи особо важной государственной информации.

Теперь уже понятно, что чаще всего для защиты своей информации законные пользователи вынуждены применять неабсолютно стойкие шифры.

Такие шифры, по крайней мере, теоретически могут быть вскрыты. Вопрос только в том, хватит ли у противника сил, средств и времени для разработки и реализации соответствующих алгоритмов. Обычно эту мысль выражают так: противник с неограниченными ресурсами может вскрыть любой неабсолютно стойкий шифр.

Как же должен действовать в этой ситуации законный пользователь, выбирая для себя шифр? Лучше всего, конечно, было бы доказать, что никакой противник не может вскрыть выбранный шифр, скажем, за 10 лет и тем самым получить теоретическую оценку стойкости. К сожалению, математическая теория еще не дает нужных теорем – они относятся к нерешенной *проблеме нижних оценок вычислительной сложности задач.*

Поэтому у пользователя остается единственный путь – получение практических оценок стойкости. Этот путь состоит из следующих этапов:

– понять и четко сформулировать, от какого противника мы собираемся защищать информацию; необходимо уяснить, что именно противник знает или сможет узнать о системе шифра, а также какие силы и средства он сможет применить для его вскрытия;

– мысленно стать в положение противника и пытаться с его позиций атаковать шифр, т. е. разрабатывать различные алгоритмы вскрытия шифра; при этом необходимо в максимальной мере обеспечить моделирование сил, средств и возможностей противника;

– наилучший из разработанных алгоритмов использовать для практической оценки стойкости шифра.

Здесь полезно для иллюстрации упомянуть о двух простейших методах вскрытия шифра: случайное угадывание ключа (он срабатывает с маленькой вероятностью, зато имеет маленькую сложность) и перебор всех подряд ключей вплоть до нахождения истинного (он срабатывает всегда, зато имеет очень большую сложность). Отметим также, что не всегда нужна атака на ключ: для

некоторых шифров можно сразу, даже не зная ключа, восстанавливать открытый текст по шифрованному.

Из приведенных примеров следует, что основное внимание разработчик шифра должен уделять именно системе ключей, а исполнитель обязан строго следовать правилам применения ключей в конкретной системе шифрования.

2.2.7. Новые направления

В 1976 году была опубликована работа молодых американских математиков У. Диффи и М. Э. Хеллмана «Новые направления в криптографии», которая не только существенно изменила криптографию, но и привела к появлению и бурному развитию новых направлений в математике. Центральным понятием «новой криптографии» является понятие односторонней функции [12, 14].

Односторонней называется функция $F: X \rightarrow Y$, обладающая двумя свойствами:

а) существует полиномиальный алгоритм вычисления значений $F(x)$;

б) не существует полиномиального алгоритма *инвертирования* функции F (т. е. решения уравнения $F(x) = y$ относительно x).

Отметим, что односторонняя функция существенно отличается от функций, привычных со школьной скамьи, из-за ограничений на сложность ее вычисления и инвертирования. Вопрос о существовании односторонних функций пока открыт.

Еще одним новым понятием является понятие *функции с секретом*. Иногда еще употребляется термин *функция с ловушкой*. *Функцией с секретом К* называется функция $F_K : X \rightarrow Y$, зависящая от параметра K и обладающая тремя свойствами:

а) существует полиномиальный алгоритм вычисления значения $F_K(x)$ для любых K и x;

б) не существует полиномиального алгоритма инвертирования F_K при неизвестном *K;*

в) существует полиномиальный алгоритм инвертирования F_K при известном *K.*

Про существование функций с секретом можно сказать то же самое, что сказано про односторонние функции. Для практических целей криптографии было построено несколько функций, которые могут оказаться функциями с секретом. Для них свойство б) пока строго не доказано, но считается, что задача инвертирования эквивалентна некоторой давно изучаемой трудной математической задаче. Наиболее известной и популярной из них является теоретико-числовая функция, на которой построен шифр RSA (Райвест, Шамир, Адлеман), основанный на операциях с большими (более 100 знаков) простыми числами и их произведениями [4].

Применение функций с секретом в криптографии позволяет:

1) организовать обмен шифрованными сообщениями с использованием только открытых каналов связи, т. е. отказаться от секретных каналов связи для предварительного обмена ключами;

2) включить в задачу вскрытия шифра трудную математическую задачу и тем самым повысить обоснованность стойкости шифра;

3) решать новые криптографические задачи, отличные от шифрования *(электронная цифровая подпись* и др.).

Опишем, например, как можно реализовать п. 1). Пользователь ***A***, который хочет получать шифрованные сообщения, должен выбрать какую-нибудь функцию F_K с секретом *K.* Он сообщает всем заинтересованным корреспондентам (например, публикует) описание функции F_K в качестве своего алгоритма шифрования. Но при этом значение секрета *K* он никому не сообщает и держит его в тайне. Если теперь пользователь ***B*** хочет послать пользователю ***A*** защищаемую информацию $x \in X$, то он вычисляет $y = F_K(x)$ и посылает *y* по открытому каналу пользователю ***A***.

Поскольку ***A*** для своего секрета *K* умеет инвертировать F_K, то он вычисляет *x* по полученному *y*. Никто другой не знает *K* и поэтому в силу свойства б) функции с секретом не сможет за полиномиальное время по известному шифрованному сообщению $F_K(x)$ вычислить защищаемую информацию *x*. Описанную систему называют *криптосистемой с открытым ключом,* поскольку алгоритм шифрования F_K является общедоступным или открытым (см. рис. 2.7).

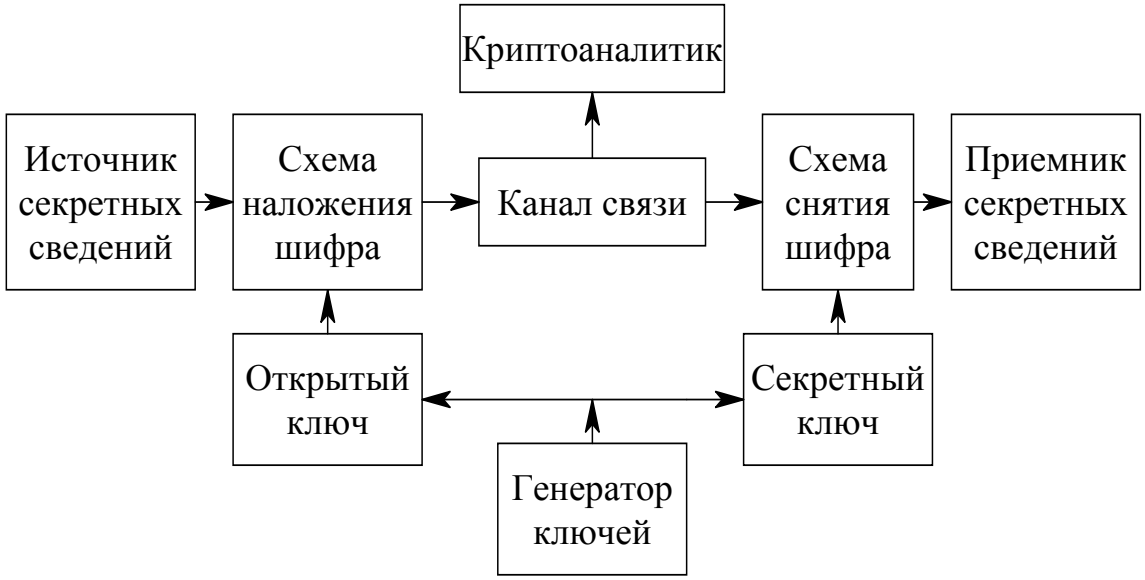


Рис. 2.7. Схема асимметричного метода шифрования

В последнее время такие криптосистемы еще называют *асимметричными,* поскольку в них есть асимметрия в алгоритмах: алгоритмы шифрования и дешифрования различны. В отличие от таких систем традиционные шифры, описанные в разделе 2.2.6, называют *симметричными:* в них ключ для шифрования и дешифрования один и тот же. Для асимметричных систем алгоритм шифрования общеизвестен, но восстановить по нему алгоритм дешифрования за полиномиальное время невозможно. Для решения задачи шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Описанную выше идею Диффи и Хеллман предложили использовать также для электронной цифровой подписи сообщений, которую невозможно подделать за полиномиальное время. Пусть пользователю ***A*** необходимо подписать сообщение *x.* Он, зная секрет *K,* находит такое *y,* что $F_K(y) = x$, и вместе с сообщением *x* посылает *y* пользователю ***B*** в качестве своей цифровой подписи. Пользователь ***B*** хранит *y* в качестве доказательства того, что ***A*** подписал сообщение *x* [9, 11].

Сообщение, подписанное цифровой подписью, можно представлять себе как пару *(x, y),* где *x* – сообщение, *y* – решение уравнения $F_K(y) = x$, $F_K(x)$: $X \to Y$ – функция с секретом, известная всем взаимодействующим абонентам. Из определения функции F_K очевидны следующие полезные свойства цифровой подписи:

1) подписать сообщение *x,* т. е. решить уравнение $F_K(y) = x$, может только абонент – обладатель данного секрета *K;* другими словами, подделать подпись невозможно;

2) проверить подлинность подписи может любой абонент, знающий открытый ключ, т. е. саму функцию F_K *;*

3) при возникновении споров отказаться от подписи невозможно в силу ее уникальности;

4) подписанные сообщения *(x, y)* можно, не опасаясь ущерба, пересылать по любым каналам связи.

Кроме принципа построения криптосистемы с открытым ключом, Диффи и Хеллман в той же работе предложили еще одну новую идею – *открытое распределение ключей.* Они задались вопросом: можно ли организовать такую процедуру взаимодействия абонентов *A* и *B* по открытым каналам связи, чтобы решить следующие задачи:

1) вначале у ***A*** и ***B*** нет никакой общей секретной информации, но в конце процедуры такая общая секретная информация (общий ключ) у ***A*** и ***B*** появляется, т. е. вырабатывается;

2) пассивный противник, который перехватывает все передачи информации и знает, что хотят получить ***A*** и ***B***, тем не менее не может восстановить выработанный общий ключ ***A*** и ***B***.

Диффи и Хеллман предложили решать эти задачи с помощью функции

$$F(x) = \alpha^x \bmod p,$$

где p – большое простое число, x – произвольное натуральное число, α – некоторый *примитивный элемент* поля Галуа $GF(p)$ [4, 5]. Общепризнанно, что инвертирование функции $\alpha^x \bmod p$, т. е. дискретное логарифмирование, является трудной математической задачей.

Сама процедура или, как принято говорить, *протокол выработки общего ключа* описывается следующим образом.

Абоненты ***A*** и ***B*** независимо друг от друга случайно выбирают по одному натуральному числу – скажем x_A и x_B. Эти элементы они держат в секрете. Далее каждый из них вычисляет новый элемент:

$$y_A = \alpha^{x_A} \bmod p, \quad y_B = \alpha^{x_B} \bmod p.$$

Числа p и α считаются общедоступными. Потом они обмениваются этими элементами по каналу связи. Теперь абонент ***A***, получив y_B и зная свой секретный элемент x_A, вычисляет новый элемент:

$$y_B^{x_A} \bmod p = (\alpha^{x_B})^{x_A} \bmod p.$$

Аналогично поступает абонент ***B***:

$$y_B^{x_B} \bmod p = (\alpha^{x_B A})^{x_B} \bmod p.$$

Тем самым у ***A*** и ***B*** появился общий элемент поля, равный $\alpha^{x_A x_B}$. Этот элемент и объявляется общим ключом ***A*** и ***B***.

Из описания протокола видно, что противник знает p, α, α^{x_A}, α^{x_B} не знает x_A и x_B и хочет узнать $\alpha^{x_A x_B}$. В настоящее время нет алгоритмов действий противника более эффективных, чем дискретное логарифмирование, а это – трудная математическая задача.

Успехи, достигнутые в разработке схем цифровой подписи и открытого распределения ключей, позволили применить эти идеи также и к другим задачам взаимодействия удаленных абонентов. Так возникло большое новое направление теоретической криптографии – криптографические протоколы.

Объектом изучения теории криптографических протоколов являются удаленные абоненты, взаимодействующие, как правило, по открытым каналам связи. Целью взаимодействия абонентов является решение какой-то задачи. Имеется также противник, который преследует собственные цели. При этом противник в разных задачах может иметь разные возможности: например, может взаимодействовать с абонентами от имени других абонентов или вмешиваться в обмены информацией между абонентами и т. д. Противником может даже оказаться один из абонентов или несколько абонентов, вступивших в сговор.

Приведем еще несколько примеров задач, решаемых удаленными абонентами.

1. Взаимодействуют два не доверяющих друг другу абонента. Они хотят подписать контракт. Это надо сделать так, чтобы не допустить следующую ситуацию: один из абонентов получил подпись другого, а сам не подписался. Протокол решения этой задачи принято называть *протоколом подписания контракта.*

2. Взаимодействуют два не доверяющих друг другу абонента. Они хотят бросить жребий с помощью монеты. Это надо сделать так, чтобы абонент, подбрасывающий монету, не мог изменить результат подбрасывания после получения догадки от абонента, угадывающего этот результат.

Протокол решения этой задачи принято называть *протоколом подбрасывания монеты.*

За последние годы криптография и криптографические методы все шире входят в нашу жизнь. Отправляя электронную почту, мы в некоторых случаях отвечаем на вопрос меню: «Нужен ли режим зашифрования?» Владелец

интеллектуальной банковской карточки, обращаясь через терминал к банку, вначале выполняет криптографический протокол аутентификации карточки. Пользователи сети Internet наверняка знакомы с дискуссиями вокруг возможного принятия стандарта цифровой подписи для тех страниц, которые содержат «критическую» информацию (юридическую, прайс-листы и др.). С недавних пор пользователи сетей стали указывать после своей фамилии наряду с уже привычным «Email ...» и менее привычное – «Отпечаток открытого ключа ...».

С каждым днем таких примеров становится все больше. Именно новые практические приложения криптографии и являются одним из источников ее развития.

2.2.8. Электронно-цифровая подпись

Важным примером криптографических алгоритмов (с открытым ключом) является электронно-цифровая подпись (ЭЦП). ЭЦП используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью. Порядок использования ЭЦП на территории Российской Федерации определен Федеральным Законом «О электронно-цифровой подписи» от 10.01.2002 № 1-ФЗ [18].
В соответствии с этим законом, ЭЦП – это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;
- конфиденциальность документов;
- установление лица, отправившего документ.

Использование ЭЦП позволяет:

- значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;

- усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;

- гарантировать достоверность документации;

- минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;

- построить корпоративную систему обмена документами.

Фактически, ЭЦП представляет собой совокупность закрытого ключа - контейнера, обладателем которого может быть только владелец сертификата, и однозначно соответствующего этому закрытому ключу открытого ключа – сертификата. Сертификат представим в виде файла формата X.509 (см. рис 2.8).

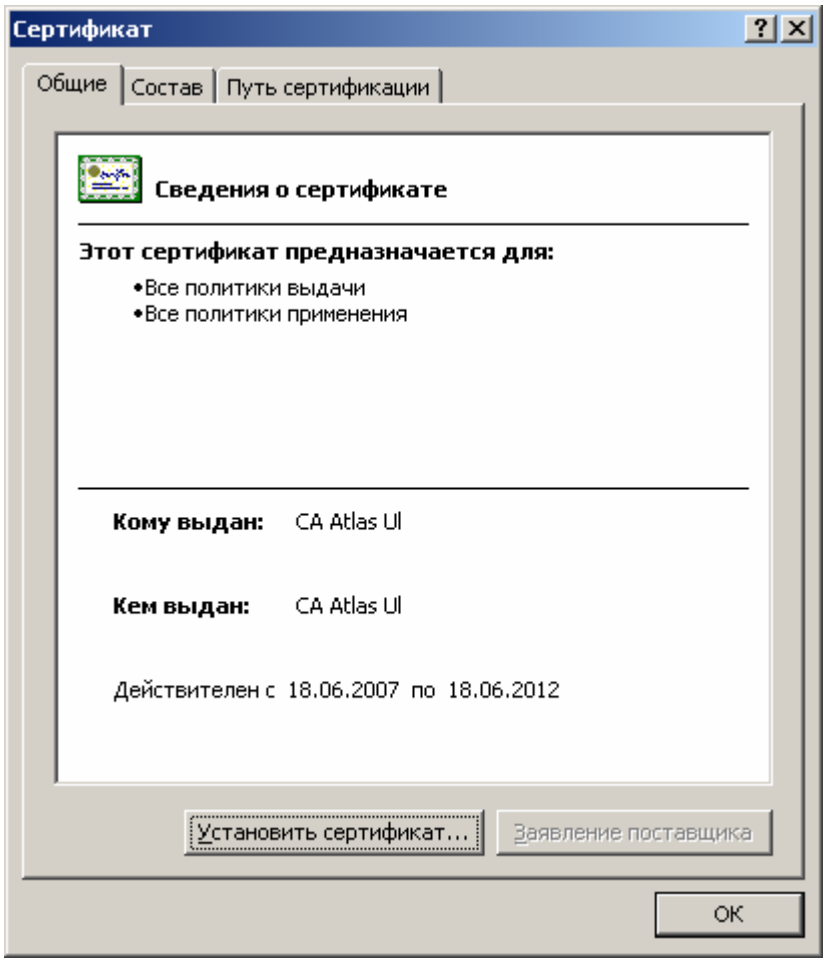


Рис. 2.8. Внешний вид сертификата ЭЦП

В отличие от закрытого ключа, который должен храниться в тайне, открытый ключ может распространяться публично.

Схема шифрования данных с использованием открытого ключа состоит из двух этапов. На первом из них производится обмен по несекретному каналу открытыми ключами. При этом необходимо обеспечить подлинность передачи ключевой информации. На втором этапе, собственно, реализуется шифрование сообщений, при котором отправитель зашифровывает сообщение открытым ключом получателя. Зашифрованный файл может быть прочитан только владельцем секретного ключа, т. е. получателем. Схема расшифрования, реализуемая получателем сообщения, использует для этого секретный ключ получателя.

Реализация схемы ЭЦП связана с вычислением хэш-функции (дайджеста) данных, которая представляет собой уникальное число, полученное из исходных данных путем его сжатия (свертки) с помощью сложного, но известного алгоритма. Хэш-функция является однонаправленной функцией, т. е. по хэш-значению невозможно восстановить исходные данные. Хэш-функция чувствительна к всевозможным искажениям данных. Кроме того, очень трудно отыскать два набора данных, обладающих одним и тем же значением хэш-функции [6].

Схема формирования подписи электронного документа его отправителем включает вычисление хэш-функции электронного документа и шифрование этого значения посредством секретного ключа отправителя. Результатом шифрования является значение ЭЦП электронного документа (реквизит электронного документа), которое пересылается вместе с самим электронным документом получателю. При этом получателю сообщения должен быть предварительно передан открытый ключ отправителя сообщения

Схема проверки (верификации) ЭЦП, осуществляемая получателем, сообщения состоит из следующих этапов. На первом из них производится расшифрование блока ЭЦП посредством открытого ключа отправителя. Затем вычисляется хэш-функция электронного документа. Результат вычисления сравнивается с результатом расшифрования блока ЭЦП. В случае совпадения

принимается решение о соответствии ЭЦП электронного документа заявленным данным. Несовпадение результатов расшифрования с результатом вычисления хэш-функции электронного документа может объясняться следующими причинами:

- в процессе передачи по каналу связи была потеряна целостность электронного документа

- при формировании ЭЦП был использован не тот (поддельный) секретный ключ;

- при проверке ЭЦП был использован не тот открытый ключ (в процессе передачи по каналу связи или при дальнейшем его хранении был модифицирован или подменен).

Реализация криптографических алгоритмов с открытыми ключами, требует по сравнению с симметричными алгоритмами, больших затрат процессорного времени. Поэтому криптография с открытыми ключами обычно используется для решения задач распределения ключей и ЭЦП, а симметричная криптография для шифрования [10].

Широко известна схема комбинированного шифрования, сочетающая высокую безопасность криптосистем с открытым ключом с преимуществами высокой скорости работы симметричных криптосистем. В этой схеме для шифрования используется случайно вырабатываемый симметричный (сеансовый) ключ, который, в свою очередь зашифровывается посредством открытой криптосистемы для его последующей передачи в начале сеанса связи.

Центральным вопросом схемы открытого распределения ключей является вопрос доверия к полученному открытому ключу партнера, который в процессе передачи или хранения может быть модифицирован или подменен. Для широкого класса практических систем (системы электронного документооборота, системы Клиент-Банк, межбанковские системы электронных расчетов), в которых возможна личная встреча партнеров до начала обмена

электронными документами, эта задача имеет относительно простое решение – взаимная сертификация открытых ключей [6].

Эта процедура заключается в том, что каждая сторона при личной встрече удостоверяет подписью уполномоченного лица и печатью бумажный документ – распечатку содержимого открытого ключа другой стороны. Этот бумажный сертификат является, во-первых, обязательством стороны использовать для проверки подписи под входящими сообщениями данный ключ, и, во-вторых, обеспечивает юридическую значимость взаимодействия. Действительно, рассмотренные бумажные сертификаты позволяют однозначно идентифицировать мошенника среди двух партнеров, если один из них захочет подменить ключи.

Таким образом, для реализации юридически значимого электронного взаимодействия двух сторон необходимо заключить договор, предусматривающий обмен сертификатами. Сертификат представляет собой документ, связывающий личностные данные владельца и его открытый ключ. В бумажном виде он должен содержать рукописные подписи уполномоченных лиц и печати.

В системах, где отсутствует возможность предварительного личного контакта партнеров, необходимо использовать цифровые сертификаты, выданные и заверенные ЭЦП доверенного посредника – удостоверяющего или сертификационного центра.

После посещения ЦС каждый из партнеров становится обладателем пары открытого и закрытого ключей. Открытый ключ ЦС позволяет его обладателю проверить подлинность открытого партнера путем проверки подлинности ЭЦП удостоверяющего центра под сертификатом открытого ключа партнера. В соответствии с Федеральным законом «Об Электронно-цифровой подписи» цифровой сертификат содержит следующие сведения:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима удостоверяющим центром вносится запись об этом в сертификат ключа подписи;
- открытый ключ ЭЦП;
- наименование средства ЭЦП, с которым используется данный открытый ключ ЭЦП;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с ЭЦП будет иметь юридическое значение.

Этот цифровой сертификат подписан на секретном ключе ЦС, поэтому любой обладатель открытого ключа ЦС может проверить его подлинность. Таким образом, использование цифрового сертификата предполагает следующую схему электронного взаимодействия партнеров. Один из партнеров посылает другому собственный сертификат, полученный из ЦС, и сообщение, подписанное ЭЦП. Получатель сообщения осуществляет проверку подлинности сертификата партнера, которая включает три обязательных этапа:

1. Проверку доверия эмитенту сертификата и срока его действия;
2. Проверку ЭЦП эмитента под сертификатом;
3. Проверку аннулирования сертификата.

В случае если сертификат партнера не утратил свою силу, а ЭЦП используется в отношениях, в которых она имеет юридическое значение, открытый ключ партнера извлекается из сертификата. На основании этого открытого ключа может быть проверена ЭЦП партнера под электронным документом. Важно отметить, что, в соответствии с Федеральным законом «Об

Электронной цифровой подписи», подтверждением подлинности ЭЦП в ЭД является положительный результат проверки соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа подписи ЦС. ЦС, обеспечивая безопасность взаимодействия партнеров, выполняет следующие функции

- регистрирует ключи ЭЦП;
- создает по обращению пользователей закрытые и открытые ключи;
- приостанавливает и возобновляет действие сертификатов ключей, а также аннулирует их;
- ведет реестр сертификатов ключей подписей, обеспечивает актуальность реестра и возможность свободного доступа пользователей к реестру;
- выдает сертификаты ключей подписей на бумажных носителях; электронные документы с информацией об их действительности.
- проводит, по обращениям пользователей, подтверждение подлинности или недействительности подписи в электронных документах в отношении зарегистрированных ЭЦП.

В ЦС создаются условия безопасного хранения секретных ключей на дорогом защищенном оборудовании, а также условия администрирования доступа к секретным ключам.

Регистрация каждой ЭЦП осуществляется на основе заявления, содержащего сведения, необходимые для выдачи сертификата, а также сведения, необходимые для идентификации ЭЦП обладателя и передачи ему сообщений. Заявление подписывается собственноручной подписью обладателя ЭЦП, содержащиеся в нем сведения подтверждаются предъявлением соответствующих документов. При регистрации проверяется уникальность открытых ключей ЭЦП в реестре и архиве ЦС.

Важно отметить, что в соответствии с законом «Об ЭЦП» владелец сертификата подписи – исключительно физическое лицо, на имя которого

удостоверяющим центром выдан сертификат ключа и которое владеет соответствующим закрытым ключом.

Кроме того, сертификат ключа подписи – электронный документ с ЭЦП уполномоченного лица удостоверяющего центра. Поэтому устойчивость всей инфраструктуры открытых ключей связана с сертификатом, выданным на уполномоченное физическое лицо. Смена работы или завершение земного пути уполномоченного лица УЦ приведет к компрометации всех сертификатов, сформированных данным УЦ.

При регистрации в ЦС оформляются на бумажных носителях два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями обладателя ЭЦП и уполномоченного лица удостоверяющего центра и печатью удостоверяющего центра. Один экземпляр выдается обладателю ЭЦП, второй остается в удостоверяющем центре.

В реальных системах каждым партнером может использоваться несколько сертификатов, выданных различными ЦС. Различные ЦС могут быть объединены инфраструктурой открытых ключей или PKI (Public Key Infrastructure). ЦС в рамках PKI обеспечивает не только хранение сертификатов, но и управление ими (выпуск, отзыв, проверку доверия). Наиболее распространенная модель PKI – иерархическая. Фундаментальное преимущество этой модели состоит в том, что проверка сертификатов требует доверия только относительно малому числу корневых ЦС. В то же время эта модель позволяет иметь различное число ЦС, выдающих сертификаты.

Отметим, что для использования ЭЦП при электронном документообороте с государственными органами, в соответствии с законодательством РФ, должны использоваться только сертифицированные средства, реализующие стандартные алгоритмы хэширования (в соответствии с ГОСТ 34.11–94), шифрования (в соответствии с ГОСТ 28147–89) и подписи (в соответствии с ГОСТ Р 34.11/34.10–2001). Наиболее распространенным средством, удовлетворяющим

этим условиям, является программа КриптоПро CSP (Версии 2.0, 3.0, 3,6). На рис. 2.9 представлен ее интерфейс.

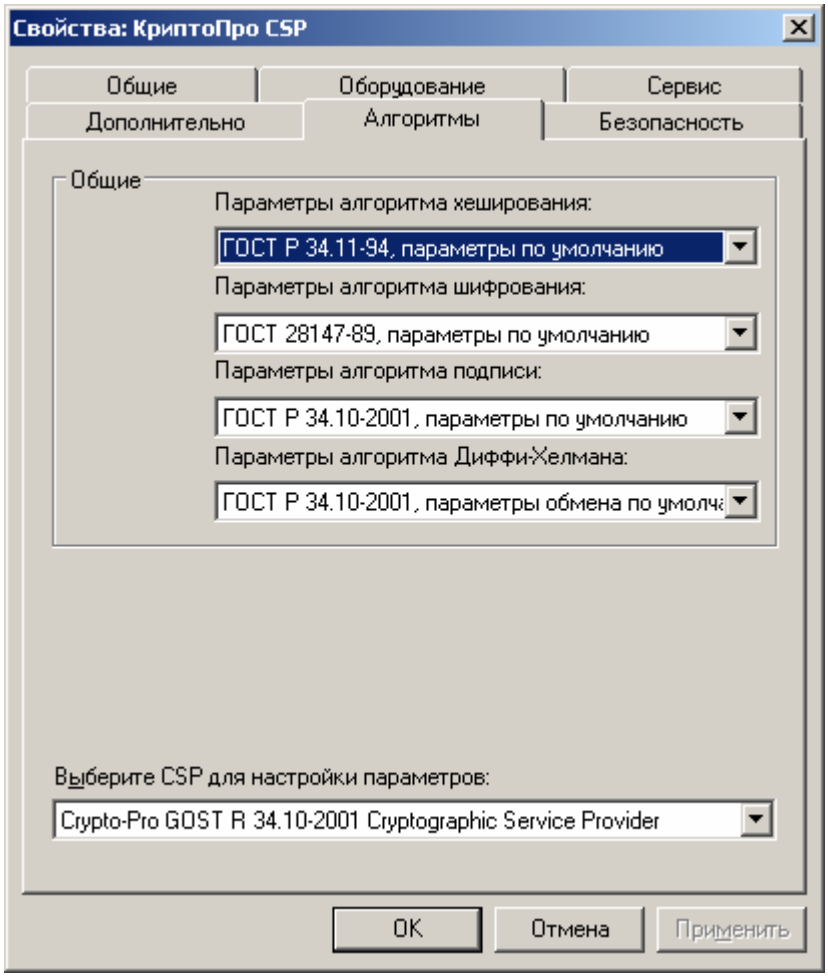


Рис. 2.9. Внешний вид программы КриптоПро

Структурно КриптоПро CSP реализован таким образом, что его алгоритмы «встраиваются» в ядро операционной системы и заменяют стандартные алгоритмы шифрования. Благодаря этому в сторонних программах, использующих ЭЦП, становится ненужной реализация алгоритмов шифрования/подписи и, соответственно, сертификация этих программ. Программы, подобные КриптоПро CSP, называют «криптопровайдерами».

2.3. Идентификация и аутентификация

Основой любых систем защиты информационных систем являются идентификация и аутентификация, так как все механизмы защиты информации

рассчитаны на работу с поименованными субъектами и объектами АС. Напомним, что в качестве субъектов АС могут выступать как пользователи, так и процессы, а в качестве объектов АС – информация и другие информационные ресурсы системы.

Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем называется *идентификацией.* Идентификация обеспечивает выполнение следующих функций:

– установление подлинности и определение полномочий субъекта при его допуске в систему,

– контролирование установленных полномочий в процессе сеанса работы;

– регистрация действий и др.

Аутентификацией (*установлением подлинности)* называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Общая процедура идентификации и аутентификации пользователя при его доступе в АС представлена на рис. 2.10. Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

По контролируемому компоненту системы способы аутентификации можно разделить на аутентификацию партнеров по общению и аутентификацию источника данных. Аутентификация партнеров по общению используется при установлении (и периодической проверке) соединения во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация источника данных – это подтверждение подлинности источника отдельной порции данных.

По направленности аутентификация может быть односторонней (пользователь доказывает свою подлинность системе, например при входе в систему) и двусторонней (взаимной).

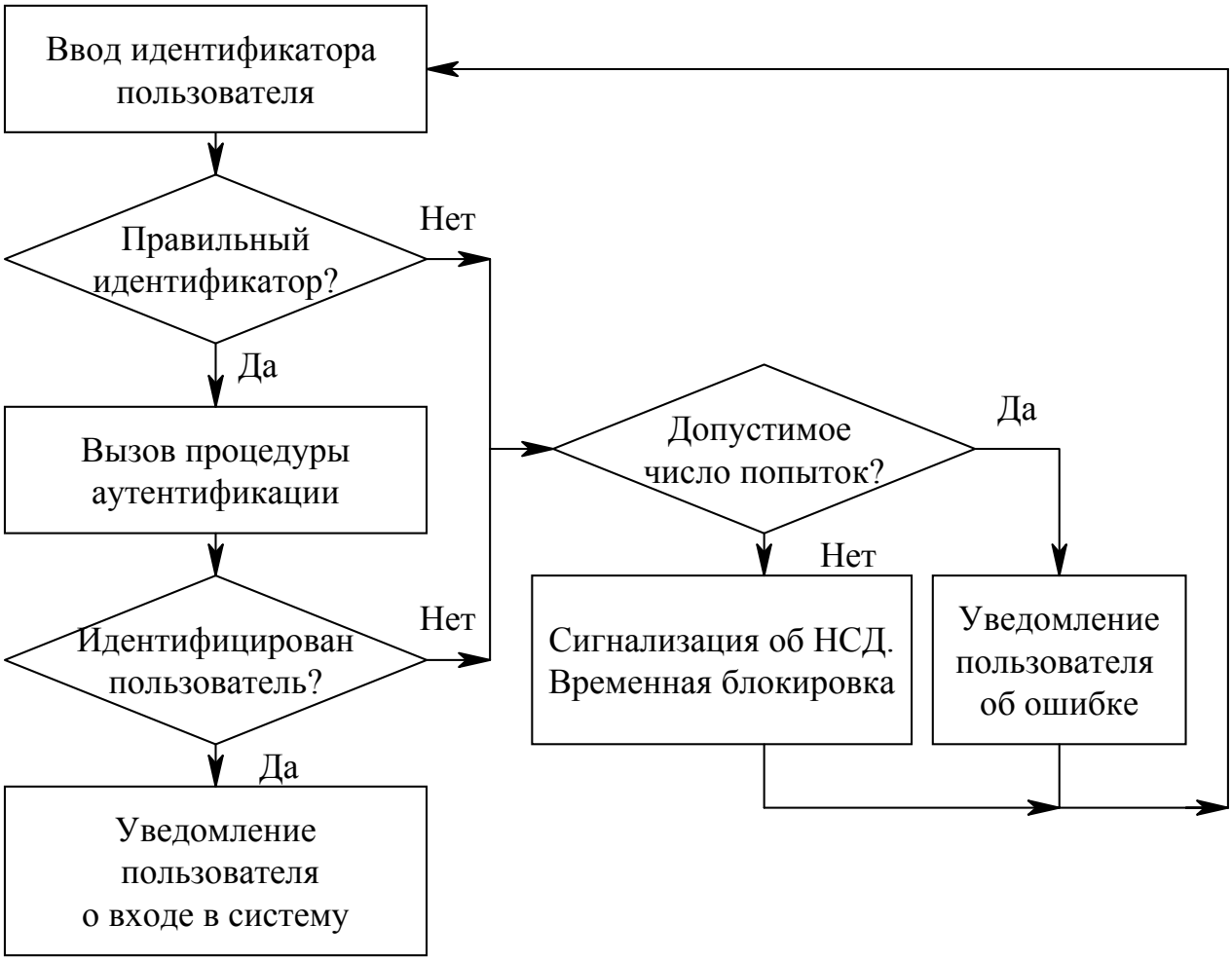


Рис. 2.10. Классическая процедура идентификации и аутентификации

Обычно методы аутентификации классифицируют по используемым средствам. В этом случае указанные методы делят на четыре группы:

1. Основанные на знании лицом, имеющим право на доступ к ресурсам системы, некоторой секретной информации – пароля.

2. Основанные на использовании уникального предмета: жетона, электронной карточки и др.

3. Основанные на измерении биометрических параметров человека – физиологических или поведенческих атрибутах живого организма.

4. Основанные на информации, ассоциированной с пользователем, например, с его координатами.

Рассмотрим эти группы.

1. Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на *паролях* – секретных идентификаторах субъектов. Здесь при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам АС.

Парольные методы следует классифицировать по степени изменяемости паролей:

– методы, использующие постоянные (многократно используемые) пароли,

– методы, использующие одноразовые (динамично изменяющиеся) пароли.

В большинстве АС используются многоразовые пароли. В этом случае пароль пользователя не изменяется от сеанса к сеансу в течение установленного администратором системы времени его действительности. Это упрощает процедуры администрирования, но повышает угрозу рассекречивания пароля. Известно множество способов вскрытия пароля: от подсмотра через плечо до перехвата сеанса связи. Вероятность вскрытия злоумышленником пароля повышается, если пароль несет смысловую нагрузку (год рождения, имя девушки), небольшой длины, набран на одном регистре, не имеет ограничений на период существования и т. д. Важно, разрешено ли вводить пароль только в диалоговом режиме или есть возможность обращаться из программы.

В последнем случае, возможно запустить программу по подбору паролей – «дробилку».

Более надежный способ – использование одноразовых или динамически меняющихся паролей.

Известны следующие методы парольной защиты, основанные на одноразовых паролях:

- методы модификации схемы простых паролей;
- методы «запрос-ответ»;
- функциональные методы.

В первом случае пользователю выдается список паролей. При аутентификации система запрашивает у пользователя пароль, номер в списке которого определен по случайному закону. Длина и порядковый номер начального символа пароля тоже могут задаваться случайным образом.

При использовании метода «запрос-ответ» система задает пользователю некоторые вопросы общего характера, правильные ответы на которые известны только конкретному пользователю.

Функциональные методы основаны на использовании специальной функции парольного преобразования $f(x)$. Это позволяет обеспечить возможность изменения (по некоторой формуле) паролей пользователя во времени. Указанная функция должна удовлетворять следующим требованиям:

- для заданного пароля *x* легко вычислить новый пароль $y = f(x)$;
- зная x и y, сложно или невозможно определить функцию $f(x)$.

Наиболее известными примерами функциональных методов являются: метод функционального преобразования и метод «рукопожатия».

Идея метода функционального преобразования состоит в периодическом изменении самой функции $f(x)$. Последнее достигается наличием в функциональном выражении динамически меняющихся параметров, например, функции от некоторой даты и времени. Пользователю сообщается исходный пароль, собственно функция и периодичность смены пароля. Нетрудно видеть, что паролями пользователя на заданных n-периодах времени будут следующие: $x, f(x), f(f(x)), \ldots, f(x)^{n-1}$.

Метод «рукопожатия» состоит в следующем. Функция парольного преобразования известна только пользователю и системе защиты. При входе в АС подсистема аутентификации генерирует случайную последовательность x, которая передается пользователю. Пользователь вычисляет результат функции $y=f(x)$ и возвращает его в систему. Система сравнивает собственный вычисленный результат с полученным от пользователя. При совпадении указанных результатов подлинность пользователя считается доказанной.

Достоинством метода является то, что передача какой-либо информации, которой может воспользоваться злоумышленник, здесь сведена к минимуму.

В ряде случаев пользователю может оказаться необходимым проверить подлинность другого удаленного пользователя или некоторой АС, к которой он собирается осуществить доступ. Наиболее подходящим здесь является метод «рукопожатия», так как никто из участников информационного обмена не получит никакой конфиденциальной информации.

Отметим, что методы аутентификации, основанные на одноразовых паролях, также не обеспечивают абсолютной защиты. Например, если злоумышленник имеет возможность подключения к сети и перехватывать передаваемые пакеты, то он может посылать последние как собственные.

2. В последнее время получили распространение комбинированные методы идентификации, требующие, помимо знания пароля, наличие карточки (token) – специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

– пассивные (карточки с памятью);

– активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает

доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двухкомпонентной аутентификацией.

Иногда (обычно для физического контроля доступа) карточки применяют сами по себе, без запроса личного идентификационного номера.

К достоинству использования карточек относят то, что обработка аутентификационной информации выполняется устройством чтения, без передачи в память компьютера. Это исключает возможность электронного перехвата по каналам связи.

Недостатки пассивных карточек следующие: они существенно дороже паролей, требуют специальных устройств чтения, их использование подразумевает специальные процедуры безопасного учета и распределения. Их также необходимо оберегать от злоумышленников, и, естественно, не оставлять в устройствах чтения. Известны случаи подделки пассивных карточек.

Интеллектуальные карточки кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты: многоразовые пароли, динамически меняющиеся пароли, обычные запрос-ответные методы. Все карточки обеспечивают двухкомпонентную аутентификацию.

К указанным достоинствам интеллектуальных карточек следует добавить их многофункциональность. Их можно применять не только для целей безопасности, но и, например, для финансовых операций. Сопутствующим недостатком карточек является их высокая стоимость.

Перспективным направлением развития карточек является наделение их стандартом расширения портативных систем PCMCIA (PC Card). Такие карточки являются портативными устройствами типа PC Card, которые вставляются в разъем PC Card и не требуют специальных устройств чтения. В настоящее время они достаточно дороги.

3. Методы аутентификации, основанные на измерении биометрических параметров человека (см. таблицу 2.6), обеспечивают почти 100 % идентификацию, решая проблемы утраты паролей и личных идентификаторов. Однако такие методы нельзя использовать при идентификации процессов или данных (объектов данных), так как они только начинают развиваться (имеются проблемы со стандартизацией и распространением), требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах и системах.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, отпечаткам ладони, формам ушей, инфракрасной картине капиллярных сосудов, по почерку, по запаху, по тембру голоса и даже по ДНК.

Таблица 2.6

Примеры методов биометрии

Физиологические методы	Поведенческие методы
• Снятие отпечатков пальцев • Сканирование радужной оболочки глаза • Сканирование сетчатки глаза • Геометрия кисти руки • Распознавание черт лица	• Анализ подписи • Анализ тембра голоса • Анализ клавиатурного почерка

Новым направлением является использование биометрических характеристик в интеллектуальных расчетных карточках, жетонах-пропусках и элементах сотовой связи. Например, при расчете в магазине предъявитель карточки кладет палец на сканер в подтверждение, что карточка действительно его.

Назовем наиболее используемые биометрические атрибуты и соответствующие системы.

- ***Отпечатки пальцев.*** Такие сканеры имеют небольшой размер, универсальны, относительно недороги. Биологическая повторяемость отпечатка пальца составляет 10^{-5} %. В настоящее время пропагандируются

правоохранительными органами из-за крупных ассигнований в электронные архивы отпечатков пальцев.

- ***Геометрия руки.*** Соответствующие устройства используются, когда из-за грязи или травм трудно применять сканеры пальцев. Биологическая повторяемость геометрии руки около 2 %.

- ***Радужная оболочка глаза.*** Данные устройства обладают наивысшей точностью. Теоретическая вероятность совпадения двух радужных оболочек составляет 1 из 10^{78}.

- ***Термический образ лица***. Системы позволяют идентифицировать человека на расстоянии до десятков метров. В комбинации с поиском данных по базе данных такие системы используются для опознания авторизованных сотрудников и отсеивания посторонних. Однако при изменении освещенности сканеры лица имеют относительно высокий процент ошибок.

- ***Голос.*** Проверка голоса удобна для использования в телекоммуникационных приложениях. Необходимые для этого 16-разрядная звуковая плата и конденсаторный микрофон стоят менее 25 $. Вероятность ошибки составляет 2 – 5%. Данная технология подходит для верификации по голосу по телефонным каналам связи, она более надежна по сравнению с частотным набором личного номера. Сейчас развиваются направления идентификации личности и его состояния по голосу – возбужден, болен, говорит правду, не в себе и т.д.

- ***Ввод с клавиатуры.*** Здесь при вводе, например, пароля отслеживаются скорость и интервалы между нажатиями.

- ***Подпись.*** Для контроля рукописной подписи используются дигитайзеры.

4. Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации, типа GPS (Global Positioning System). Пользователь, имеющий

аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить месторасположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что сводит на нет возможность их перехвата.

Аппаратура GPS проста и надежна в использовании и сравнительно недорога. Это позволяет ее использовать в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Суммируя возможности средств аутентификации, ее можно классифицировать по уровню информационной безопасности на три категории:

1. Статическая аутентификация;
2. Устойчивая аутентификация;
3. Постоянная аутентификация.

Первая категория обеспечивает защиту только от НСД в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Для компрометации статической аутентификации нарушитель может подсмотреть, подобрать, угадать или перехватить аутентификационные данные и т. д.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Усиленная аутентификация обеспечивает

защиту от атак, где злоумышленник может перехватить аутентификационную информацию и пытаться использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

2.4. Разграничение доступа

После выполнения идентификации и аутентификации необходимо установить полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования вычислительных ресурсов, доступных в АС. Такой процесс называется *разграничением (логическим управлением) доступа*.

Обычно полномочия субъекта представляются: списком ресурсов, доступных пользователю, и правами по доступу к каждому ресурсу из списка. В качестве вычислительных ресурсов могут быть программы, информация, логические устройства, объем памяти, время процессора, приоритет и т. д.

Обычно выделяют следующие методы разграничения доступа:

- разграничение доступа по спискам;
- использование матрицы установления полномочий;
- по уровням секретности и категориям;
- парольное разграничение доступа.

При ***разграничении доступа по спискам*** задаются соответствия:

– каждому пользователю – список ресурсов и прав доступа к ним или

– каждому ресурсу – список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в большинстве ОС и СУБД.

Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице (см. таблицу 2.7) строками являются идентификаторы субъектов, имеющих доступ в АС, а столбцами – объекты (информационные ресурсы) АС. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Таблица 2.7

Фрагмент матрицы установления полномочий

Субъект	Каталог d:\Heap	Программа prty	Принтер
Пользователь 1	cdrw	e	w
Пользователь 2	r		w с 9:00 до 17:00

c – создание, d – удаление, r – чтение, w – запись, e – выполнение.

Данный метод предоставляет более унифицированный и удобный подход, т. к. вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и не совсем оптимальное использование ресурсов (большинство клеток – пустые).

Разграничения доступа ***по уровням секретности и категориям*** состоят в том, что ресурсы АС разделяются в соответствии с уровнями секретности или категорий.

При разграничении по уровню секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень (гриф) секретности не выше, чем он имеет.

При разграничении по категориям задается и контролируется ранг категории, соответствующей пользователю. Соответственно, все ресурсы АС декомпозируют по уровню важности, причем определенному уровню соответствует некоторый ранг персонала (типа: руководитель, администратор, пользователь).

Парольное разграничение, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты [13]. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

На практике обычно сочетают различные методы разграничения доступа. Например, первые три метода усиливают парольной защитой.

В завершении подраздела заметим, что руководящие документы могут регламентировать два вида (принципа) разграничения доступа:

- дискретное управление доступом;
- мандатное управление доступом.

Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

Мандатное управление доступом регламентирует разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. Иначе, для реализации мандатного управления доступом каждому субъекту и каждому объекту присваивают классификационные метки, отражающие их место в соответствующей иерархии. С помощью этих меток субъектам и объектам должны быть назначены классификационные уровни, являющиеся комбинациями уровня иерархической классификации и иерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа. Ясно, что методы разграничения доступа по уровням секретности и категориям являются примерами мандатного управления доступом.

2.5. Регистрация и аудит

Регистрация представляет собой механизм подотчетности системы ОБИ, фиксирующий все события, касающиеся безопасности, такие как: вход и выход субъектов доступа, запуск и завершение программ, выдача печатных документов, попытки доступа к защищаемым ресурсам, изменение полномочий субъектов доступа и статуса объектов доступа и т. д. Эффективность системы ОБИ принципиально повышается в случае дополнения регистрации аудитом – анализом протоколируемой информации. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т. д.

Реализация механизма регистрации и аудита преследует следующие цели:

– обеспечение подотчетности пользователей и администраторов;

– обеспечение возможности реконструкции последовательности событий;

– обнаружение попыток нарушений информационной безопасности;

– предоставление информации для выявления и анализа проблем.

Кроме того, механизм регистрации и аудита является психологическим средством, напоминающим потенциальным нарушителям о неотвратимости возмездия за проступки и оплошности.

Практическими средствами регистрации и аудита могут быть следующие:

– различные системные утилиты и прикладные программы,

– регистрационный (системный или контрольный) журнал (audit trail).

Первое средство является обычно дополнением к мониторингу, осуществляемому администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал – это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата. Типовая запись регистрационного журнала представлена на рис. 2.11.

Тип записи	*Дата*	*Время*	*Терминал*	*Пользователь*	*Событие*	*Результат*

Рис. 2.11. Типовая запись регистрационного журнала

Процесс ведения регистрационного журнала состоит из четырех этапов:

1. Сбор и хранение;

2. Защита;

3. Интеграция;

4. Анализ.

На первом этапе определяются данные, подлежащие сбору и хранению, период чистки и архивации журнала, степень централизации управления, место

и средства хранения журнала, возможность регистрации шифрованной информации и др.

Регистрируемые данные должны быть защищены, в первую очередь от несанкционированной модификации и, возможно, раскрытия. Дополнительные требования по безопасности определяются концентрацией информации обо всей АС, множеством сегментов АС с различными уровнями доступа, разницей зон административной ответственности и др.

Этап интеграции необходим для объединения и согласования форматов регистрируемых данных из различных систем. Некоторые системы не имеют механизмов контроля и регистрации данных. Возможно, здесь придется разработать программы дополнительного контроля данных и программы трансформации данных в единый формат.

Самым важным этапом является анализ регистрационной информации. Известны несколько методов анализа информации с целью выявления НСД.

Статистические методы. Здесь накапливаются среднестатистические параметры функционирования подсистем (исторический профиль трафика) и сравниваются с текущими. Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз. Например, так выявляются: сбои в работе сервера из-за лавинного потока запросов (queue storm), быстро распространяемый компьютерный вирус, нарушитель, маскирующийся под легального пользователя, но ведущий себя иначе («маскарад») и др.

Эвристические методы. В данном случае в логических правилах системы поддержки принятия решений закодированы известные сценарии НСД, характеристики наблюдаемой системы, сигнализирующие о нарушениях, или модели действий, по совокупности приводящие к НСД. Понятно, что данные методы идентифицируют только известные угрозы, определенные в базе знаний системы поддержки принятия решений.

Контрольные вопросы к главе 2

1. Что понимается под антивирусными средствами в компьютерных технологиях?
2. Каковы основные пути распространения компьютерных вирусов?
3. Назовите уровни и средства антивирусной защиты.
4. Методы защиты от известных вирусов?
5. Методы защиты от неизвестных вирусов?
6. Что понимается под термином «сканер» в системе с антивирусной защитой?
7. Принципы защиты от проявления вирусов?
8. Дайте оценку антивирусного средства, установленного на Вашем личном компьютере.
9. Что понимается под проактивной защитой от вирусов?
10. Может ли быть опасным почтовый трафик?
11. Что понимается под криптографическими методами защиты информации?
12. Каковы особенности схемы шифрования с симметричным ключом?
13. Дайте определение процесса шифрования.
14. Что понимается под процедурой дешифрования?
15. Назовите свойства источника сообщений.
16. Какие требования предъявляются к источнику ключа?
17. Суть процесса взламывания шифра?
18. Особенности пассивного сценария перехвата информации?
19. Особенности активного перехвата информации?
20. Основные свойства схемы наложения шифра?
21. Что понимается под стойкостью шифра?
22. Асимметричная схема шифрования, ее особенности?
23. Суть криптосистемы с открытым ключом?

24. Дайте сравнительную характеристику для симметричной и асимметричной схем шифрования.
25. Что понимается под электронной цифровой подписью?
26. Дайте определение сертификата, используемого в электронной цифровой подписи?
27. Порядок оформления электронной цифровой подписи?
28. Дайте определение процесса идентификации пользователя в вычислительной системе.
29. Дайте определение аутентификации пользователя в вычислительной системе?
30. Дайте классификацию биометрических методов идентификации?
31. Суть системы разграничения доступа к информационным и сетевым ресурсам?
32. Что понимается под матрицей установки полномочий?
33. Что понимается под процессом регистрации?
34. Что понимается под процессом аудита?
35. Зачем необходим регистрационный журнал?
36. Предложите порядок повышения квалификации персонала в вопросах обеспечения информационной безопасности на основе анализа записей в регистрационном журнале.

3. АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На программно-технические методы защиты информации опираются организационные меры. К ним можно отнести:

1. Разработку политики безопасности;
2. Проведение анализа рисков;
3. Планирование обеспечения информационной безопасности;
4. Планирование действий в чрезвычайных ситуациях;
5. Подбор механизмов и средств обеспечения информационной безопасности.

Первые два этапа обычно трактуются как выработка политики безопасности и составляют так называемый административный уровень системы ОБИ предприятия.

Третий и четвертый этапы заключаются в разработке процедур безопасности. На этих этапах формируется уровень планирования системы ОБИ.

На последнем этапе практических мероприятий определяется программно-технический уровень системы ОБИ.

Законы и стандарты в области информационной безопасности являются лишь отправным нормативным базисом системы ОБИ информационной системы. Основой практического построения интегрированной системы является создание *административного уровня* системы, определяющего генеральное направление работ по ОБИ.

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения. Программа представляет официальную политику безопасности, отражающую собственный концептуальный подход организации к ОБИ. Конкретизация политики безопасности выражается в планах по информационной защите АС.

3.1. Разработка политики безопасности

Политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. На практике политика безопасности трактуется несколько шире – как совокупность документированных административных решений, направленных на обеспечение безопасности информационного ресурса. Результатом политики является высокоуровневый документ, представляющий систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Данный документ представляет методологическую основу практических мер (процедур) по реализации ОБИ и содержит следующие группы сведений.

1. Основные положения информационной безопасности.
2. Область применения.
3. Цели и задачи обеспечения информационной безопасности.
4. Распределение ролей и ответственности.
5. Общие обязанности.

Основные положения определяют важность ОБИ, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

Областью применения политики безопасности являются основные активы и подсистемы АС, подлежащие защите. Типовыми активами являются программно-аппаратное и информационное обеспечение АС, персонал, в отдельных случаях – информационная инфраструктура предприятия.

Цели, задачи, критерии ОБИ вытекают из функционального назначения предприятия. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности (оперативной готовности) подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т. д. Здесь указываются законы и

правила организации, которые следует учитывать при проведении работ по ОБИ.

Типовыми целями могут быть следующие:

– обеспечение уровня безопасности, соответствующего нормативным документам предприятия;

– следование экономической целесообразности в выборе защитных мер;

– обеспечение соответствующего уровня безопасности в конкретных функциональных областях АС;

– обеспечение подотчетности всех действий пользователей с информационными ресурсами и анализа регистрационной информации;

– выработка планов восстановления после критических ситуаций и обеспечения непрерывности работы АС и др.

Если предприятие не является изолированным, цели и задачи рассматриваются в более широком контексте: должны быть оговорены вопросы безопасного взаимного влияния локальных и удаленных подсистем.

В рассматриваемом документе могут быть конкретизированы некоторые стратегические принципы безопасности (вытекающие из целей и задач ОБИ). Таковыми являются стратегии действий в случае нарушения политики безопасности предприятия и сторонних организаций, взаимодействия с внешними организациями, правоохранительными органами, прессой и др. В качестве примера можно привести две стратегии ответных действий на нарушение безопасности:

– «выследить и осудить», когда злоумышленнику позволяют продолжить действия с целью его компрометации и наказания (данную стратегию одобряют правоохранительные органы!);

– «защититься и продолжить», когда организация опасается за уязвимость информационных ресурсов и оказывает максимальное противодействие нарушению.

Перечень обстоятельств, позволяющих выбрать стратегию ответных мер, приведен в таблице 3.1.

Таблица 3.1

Критерии выбора ответных мер

Защититься и продолжить	Выследить и осудить
⬩ активы ИВС недостаточно защищены; ⬩ продолжительность вторжения сопряжена с финансовым риском; ⬩ неизвестен круг пользователей; ⬩ пользователи могут привлечь к ответственности организацию ИВС за нанесенный ущерб и др.	⬩ ИВС хорошо защищена, имеются надежные средства резервирования; ⬩ наблюдаются повторяющиеся и частые атаки; ⬩ действия злоумышленника можно контролировать; ⬩ организация имеет положительный опыт работы с правоохранительными и правозащитными органами и др.

Политика безопасности затрагивает всех пользователей компьютеров в организации. Поэтому важно решить так называемые политические вопросы наделения всех категорий пользователей соответствующими правами, привилегиями и обязанностями.

Для этого определяется круг лиц, имеющий доступ к подсистемам и сервисам АС. Для каждой категории пользователей описываются правильные и неправильные способы использования ресурсов – что запрещено и разрешено. Здесь специфицируются уровни и регламентация доступа различных групп пользователей. Следует указать, какое из правил умолчания на использование ресурсов принято в организации, а именно:

– что явно не запрещено, то разрешено;

– что явно не разрешено, то запрещено.

Одним из самых уязвимых мест в ОБИ является распределение прав доступа. В политике безопасности должна быть утверждена схема управления распределением прав доступа к сервисам – централизованная или децентрализованная, или иная. Должно быть четко определено, кто

распоряжается правами доступа к сервисам и какими именно правами. Целесообразно детально описать практические процедуры наделения пользователей правами. Здесь следует указать должностных лиц, имеющих административные привилегии и пароли для определенных сервисов.

Права и обязанности пользователей определяются применительно к безопасному использованию подсистем и сервисов АС. При определении прав и обязанностей администраторов следует стремиться к некоторому балансу между правом пользователей на тайну и обязанностью администратора контролировать нарушения безопасности.

Важным элементом политики является распределение ответственности. Политика не может предусмотреть всего, однако, она должна для каждого вида проблем найти ответственного.

Обычно выделяются несколько уровней ответственности. На первом уровне каждый пользователь обязан работать в соответствии с политикой безопасности (защищать свой счет), подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях. Системные администраторы отвечают за защиту соответствующих информационно-вычислительных подсистем. Администраторы сетей должны обеспечивать реализацию организационно-технических мер, необходимых для проведения в жизнь политики безопасности АС. Руководители подразделений отвечают за доведение и контроль положений политики безопасности.

С практической точки зрения, политику безопасности целесообразно разделить на несколько уровней. Как правило, выделяют два-три уровня.

Верхний уровень носит общий характер и определяет политику организации в целом. Здесь основное внимание уделяется: порядку создания и пересмотра политики безопасности; целям, преследуемым организацией в области информационной безопасности; вопросам выделения и распределения ресурсов; принципам технической политики в области выбора методов и

средств защиты информации; координированию мер безопасности; стратегическому планированию и контролю; внешним взаимодействиям и другим вопросам, имеющим общеорганизационный характер.

На указанном уровне формулируются главные цели в области информационной безопасности (определяются сферой деятельности предприятия): обеспечение конфиденциальности, целостности и/или доступности.

Средний уровень политики безопасности выделяют в случае структурной сложности организации либо при необходимости обозначить специфичные подсистемы организации. Это касается отношения к перспективным, еще не достаточно апробированным технологиям. Например, использование новых сервисов Internet, организация связи и обработка информации на домашних и портативных компьютерах, степень соблюдения положений компьютерного права и др. Кроме того, на среднем уровне политики безопасности могут быть выделены особо значимые контуры АС организации, например, обрабатывающие секретную или критически важную информацию.

За разработку и реализацию политики безопасности верхнего и среднего уровней отвечают руководитель службы безопасности, администраторы безопасности АС, администратор корпоративной сети.

Нижний уровень политики безопасности относится к конкретным службам или подразделениям организации и детализирует верхние уровни политики безопасности. Данный уровень необходим, когда вопросы безопасности конкретных подсистем требуют решения на управленческом, а не только на техническом уровне.

Понятно, что на данном уровне определяются конкретные цели, частные критерии и показатели информационной безопасности, определяются права конкретных групп пользователей, формулируются соответствующие условия доступа к информации и т. п. Здесь из конкретных целей выводятся (обычно формальные) *правила безопасности*, описывающие, кто, что и при каких

условиях может делать или не может. Более детальные и формальные правила упростят внедрение системы и настройку средств ОБИ.

На этом уровне описываются механизмы защиты информации и используемые программно-технические средства для их реализации (в рамках, конечно, управленческого уровня, но не технического).

За политику безопасности нижнего уровня отвечают системные администраторы.

В рамках разработки политики безопасности проводится анализ рисков (risk analysis). Это делается с целью минимизации затрат на ОБИ. Напомним, что основной принцип безопасности – затраты на средства защиты не должны превышать стоимости защищаемых объектов. При этом если политика безопасности оформляется в виде высокоуровневого документа, описывающего общую стратегию, то анализ рисков (как приложение) оформляется в виде списка активов, нуждающихся в защите. Рассмотрим этап анализа риска подробнее.

3.2. Проведение анализа риска

Использование АС связано с определенной совокупностью рисков, под которыми понимаются стоимостные выражения событий (обычно вероятностных), ведущих к потерям. Если риск не приемлем, то необходимо предпринять защитные меры, не превышающие по стоимости возможный ущерб.

Анализ риска, главным образом, необходим для следующего:

- выявления уязвимости АС и ее системы защиты,
- определения необходимых и достаточных затрат на ОБИ,
- выбора конкретных мер, методов, средств и систем защиты,
- повышения информированности и компетентности персонала АС.

В целом, периодический анализ риска необходим для планирования компромисса между степенью безопасности АС и ее качественными

характеристиками: стоимость, производительность, функциональность, удобство работы, масштабируемость, совместимость и др.

3.2.1. Основные этапы анализа риска

Работа по анализу риска состоит в том, чтобы оценить величину рисков, выработать меры по их уменьшению и затем убедиться, что риски заключены в приемлемые рамки.

Анализ риска – процесс нелинейный и взаимосвязанный. Практически все его этапы связаны между собой, и по завершении почти любого из них может выявиться необходимость возврата к предыдущему.

На начальном этапе методом экспертной оценки решаются общие вопросы проведения анализа риска.

Первым делом выбираются компоненты АС и степень детальности их рассмотрения. Всеобъемлющий анализ требует рассмотрения всей информационной инфраструктуры. Но на практике из принципа разумной достаточности могут быть выделены и подвергнуты большей детализации отдельные наиболее важные компоненты и службы, в первую очередь, где риски велики или неизвестны. Более тщательному анализу подвергаются новые и модифицированные компоненты АС, а также компоненты, в которых были новые инциденты и нарушения безопасности.

Далее выбираются методологии оценки рисков как процесса получения количественной или качественной оценки ущерба, который может произойти в случае реализации угроз безопасности АС. Методологии носят частный характер, присущий организации и АС, и зависят от конкретного множества дестабилизирующих факторов и условий функционирования АС, возможности их количественной оценки, степени их неточности, неполноты, нечеткости и т. д. На практике, с учетом допустимой приближенной оценки рисков, часто используют простые наглядные методы, основанные на элементах теории вероятности и математической статистики.

Этап идентификации активов. Основу процесса анализа риска составляет определение: что надо защищать, от кого и как. Для этого выявляются активы (компоненты АС), нуждающиеся в защите. Некоторые активы (например, технические и программные средства) идентифицируются очевидным образом. Про некоторые активы (люди, расходные материалы) часто забывают. При идентификации активов могут быть затронуты и нематериальные ценности, способные, однако, пострадать от нарушения режима безопасности, например: репутация компании, моральный климат в коллективе.

В некоторых специфичных АС активы, уникальные для организации, могут быть выделены в отдельные группы, например: коммуникационное, алгоритмическое или лингвистическое обеспечение. Кроме того, могут подлежать защите части инфраструктуры, в частности подсистемы электроснабжения и др.

В процессе идентификации активов фиксируются технологии ввода, хранения, обработки и передачи информации в системе. Главным результатом процесса идентификации активов является получение детальной информационной структуры организации и способов использования информации. Дальнейшие этапы анализа риска основываются именно на данной, зафиксированной на некоторый момент времени информации.

Этап анализа угроз. После идентификации активов АС следует рассмотреть все возможные угрозы указанным активам, оценить риски и ранжировать их по степени возможного ущерба.

Под угрозой обычно понимают любое событие (действие), которое потенциально может нанести ущерб АС путем нарушения конфиденциальности, целостности или доступности информации. Угрозы могут быть преднамеренными, являющимися следствием умышленных (злонамеренных) действий людей, и непреднамеренные, вызванные ошибками

человека или сбоями и отказами работы технических и программных средств, или стихийными действиями.

При анализе угроз необходимо выявить их источники и условия реализации. Это поможет в выборе дополнительных средств защиты. Часто одни угрозы могут быть следствием или условием проявления ряда других угроз. Например, несанкционированный доступ (в различных формах его проявления) к ресурсам облегчает реализацию практически любой угрозы: от порчи магнитного носителя до комплексной удаленной атаки.

Этап оценки рисков. После идентификации угрозы необходимо оценить риск проявления угрозы. В большинстве случаев возможно получить количественную оценку риска. Она может быть получена на базе экспертного опроса, оценена статистически или рассчитана по некоторой математической зависимости (адекватной конкретной угрозе конкретному активу).

Кроме вероятности осуществления угрозы, важен размер ожидаемых потерь. В общем случае ожидаемые потери рассчитываются по следующей формуле: $e = p \cdot v$, где p – вероятностная оценка риска проявления угрозы, v – ущерб при реализации угрозы. Однако как вероятности угрозы, так и ожидаемые потери не всегда можно оценить количественно. Например, рассчитать замену компьютера достаточно просто, но трудно оценить потенциальный ущерб в случае задержки выдачи данных, искажения информации, разглашения отдельных сведений и т. д. Некоторые инциденты могут нанести ущерб репутации фирмы, вызвать социальную напряженность в коллективе, повлечь юридическое преследование предприятия со стороны пользователей и т. д.

Следует оговориться, что методы анализа риска обычно не отличаются высокой точностью. Дело в том, что основная задача анализа риска (как инструмента планирования) – оценить уровень возможных потерь и уровень затрат на защиту. Для практики, когда разнородные исходные данные имеют

приближенный или субъективный характер оценки, высокая точность расчета и не требуется. Иногда вообще невозможно оценить точность результата.

3.2.2. Выбор и проверка защитных мер

Для уменьшения размера ущерба необходим выбор соответствующих мер защиты: организационных, физических, программно-технических и др. Каждая угроза может быть предотвращена различными способами. Поэтому на данном этапе решается задача анализа и синтеза мер, методов и средств защиты по критерию эффективность/стоимость с учетом, конечно, технической политики организации и других жизненно важных характеристик АС.

После выбора способов защиты АС производится проверка их эффективности. Если остаточные риски стали опять-таки неприемлемы, весьма разумно повторить этапы анализа риска.

Завершая подраздел, следует отметить, что разработка политики безопасности и проведение анализа риска являются кропотливыми научно-техническими задачами. Поэтому важно правильно подобрать коллектив разработчиков. Обычно этим профессионально занимается группа информационной безопасности предприятия. Однако возможно привлечение администраторов и разработчиков систем и сетей, специалистов по аудиту и управлению, психологов, представителей службы режима.

3.3. Планирование мер обеспечения информационной безопасности

Политика безопасности определяет, что нужно защищать, а процедуры защиты – как надо защищать. Поэтому после определения официальной политики безопасности следует подготовить конкретизирующие ее плановые документы, описывающие практические процедуры защиты при работе АС. Таких документов обычно два:

1. План защиты.

2. План обеспечения непрерывной работы и восстановления функционирования АС.

3.3.1. План защиты

План защиты – документ, определяющий текущую реализацию системы ОБИ и необходимый в повседневной работе. План защиты периодически пересматривается с целью совершенствования и приведения в соответствии с текущим состоянием АС и системы ОБИ.

Указанный план необходим для следующего:

– определения общих правил обработки информации в АС, ее систему ОБИ, подготовку специалистов и т. п.

– фиксирования текущего состояния и состава АС и системы ОБИ,

– определения должностных обязанностей и степени ответственности сотрудников.

План может содержать следующие группы сведений:

1. Общие положения, отражающие политику безопасности;

2. Текущее состояние системы и ее уязвимость;

3. Рекомендации по реализации системы защиты;

4. Ответственность персонала;

5. Порядок ввода в действие средств защиты;

6. Порядок пересмотра средств защиты.

Следует помнить, что дублирование сведений в различных документах не допустимо. То есть в планах отражаются лишь требующие конкретизации положения политики безопасности.

В нашей стране на 2008 год стандарты и рекомендации в области информационной безопасности корпоративных сетей находятся на стадии становления. Потому основное содержание плана защиты мы рассмотрим в контексте Руководства по информационной безопасности предприятия в США .

Итак, общие положения плана отражают политику безопасности и анализ риска. Это является базой выработки процедур безопасности, в деталях описывающих шаги, предпринимаемые организацией для ОБИ.

Следующим разделом плана является детальное описание текущего состояния АС и ее уязвимости. Данный раздел является отражением анализа риска. Перечислим наиболее характерные уязвимости АС предприятия, на которые следует особо обратить внимание при составлении плана защиты, это:

- точки доступа;
- неправильно сконфигурированные системы;
- программные ошибки;
- внутренние враги.

Следует, однако, помнить, что в каждой организации есть собственные, присущие только ей, уязвимые места: для этого и проводится анализ риска.

Стержнем плана являются рекомендации по реализации системы ОБИ, т. е. реальному воплощению политики безопасности в жизнь [15]. Здесь целесообразно отметить следующие сведения:

1. *Рекомендации по выбору общих средств и способов защиты.* Выбираемые средства защиты образуют первостепенную линию обороны. Поэтому важно, чтобы средства и способы ОБИ были выбраны правильно. Например, если самой большой угрозой для АС считаются стихийные бедствия, то, видимо, нет смысла использовать биометрические устройства для аутентификации. С другой стороны, если велика опасность в несанкционированных действиях со стороны сотрудников организации, то следует сделать упор на средствах регистрации и аудита совершаемых действий.

2. *Определение стратегий защиты.* Важнейшим способом защиты активов является использование нескольких различных стратегий (принцип эшелонированности обороны). Если одна линия обороны прорвана, вступает следующая стратегия. Например, хранение съемного винчестера в личном

сейфе может удачно сочетаться с динамическим кодированием информации на нем. Комбинация из нескольких несложных стратегий может оказаться более прочной, чем один даже очень сложный метод защиты.

3. *Физическая защита.* Понятно, что свободный физический доступ является плацдармом для поражения информационного ресурса предприятия. Теоретически, одни программно-аппаратные средства не обеспечивают абсолютной защиты АС. Кроме того, некоторые механизмы безопасности выполняют свои функции исключительно при условии физической защиты. Поэтому, критически важные коммуникационные каналы, серверы, системы хранения информации и другие важные компоненты АС должны находиться в физически защищенных помещениях.

4. *Выявление неавторизованной деятельности.* Для этого могут использоваться следующие способы и средства:

Анализ сообщений пользователей. Пользователи в своей работе сталкиваются с различными некорректными ситуациями, отдельные из которых могут свидетельствовать о неавторизованной деятельности нарушителей либо собственной оплошности. Например, пользователь (соблюдающий политику безопасности) зафиксировал более поздний вход в систему, чем был на самом деле. Или пользователь обнаружил истощение или изменение личных ресурсов (памяти на диске), неудачу при входе в систему, появление неизвестных файлов или еще что-то необычное.

Отслеживание использования системы с помощью несложных пакетных файлов и программ. Такие программы можно разработать самому. К примеру, создать стандартный список пользователей и прав к ним (с помощью команд ОС) и его периодически сравнивать с текущим списком (опять же командой ОС). Обычно администратор с помощью «подручных» команд и утилит может: сравнивать текущий список активных пользователей, контролировать учетные записи с целью определения профиля использования системы (необычные записи и др.), просматривать системные средства регистрации (syslog в UNIX),

контролировать сообщения об ошибках – неудачных входах, выявлять запуск программ, которые не авторизованы или к которым нет прав у нарушителя.

Мониторинг системы администратором. Мониторинг представляет собой оперативное получение и анализ информации о состоянии АС с помощью специализированных средств контроля. Это является наиболее мощным средством выявления неавторизованной деятельности в режиме реального времени.

Ведение и анализ регистрационного журнала системы. Это позволяет фиксировать заданные события, связанные с информационной безопасностью. Важность анализа (аудита) регистрационных журналов трудно переоценить: они важны и для обнаружения и отслеживания нарушителя, выявления слабых мест в системе защиты, оптимизации производительности и безопасности, наконец, для выявления пассивных сотрудников и др.

Для мониторинга и аудита обычно требуются специализированные системы контроля и сетевые анализаторы.

5. В разделе могут быть освещены действия в случае подозрений неавторизованной деятельности, однако, подробное изложение данного вопроса представлено в плане обеспечения непрерывной работы и восстановления.

6. Правила безопасной работы персонала. Обычно правила делятся в соответствии с категориями персонала, а именно:

– правила безопасной работы, различные действия, процедуры докладов пользователей,

– правила администрирования, конфигурационного управления, процедуры сохранения/восстановления, процедуры докладов администраторов.

7. Ресурсы для предупреждения нарушений безопасности. В данном разделе описываются программные, аппаратные и процедурные ресурсы, реализующие политику безопасности. Интегрированная система безопасности корпоративной сети обычно включает следующие средства:

– системы и средства аутентификации (действия администратора, запрос-ответные парольные системы, система Kerberos, интеллектуальные карты и др.);

– средства обеспечения целостности информации (контрольные суммы, иммитовставки, хеширование);

– средства обеспечения конфиденциальности (шифрование) и средства аутентификации источника данных (электронная подпись);

– сетевые соединения, межсетевые экраны и средства ограничения сетевого доступа (шлюзовые маршрутные таблицы, фильтрующие маршрутизаторы).

Особо в плане могут быть выделены типы процедур безопасности АС предприятия.

Перечислим наиболее типичные процедуры защиты информации:

1. Проверка системной безопасности. Элементом таких проверок является ревизия политики безопасности и защитных механизмов. Примерами могут быть плановые учения и отдельные проверки некоторых процедур.

2. Процедуры управления счетами. Это необходимо для предотвращения несанкционированного доступа к системе. Должны быть процедуры управления счетами и администраторов, и пользователей. Администратор отвечает за заведение, удаление счетов и осуществляет общий контроль. Пользователь может контролировать, пользовался ли кто-нибудь его счетом.

3. Процедуры управления паролями (процедуры выбора пароля и смены пароля).

4. Процедуры конфигурационного управления.

После рекомендаций по реализации защиты в плане могут быть конкретизированы ответственность и обязанности персонала.

Заканчивается план определением общих вопросов жизненного цикла системы защиты: внедрение, эксплуатация, сопровождение и снятие с эксплуатации. Здесь могут быть определены сроки и периодичность проверки

систем защиты в соответствии с порядком пересмотра политики безопасности и анализа риска.

3.3.2. План обеспечения непрерывной работы и восстановления функционирования автоматизированной системы

Частью реакции на нарушения безопасности является предварительная подготовка ответных мер. Под этим понимается поддержание должного уровня защиты так, чтобы ущерб мог быть ограничен, а в дальнейшем исключен. Указанный план определяет действия персонала АС в критических ситуациях с целью обеспечения непрерывной работы и восстановления функционирования АС. Он должен исключить двусмысленности, возникающие во время инцидента.

Необходимость указанного плана диктуется следующим:

- предотвращением угрозы жизни людей;
- экономическими целями;
- требованиями по защите секретной, критически важной (особенно невосстановимой) информации;
- нежелательной оглаской в прессе;
- правовым аспектом (например, возможно преследование организации в судебном порядке).

Кроме того, наличие плана благотворно влияет на моральную обстановку в коллективе. Руководство знает, что при неблагоприятных условиях не придется начинать все сначала, пользователи уверены – какая-то часть их труда будет сохранена.

Обычно план состоит из двух частей, описывающих:

1. Меры реагирования на нарушения безопасности.
2. Восстановительные работы.

Меры реагирования на нарушения

Данные меры направлены на обнаружение и нейтрализацию нарушений. Они преследуют две основные цели:

- ограничение распространения угрозы и снижение ущерба,
- недопущение повторных нарушений.

В соответствии с этим строится указанная часть плана, которая содержит следующие группы сведений:

1. Основные положения.
2. Оценка инцидента.
3. Оповещение.
4. Ответные меры.
5. Правовой аспект.
6. Регистрационная документация.

В основных положениях документа формулируются цели политики безопасности в вопросах реакции на нарушения. Важно заранее определить приоритеты при решении спорных вопросов. После уяснения целей и приоритетов, они подлежат упорядочиванию по степени важности. В таблице 3.2 представлен пример типовых целей и приоритетов системы безопасности АС предприятия.

Большинство нарушений безопасности достаточно трудно идентифицируются. Для выявления нарушений безопасности в документе могут быть определены признаки нарушений. Таковыми могут быть: отказы подсистем, неестественная активность и ненормальные действия некоторых пользователей, новые файлы со странными именами, рассогласование в учетной информации, необычно низкая производительность, подозрительные пробы (многочисленные неудачные попытки входа), подозрительное изменение размеров и дат файлов или их удаление, появление новых пользовательских счетов, попытки записи в системные файлы, аномалии (звуковые сигналы и сообщения) и т. д.

Таблица 3.2

Вариант упорядочивания целей и приоритетов

Цели	Приоритеты
• Гарантировать целостность критически важных подсистем. • Сохранить и восстановить данные. • Сохранить и восстановить сервисы. • Выяснить причину инцидента. • Предотвратить развитие инцидента и будущие инциденты. • Избежать нежелательной огласки. • Найти виновников. • Наказать нарушителей.	• Защита жизни и здоровья людей. • Защита секретных и критически важных данных. • Защита прочих данных. • Предотвратить повреждение системы. • Минимизировать урон вычислительным ресурсам.

Идентификации инцидента сопутствует определение масштаба его последствия. Здесь целесообразно выяснить: затрагивает ли нарушение несколько организаций и подсистем АС, находится ли под угрозой критически важная информация, какой источник нарушения, каковы могут быть потенциальные потери, какие материальные и временные ресурсы могут понадобиться для ликвидации нарушения и др.

В плане описывается схема оповещения конкретных лиц, указывается руководство и ответственные лица, оговариваются вопросы взаимодействия с группами быстрого реагирования (собственная группа или внешняя), связи с общественностью (могут быть подготовлены пресс-релизы), с правоохранительными органами. Здесь же рекомендуется осветить стандартные формулировки докладов.

При выработке ответных мер определяются следующие процедуры:

– сдерживания распространения нарушения (как ограничить атакуемую область),

– ликвидации последствий,

– восстановление,

– анализ случившегося с извлечением уроков.

Очень важно, чтобы реакции на нарушения были зарегистрированы. По крайней мере, фиксируются: системные события (следует приобщить к документации регистрационный журнал системы), все действия с указанием времени, все телефонные разговоры.

Восстановительные работы

После нарушения следует предпринять ряд действий по восстановлению нормального функционирования АС. Этому посвящена данная часть плана. Основными положениями документа являются следующие:

1. Оперативный пересмотр политики.

2. Устранение слабостей.

3. Усвоение уроков.

4. Совершенствование политики и процедур.

Оперативный пересмотр политики начинается со следующих действий:

– переучета системных активов (как инцидент повлиял на состояние системы),

– пересмотра программы ОБИ с учетом извлеченных уроков,

– производства нового анализа риска,

– проведения следствия против нарушителей.

Самым ответственным пунктом является описание процесса восстановления и устранения слабостей системы. Здесь перечисляются следующие процедуры: определения механизма вторжения, оценки нанесенного ущерба, определения порядка восстановительных работ, подведения итогов с уяснением уроков после восстановления, определения порядка ведения журнала безопасности.

После этого описывается порядок «разбора полетов». Здесь рекомендуется составить отчет, в котором описывается инцидент и его ликвидация, описываются дополнительные ресурсы: дополнительные и новые

методы, устройства и средства защиты информации, библиотека по ОБИ. Здесь же определяется порядок формирования группы из системных администраторов, которая станет ядром службы безопасности предприятия.

В заключение документа описывается порядок пересмотра политики ОБИ и порядок доклада об инцидентах.

3.3.3. Реализация планов

Планы, как известно, являются не догмой, а руководством к действию. Поэтому рассмотрим подробнее основные *процедуры обеспечения безопасности* АС. Многие из них являются обычными действиями администраторов по поддержанию нормального функционирования системы, однако так или иначе, они связаны с информационной безопасностью.

К основным процедурам обеспечения безопасности относятся:

– проверка системы и средств безопасности; управление паролями; управление счетами; поддержка пользователей; сопровождение программного обеспечения; конфигурационное управление; резервное копирование; управление носителями; документирование.

Систематические проверки безопасности – необходимое условие надежного функционирования АС. Проверки должны включать: проведение учений и регламентные работы по контролю политики и всей системы безопасности, постоянное тестирование основных процедур, программно-аппаратных механизмов и средств. Важным элементом проверки является определение достаточной степени полноты проверок и периодичности с целью получения уверенности в защищенности АС.

Управление паролями является наиболее важной процедурой обеспечения безопасности работы пользователей. По данным CERT/CC не менее 80 % инцидентов в АС связаны с плохим выбором паролей. Процедуры управления паролями варьируются от эпизодических просьб по смене пароля

до анализа устойчивости системы аутентификации. Для последнего используются сетевые анализаторы либо программы вскрытия паролей.

Управление счетами – рутинные действия администратора по предотвращению НСД. Администратор отвечает за заведение, контроль длительности действия и ликвидацию счетов, а также осуществляет общий контроль. Важно, чтобы пользователи сами принимали активное участие в проверке безопасности собственных систем, например, отслеживали время использования своего счета. Так же, как и с паролями, администратор должен периодически контролировать легитимность использования счетов путем использования сетевых анализаторов и анализа системных журналов.

Поддержка пользователей состоит в обучении, консультировании, оказании помощи при их работе в системе, а также в контроле соблюдения ими правил безопасности и выяснении причин возникших проблем или подозрительных событий. Для обучения и консультирования могут быть определены специальные часы занятий. Для оказания помощи в работе, кроме администратора системы, может назначаться специальная группа сопровождения пользователей или группа реагирования на нарушения. Целесообразно вести учет всех вызовов пользователями. Это способствует проведению оценки и совершенствованию качества системы безопасности. Важным является выяснение причин возникших трудностей. Это позволяет оперативно выявить разного рода нарушения, в том числе неавторизованную деятельность злоумышленника.

Первая обязанность администратора – это эксплуатация и научно-техническое сопровождение вверенного ему программного обеспечения. В связи с этим, администратор должен выполнять следующие действия:

– контролировать безопасность вычислительного процесса с целью выявления компьютерных вирусов, сбоев и отказов функционирования программ и запуска неавторизованных программ и процессов;

– контролировать целостность программного обеспечения (неавторизованную модификацию) на предмет выявления программных закладок, недокументированных функций и других программных дефектов;

– обеспечивать восстановление программ с эталонных копий (возможно, с привлечением сил и средств фонда алгоритмов и программ предприятия), их обновление, замену и другие вопросы, касающиеся жизненного цикла программного обеспечения.

Процедуры конфигурационного управления. Администратор обеспечивает функциональную совместимость компонентов системы и их настройку с целью максимальной производительности и безопасности. Следует отметить, что зачастую именно ошибки в конфигурации систем являются причиной незащищенности распределенных АС. Дело в том, что конфигурирование особенно сетевых и устаревших аппаратных компонентов может быть делом очень трудным и требовать высокой квалификации технических работников. Поэтому стараются выбирать стандартные настройки подсистем. Это упрощает установку, администрирование и развитие системы, но может не соответствовать специфическим особенностям безопасности АС. Кроме того, стандартные конфигурации более уязвимы перед внешними вторжениями. Поэтому на практике нестандартное конфигурирование, как правило, используют для экранирующих систем - для исключения «стандартных» атак. Конфигурации внутренних систем, расположенных за межсетевым экраном, делают стандартными.

Резервное копирование – традиционный способ обеспечения работоспособности системы на случай порчи или утраты информационно-программного ресурса АС. При оценке возможных нарушений производится оценка возможности восстановления информации и программ и требуемые для этого ресурсы. Исходя из этого, рассчитывается периодичность и полнота создания резервных копий. Разумеется, копии должны храниться так, чтобы исключить их утрату вместе с оригиналом. Обычно их содержат в отдельных

защищенных помещениях или/и специальных сейфах на случай пожара, затопления, всплеска радиации или другого стихийного бедствия и действия злоумышленника.

Управление носителями включает процедуры по их хранению, учету, выдаче, контролю правильности использования и уничтожения носителей. Сюда относится контроль и учет выдачи информации и на печатающие устройства. На некоторых предприятиях имеются ограничения на использование определенных носителей. Например, разрешается пользоваться только зарегистрированными носителями.

Вся деятельность по безопасности отягощена документированием. Система документации очень разнообразна: от идеологии фирмы и конструкторской документации до журнала выдачи магнитных носителей и учета времени работы. Основное внимание в документировании уделяется вопросам сбора, выдачи и хранения документов. Важно выделить документы, действительно важные для безопасности системы. Последнее время наметилась тенденция в реализации безбумажной технологии – создание электронных архивов документов администратора безопасности. Однако следует знать, что в России такие документы пока не имеют юридической силы.

Контрольные вопросы к главе 3

1. Какие меры обеспечения информационной безопасности первичны относительно друг друга: организационные или программно-технические?
2. Что следует понимать под политикой безопасности?
3. Основные цели проведения политики безопасности в вычислительных системах.
4. Что понимается под процедурой анализа рисков при обеспечении информационной безопасности?
5. Основные составляющие анализа рисков?

4. ЗАКОНОДАТЕЛЬНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Информационная безопасность Российской Федерации

Наряду с политической, экономической, военной, социальной и экологической безопасностью составной частью национальной безопасности Российской Федерации является информационная безопасность.

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

Информационная сфера представляет собой совокупность информационных ресурсов и информационной инфраструктуры объекта защиты.

Совокупность хранимой, обрабатываемой и передаваемой информации, используемой для обеспечения процессов управления, называют *информационным ресурсом.*

К информационным ресурсам относятся:

- информационные ресурсы предприятий оборонного комплекса, содержащие сведения об основных направлениях развития вооружения, о научно-техническом и производственном потенциале, об объемах поставок и запасах стратегических видов сырья и материалов;
- информационное обеспечение систем управления и связи;
- информация о фундаментальных и прикладных НИР, имеющих государственное значение и др.

Информационная инфраструктура – это совокупность информационных подсистем, центров управления, аппаратно-программных

средств и технологий обеспечения сбора, хранения, обработки и передачи информации.

Информационная инфраструктура включает:

- информационную инфраструктуру центральных, местных органов государственного управления, научно-исследовательских учреждений;
- информационную инфраструктуру предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;
- программно-технические средства автоматизированных и автоматических систем управления и связи.

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Угрозы информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения, являются:

- все виды разведывательной деятельности зарубежных государств;
- информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети);
- диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;
- деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

К *внутренним угрозам*, которые будут представлять особую опасность в условиях обострения военно-политической обстановки, относятся:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях силовых структур Российской Федерации, на предприятиях оборонного комплекса;
- преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;
- ненадежное функционирование информационных и телекоммуникационных систем специального назначения;
- возможная информационно-пропагандистская деятельность, подрывающая престиж силовых структур Российской Федерации и их боеготовность;
- нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов.

К угрозам безопасности уже развернутых и создаваемых информационных и телекоммуникационных средств и систем относятся:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или

разрушение средств и систем обработки информации, телекоммуникации и связи;

- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств, предназначенных для перехвата информации, в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

Основными направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации являются:

- систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности и определение соответствующих практических задач;
- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления и связи, имеющих в своем составе элементы вычислительной техники;
- постоянное совершенствование средств защиты информации, развитие защищенных систем связи и управления, повышение надежности специального программного обеспечения;
- совершенствование структуры функциональных органов системы, координация их взаимодействия.

Оценка состояния информационной безопасности базируется на анализе источников угроз (потенциальной возможности нарушения защиты).

Деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на нее, называют *защитой информации. Объектом защиты* является информация или носитель информации, или информационный процесс, которые нужно защищать.

Защита информации организуется по трем направлениям: от утечки, от несанкционированного воздействия и от непреднамеренного воздействия (см. рис. 4.1).

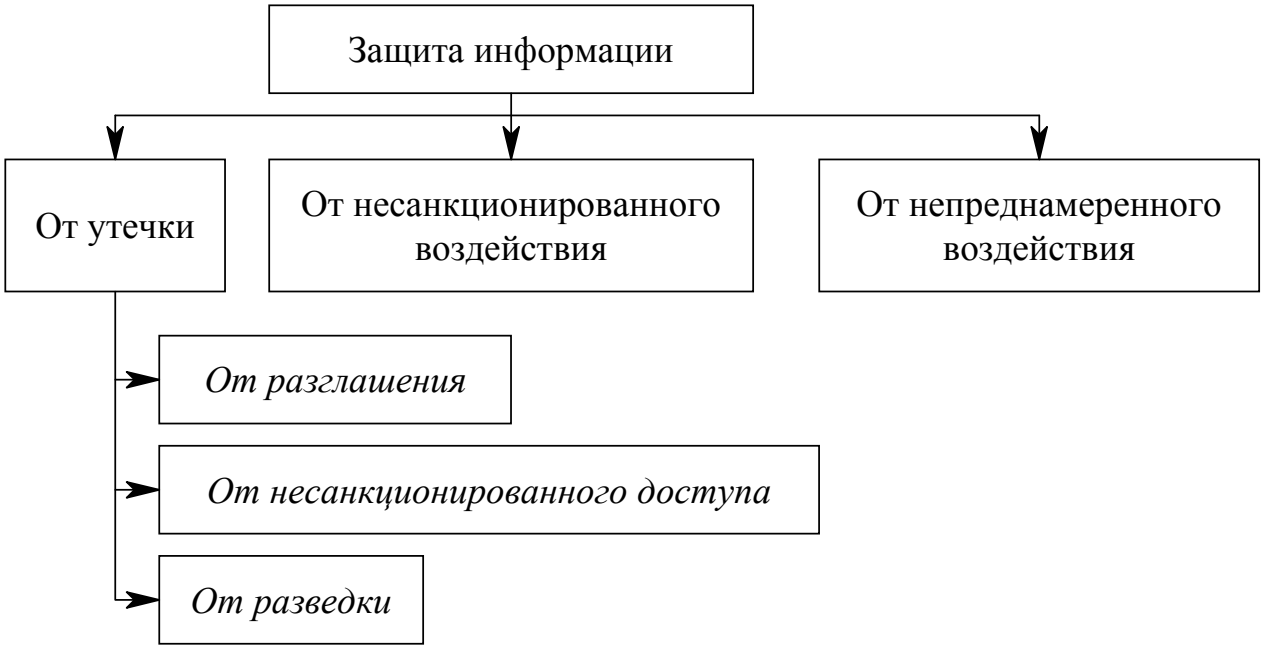


Рис. 4.1. Направления защиты информации

Первое направление – *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 разглашения* направлена на предотвращение несанкционированного доведения ее до потребителя, не имеющего права доступа к этой информации.

Защита информации *от несанкционированного доступа* направлена на предотвращение получения 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 технической разведки* направлена на предотвращение получения информации разведкой с помощью технических средств.

Второе направление – *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.

Третье направление – *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 мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате уничтожению или сбою функционирования носителя информации.

Организовать защиту информации – значит создать систему защиты информации, а также разработать мероприятия по защите и контролю эффективности защиты информации (см. рис. 4.2).

Рис. 4.2. Основная схема защиты информации

4.2. Система защиты информации

Для защиты информации создается *система защиты информации,* состоящая из совокупности органов и (или) исполнителей, используемой ими техники защиты, организованная и функционирующая по правилам,

установленным правовыми, распорядительными и нормативными документами в области защиты информации [18-23].

Государственную систему защиты информации образуют:

- Федеральная служба по техническому и экспортному контролю (ФСТЭК России) и ее центральный аппарат;
- ФСБ, МО, СВР, МВД, их структурные подразделения по защите информации;
- структурные и межотраслевые подразделения по защите информации органов государственной власти;
- специальные центры ФСТЭК России;
- организации по защите информации органов государственной власти;
- головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские учреждения;
- предприятия оборонных отраслей промышленности, их подразделения по защите информации;
- предприятия, специализирующиеся на проведении работ в области защиты информации;
- вузы, институты по подготовке и переподготовке специалистов в области защиты информации.

ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

- обеспечения безопасности информации в ключевых системах информационной инфраструктуры;
- противодействия иностранным техническим разведкам;
- обеспечения защиты информации, содержащей государственную тайну, некриптографическими способами;

- предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней;
- предотвращения специальных воздействий на информацию (ее носители) с целью ее добывания, уничтожения, искажения и блокирования доступа к ней.

Руководство деятельностью ФСТЭК России осуществляет президент РФ.

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

В органе государственной власти могут создаваться технические комиссии, межотраслевые советы.

Головные и ведущие НИО органов государственной власти разрабатывают научные основы и концепции, проекты нормативно-технических и методических документов по защите информации. На них возлагается разработка и корректировка моделей иностранных технических разведок.

Предприятия, занимающиеся деятельностью в области защиты информации, должны получить лицензию на этот вид деятельности. Лицензии выдаются ФСТЭК России, ФСБ, СВР в соответствии с их компетенцией и по представлению органа государственной власти.

Организация работ по защите информации возлагается на руководителей организаций. Для методического руководства и контроля за обеспечением защиты информации может быть создано подразделение по защите информации или назначен ответственный (штатный или внештатный) за безопасность информации.

Разработка системы ЗИ производится подразделением по технической защите информации или ответственным за это направление во взаимодействии с разработчиками и ответственными за эксплуатацию объектов ТСОИ. Для проведения работ по созданию системы ЗИ могут привлекаться на договорной

основе специализированные предприятия, имеющие соответствующие лицензии.

Работы по созданию системы ЗИ *проводятся в три этапа* (см. рис. 4.3).

На I этапе разрабатывается техническое задание на создание СЗИ:

- вводится запрет на обработку секретной (служебной) информации на всех объектах ТСОИ до принятия необходимых мер защиты;
- назначаются ответственные за организацию и проведение работ по созданию системы защиты информации;
- определяются подразделения или отдельные специалисты, непосредственно участвующие в проведении указанных работ, сроки введения в эксплуатацию системы ЗИ;
- проводится анализ возможных технических каналов утечки секретной информации;
- разрабатывается перечень защищаемых объектов ТСОИ;
- проводится категорирование ОТСС, а также ВП;
- определяется класс защищенности автоматизированных систем, участвующих в обработке секретных (служебных) данных;
- определяется КЗ;
- оцениваются возможности средств ИТР и других источников угроз;
- обосновывается необходимость привлечения специализированных предприятий для создания системы защиты информации;
- разрабатывается техническое задание (ТЗ) на создание СЗИ.

Разработка технических проектов на установку и монтаж ТСОИ производится проектными организациями, имеющими лицензию ФСТЭК.

На II этапе:

- разрабатывается перечень организационных и технических мероприятий по защите объектов ТСОИ в соответствии с требованиями ТЗ;
- определяется состав серийно выпускаемых в защищенном исполнении ТСОИ, сертифицированных средств защиты информации, а также состав технических средств, подвергаемых специальным исследованиям и проверке; разрабатываются технические паспорта на объекты ТСОИ и инструкции по обеспечению безопасности информации на этапе эксплуатации технических средств.

На III этапе осуществляются:

- проведение специальных исследований и специальной проверки импортных ОТСС, а также импортных ВТСС, установленных в выделенных помещениях;
- размещение и монтаж технических средств, входящих в состав объектов ТСОИ;
- разработка и реализация разрешительной системы доступа к средствам вычислительной техники и автоматизированным системам, участвующим в обработке секретной (служебной) информации;
- приемосдаточные испытания системы защиты информации по результатам ее опытной эксплуатации;
- аттестация объектов ТСОИ по требованиям защиты информации.

Вводится разрешение на обработку секретной информации на объектах ТСОИ, на которые получены аттестаты.

Рис. 4.3. Этапы построения системы защиты информации

4.3. Основные организационно-технические мероприятия по защите информации

Основными организационно-техническими мероприятиями, которые проводятся государственной системой защиты информации, следует считать:

- государственное лицензирование деятельности предприятий в области защиты информации;
- аттестация объектов информации по требованиям безопасности информации, предназначенная для оценки подготовленности систем и средств информатизации и связи к обработке информации, содержащей государственную, служебную или коммерческую тайну;
- сертификация систем защиты информации;
- категорирование предприятий, выделенных помещений и объектов вычислительной техники по степени важности обрабатываемой информации.

Последовательность и содержание организации комплексной защиты информации представлена на рис. 4.4.

К организационно-техническим мероприятиям, проводимым государственной системой защиты информации, также относятся:

- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах эксплуатации технических средств, подлежащих защите;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении;
- разработка и внедрение технических решений и элементов защиты информации при создании вооружения и военной техники и при проектировании, строительстве и эксплуатации объектов информатизации, систем и средств автоматизации и связи.

Рис. 4.4. Примерная схема контроля защиты информации

4.3.1. Лицензирование в области защиты информации

Лицензированием в области защиты информации называется деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации. Государственная политика в области лицензирования отдельных видов деятельности и обеспечения защиты жизненно важных интересов личности, общества и государства определяется Постановлением Правительства Российской Федерации от 24 декабря 1994 г. № 1418 «О лицензировании отдельных видов деятельности» (в ред. Постановлений Правительства РФ от 05.05.95 № 450, от 03.06.95 № 549, от 07.08.95 № 796, от 12.10.95 № 1001, от 22.04.97 № 462, от 01.12.97 № 1513, также см. постановление от 11.02.02 № 135).

Лицензией называется разрешение на право проведения работ в области защиты информации. Лицензия выдается на конкретные виды деятельности на три года, по истечении которых осуществляется ее перерегистрация в порядке, установленном для выдачи лицензии.

Лицензия выдается в том случае, если предприятие, подавшее заявку на получение лицензии, имеет условия для проведения лицензирования: производственную и испытательную базу, нормативную и методическую документацию, располагает научным и инженерно-техническим персоналом.

Организационную структуру системы государственного лицензирования деятельности предприятий в области защиты информации образуют:

- государственные органы по лицензированию;
- лицензионные центры;
- предприятия-заявители.

Государственные органы по лицензированию:

- организуют обязательное государственное лицензирование деятельности предприятий;
- выдают государственные лицензии предприятиям-заявителям;

- согласовывают составы экспертных комиссий, представляемые лицензионными центрами;
- осуществляют контроль и надзор за полнотой и качеством проводимых лицензиатами работ в области защиты информации.

Лицензионные центры:

- формируют экспертные комиссии и представляют их состав на согласование руководителям соответствующих государственных органов по лицензированию, которыми являются ФСТЭК и ФСБ;
- планируют и проводят работы по экспертизе предприятий-заявителей;
- контролируют полноту и качество выполненных лицензиатами работ.

Лицензионные центры при государственных органах по лицензированию создаются приказами руководителей этих органов. Экспертные комиссии формируются из числа компетентных в соответствующей области защиты информации специалистов отраслей промышленности, органов государственного управления, других организаций и учреждений. Экспертные комиссии создаются по одному или нескольким направлениям защиты информации.

Лицензированию ФСТЭК России подлежат:

- сертификация, сертификационные испытания защищенных технических средств обработки информации (ТСОИ), технических и программных средств защиты, средств контроля эффективности мер защиты информации, программных средств обработки, защиты и контроля защищенности;
- аттестация систем информатизации, автоматизированных систем управления, систем связи и передачи данных, объектов ВТ и выделенных помещений на соответствие требованиям руководящих и нормативных документов по безопасности информации;

- разработка, производство, реализация, монтаж, наладка, установка, ремонт, сервисное обслуживание защищенных объектов информатики, технических средств защиты и контроля эффективности мер защиты информации, защищенных программных средств обработки, защиты и контроля защищенности информации;
- проведение специальных исследований на побочные электромагнитные излучения и наводки (ПЭМИН) ТСОИ;
- проектирование объектов в защищенном исполнении.

На орган по лицензированию возлагается:

- разработка правил, процедур и нормативно-методических документов по вопросам проведения лицензирования;
- осуществление научно-методического руководства лицензионной деятельностью;
- публикация необходимых сведений о системе лицензирования;
- рассмотрение заявлений организаций и воинских частей о выдаче лицензий;
- согласование заявлений с воинскими частями, ответственными за соответствующие направления защиты информации;
- согласование состава экспертных комиссий;
- организация и проведение специальных экспертиз;
- принятие решения о выдаче лицензии;
- выдача лицензий;
- принятие решения о приостановлении, возобновлении действия лицензии или ее аннулировании;
- ведение реестра выданных, приостановленных, возобновленных и аннулированных лицензий;
- приобретение, учет и хранение бланков лицензий;

- организация работы аттестационных центров;
- осуществление контроля за полнотой и качеством проводимых лицензиатами работ.

В соответствии со статьей 17 Федерального закона от 08.08.2001 № 128-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями, введенными Федеральным законом от 02.07.2005 № 80-ФЗ) лицензированию подлежат следующие виды деятельности (в области защиты информации):

- деятельность по распространению шифровальных (криптографических) средств;
- деятельность по техническому обслуживанию шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- деятельность по разработке и (или) производству средств защиты конфиденциальной информации; деятельность по технической защите конфиденциальной информации;
- деятельность по выявлению электронных устройств, предназначенных для негласного получения информации в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

В рамках рассматриваемых видов деятельности были выпущены отдельные постановления Правительства Российской Федерации, разъясняющие порядок лицензирования. Среди них:

- Постановление Правительства Российской Федерации от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности»; Постановление Правительства Российской Федерации от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- Постановление Правительства Российской Федерации от 31.08.2006 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»;
- Постановление Правительства Российской Федерации от 23.09.2002 № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами».

В соответствии с этими документами лицензиаты обязаны ежегодно представлять в орган по лицензированию или аттестационный центр сведения о количестве выполненных работ по конкретным видам указанной в лицензии деятельности. Лицензиаты несут ответственность за полноту и качество выполняемых работ, обеспечение сохранности государственной тайны, доверенной им в ходе практической деятельности.

4.3.2. Аттестация объектов информации

Аттестацией объектов называется комплекс организационно-технических мероприятий, в результате которых посредством специального документа, «Аттестата соответствия», подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России. «Аттестат соответствия» дает право на обработку секретной информации в течение времени, установленного в «Аттестате соответствия».

ФСТЭК организует обязательную аттестацию объектов информатики, для чего:

- создает системы аттестации и устанавливает правила проведения аттестации в этих системах;
- устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;
- утверждает нормативные и методические документы по аттестации.

Органы по аттестации объектов информатизации аккредитуются ФСТЭК и получают от нее лицензию на право проведения аттестации объектов.

Под *объектом информатики* понимается отдельное техническое средство или группа технических средств, предназначенные для обработки охраняемой информации, вместе с помещениями, в которых они размещены.

Выделенные помещения (ВП) – это помещения, предназначенные для проведения закрытых мероприятий (совещаний, конференций, заседаний, сборов, переговоров и т. п.), на которых обсуждаются вопросы, содержащие охраняемые сведения.

Обязательной аттестации подлежат объекты, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. В остальных случаях аттестация носит добровольный характер.

При аттестации объекта информатики подтверждается его соответствие требованиям по защите информации:

- от несанкционированного доступа, в том числе от компьютерных вирусов;
- утечки за счет побочных электромагнитных излучений и наводок;
- специальных воздействий на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие);
- утечки информации или воздействия на нее за счет специальных устройств.

Направления испытаний представлены на рис. 4.5.

Рис. 4.5. Примерная схема направлений испытаний

4.3.3. Сертификация

Сертификация – процедура подтверждения соответствия, посредством которой независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация удостоверяет в письменной форме, что продукция соответствует установленным требованиям.

Закон «О сертификации продукции и услуг» (в ред. Федеральных законов от 27.12.95 № 211-ФЗ, от 02.03.98 № 30-ФЗ, от 31.07.98 № 154-ФЗ) устанавливает правовые основы обязательной и добровольной сертификации продукции, услуг и иных объектов (далее – продукция) в Российской

Федерации, а также права, обязанности и ответственность участников сертификации.

Сертификация осуществляется в целях:

- создания условий для деятельности организаций и предпринимателей на едином товарном рынке Российской Федерации, а также для участия в международном экономическом, научно-техническом сотрудничестве и международной торговле;
- содействия потребителям в компетентном выборе продукции;
- защиты потребителя от недобросовестности изготовителя (продавца, исполнителя);
- контроля безопасности продукции для окружающей среды, жизни, здоровья и имущества;
- подтверждения показателей качества продукции, заявленных изготовителем.

Сертификация может иметь обязательный и добровольный характер.

Под *сертификацией средств защиты информации* понимается деятельность по подтверждению соответствия этих средств требованиям государственных стандартов или иных нормативных документов по защите информации.

К средствам защиты информации относятся технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации. Обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для защиты информации, составляющей государственную тайну, и другой информации с ограниченным доступом, а также средства, используемые в управлении экологически опасными объектами.

Организационную структуру системы сертификации образуют:

- центральный орган системы сертификации (возглавляет систему сертификации однородных средств защиты информации);
- федеральный орган по сертификации средств защиты информации;
- органы по сертификации средств защиты информации (проводят сертификацию средств защиты информации);
- испытательные лаборатории (проводят сертификационные испытания средств защиты информации);
- заявители (разработчики, изготовители, поставщики, потребители средств защиты информации).

Руководящий документ ФСТЭК России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности средств вычислительной техники» устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

В соответствии с этим руководящим документом возможные показатели защищенности исчерпываются 7 классами. По классу защищенности можно судить о номенклатуре используемых механизмов защиты – наиболее защищенным является 1 класс. Выбор класса защищенности зависит от секретности обрабатываемой информации, условий эксплуатации и расположения объектов системы. В частности, для защиты конфиденциальной информации (персональных данных, служебной тайны и др.) можно применять средства защиты 5 и 6 класса (рис. 4.6).

Рис 4.6. Классификация средств защиты

Другим важным руководящим документом ФСТЭК России является «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей», который устанавливает классификацию программного обеспечения (отечественного и импортного производства) средств защиты информации по уровню контроля отсутствия в нем недекларированных возможностей. Недекларированные возможности (НДВ) – функциональные возможности программного обеспечения (ПО), не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности и целостности обрабатываемой информации (см. рис. 4.7).

Также следует отметить руководящий документ ФСТЭК России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации.

Рис. 4.7. Классификация ПО по уровням НДВ

Показатели защищенности от несанкционированного доступа к информации», который устанавливает классификацию межсетевых экранов (МЭ) по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований (см. рис. 4.8).

Рис. 4.8. Классификация межсетевых экранов

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

4.3.4. Категорирование защищаемой информации

Документированная информация категории ограниченного доступа по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную информацию.

Информация является секретной, если она содержит сведения, отнесенные к государственной тайне.

Государственной тайной называют защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Степень секретности сведений, составляющих государственную тайну, должна соответствовать степени тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведении: особой важности, совершенно секретно и секретно. *Грифом секретности* называют реквизиты (проставляются на самом носителе и (или) в сопроводительной документации на него), свидетельствующие о степени секретности сведений, содержащихся в их носителе.

К сведениям особой важности относятся сведения в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести *ущерб интересам Российской Федерации* в указанных областях.

Совершенно секретными сведениями называются сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести *ущерб интересам министерства (ведомства*) *или отрасли экономики Российской Федерации* в одной или нескольких из перечисленных областей.

К секретным сведениям следует отнести сведения, содержащие государственную тайну, распространение которых может нанести *ущерб интересам предприятия, учреждения или организации* в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной деятельности.

Конфиденциальной информацией называют документированную информацию, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальная информация может быть личной, служебной, коммерческой, судебно-следственной, профессиональной, производственной.

К *конфиденциальной личной информации* относится информация, содержащая персональные данные (сведения о фактах, событиях и обстоятельствах частной жизни гражданина), позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленном порядке.

Служебной тайной называют защищаемые сведения, не являющиеся государственной тайной, несанкционированное распространение которых служащим, которому эти сведения были доверены в связи с исполнением им должностных обязанностей, может нанести ущерб органам государственной власти, государственным предприятиям, учреждениям, организациям или нарушить их функционирование.

К *коммерческой тайне* относятся сведения, содержащие действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам. К ней нет свободного доступа на законном основании, и обладатель информации принимает меры по охране ее конфиденциальности.

Судебно-следственная конфиденциальная информация содержит сведения, составляющие тайну следствия и судопроизводства.

К профессиональной конфиденциальной информации относится информация, содержащая сведения, связанные с профессиональной

деятельностью, доступ к которым ограничен законами (врачебными, нотариальными, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений).

Производственная конфиденциальная информация содержит сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Категорированием защищаемой информации называют установление градации важности информации.

В зависимости от степени секретности обрабатываемой информации объекты ВТ и выделенные помещения также категорируются.

При определении категорий объектов информатики технические средства и системы могут быть составной частью стационарных или подвижных объектов. В пределах одной контролируемой зоны могут располагаться несколько объектов, в том числе имеющих разные категории. Категория объекта определяется высшим грифом обрабатываемой информации.

При категорировании учитывается не только степень секретности обрабатываемой информации, но и условия расположения объектов – особые или обычные.

Условия расположения считаются особыми, если объект информатики расположен на удалении менее 100 м от учреждений иностранных государств (посольств, консульств, миссий, постоянных представительств иностранных государств, офисов иностранных и совместных с инофирмами предприятий, квартир и дач их иностранных сотрудников, пользующихся экстерриториальностью).

Если объект информатики расположен на расстоянии более 100 м от учреждений иностранных государств, то условия расположения считаются обычными.

К *первой категории* относят объекты информатики, где обрабатывается информация особой важности, независимо от условий их расположения, а

также совершенно секретная информация при расположении объектов ВТ и выделенных помещений в особых условиях.

Объекты ВТ, где обрабатывается информация с грифом «совершенно секретно» при обычных условиях расположения и «секретно» в особых условиях, относятся ко *второй категории.*

Если объект ВТ расположен в обычных условиях и на объекте обрабатывается информация с грифом «секретно», то объект ВТ относится к *третьей категории.*

По требованиям обеспечения защиты информации объекты органов управления, военные и промышленные объекты делятся на 3 категории:

- первая – объекты, при строительстве, реконструкции и эксплуатации которых необходимо сокрытие или искажение информации об их местоположении, предназначении или профиле деятельности;
- вторая – объекты, на которых необходимо обеспечить защиту информации, циркулирующей в технических средствах, а также информации о разрабатываемых (производимых, испытываемых) или эксплуатируемых образцах вооружения и военной техники или о производствах и технологиях, подлежащих защите;
- третья – объекты, на которых необходимо обеспечить защиту информации, циркулирующей в технических средствах, а также предприятия, проводящие в инициативном порядке и на основе самофинансирования научно-исследовательские и опытно-конструкторские работы, необходимость защиты информации о которых может появиться в ходе проводимых работ.

Контрольные вопросы к главе 4

1. Что понимается под информационной безопасностью Российской Федерации?
2. Что понимается под информационной сферой?
3. Дайте понятие информационного ресурса.
4. Что понимается под информационной инфраструктурой?
5. Что понимается под внутренними и внешними угрозами информационной безопасности?
6. Что следует понимать под объектом защиты информации?
7. Назовите основные направления защиты информации.
8. Перечислите основные элементы схемы защиты информации?
9. Какие структуры обеспечивают государственную систему защиты информации?
10. Назовите последовательность создания системы защиты информации?
11. Основные элементы схемы контроля системы защиты информации?
12. Назовите порядок лицензирования системы защиты информации предприятия?
13. Что понимается под аттестацией объектов информации?
14. Что понимается под сертификацией средств защиты информации?
15. Как определяется категория защищаемой информации?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аксен, Б. А. Электронные системы расчетов в Internet: от реальной витрины к виртуальной / Б. А. Аксен // Конфидент. – 1996. – № 6. – С. 43-48.

2. Андерсон, Р. UEPS – электронный бумажник второго поколения /Р. Адерсон // Конфидент. – 1997. – № 1. – С. 49-53.

3. Андрианов, В. В. Защита авторства, безотказности и целостности электронных документов / В. В. Андрианов, В. Г. Калинский, Л. Н. Сапегин // Конфидент. – 1997. – № 1. – С. 80-84.

4. Анин, Б. Р. О шифровании и дешифровании / Б. Р. Анин // Конфидент. – 1997. – № 1. – С. 71-79.

5. Аснис, И. Л. Краткий обзор криптосистем с открытым ключом / И. Л. Аснис, С. В. Федоренко, К. Б. Шабунов // Защита информации. – 1994. – № 2. – С. 35-43.

6. Балакирский, В. Б. Безопасность электронных платежей / В. Б. Балакирский // Конфидент. – 1996. – № 5. – С. 47-53.

7. Балакирский, В. Б. Принципы квантовой криптографии / В. Б. Балакирский, В. И. Коржик, Д. В. Кушнир // Защита информации. – 1995. – № 3. – С. 43-51.

8. Беззубцев, О. Е. О лицензировании и сертификации в области защиты информации http://www.jetinfo/ru/1997/4/1/articlel/4/1997.html

9. Биркгоф, Г. Современная прикладная алгебра : Пер. с англ./ Г. Биркгоф, Т. Барти. – М. Мир, 1976. – 400 с.

10. Гайкович, В. Компьютерная безопасность: заметки о текущем состоянии дел / В. Гайкович // Банковские технологии. – 1997.- Июнь. – С.56-58.

11. Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко; под ред. академика РАН В. Б. Бетелина, – 4-е изд. – М.: Интернет-Университет Информационных технолгий; БИНОМ. Лаборатория знаний, 2008. – 205 с.

12. Герасименко, В. А. Защита информации в автоматизированных системах обработки данных: развитие, итоги, перспективы / В. А. Герасименко // Зарубежная радиоэлектроника. – 1993. – № 3. – С. 3-21.

13. Дергалин, Н. Л. Практика применения паролей / Н. Л. Дергалин // Защита информации. – 1995. – № 3. – С. 25-27.

14. Мельников, В. В. Защита информации в компьютерных системах / В. В. Мельников. – М.: Финансы и статистика; Электроинформ, 1997. – 367 с.

15. Оценка безопасности информационных технологий / А. П. Трубачев, И. А. Семичев, В. Н. Шакунов и др. – М.: СИП РИА, 2001. – 388 с.: ил.

16. Шеннон, К. Э. Теория связи в секретных системах / К. Э. Шеннон // Работы по теории информации и кибернетике –М.: ИЛ, 1963.-С.243-332.

17. Ященко, В. В. Введение в криптографию / Под общей ред. В. В. Ященко. – СПб.: Питер, 2001. – 288 с.: ил

Сайты по теме курса на май 2009 г.

18. Web-сервер властных структур Российской Федерации. http://www.gov.ru/

19. Web-сервер Совета безопасности РФ. http://www.scrf.gov.ru/

20. Web-сервер Федерального агентства правительственной связи и информации при Президенте Российской Федерации. http://www.fagci.ru/

21. Web-сервер Государственной технической комиссии при Президенте Российской Федерации. http://www.infotecs.ru/gtc/

22. Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и баз данных. http://www.cyberpolice.ru/

23. Web-сервер Федеральной службы по таможенному и экспортному контролю http://www.fstec.ru/

СОДЕРЖАНИЕ

Учебное издание

ГЛАДКИХ Анатолий Афанасьевич
ДЕМЕНТЬЕВ Виталий Евгеньевич

БАЗОВЫЕ ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Корректор М.В. Теленкова

Подписано в печать 25.06ю2009. Формат 60х84/16
Усл. печ. л. 10,00 Тираж 150 экз. Заказ

Ульяновский государственный технический университет
432027, Ульяновск, Северный Венец, д. 32.
Типография УлГТУ, 432027, Ульяновск, Северный Венец, д. 32.