МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»
Озерский технологический институт -
филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»
(ОТИ НИЯУ МИФИ)

Кафедра прикладной математики

Вл. Пономарев

# Методы и средства защиты информации

Учебно-методическое пособие

Озерск, 2017

УДК 681.3.06
П 56

Вл. Пономарев. Методы и средства защиты информации. Учебно-методическое пособие. Озерск: ОТИ НИЯУ МИФИ, 2017. — 97 с., ил.

В пособии кратко излагаются основы информационной безопасности, а также методы и средства защиты информации. Пособие предназначено для студентов, обучающихся по направлению подготовки 09.03.01 «Информационная и вычислительная техника», и специальности 09.05.01 «Применение и эксплуатация автоматизированных систем специального назначения».

Рецензенты:
1. Ведущий инженер-программист группы администрирования и защиты информации УИТ ФГУП «ПО «Маяк» Чуплыгин А.В.
2. Зав. кафедрой прикладной математики ОТИ НИЯУ МИФИ, к.ф.-м.н. Акопян Р.Р.

УТВЕРЖДЕНО
Редакционно-издательским
Советом ОТИ НИЯУ МИФИ

**Содержание**

# Введение

Защита компьютерной (электронной) информации — сложная и многогранная задача, решение которой охватывает множество проблем законодательного, административного, процедурного и технического характера. Описать все аспекты этой задачи детально и в полном объеме в пределах небольшого учебного пособия не представляется возможным. Поэтому пособие освещает задачу защиты информации в целом, и кратко описывает используемые при этом основные средства и методы.

В главе «Основы информационной безопасности» раскрываются основные понятия, описываются основные угрозы информационной безопасности, а также меры законодательного, административного и процедурного уровней обеспечения информационной безопасности.

В главе «Стандарты информационной безопасности» описываются важнейшие стандарты и спецификации в области информационной безопасности, руководящие документы ФСТЭК (Гостехкомисии) России, руководящие документы госкорпорации «Росатом».

В главе «Сервисы безопасности» описываются средства программно-технического уровня, которые и являются мерами, используемыми в компьютерных системах для их защиты. Всего рассматривается одиннадцать сервисов безопасности, составляющие полный набор средств, обеспечивающих требуемый уровень защиты информационных систем при условии их правильной организации. Следует отметить, что основными средствами защиты являются идентификация и аутентификация, управление доступом, протоколирование и аудит, шифрование и контроль целостности, экранирование и анализ защищенности.

В главе «Криптографические методы» кратко освещаются основные положения криптографии, приводятся известные методы шифрования, классификация криптоалгоритмов, рассматриваются два основных алгоритма: алгоритм симметричного шифрования DES и алгоритм асимметричного шифрования RSA.

В главе «Сетевые (удаленные) атаки» приводится классификация сетевых атак, рассматриваются типовые сетевые (удаленные) атаки, приводятся примеры конкретных атак.

При написании первых трех глав использовались источники [1][2], главы «Криптографические методы» — источники [3][5], а главы «Сетевые (удаленные) атаки» — источник [4].

# Основы информационной безопасности

## Необходимость защиты информации

Информация в том виде, в котором мы ее понимаем (сообщение), появилась, видимо, после появления членораздельной речи (около 40-50 тысяч лет назад), — для первых сообщений использовались различные предметы. Дары скифов были своеобразным способом передачи информации, который учёные называют предметным письмом.

Сокрытие информации в виде письменного сообщения, очевидно, зародилось с появлением письменности (примерно 4-5 тысяч лет назад). Глиняная табличка, сделанная за 1500 лет до нашей эры, является одним из самых ранних примеров тайнописи — она содержит закодированную клинопись формулы изготовления глазури для покрытия сосудов.

Отличительная особенность современного состояния общества заключается в его глобальной информатизации. Компьютерные технологии пронизывают все области практической деятельности человека, а информация в электронном виде является неотъемлемой и существенной составляющей нашей жизни. В связи с этим на первый план выходит проблема безопасности именно электронной информации.

Понятие «безопасности информации» охватывает широкий круг интересов как отдельных лиц, так и целых государств.

С одной стороны, под безопасностью информации понимается сохранение ее целостности и достоверности. В этом смысле проблема обеспечения безопасности информации появилась задолго до появления компьютерных технологий — вспомним хотя бы пожар, уничтоживший большую часть Каирской библиотеки в Египте. Сохранение файлов пользователя на его личном компьютере является современным типичным примером обеспечения целостности информации.

С другой стороны, важным является обеспечение защиты конфиденциальной информации, такой, как персональные данные, военная и государственная тайна. О важности сохранения информации в тайне знали уже в древние времена, когда с появлением письменности появилась и опасность прочтения ее нежелательными лицами. В современном обществе, охваченном всемирной глобальной сетью Интернет, проблема защиты конфиденциальной информации является насущной.

С третьей стороны, отказ компьютерной техники и невозможность в связи с этим обеспечить доступность информации может привести к трагичным и разорительным последствиям.

Несколько примеров нарушения информационной безопасности можно найти в курсе «Основы информационной безопасности» издательства Интуит.ру.

1) Американский ракетный крейсер «Йорктаун» был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию коммерческого программного обеспечения с целью снижения стоимости военной техники.

2) Согласно результатам совместного исследования Института информационной безопасности и ФБР, в 1997 году ущерб от компьютерных преступлений составил 136 миллионов долларов. Каждое компьютерное преступление наносит ущерб примерно в 200 тысяч долларов.

3) В середине июля 1996 года корпорация General Motors отозвала почти 300 тыс. автомобилей марки Pontiac, Oldsmobile и Buick моделей 1996 и 1997 годов, поскольку ошибка в программном обеспечении двигателя могла привести к пожару.

4) В феврале 2001 года двое бывших сотрудников компании Commerce One, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика.

5) Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.

Примеров нарушения информационной безопасности на самом деле очень много и уменьшения их числа в обозримом будущем не предвидится. Информационная безопасность есть составная часть информационных технологий — области, развивающейся самыми высокими темпами. Здесь важны не только отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, но и механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует развитию средств обеспечения ИБ. Приходится исходить из того, что конструирование надежных систем информационной безопасности производится с помощью ненадежных программных компонентов. Это требует соблюдения определенных архитектурных принципов и контроля состояния защищенности на всем протяжении жизненного цикла информационной системы.

Заметим, что современные методы обеспечения информационной защиты на основе *объектно-ориентированного* подхода представляются наиболее адекватными в плане надежности и устойчивости.

## Основные понятия

***Определение***

*Информационная безопасность (ИБ) — это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений (владельцам и пользователям информации).*

В разных контекстах термин «информационная безопасность» может принимать разный смысл. Так, в Доктрине информационной безопасности Российской Федерации под «информационной безопасностью» понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства. В данном случае информационная безопасность понимается в «широком смысле».

В пособии информационная безопасность рассматривается в более «узком смысле» — вне зависимости от целей защиты информации, а также от того, кто является ее владельцем и пользователем.

Существуют также понятия «компьютерной» и «сетевой безопасности». К безопасности компьютера относятся проблемы защиты данных отдельного компьютера. Эти проблемы решаются средствами операционной системы и приложениями, такими, как базы данных, а также встроенными аппаратными средствами.

Под сетевой безопасностью понимают вопросы обеспечения защиты данных в момент их передачи по сети и защиты от несанкционированного удаленного доступа. Все большее использование компьютеров в различных публичных сетях выводят проблемы сетевой безопасности в ряд наиболее актуальных.

В отличие от сетевой и компьютерной безопасности, информационная безопасность имеет отношение ко всем аспектам, связанным с использованием информации как таковой. Информационная безопасность включает в себя не только компьютеры и компьютерные технологии, но и поддерживающую их *инфраструктуру*, к которой относятся системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникации, здания и сооружения, мебель, обслуживающий персонал и т.п.

Обратим внимание, что нарушение информационной безопасности определяется как нанесение *неприемлемого ущерба*. Невозможно или экономически нецелесообразно застраховаться или защититься от всех видов нарушений информационной безопасности. Приходится *мириться* с теми нарушениями информационной безопасности, расходы на защиту от которых превышают возможный ущерб.

***Определение***

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

Заметим что, во-первых, информационная безопасность является частью общей безопасности независимо от уровня, на котором она рассматривается — национального, отраслевого, корпоративного или персонального (личного). Во-вторых, обеспечение информационной безопасности является комплексной проблемой, охватывающей множество взаимосвязанных аспектов законодательного, административного, процедурного и технического характера.

Простой пример — невозможно обеспечить защиту конфиденциальной информации только при помощи ее шифрования. Любое зашифрованное сообщение может быть расшифровано. Однако на пути к зашифрованному сообщению могут стоять другие программные средства, например авторизация и аутентификация. Меры процедурного уровня при этом могут ограничить физический доступ к источнику информации, а законодательные акты создают негативное отношение общества к нарушению конфиденциальности.

Очевидно, никакие средства защиты информации не могут в полной мере препятствовать нарушениям информационной безопасности. В некоторых случаях нарушение информационной безопасности является целью профессиональной деятельности (например, в разведке, как экономической, так и политической). Это ведет к тому, что средства и методы защиты информации, а также средства нарушения ИБ непрерывно совершенствуются.

***Составляющие информационной безопасности***

Понятия информации, информационной технологии, информационной системы и другие определены в законе РФ «Об информации, информационных технологиях и о защите информации». Хотя понятия информационной безопасности можно применять и к некомпьютерным информационным системам, здесь имеются ввиду именно компьютерные ИС.

Будем понимать под безопасной информационной системой такую систему, которая:

а) вовремя доставляет данные своим пользователям;

б) гарантирует неизменность и достоверность данных.

в) защищает данные от несанкционированного доступа;

Иначе говоря, безопасная информационная система обладает свойствами доступности, целостности и конфиденциальности, которые являются тремя составляющими информационной безопасности.

***Определение***

*Доступность (availability) — гарантия того, что авторизованные пользователи получат доступ к данным за приемлемое время.*

Доступность является важнейшим элементом информационной безопасности, поскольку недоступность информационных услуг, предоставляемых информационной системой, наносит ущерб всем субъектам информационных отношений. Ведущая роль доступности наиболее заметно проявляется в системах управления, например, производством и транспортом, в предоставлении информационных услуг населению (например, в продаже билетов, банковских услугах и т.п.).

***Определение***

*Целостность (integrity) — гарантия актуальности и непротиворечивости информации, ее защищенность от разрушения и несанкционированного изменения.*

Различают статическую и динамическую целостность. Статическая целостность — это неизменность состояния информационных объектов. Динамическая целостность проявляется в корректности выполнения сложных действий (таких, как транзакции). Контроль динамической целостности используется, например, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования сообщений.

Нарушение целостности становится особенно важным элементом ИБ, когда информация служит «руководством к действию». Рецептуры лекарств, характеристики комплектующих изделий, ход технологического процесса — примеры информации, нарушение целостности которой может привести в буквальном смысле к смертельным последствиям.

***Определение***

*Конфиденциальность (confidentiality) — это защита от несанкционированного доступа, гарантирующая, что секретные данные будут доступны только тем пользователям, которым этот доступ разрешен (авторизованным пользователям).*

Конфиденциальные сведения существуют практически в любой информационной системе. Даже если сама информация не содержит секретных сведений, пароли администраторов, операторов, модераторов и других пользователей информационной системы являются конфиденциальной информацией. В России конфиденциальность является наиболее разработанным аспектом информационной безопасности, что связано с закрытым характером российского общества в течение нескольких десятилетий.

## Угрозы информационной безопасности

Возможность нарушения безопасности информационной системы возникает из-за наличия в защите уязвимых мест — это может быть, например, возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении.

***Определение***

*Уязвимость — слабое место в системе, с использованием которого может быть осуществлена атака.*

Заметим, что построить полностью безопасную систему невозможно, — можно только ограничить риск потенциального ущерба, который может быть причинен в результате атаки на безопасность информационной системы.

***Определение***

*Риск — это вероятностная оценка величины возможного ущерба, который могут понести субъекты информационных отношений в результате успешной атаки.*

Существует множество причин, препятствующих полному устранению уязвимых мест.

1) Сложность информационных систем затрудняет устранение всех возможных ошибок в программном обеспечении, равно как и анализ системы и ее компонентов на безопасность.

2) Распределенный характер информационных систем дает возможность удаленного несанкционированного доступа к отдельным компьютерам и компонентам системы. Невозможно заключить всю распределенную систему в единую защитную оболочку (хотя такие случаи известны).

3) Развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, увеличение пропускной способности каналов связи расширяет круг потенциальных злоумышленников, имеющих техническую возможность осуществления атаки.

4) Беспрецедентный рост производительности компьютеров, развитие архитектур с высокой степенью параллелизма позволяет лобовыми атаками (перебором) разрушать криптографические барьеры, которые ранее казались неприступными.

5) Погоня за непрерывно совершенствующимися технологиями ведет к замене апробированных систем и архитектур новыми, что, с одной стороны, ведет к появлению новых уязвимых мест, а с другой — к снижению ассигнований на обеспечение безопасности из-за финансовых ограничений.

6) Комплексное обеспечение безопасности информационной системы включает в себя неизбежный «человеческий фактор». Ошибки человека чаще всего являются наиболее уязвимым местом информационной системы.

Уязвимость системы ведет к появлению *угроз* информационной безопасности.

***Определение***

*Угроза — это потенциальная возможность определенным образом нарушить информационную безопасность.*

***Определение***

*Атака — попытка реализации угрозы.*

Того, кто предпринимает попытку реализации угрозы, называют *злоумышленником*, а потенциального злоумышленника *называют источником угрозы*.

Заметим, что некоторые угрозы не являются следствием ошибок или просчетов — они существуют в силу самой природы современных информационных систем. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания. С этой точки зрения некоторые угрозы безопасности присущи всем информационным системам.

***Определение***

*Окно опасности — промежуток времени от момента, когда появляется уязвимое место в защите системы до момента, когда данное слабое место в защите ликвидируется.*

Пока существует окно опасности, возможны успешные атаки на информационную систему. Так как в работающей (и развивающейся) системе постоянно появляются новые уязвимые места, в ней появляются и новые окна опасности.

### *Классификация угроз информационной безопасности*

Рассмотрим наиболее распространенные угрозы безопасности информационных систем. Иметь представление о возможных угрозах необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Универсальной и единой классификации угроз безопасности, по-видимому, не существует. Этому способствует появление новых способов проникновения в сеть, средств мониторинга сетевого трафика, а также появление новых вирусов, изъянов в аппаратном и программном

обеспечении, что, в свою очередь, ведет к появлению новых средств защиты от этих угроз.

Угрозы можно классифицировать по разным критериям, например:

- по элементу информационной безопасности, против которого угрозы направлены в первую очередь (доступность, целостность, конфиденциальность);
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратные средства, инфраструктура);
- по умыслу (случайные или преднамеренные);
- по характеру (природного или техногенного характера);
- по расположению источника угроз (внутри или вне ИС).

**Основные угрозы доступности**

Рассмотрим основные угрозы доступности.

1) Непреднамеренные ошибки штатных пользователей, операторов, системных администраторов, обслуживающего персонала и других. По некоторым данным, ущерб от этих ошибок составляет более половины всех потерь. Способ борьбы с непреднамеренными ошибками — максимальная автоматизация и строгий контроль.

2) Внутренние отказы ИС. Они происходят в результате:

- нарушения правил эксплуатации ИС;
- выхода ИС из штатного режима вследствие атак из внешней сети; в этом случае работа сервисов ИС может остановиться из-за необходимости непрерывного обслуживания фиктивных запросов;
- отказов программного или аппаратного обеспечения, например, в случае их несовместимости, ошибок в программах, заражения вредоносным программным обеспечением (вирусами);
- уничтожения или разрушения данных (вследствие несоблюдения правил архивирования и резервирования данных и других причин).

3) Отказ пользователей. Это может быть нежелание пользователей работать с ИС (например, из-за необходимости осваивать ее), невозможность работать с ИС из-за отсутствия технической поддержки или подготовки пользователей и персонала.

4) Отказы поддерживающей инфраструктуры, такие, как нарушение работы систем связи, электро-, водо- или теплоснабжения, кражи, пожары, нежелание персонала выполнять свои обязанности и т.п.

**Основные угрозы целостности**

Рассмотрим основные угрозы целостности.

1) Кражи и подлоги. Они занимают второе место по размеру наносимого ущерба. Виновниками часто являются штатные сотрудники, знакомые с режимом работы организации и мерами защиты.

При этом злоумышленник может:

- ввести неверные данные или изменить их;
- подделать электронный документ;
- внедрить вредоносное программное обеспечение и т.п.

2) Разрушение данных вследствие действия вредоносного программного обеспечения, атак из внешней сети, предумышленно заложенных в программах ошибок («бомб»), сбоев в работе программного и аппаратного обеспечения, в том числе из-за отказа инфрастуктуры.

**Основные угрозы конфиденциальности**

Угрозы конфиденциальности занимают особое положение среди всех других угроз. Нарушения конфиденциальности данных зачастую не ведут к ощутимому физическому ущербу, но могут выражаться в нематериальных потерях, таких, как имидж или престиж государства, организации или отдельного лица. Кроме того, нарушение конфиденциальности может вести также к нарушениям целостности и доступности.

1) Часто угрозы конфиденциальности носят нетехнический характер. Так, одной из серьезных проблем является сохранение в тайне паролей, которые могут размещаться в местах, не обеспечивающих надлежащую их защиту. Пользователи могут размещать их в легко доступных местах (на мониторах, под стеклом на рабочем столе и т.п.), передавать открытым текстом в разговорах, в том числе телефонных, в сообщениях электронной почты и т.п. Нужно всегда помнить о том, что «враг не дремлет». Компьютеры организации могут выноситься на различные выставки и презентации, пароли могут сообщаться посторонним лицам, таким, как персонал, выполняющий сервисное обслуживание и т.п.

Сами пароли зачастую могут быть легко вычислены. Классический пример — советский разведчик Рихард Зорге узнал ключ к секретному сейфу благодаря тому, что его подопечный через слово вставлял слово «карамба», — именно оно и оказалось ключом к сейфу.

Часто конфиденциальная информация доступна непосредственным образом. Так, в учреждениях мониторы могут располагаться таким образом, что посетитель видит все, что на них находится.

2) Злоупотребление полномочиями. Привилегированный пользователь (такой, как системный администратор) получает доступ ко всем файлам ИС и может просмотреть любую информацию.

3) Перехват данных, передаваемых по сети, а также во время работы отдельных компьютеров. Средства перехвата данных в настоящее время чрезвычайно совершенны. Так, можно получить текст документа, набираемого на компьютере, при помощи средств, фиксирующих изменение электромагнитного поля, излучаемого монитором, системным блоком, другими компонентами вычислительной системы (сетями).

## Уровни обеспечения информационной безопасности

Обеспечение информационной безопасности — это сложная и многогранная область деятельности, успех в которой может принести только комплексный подход. Проблему обеспечения информационной безопасности принято рассматривать на следующих четырех уровнях:

1) *Законодательный уровень*.

Он определяется законами и другими правовыми актами, направленными на создание в обществе определенного отношения к нарушениям информационной безопасности, а также определяющими права и обязанности субъектов информационных отношений.

2) *Административный уровень*.

Он определяется документами и действиями руководства организации, направленными на обеспечение информационной безопасности. Важнейшими документами организации в отношении информационной безопасности являются *политика безопасности* и программа безопасности. Для создания эффективной и экономичной системы безопасности организация должна осуществлять *управление рисками*.

3) *Процедурный уровень*.

Меры процедурного уровня направлены на участников информационных отношений. Этот уровень включает в себя управление персоналом, физическую защиту, поддержание работоспособности, реагирование на нарушения информационной безопасности и планирование восстановительных работ.

4) *Программно-технический уровень*.

Он определяется сервисами безопасности — программно-техническими механизмами защиты, используемыми для организации системы безопасности информационной системы.

Полный набор сервисов безопасности составляют:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

***Законодательный уровень обеспечения ИБ***

Законодательный уровень является важным аспектом обеспечения информационной безопасности. Он создает в обществе гражданскую позицию к нарушениям информационной безопасности, и определяет нормативно-правовую базу взаимоотношений между участниками информационных отношений.

На законодательном уровне можно выделить две группы мер:

- меры *ограничительной направленности*, направленные на создание и поддержание негативного отношения к нарушениям и нарушителям информационной безопасности; большинство людей не совершают противоправных действий не потому, что это невозможно технически, а потому, что это осуждается сообществом граждан;
- меры *созидательной направленности*, способствующие повышению образованности общества в отношении информационной безопасности, помогающие разрабатывать и распространять средства обеспечения информационной безопасности.

Важной и сложной задачей в области законодательного уровня является согласование процесса разработки законов с прогрессом информационных технологий, и обеспечение соответствие правового поля реалиям современного состояния информационных отношений.

Рассмотрим основные законодательные акты Российской Федерации, имеющие отношение к информационной безопасности.

**Конституция РФ**

Конституция — основной закон государства, определяющий нормативно-правовую базу для всех других законов и законных актов.

Статья 23 гарантирует право на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Статья 24 определяет, что каждый гражданин имеет право ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы (если иное не предусмотрено законом).

Статья 29 гарантирует право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей.

Статья 42 обеспечивает право на знание достоверной информации о состоянии окружающей среды.

**Гражданский кодекс**

Статья 139 определяет понятия *банковской*, *коммерческой* и *служебной* тайны. Согласно этой статье, информация составляет служебную

или коммерческую тайну, если она имеет действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

**Уголовный кодекс**

УК РФ определяет ответственность в сфере нарушений информационной безопасности.

Статья 138 защищает конфиденциальность персональных данных, предусматривая наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

Глава 28 — «Преступления в сфере компьютерной информации» — содержит следующие три статьи:

статья 272 — неправомерный доступ к компьютерной информации;

статья 273 — создание, использование и распространение вредоносных программ для ЭВМ;

статья 274 — нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

**Закон о государственной тайне**

Государственная тайна определяется этим законом как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Здесь же дается определение средств защиты информации. Согласно данному закону, это 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.

**Закон «Об информации, информационных технологиях и о защите информации»**

Один из основополагающих законов (от 27 июля 2006 г.).

Статья 1 определяет цели закона:

«… закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.»

Статья 2 дает следующие определения, используемые в законе:

«1) *информация* — сведения (сообщения, данные) независимо от формы их представления;

2) *информационные технологии* — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) *информационная система* — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) *информационно-телекоммуникационная сеть* — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;», и другие.

Статья 3 определяет принципы правового регулирования в сфере информационных отношений:

«1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;»

Статья 5 определяет информацию как объект правовых отношений.

«1. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения…

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.»

Статья 7 определяет общедоступную информацию:

«1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.»

Статья 16 определяет защиту информации:

«1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

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

2) соблюдение конфиденциальности информации ограниченного доступа,

3) реализацию права на доступ к информации.»

Пункт 4 определяет обязанности обладателя информации:

«4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.»

Статья 17 определяет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

**Закон «О лицензировании отдельных видов деятельности»**

Данный закон (от 8 августа 2001 г.) дает определения, связанные с лицензированием. Приведем некоторые из них:

«*Лицензия* — специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому лицу или индивидуальному предпринимателю.

*Лицензируемый вид деятельности* — вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с настоящим Федеральным законом.

*Лицензирование* — мероприятия, связанные с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензий, приостановлением и возобновлением действия лицензий, аннулированием лицензий и контролем лицензирующих органов за соблю

дением лицензиатами при осуществлении лицензируемых видов деятельности соответствующих лицензионных требований и условий.

*Лицензирующие органы* — федеральные органы исполнительной власти, органы исполнительной власти субъектов Российской Федерации, осуществляющие лицензирование в соответствии с настоящим Федеральным законом.

*Лицензиат* — юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности.»

Статья 17 устанавливает виды деятельности, требующие лицензирования:

- распространение шифровальных (криптографических) средств;
- техническое обслуживание шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- выдача сертификатов ключей электронных цифровых подписей, регистрация владельцев электронных цифровых подписей, оказание услуг, связанных с использованием электронных цифровых подписей и подтверждением подлинности электронных цифровых подписей;
- выявление 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);
- разработка и (или) производство средств защиты конфиденциальной информации;
- техническая защита конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

**Лицензирующие органы**

Основными лицензирующими органами в области защиты информации являются Федеральное агентство правительственной связи и информации (ФАПСИ) и Гостехкомиссия России.

ФАПСИ ведает всем, что связано с криптографией, Гостехкомиссия лицензирует деятельность по защите конфиденциальной информации. Эти же организации возглавляют работы по сертификации средств информационной безопасности.

Кроме того, ввоз и вывоз средств криптографической защиты информации (шифровальной техники) и нормативно-технической документации к ней может осуществляться только на основании лицензии Министерства внешних экономических связей Российской Федерации, выдаваемой на основании решения ФАПСИ.

**Закон «Об электронной цифровой подписи»**

Статья 1 поясняет роль этого закона (от 10 января 2002 г.):

«1) Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.»

Закон вводит следующие основные понятия:

*Электронный документ*, *электронная цифровая подпись*, *средства электронной цифровой подписи*, *закрытый ключ электронной цифровой подписи*, *открытый ключ электронной цифровой подписи* и другие.

Согласно закону, электронная цифровая подпись (ЭЦП) в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении условий:

- сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность ЭЦП в электронном документе;
- ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Закон определяет сведения, которые должен содержать сертификат ключа подписи:

- 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;
- открытый ключ ЭЦП;
- наименование средств ЭЦП, с которыми 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.

**Закон «О персональных данных»**

Федеральный закон РФ «О персональных данных» (27 июля 2006 г.) в статье 1 определяет сферу действия:

«1. Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами…, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами…, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.»

Статья 2 закона определяет, что его действие не распространяется на отношения, возникающие при:

«1) обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

3) обработке подлежащих включению в единый государственный реестр индивидуальных предпринимателей сведений о физических лицах, если такая обработка осуществляется в соответствии с законодательством Российской Федерации в связи с деятельностью физического лица в качестве индивидуального предпринимателя;

4) обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.»

Закон дает следующее определение персональных данных (статья 3):

«персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация».

Статья 5 описывает принципы обработки персональных данных, статья 6 — условия обработки персональных данных. В статье 7 отмечается, что «Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных». Статья 14 определяет право субъекта персональных данных на доступ к своим персональным данным.

Статья 24 устанавливает ответственность за нарушение требований данного Закона:

«Лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.»

***Административный уровень обеспечения ИБ***

Цель мер административного уровня — сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя ход дел.

Важным документом является политика безопасности.

**Политика безопасности**

***Определение***

*Политика безопасности — совокупность документированных решений, принимаемых руководством организации для обеспечения информационной безопасности.*

Политика безопасности вырабатывается на основе анализа и оценки рисков, являющихся реальными для данной организации. Политику безопасности принято рассматривать на трех уровнях детализации.

На верхнем уровне определяются решения, затрагивающие организацию в целом. Примерный список таких решений:

- решение сформировать программу обеспечения информационной безопасности, назначение ответственных за реализацию;
- формулирование целей организации в области информационной безопасности, определение общих направлений;
- обеспечение базы для соблюдения законов и правил, определение системы мер поощрений и наказаний;
- формулирование административных решений, касающихся организации в целом.

Политика безопасности верхнего уровня формулирует цели организации в терминах доступности, целостности и конфиденциальности, исходя из практических задач организации. Например, если организация отвечает за поддержание баз данных, целью политики безопасности яв

ляется уменьшение потерь и искажений данных. Если организация занимается продажами, целью является актуальность и доступность информации об услугах и ценах. Для режимного предприятия целью может являться защита от несанкционированного доступа.

На верхнем уровне осуществляется управление защитными ресурсами, координация их использования, определение ответственного персонала, взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

*На среднем уровне* рассматриваются вопросы, касающиеся отдельных аспектов информационной безопасности, важные для различных используемых информационных систем организации. Это могут быть отношение к передовым технологиям, использование личных компьютеров, неофициального программного обеспечения и т.п.

Для каждого аспекта политика среднего уровня освещает вопросы:

- описание аспекта; например, если рассматривается неофициальное программное обеспечение, его можно определить как ПО, которое не было одобрено и (или) приобретено на уровне организации;
- область применения аспекта; например, если рассматривается неофициальное программное обеспечение, то касается ли политика организаций-субподрядчиков;
- позиция организации по данному аспекту; например, если рассматривается неофициальное программное обеспечение, то политика может запрещать его использование или определять процедуру его приемки, установки и т.п.;
- роли и обязанности; политика безопасности должна определять, кто отвечает за ее соблюдение; например, если для использования неофициального программного обеспечения требуется разрешение руководства, то должно быть известно, кто и как такое разрешение выдает;
- ответственность; политика должна определять запрещенные действия и ответственность за их совершение;
- точки контакта; политика должна определять, куда следует обращаться за разъяснениями, помощью и дополнительной информацией.

*На нижнем уровне* политика безопасности относится к конкретным информационным сервисам организации. На этом уровне политика безопасности определяется более подробно. Политика безопасности нижнего уровня должна, например, давать ответы на конкретные вопросы:

- кто имеет право доступа к объектам информационного сервиса?
- при каких условиях можно читать и модифицировать данные?
- как организован доступ к информационному сервису и т.п.

**Программа безопасности**

***Определение***

*Программа безопасности — документ или совокупность документов, описывающих детали реализации политики безопасности.*

Программа безопасности структурируется по уровням в соответствии со структурой организации. В простейшем случае она описывает два уровня: верхний (центральный), охватывающий организацию в целом, и нижний (служебный), относящийся к отдельным услугам или группам однородных сервисов.

За программу верхнего уровня отвечает лицо, ответственное за информационную безопасность организации. Программа верхнего уровня определяет стратегические решения по обеспечению безопасности. Ее главные цели:

- управление рисками;
- координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- стратегическое планирование;
- контроль деятельности в области информационной безопасности.

Программа нижнего уровня должна обеспечивать надежную и экономичную защиту конкретных сервисов или группы однородных сервисов. На нижнем уровне решается, какие следует использовать механизмы защиты, закупаются и устанавливаются технические средства, выполняется повседневное администрирование, отслеживается состояние уязвимых мест и т.п.

**Управление рисками**

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая оценка и переоценка рисков необходима для контроля эффективности деятельности в области безопасности.

Управление рисками и определение собственной политики безопасности актуально для тех организаций, информационные системы которых являются нестандартными. Обычную организацию устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков.

Управление рисками — циклический процесс, включающий в себя:

- оценку (или переоценку) рисков;
- выбор эффективных и экономичных защитных средств.

По отношению к рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения причины);

- уменьшение риска (например, за счет использования дополнительных защитных средств);

- принятие риска (и выработка плана действия в соответствующих условиях);

- переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на этапы:

1) *Выбор анализируемых объектов* и уровня детализации их рассмотрения. При этом целесообразно составить карту информационной системы организации — наглядно показывает, какие сервисы анализируются, а какие нет.

2) *Выбор методологии оценки рисков*. Целью оценки рисков является получение ответа на вопрос: приемлемы ли существующие риски, и если нет, какие защитные средства использовать. Управление рисками — это оптимизационная задача, для решения которой существуют программные средства.

3) *Идентификация активов*. При этом учитывают ресурсы, которые подлежат защите (компьютеры, кабели, сетевое оборудование, программное обеспечение, данные и т.п.), поддерживающую инфраструктуру, персонал и нематериальные ценности (например, репутация).

4) *Анализ угроз* и их последствий, выявление уязвимых мест в защите. Угрозы следует идентифицировать, определить источники, оценить вероятность осуществления и вероятную тяжесть ущерба по трехбалльной шкале.

5) *Оценка рисков*. Количественно риск можно оценить, перемножая вероятность осуществления угрозы на вероятную тяжесть ущерба. Полученные результаты приводятся к трехбалльной шкале.

6) *Выбор защитных мер*. Для защиты от конкретной угрозы существуют разные по стоимости и эффективности средства защиты. Например, если велика вероятность нелегального входа в систему, можно потребовать, чтобы пользователи выбирали длинные пароли, приобрести программу для генерации паролей или систему аутентификации на основе интеллектуальных карт. При выборе защитных мер следует также учитывать возможность экранирования одним механизмом нескольких угроз.

7) *Реализация и проверка* выбранных мер. На этом этапе должно быть проведено планирование работ с учетом финансирования и обучения персонала.

8) *Оценка остаточного риска*. Если в результате мероприятий по нейтрализации угроз оценки рисков стали приемлемыми, намечается дата следующей переоценки, иначе весь процесс повторяется.

***Процедурный уровень обеспечения ИБ***

На процедурном уровне можно выделяют следующие классы мер:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

***Управление персоналом*** начинается с определения должностных обязанностей и соответствующих компьютерных привилегий, что позволяет сформировать требования к отбору кандидатов.

Следующий шаг — обучение персонала и контроль знаний ими режима безопасности и мер защиты. Нет смысла требовать от сотрудника соблюдения режима безопасности, если он не знает политики безопасности и используемых средств защиты.

После заведения системного счета сотрудника начинается его администрирование, протоколирование и анализ действий. При изменении условий труда и (или) служебных обязанностей системный счет сотрудника должен модифицироваться. Следует учитывать временные перемещения сотрудника, отпуска и другие обстоятельства, когда те или иные полномочия предоставляются, а затем забираются обратно.

К управлению персоналом относится также администрирование лиц, работающих по контракту (например, выполняющих пуско-наладочные, ремонтные работы, техобслуживание и т.п.).

При выделении привилегий используют два принципа:

- разделение обязанностей — роли и ответственности распределяются так, чтобы один человек не мог нарушить критически важный для организации процесс;
- минимизация привилегий — пользователю выделяются только те права доступа, которые необходимы для выполнения его служебных обязанностей.

***Физическая защита*** включает в себя:

- физическое управление доступом — ограничение входа и выхода, разграничение (идентификация) штатных сотрудников и посетителей, использование охраны, дверей с замками, перегородок, шлагбаумов, телекамер, датчиков движения т.п.;
- противопожарные меры — использование, например, противопожарной сигнализации и автоматических средств тушения пожаров;
- защита поддерживающей инфраструктуры — предотвращение нарушения целостности (например, вследствие кражи) и работоспособности (доступности) систем электро-, водо-, теплоснабжения, кондиционирования, коммуникационных средств;

- защита от перехвата данных — злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, анализировать побочные электромагнитные излучения и наводки;

- защита мобильных систем — портативные компьютеры легко украсть вместе с важной информацией, находящейся в них.

***Поддержание работоспособности*** включает в себя следующие направления повседневной деятельности:

- поддержка пользователей — консультирование и оказание помощи по проблемам информационной безопасности;

- поддержка программного обеспечения — контроль установленного программного обеспечения, контроль за отсутствием неавторизованного изменения программ и прав доступа к ним, создание эталонных копий программных систем;

- конфигурационное управление — контроль и фиксация изменений, вносимых в программную конфигурацию, обеспечение легкого восстановления предыдущей конфигурации;

- резервное копирование — периодическое создание полных и инкрементных копий (по расписанию), обеспечение сохранности копий, в том числе физическую защиту от, например, краж или разрушения;

- управление носителями — учет и физическая защита съемных носителей информации для обеспечения их целостности, доступности и конфиденциальности;

- документирование — документация должна быть актуальной, непротиворечивой и доступной;

- регламентные работы — сотрудник, выполняющий регламентные работы, часто получает неограниченный доступ к системе.

***Реагирование на нарушения режима безопасности*** заключается в локализации инцидента и уменьшении вреда, выявлении нарушителя и предупреждении повторных нарушений.

***Планирование восстановительных работ*** позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить работоспособность. Включает в себя следующие этапы:

- выявление критически важных функций организации, установление приоритетов;

- идентификация ресурсов, необходимых для выполнения критически важных функций;

- определение перечня возможных аварий;

- разработка стратегии восстановительных работ;

- подготовка к реализации выбранной стратегии;

- проверка стратегии.

## Стандарты информационной безопасности

Специалист в области информационной безопасности должен знать соответствующие стандарты и спецификации [2].

Во-первых, необходимость следования стандартам (например, руководящим документам ФСТЭК России) закреплена законодательно.

Во-вторых, стандарты и спецификации — одна из форм накопления знаний, прежде всего о процедурном и программно-техническом уровнях информационной безопасности. В них зафиксированы апробированные, высококачественные решения и методологии, разработанные квалифицированными специалистами. Стандарты и спецификации являются основным средством обеспечения взаимной совместимости аппаратно-программных систем и их компонентов. Эта роль стандартов зафиксирована в основных понятиях закона РФ «О техническом регулировании» (от 27 декабря 2002 г.):

«- *стандарт* — документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. … ;

- *стандартизация* — деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.»

В упомянутом законе отмечается, что один из принципов стандартизации — применение международного стандарта как основы разработки национального, за исключением случаев, если «такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям Российской Федерации, техническим и (или) технологическим особенностям или по иным основаниям, либо Российская Федерация, в соответствии с установленными процедурами, выступала против принятия международного стандарта или отдельного его положения».

В настоящем пособии рассматриваются наиболее важные стандарты и спецификации.

Различают оценочные стандарты и технические спецификации.

*Оценочные стандарты* направлены на классификацию ИС и средств защиты по требованиям безопасности. *Технические спецификации* регламентируют различные аспекты реализации средств защиты. Оценочные стандарты играют роль архитектурных спецификаций, а технические спецификации определяют, как строить ИС данной архитектуры.

**«Оранжевая книга»**

Исторически первым оценочным стандартом, оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства Обороны США «Критерии оценки доверенных систем», известный по цвету обложки как «Оранжевая книга» (август 1983 г.).

Этот стандарт ввел понятие «доверенной вычислительной системы». Согласно стандарту, абсолютно безопасных систем не существует. Поэтому имеет смысл оценивать степень доверия той или иной системе.

Доверенная вычислительная система определяется «Оранжевой книгой» как «система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа».

Степень доверия оценивается по двум критериям.

1) *Политика безопасности* — набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Политика безопасности — это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

2) *Уровень гарантированности* — мера доверия, которая может быть оказана архитектуре и реализации ИС. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

«Оранжевая книга» вводит также и другие понятия.

*Доверенная вычислительная база* — это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности.

Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных.

Основное назначение доверенной вычислительной базы — выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами определенных операций над объектами.

Монитор обращений должен обладать тремя качествами:

1) *Изолированность*. Необходимо предупредить возможность отслеживания работы монитора.

2) *Полнота*. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

3) *Верифицируемость*. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности.

*Ядро безопасности* — это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу доверенной вычислительной базы называют *периметром безопасности*. Компоненты, лежащие вне периметра безопасности, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию «периметр безопасности» все чаще придают другой смысл, имея в виду границу владений определенной организации.

***Механизмы безопасности***

Согласно «Оранжевой книге», политика безопасности должна включать в себя следующие элементы:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

*Произвольное* (*дискреционное*) *управление доступом* — это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа.

*Безопасность повторного использования объектов* предохраняет от случайного или преднамеренного извлечения конфиденциальной информации из «мусора». Безопасность повторного использования должна гарантироваться для областей оперативной памяти, для дисковых блоков и магнитных носителей в целом.

Для реализации принудительного управления доступом с субъектами и объектами ассоциируются *метки безопасности*. Метка субъекта описывает его благонадежность, метка объекта — степень конфиденциальности содержащейся в нем информации.

Метки безопасности состоят из двух частей — уровня секретности и списка категорий. Назначение списка категорий — описать предметную область, к которой относятся данные.

*Принудительное* (мандатное) *управление доступом* основано на сопоставлении меток безопасности субъекта и объекта.

Субъект может *читать* информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта.

Субъект может *записывать* информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, «кон

фиденциальный» субъект может записывать данные в секретные файлы, но не может — в несекретные.

Дополнением политики безопасности является механизм *подотчетности*. Цель подотчетности — в каждый момент времени знать, кто работает в системе и что делает.

Средства подотчетности делятся на три категории:

- идентификация и аутентификация;
- предоставление доверенного пути;
- анализ регистрационной информации.

Обычный способ идентификации — ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности пользователя — это пароль.

*Доверенный путь* связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие, потенциально опасные компоненты ИС. Цель предоставления доверенного пути — дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Анализ регистрационной информации (аудит) имеет дело с событиями, затрагивающими безопасность системы. «Оранжевая книга» предусматривает наличие средств выборочного протоколирования.

Переходя к пассивным аспектам защиты, заметим, что в «Оранжевой книге» рассматривается два вида гарантированности — операционная и технологическая. Операционная гарантированность относится к архитектурным и реализационным аспектам системы, а технологическая — к методам построения и сопровождения.

***Классы безопасности***

«Критерии оценки доверенных систем» позволяют ранжировать информационные системы по степени доверия безопасности. «Оранжевая книга» определяется четыре уровня безопасности — D, C, B и A (по возрастанию степени доверия).

Система класса D определяется как система, уровень обеспечения безопасности в которой является неудовлетворительным.

Система класса C характеризуется произвольным управлением доступом. Данный класс содержит два подкласса — C1 и C2. Например, известная операционная система Windows относится по данной классификации к классу C2.

Систему класса B можно охарактеризовать как систему с принудительным управлением доступа. Этот класс содержит три подкласса — B1, B2 и B3 с постепенным возрастанием степени доверия.

Информационную систему класса А можно охарактеризовать как систему с верифицируемым (гарантированным) уровнем доверия. Построить такую систему практически очень сложно.

Критерии определения класса безопасности ИС представлены в виде списка требований. При этом требования, предъявляемые к классу С2, включают в себя требования, предъявляемые к классу С1, — можно сказать, что класс С2 «наследует» требования к классу С1. Аналогично класс В1 наследует требования к классу С2. В целом получается иерархия требований (по возрастанию): D→C1→C2→B1→B2→B3→A.

## Рекомендации X.800

Техническая спецификация X.800, появившаяся немногим позднее «Оранжевой книги», освещает вопросы информационной безопасности *распределенных систем*. В этом документе выделяют следующие сервисы безопасности и исполняемые ими роли:

- *аутентификация*. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

- *управление доступом*. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

- *конфиденциальность данных*. Обеспечивает защиту от несанкционированного получения информации. Конфиденциальность трафика обеспечивает защиту информации, которую можно получить, анализируя сетевые потоки данных.

- *целостность данных* подразделяется на подвиды в зависимости от типа взаимодействия — с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

- *неотказуемость* — это невозможность отказаться от совершенных действий. Различают неотказуемость с подтверждением подлинности источника данных (ведущую к аутентификации источника данных) и неотказуемость с подтверждением доставки.

Спецификация определяет сетевые механизмы безопасности, с помощью которых реализуются сервисы. К ним относятся:

- шифрование;
- электронная цифровая подпись (ЭЦП);
- механизмы управления доступом;

- механизмы контроля целостности данных; различают целостность отдельного сообщения или поля данных, а также целостность потока сообщений или полей данных;

- механизмы аутентификации; аутентификация может достигаться использованием паролей, личных карточек, устройств измерения и анализа биометрических характеристик, криптографических методов;

- механизмы дополнения трафика;

- механизмы управления маршрутизацией;

- механизмы нотаризации, использующие, как правило, ЭЦП.

*Администрирование средств безопасности* включает в себя администрирование ИС в целом, а также администрирование сервисов и механизмов безопасности.

Администрирование сервисов безопасности заключается в определении защищаемых объектов и правил определения используемых механизмов, комбинирование механизмов при реализации сервисов.

Администрирование механизмов безопасности включает в себя управление: ключами, шифрованием, доступом, аутентификацией, маршрутизацией, нотаризацией, дополнением трафика.

## Интерпретация «Оранжевой книги» для сетевых конфигураций

Данный документ (1987 г.) рассматривает интерпретацию «Оранжевой книги» для сетевых конфигураций, а также сервисы безопасности, специфичные или особо важные для сетевых конфигураций.

Интерпретация вводит понятие *сетевой доверенной вычислительной базы*. Сетевая доверенная вычислительная база формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. *Доверенная сетевая система* должна обеспечивать такое распределение защитных механизмов, чтобы общая политика безопасности реализовывалась, несмотря на уязвимость коммуникационных путей и на параллельную, асинхронную работу компонентов.

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит *криптография*, обеспечивающая поддержание конфиденциальности и целостности. Следствием использования криптографических методов является необходимость реализации механизмов *управления ключами*.

Особое внимание уделено *доступности* сетевых сервисов. Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслу

живании пользователей. Доверенная система должна иметь возможность обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

- *избыточность* конфигурации (резервное оборудование, запасные каналы связи и т.п.);
- наличие средств *переконфигурирования* для изоляции или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;
- *рассредоточенность* сетевого управления, отсутствие единой точки отказа;
- наличие средств *нейтрализации* отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);
- выделение подсетей и изоляция групп пользователей друг от друга.

## Гармонизированные критерии Европейских стран

«Гармонизированные критерии» созданы совместными усилиями Франции, Германии, Нидерландов и Великобритании (1991 г.).

Принципиально важной чертой «Европейских Критериев» является отсутствие требований к условиям, в которых должна работать информационная система. Так называемый *спонсор*, то есть организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции.

Задача органа сертификации — оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и реализация *механизмов безопасности* в описанных спонсором условиях.

В «Европейских Критериях» проводится различие между системами и продуктами. *Система* — это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. *Продукт* — это аппаратно-программный «пакет», который можно купить и по своему усмотрению встроить в ту или иную систему.

С точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и детально изучить, а продукт должен быть рассчитан на использование в различных условиях.

«Европейские Критерии» не содержат требований к политике безопасности и наличию защитных механизмов.

Каждая система или продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности. Чтобы удовлетворить эти требования, необходимо предоставить соответствующий набор *функций* (*сервисов*) *безопасности*, таких как идентификация и аутентификация, управление доступом или восстановление после сбоев.

Оценивается эффективность и корректность средств безопасности.

При проверке *эффективности* анализируется соответствие между целями, сформулированными для объекта оценки, и набором функций безопасности. В понятие эффективности входит способность механизмов защиты противостоять прямым атакам (*мощность механизма*). Определяются три градации мощности — базовая, средняя и высокая.

Под корректностью понимается правильность реализации функций и механизмов безопасности. Критерии определяют семь уровней гарантированности корректности — от E0 до E6 (в порядке возрастания). Уровень E0 означает отсутствие гарантированности. При проверке корректности анализируется весь жизненный цикл объекта оценки — от проектирования до эксплуатации и сопровождения.

Общая оценка системы складывается из минимальной мощности механизмов безопасности и уровня гарантированности корректности.

## «Общие критерии» (основные положения)

Оценочный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» называемый «Общими критериями» или просто «ОК», является самым современным и полным (1999 г.).

«Общие критерии» являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. Он определяет не классы безопасности, как «Оранжевая книга», а способ их построения, исходя из требований безопасности, существующих для конкретной организации или информационной системы.

«Общие критерии», как и «Оранжевая книга», содержат два основных вида требований безопасности:

- функциональные, соответствующие активному аспекту защиты; они предъявляются к функциям безопасности;
- требования доверия, соответствующие пассивному аспекту; они предъявляются к технологии и процессам разработки и эксплуатации.

Требования безопасности предъявляются для оценки, а их выполнение проверяется для конкретного объекта оценки (продукта или ИС).

Безопасность рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;

- проектирование и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация.

Объект оценки рассматривается в контексте *среды безопасности*, которая характеризуется определенными условиями и угрозами. Угрозы характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в:

- требованиях безопасности;
- проектировании;
- эксплуатации.

Пространство требований структурировано в виде иерархии «класс - семейство - компонент - элемент».

*Классы* определяют наиболее общую, «предметную» группировку требований (например, функциональные требования подотчетности).

*Семейства* в пределах класса различаются по строгости и другим нюансам требований.

*Компонент* — это минимальный набор требований, фигурирующий как целое.

*Элемент* — это неделимое требование.

На основе требований формируются два вида нормативных документов: профиль защиты и задание по безопасности.

*Профиль защиты* представляет собой типовой набор требований, которым должны удовлетворять продукты и системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

*Задание по безопасности* содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

В ОК нет готовых классов защиты. Сформировать классификацию в терминах «Общих критериев» — значит определить несколько иерархически упорядоченных профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования доверия безопасности.

*Функциональный пакет* — это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения.

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. При этом сформировано 11 классов: идентификация и аутентификация, защита данных пользователя, защита функций безопасности, управление безопасностью, аудит безопасности, доступ к объекту оценки, приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных), использование ресурсов, криптографическая поддержка, связь, доверенный маршрут (канал).

Требования доверия безопасности сгруппированы в 10 классов: действия разработчиков, представление и содержание свидетельств, поддержка жизненного цикла, тестирование, оценка уязвимостей (включая оценку стойкости функций безопасности), поставка и эксплуатация, управление конфигурацией, руководства (требования к документации), поддержка доверия (после сертификации), оценка профиля защиты.

## Руководящие документы ФСТЭК России

Важными документами ФСТЭК (Гостехкомиссии) России являются следующие *руководящие документы*:

1. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации», Москва, 1992.

2. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», Москва, 1992.

3. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации», Москва, 1992.

4. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации», Москва, 1998.

5. «Защита от несанкционированного доступа к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей», Москва, 1999.

6. Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР-97), утвержденные решением Государственной технической комиссии при Президенте РФ № 55 от 23.05.1997.

7. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденные приказом Государственной технической комиссии при Президенте РФ от 30.08.2002 № 282.

В классификации автоматизированных систем (АС) устанавливается девять классов защищенности [10]. Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

### Третья группа АС

- работает один пользователь, допущенный ко всей информации АС;
- все носители одного уровня конфиденциальности;
- содержит 2 класса – 3А и 3Б.

Администратор не является пользователем, если не участвует в технологическом процессе обработки информации.

## Вторая группа АС

- пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС;
- носители различного уровня конфиденциальности;
- содержит 2 класса – 2А и 2Б.

## Первая группа АС

- пользователи имеют разные права доступа к информации АС;
- носители различного уровня конфиденциальности;
- содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А (по возрастанию уровня защищенности).

## Требования к АС

| | Подсистемы и требования | Классы | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | 3Б | 3А | 2Б | 2А | 1Д | 1Г | 1В | 1Б | 1А |
| 1. | Подсистема управления доступом | | | | | | | | | |
| 1.1. | Идентификация, проверка подлинности и контроль доступа субъектов: | | | | | | | | | |
| | в систему; | + | + | + | + | + | + | + | + | + |
| | к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ; | – | + | – | + | – | + | + | + | + |
| | к программам; | – | + | – | + | – | + | + | + | + |
| | к томам, каталогам, файлам, записям, полям записей | – | + | – | + | – | + | + | + | + |
| 1.2. | Управление потоками информации. | – | – | – | + | – | + | + | + | + |
| 2. | Подсистема регистрации и учета | | | | | | | | | |
| 2.1. | Регистрация и учет: | | | | | | | | | |
| | входа/выхода субъектов доступа в/из системы (узла сети); | + | + | + | + | + | + | + | + | + |
| | выдачи печатных (графических) выходных документов; | – | + | – | + | – | + | + | + | + |
| | запуска/завершения программ и процессов (заданий, задач); | – | + | – | + | – | + | + | + | + |
| | доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи; | – | – | – | + | – | + | + | + | + |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей; | – | – | – | + | – | + | + | + | + |
| | изменения полномочий субъектов доступа; | – | – | – | – | – | – | + | + | + |
| | создаваемых защищаемых объектов доступа. | – | – | – | + | – | – | + | + | + |
| 2.2. | Учет носителей информации. | + | + | + | + | + | + | + | + | + |
| 2.3. | Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. | – | + | – | + | – | + | + | + | + |
| 2.4. | Сигнализация попыток нарушения защиты. | – | – | – | – | – | – | + | + | + |
| 3. | Криптографическая подсистема | | | | | | | | | |
| 3.1. | Шифрование конфиденциальной информации. | – | – | – | + | – | – | – | + | + |
| 3.2. | Шифрование информации, принадлежащей различным субъектам доступа(группам субъектов) на разных ключах. | – | – | – | – | – | – | – | + | + |
| 3.3. | Использование аттестованных (сертифицированных) криптографических средств. | – | – | – | + | – | – | – | + | + |
| 4. | Подсистема обеспечения целостности | | | | | | | | | |
| 4.1. | Обеспечение целостности программных средств и обрабатываемой информации. | + | + | + | + | + | + | + | + | + |
| 4.2. | Физическая охрана средств вычислительной техники и носителей информации. | + | + | + | + | + | + | + | + | + |
| 4.3. | Наличие администратора (службы) защиты информации в АС. | – | – | – | + | – | – | + | + | + |
| 4.4. | Периодическое тестирование СЗИ НСД. | + | + | + | + | + | + | + | + | + |
| 4.5. | Наличие средств восстановления СЗИ НСД. | + | + | + | + | + | + | + | + | + |
| 4.6. | Использование сертифицированных средств защиты. | – | + | – | + | – | – | + | + | + |

## Руководящие документы госкорпорации «Росатом»

Основные руководящие документы госкорпорации «Росатом» в области информационной безопасности следующие:

1. Стандарт отрасли. Оснащение программно-аппаратных систем учета и контроля ядерных материалов. Общие требования. ОСТ 95 10537-97.

2. Типовая инструкция по защите информации в автоматизированных системах предприятий и организаций Федерального агентства по атомной энергии (утверждена приказом руководителя Федерального агентства от 04.08.2006 №395).

## Классификация СУиК ЯМ

Критерии при выборе класса защищенности, по которым производится группировка СУиК ЯМ (систем управления и контроля ядерных материалов) по классам:

- наличие в СУиК ЯМ информации различной степени секретности;
- уровень полномочий субъектов доступа (пользователей) на доступ к секретной информации;
- порядок и условия размещения и функционирования, физическая защищенность средств вычислительной техники СУиК ЯМ.

Комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках СЗИ НСД, состоящей четырех подсистем, аналогичных подсистемам, определяемых руководящими документами ФСТЭК (Гостехкомиссии) России (управления доступом, регистрации и учета, криптографической, обеспечения целостности).

К каждой подсистеме в зависимости от класса СУиК ЯМ устанавливаются сертификационные и аттестационные требования.

### *Третий класс СУиК ЯМ*

- Информация строго одной степени секретности.
- Все субъекты доступа имеют равные права доступа (полномочия) ко всей информации СУиК ЯМ.
- Все средства вычислительной техники СУиК ЯМ размещаются в контролируемой зоне и не имеют внешних (выходящих за пределы контролируемой зоны) физических информационных связей.

### *Второй класс СУиК ЯМ*

- Информация нескольких степеней секретности
- Субъекты доступа имеют разные права доступа к информации СУиК ЯМ.

- Все средства вычислительной техники СУиК ЯМ размещаются в пределах одной или нескольких контролируемых зон, и не имеют незащищенных внешних физических информационных связей.

Защищенная физическая информационная связь — линия связи, оборудованная сертифицированными средствами, гарантирующими защиту передаваемой информации с требуемой степенью секретности.

***Первый класс СУиК ЯМ***

- Информация нескольких степеней секретности.
- Субъекты доступа имеют разные права доступа к информации СУиК ЯМ.
- Средства вычислительной техники СУиК ЯМ размещаются в контролируемой зоне и имеют внешние физические информационные связи со средствами вычислительной техники, не относящиеся к СУиК ЯМ.

## Сертификация и аттестация

Сертификация СЗИ – установление соответствия СЗИ набору требований, обеспечивающих защиту сведений, соответствующей степени секретности.

Аттестация – документированное подтверждение соответствия применяемого при эксплуатации комплекса организационно-технических мероприятий требованиям стандартов и иных нормативных документов по безопасности информации. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемой АС в реальных условиях эксплуатации с целью оценки соответствия используемого комплекса мер и средств защиты требуемому уровню безопасности.

***Органы по аттестации***

1. Центр «Атомзащитаинформ» - отраслевой орган по аттестации.
2. В качестве органов по аттестации могут выступать специальные подразделения некоторых предприятий отрасли, аккредитованные в установленном порядке (СНТО). Ряд из них имеет право аттестации АС и других предприятий отрасли (СНИО РФЯЦ ВНИИТФ).
3. Для АС, обрабатывающих информацию, не составляющую государственную тайну, аттестация может проводиться в установленном на предприятии порядке с привлечением необходимых специалистов.

***Особенности сертификационных требований 3 класса:***

Подсистема 1. Управление доступом

- идентификация и аутентификация при входе в ОС/доступу к СУБД (пароль — 8 символов);

- идентификация серверов, рабочих станций, внешних и сетевых устройств по физическим адресам;
- идентификация субъектов (процессов) и объектов по именам;
- идентификация объектов баз данных по именам.

Подсистема 2. Регистрация и учет
- входа/выхода пользователей в/из ОС;
- запуска/завершения программ;
- попыток доступа программ к защищаемым файлам;
- доступа к объектам базы данных.

Подсистема 4. Обеспечение целостности
- целостность программных средств и информационной базы СЗИ НСД (целостность СЗИ НСД проверяется при загрузке ОС);
- целостность информационной базы СЗИ НСД в СУБД обеспечивается посредством ее изолирования от пользователей и оперативного восстановления со стороны администратора.

***Особенности сертификационных требований 2 класса:***

Подсистема 1. Управление доступом (в дополнение к 3 классу)
- усилен контроль доступа к защищаемым объектам ОС и СУБД на основе дискреционной матрицы доступа;
- вводится требование ограничения доступа к объектам только через разрешенные процессы (замкнутая программная среда);
- вводятся требования мандатного разграничения доступа (метки секретности).

Подсистема 2. Регистрация и учет (в дополнение к 3 классу)
- регистрация печати секретных документов;
- регистрация доступа к узлам и фрагментам сети;
- регистрация выявленных ошибок при обмене данных по сети;
- автоматический учет создаваемых защищаемых файлов (с помощью меток секретности);
- двукратная очистка освобождаемых областей ОЗУ и внешних накопителей.

Подсистема 4. Обеспечение целостности
- требования совпадают с 3 классом.

***Особенности сертификационных требований 1 класса:***

Подсистема 1. Управление доступом (в дополнение ко 2 классу)
- усилены требования к аутентификации (методы, устойчивые к прослушиванию каналов и активному воздействию на передаваемые данные) пользователей при удаленном доступе к серверам и рабочим станциям, а также субъектов — источников данных.

Подсистема 2. Регистрация и учет (в дополнение ко 2 классу)

- регистрация изменений полномочий субъектов доступа и статуса объектов доступа;

- регистрация установления соединения между удаленными процессами;

- сигнализация попыток нарушения защиты на дисплей рабочей станции администратора и нарушителя.

- доступ к ключам – посредством подсистемы управления доступом.

Подсистема 3. Криптографическая подсистема (ранее не было)

- шифрование секретной информации на носителях и в каналах связи.

Подсистема 4. Обеспечение целостности (в дополнение ко 2 классу)

- целостность соединения для защиты передаваемых по сети данных пользователя (методы, устойчивые от прослушивания);

- доказательство источника данных/доставки данных с целью предотвращения попытки отрицать факт передачи/получения.

***Особенности аттестационных требований 3 класса***

Подсистема 1. Управление доступом

- доступ персонала к информации — в соответствии с действующей разрешительной системой допуска исполнителей к секретным документам и сведениям.

Подсистема 2. Регистрация и учет

- учет всех защищаемых носителей информации с помощью их любой маркировки;

- регистрация и учет печати документов — ручным способом в соответствии с требованиями делопроизводства соответствующей степени секретности, выдача документов на печать — в соответствии с установленным перечнем.

Подсистема 4. Обеспечение целостности

- целостность среды — отсутствие средств разработки и отладки программ;

- периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала СУиК ЯМ;

- средства восстановления СЗИ НСД;

- помещения СУиК ЯМ должны быть оборудованы техническими средствами охраны;

- СЗИ НСД должны быть сертифицированы для данного класса СУиК ЯМ.

***Особенности аттестационных требований 2 класса***

Подсистема 1. Управление доступом (см. 3 класс)

Подсистема 2. Регистрация и учет (см. 3 класс)

Подсистема 4. Обеспечение целостности (в дополнение к 3 классу)

- администратор защиты информации, ответственный за функционирование и контроль работы СЗИ НСД, выделенная рабочая станция средства контроля и воздействия на безопасность СУиК ЯМ;
- защищенные линии связи, выходящие за пределы контролируемых зон.

***Особенности аттестационных требований 1 класса***

Подсистема 1. Управление доступом (см. 3 класс)

Подсистема 2. Регистрация и учет (см. 3 класс)

Подсистема 3. Криптографическая подсистема

- сертифицированные СКЗИ.

Подсистема 4. Обеспечение целостности в дополнение ко 2 классу)

- межсетевые экраны, сертифицированные для СУиК ЯМ первого класса.

***Базовое программное обеспечение, сертифицированное для использования в компьютеризированных СУ и К ЯМ***

Операционные системы:

- MS Windows NT 4.0 Workstation (Russian) с пакетом обновления SP3 или SP5;
- MS Windows NT 4.0 Server с пакетом обновления SP3 или SP5;
- MS Windows NT 4.0 Server Enterprise Edition с пакетом обновления SP5;

Системы управления базами данных (СУБД):

Microsoft SQL Server версии 6.5 с пакетом обновления SP4 или SP5a.

- Oracle7 Server и Workgroup Server версии 7.3.4.0.0.
- Oracle8i Enterprise Edition версии 8.1.7.0.0.

## Сервисы безопасности

Программно-технические меры направлены на контроль компьютерных сущностей, — оборудования, программ и данных, — и образуют последний и самый важный рубеж информационной безопасности. Напомним, что ущерб наносят в основном действия легальных пользователей, по отношению к которым процедурные регуляторы неэффективны. Главные враги информационной безопасности — *некомпетентность* и *неаккуратность* при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

Следующий набор сервисов безопасности называют *полным* [1]:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

Считается, что данного набора достаточно для построения надежной защиты на программно-техническом уровне, правда, при соблюдении целого ряда дополнительных условий (таких, как отсутствие уязвимых мест, безопасное администрирование и т.п.).

Для проведения классификации сервисов безопасности и определения их места в общей архитектуре меры безопасности можно разделить на следующие виды:

- *превентивные*, препятствующие нарушениям ИБ;
- меры *обнаружения нарушений*;
- *локализующие*, сужающие зону действия нарушений;
- меры по *выявлению нарушителя*;
- меры по *восстановлению режима безопасности*.

Большинство сервисов безопасности являются превентивными.

Аудит и контроль целостности помогают обнаружить нарушения; активный аудит, кроме того, позволяет определить реакцию на нарушение с целью локализации или отслеживания действий. Направленность сервисов обеспечения отказоустойчивости и безопасного восстановления очевидна. Наконец, управление играет инфраструктурную роль, обслуживая все аспекты ИС.

## Архитектурная безопасность

Сервисы безопасности, какими бы мощными они ни были, сами по себе не могут гарантировать надежность защиты. Только проверенная архитектура способна сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

Теоретической основой решения проблемы архитектурной безопасности является следующее фундаментальное утверждение.

«Пусть каждый субъект (процесс, действующий от имени пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Пусть каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы проводят в жизнь согласованную политику безопасности. Наконец, пусть коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений всей сетевой конфигурации.»

С практической точки зрения наиболее важными являются следующие принципы архитектурной безопасности:

- *непрерывность защиты* в пространстве и времени, невозможность миновать защитные средства;
- *следование признанным стандартам*, использование апробированных решений; это повышает надежность ИС и уменьшает вероятность попадания в ситуацию, когда обеспечение безопасности потребует непомерно больших затрат и принципиальных модификаций;
- *иерархическая* организация информационной системы с ограниченным числом сущностей на каждом уровне; при нарушении данного принципа система может стать неуправляемой;
- усиление самого *слабого звена*; именно слабое звено определяет надежность всей системы защиты;
- невозможность перехода в *небезопасное состояние*; в любых ситуациях защитное средство должно либо полностью выполнять свои функции, либо полностью блокировать доступ;
- *минимизация* привилегий;
- *разделение* обязанностей;
- *эшелонированность* обороны;
- *разнообразие* защитных средств;
- *простота* и *управляемость* информационной системы.

## Идентификация и аутентификация

*Идентификация* позволяет пользователю или процессу, действующему от имени пользователя, обозначить себя при помощи соответствующего *учетного* имени.

*Аутентификация* удостоверяет, что субъект является тем, за кого он себя выдает. Синонимом термина «аутентификации» является термин «проверка подлинности».

Аутентификация может быть *односторонней* (в этом случае клиент доказывает свою подлинность серверу) или *двусторонней* (взаимной).

Примером односторонней аутентификации является обычная процедура входа пользователя в систему.

Субъект подтверждает свою подлинность, предъявляя по крайней мере одну из следующих сущностей:

- нечто, что он знает (например, пароль);
- нечто, чем он владеет (например, личную карточку);
- нечто, что есть часть его самого (биометрические характеристики).

В открытой сетевой среде, когда стороны идентификации и аутентификации территориально разнесены, данный сервис должен обеспечивать защиту данных во время их передачи по сети. Заметим, что передача пароля по сети в зашифрованном виде ничем не лучше передачи пароля в открытом виде. При прослушивании трафика злоумышленник фиксирует передаваемые данные в том виде, в каком они передаются. Поэтому для идентификации и аутентификации должны использоваться алгоритмы, не позволяющие воспроизвести протокол обмена.

Современные средства идентификации и аутентификации должны также поддерживать принцип *единого входа* в систему — если пользователь пользуется несколькими информационными сервисами, ему достаточно войти в систему один раз. Это ведет, с одной стороны, к усложнению систем идентификации и аутентификации, а с другой, — к поиску компромисса между надежностью защиты и удобством.

Заметим, что данный сервис может стать объектом атаки на доступность. Если сервис предоставляет возможность, например, только трех попыток входа в систему, после чего блокирует вход, злоумышленник легко может блокировать работу легального пользователя.

### *Парольная аутентификация*

Главное достоинство парольной аутентификации — простота и привычность. Пароли давно встроены в операционные системы и всевозможные сервисы, например, в СУБД. При правильном использовании парольная аутентификация обеспечивает необходимый уровень защиты.

Недостатки парольной аутентификации хорошо известны.

Пользователи часто выбирают хорошо запоминающиеся пароли, что позволяет легко угадывать их. Не менее часто пароли не устанавливаются совсем — используются пароли по умолчанию. Пароли записывают на листочках, которые приклеивают на, например, монитор, передают друзьям по телефону, в сообщениях электронной почты и т.п.

Ввод пароля можно подсмотреть при помощи, например, оптических средств или специальных программ. Пароль можно «взломать» методом «грубой силы» (перебором).

Следующие условия повышают надежность парольной защиты:

- пароль не должен быть коротким, и должен содержать не только буквы и цифры, н также знаки пунктуации и другие символы;
- срок действия пароля должен быть ограничен;
- доступ к файлу паролей должен быть исключен;
- вход в систему должен блокироваться после нескольких неудачных попыток входа.

***Одноразовые пароли***

Рассмотренные пароля можно назвать *многоразовыми*. Более устойчивыми к пассивному прослушиванию сети являются так называемые *одноразовые* пароли.

Рассмотрим систему S/KEY (компания Bellcore), которая имеет статус Internet-стандарта. Идея системы состоит в следующем. Пусть имеется односторонняя функция $f$, известная и пользователю, и серверу аутентификации, а также секретный ключ $K$, известный только пользователю. На этапе начального администрирования пользователя функция $f$ применяется $n$ раз к ключу $K$, результат сохраняется на сервере. Проверка подлинности пользователя происходит следующим образом:

- сервер присылает на пользовательскую систему число $(n–1)$;
- пользователь применяет функцию $f$ к секретному ключу $K$ $(n–1)$ раз и отправляет результат по сети на сервер аутентификации;
- сервер применяет функцию $f$ к полученному от пользователя значению и сравнивает результат с ранее сохраненным значением. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик $n$.

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или специальные интеллектуальные карты. Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронизированы.

### *Аутентификация с помощью биометрических данных*

В основе идентификации и аутентификации с помощью биометрических данных лежат физиологические и поведенческие характеристики конкретного человека. Биометрическими характеристиками являются, например, отпечатки пальцев, особенности сетчатки и роговицы глаза, геометрия рук и лица и т.п. К поведенческим характеристикам относятся стиль работы с клавиатурой, динамика ручной подписи и т.п. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

Для идентификации и аутентификации биометрических характеристик создается база данных, в которую заносятся *биометрические шаблоны*. В процессе идентификации (и аутентификации) биометрические характеристики обрабатываются тем же способом, что и при получении шаблона, а результат используется для поиска в базе данных.

Биометрическая идентификация часто используется вместе с другими средствами аутентификации, например, интеллектуальными картами. Иногда биометрическая аутентификация используется лишь для активизации интеллектуальной карты, которая содержит криптографические ключи и т.п. Биометрический шаблон в этом случае хранится на карте.

Несмотря на то, что биометрия кажется надежным средством идентификации и аутентификации, она также подвержена угрозам безопасности. Биометрические данные можно, например, подделать (воспроизвести). Кроме того, серьезную проблему составляют скомпрометированные биометрические данные.

### *Протокол Kerberos*

Протокол Kerberos был разработан в Массачусетском технологическом институте в середине 1980-х годов и сейчас является фактическим стандартом системы централизованной аутентификации и распределения ключей симметричного шифрования. Он поддерживается операционными системами семейства Unix, Windows NT и другими.

Протокол Kerberos обеспечивает распределение ключей симметричного шифрования и проверку подлинности пользователей, работающих в незащищенной сети. Реализация Kerberos — это программная система, построенная по архитектуре «клиент-сервер». Серверная часть Kerberos называется центром распределения ключей (Key Distribution Center, KDC) и состоит из двух компонент:

- сервер аутентификации (Authentication Server, AS);
- сервер выдачи разрешений (Ticket Granting Server, TGS).

Упрощенная схема функционирования протокола Kerberos показана на рисунке 1.

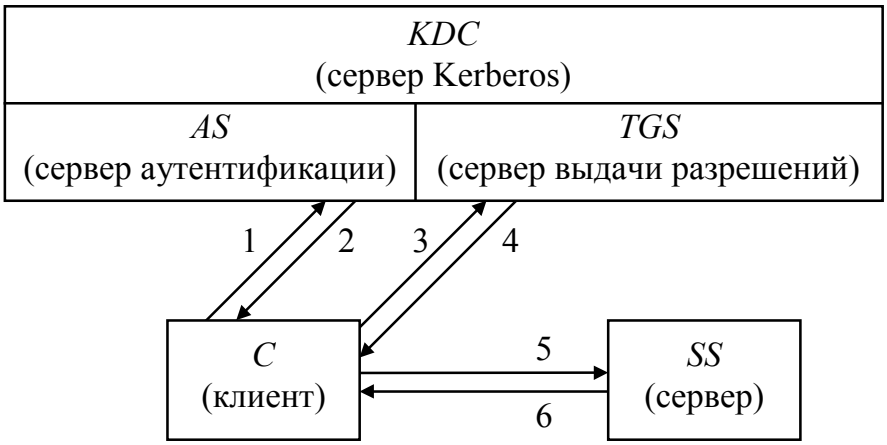


Рисунок 1 — Функционирование протокола Kerberos

Каждому субъекту сети сервер Kerberos назначает разделяемый с ним ключ симметричного шифрования и поддерживает базу данных субъектов и их секретных ключей.

В упрощенном виде протокол предполагает следующие шаги.

1. *C*→*AS*: {*c*}.

Клиент C посылает серверу аутентификации AS идентификатор клиента *c* (открытым текстом).

2. *AS*→*C*: $\{\{TGT\}K_{AS\text{-}TGS}, K_{C\text{-}TGS}\}K_C$,

$K_C$ — основной ключ *C*, $K_{C\_TGS}$ — ключ, выдаваемый *C* для доступа к серверу выдачи разрешений TGS, {TGT} — Ticket Granting Ticket — билет на доступ к серверу выдачи разрешений.

$\{TGT\} = \{c, tgs, t_1, p_1, K_{C\text{-}TGS}\}$, *tgs* — идентификатор сервера выдачи разрешений, $t_1$ — отметка времени, $p_1$ — период действия билета.

Запись $\{Y\}K_X$ означает, что Y зашифровано на ключе $K_X$.

Если нарушитель *X* посылает идентификатор клиента *c*, расшифровать посылку нельзя, не зная ключ клиента $K_C$. Доступ к содержимому билета TGT невозможен как для нарушителя, так и для клиента, т.к. он зашифрован ключом, известным только *AS* и *TGS*.

3. C→TGS: $\{\{TGT\}K_{AS\text{-}TGS}, \{Au_1\}K_{C\text{-}TGS}, \{ID\}\}$,

Клиент посылает серверу выдачи разрешений *TGS* полученный билет TGS, аутентификационный блок $Au_1 = \{c, t_2\}$, ключ $K_{C\_TGS}$, идентификатор ID сервиса, к которому требуется доступ; $t_2$ — метка времени.

Сервер выдачи разрешений расшифровывает билет TGT и получает информацию о том, кому, когда и на какой срок был выдан билет, ключ шифрования $K_{C\text{-}TGS}$. С помощью ключа $K_{C\text{-}TGS}$ расшифровывается аутентификационный блок. Если метка в блоке совпадает с меткой в билете, это доказывает, что посылку сгенерировал на самом деле *C*. Если проверка проходит и действующая в системе политика позволяет клиенту *C* обращаться к серверу *SS*, тогда выполняется шаг 4.

4. *TGS*→*C*: $\{\{TGS\}K_{TGS\text{-}SS}, K_{C\text{-}SS}\}K_{C\text{-}TGS}$,

$K_{C\text{-}SS}$ — ключ для взаимодействия *C* и *SS*, $\{TGS\} = \{c, ss, t_3, p_2, K_{C\text{-}SS}\}$ — Ticket Granting Service — билет для доступа к *SS*.

Здесь сервер выдачи разрешений *TGS* посылает клиенту *C* ключ шифрования и билет, необходимые для доступа к серверу *SS*.

5. *C*→*SS*: $\{\{TGS\}K_{TGS\text{-}SS}, \{Au_2\}K_{C\text{-}SS}\}$,

$Au_2 = \{c, t_4\}$.

Клиент *C* посылает билет, полученный от сервера выдачи разрешений, и свой аутентификационный блок серверу *SS*. Предполагается, что *SS* зарегистрирован и получил ключ шифрования $K_{TGS\text{-}SS}$. С помощью этого ключа *SS* может расшифровать билет, получить ключ шифрования $K_{C\text{-}SS}$ и проверить подлинность отправителя сообщения.

6. *SS*→*C*: $\{t_4+1\}K_{C\text{-}SS}$

Смысл этого шага заключается в том, что сервер *SS* должен доказать клиенту *C* свою подлинность. Он может сделать это, показав, что правильно расшифровал предыдущее сообщение. Поэтому *SS* берет отметку времени $t_4$, изменяет ее заранее определенным образом (увеличивает на единицу), шифрует на ключе $K_{C\text{-}SS}$ и возвращает *C*.

Если все шаги выполнены правильно и все проверки прошли успешно, то стороны взаимодействия *C* и *SS*, во-первых, удостоверились в подлинности друг друга, а во-вторых, получили ключ шифрования $K_{C\text{-}SS}$ для защиты сеанса связи.

## Управление доступом

Средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). Задача логического управления доступом состоит в том, чтобы для каждой пары «субъект-объект» определить множество допустимых операций и контролировать выполнение установленного порядка. Отношение «субъекты-объекты» можно представить в виде матрицы

$M = S \times Q \times R$,

S — множество субъектов, Q — множество объектов, R — множество прав доступа.

Это отношение можно представить в виде таблицы, в строках которой перечислены субъекты, в столбцах — объекты, а в ячейках — права доступа и дополнительные условия (например, время и место действия).

Права доступа могут быть:

Owner (O) — владелец объекта; это право разрешает передавать права доступа другим субъектам;

Read (R) — разрешение на чтение информации;

Write (W) — разрешение на запись (модификацию) информации;

Execute (E) — разрешение на выполнение;

Append (A) — разрешение на добавление информации и другие.

Задача управления доступом является достаточно сложной.

Во-первых, понятия объекта и прав доступа к нему в значительной степени зависят от защищаемого сервиса. Например, в операционной системе объектами являются процессы, потоки, файлы, события и другие. Процессы и потоки можно создавать, уничтожать, управлять их приоритетом, доступом к ресурсам и т.п. Файлы можно создавать, записывать, читать, выполнять и т.п. В СУБД объектами являются базы данных, таблицы, представления, хранимые процедуры, записи, отдельные поля и т.п. Многообразие объектов приводит к тому, что эффективное управление доступом может быть реализовано только в рамках конкретного сервиса, в котором множество объектов и операций постоянно, а это приводит к децентрализации управления доступом. Проблемой является также то, что к одним и тем же объектам можно получить доступ различными способами. Например, файл базы данных можно прочитать непосредственным образом (зная его структуру).

Во-вторых, права доступа существуют сами по себе, независимо от объектов. Например, после разрешенного извлечения информации из базы данных права на доступ к ней теряются (остаются в базе данных). То же происходит и при передаче файла на другую машину.

Существует два вида управления доступом: произвольное (или дискреционное) и принудительное (или мандатное).

Основой произвольного управления доступом является идентификатор субъекта. При этом права доступа легко гранулируются с точностью до пользователя (субъекта). При мандатном управлении доступом используются *метки безопасности*, приписываемые как субъектам, так и объектам.

Наиболее удобным и распространенным способом произвольного управления доступом являются списки управления доступом. Так как матрица управления доступом обычно является сильно разреженной, ее разбивают по столбцам с получением списков доступа — для каждого объекта поддерживается список допущенных субъектов вместе с их правами. При этом элементами списков могут быть имена групп и шаблоны субъектов, что упрощает администрирование.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают возможности совершения несанкционированных действий: интерфейс включает в число видимых объектов только те, к которым пользователь имеет доступ.

***Ролевое управление доступом***

При ролевом управлении доступом привилегии на доступ к информации определяются для *ролей*, а не для отдельных пользователей, а пользователи приписываются к определенным ролям (рисунок 2).

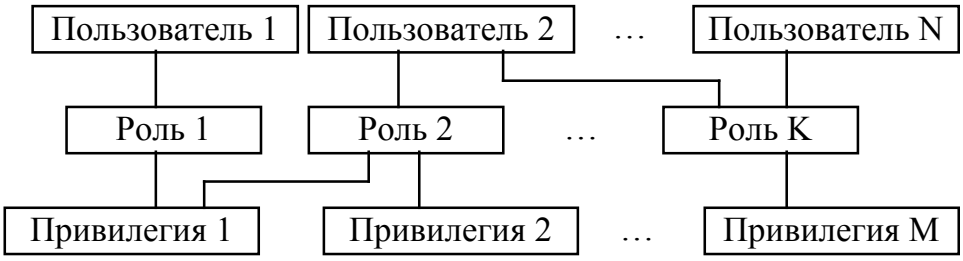


Рисунок 2 — Пользователи, роли и привилегии

Ролевое управление доступом оперирует следующими понятиями:
- пользователь;
- сеанс работы пользователя;
- роль;
- объект;
- операция;
- право доступа.

Ролям приписываются пользователи и права доступа. Во время сеанса работы пользователя активизируется подмножество ролей, которым он приписан с соответствующим предоставлением прав. Одновременно пользователь может открыть несколько сеансов.

Между ролями может быть определено отношение частичного порядка (наследование). Если роль B является наследницей A, то все права A приписываются B, а все пользователи B приписываются A.

Иерархия ролей начинается с минимума прав (и максимума пользователей), приписываемых наиболее общей роли, с постепенным уточнением состава пользователей и добавлением прав (рисунок 3).

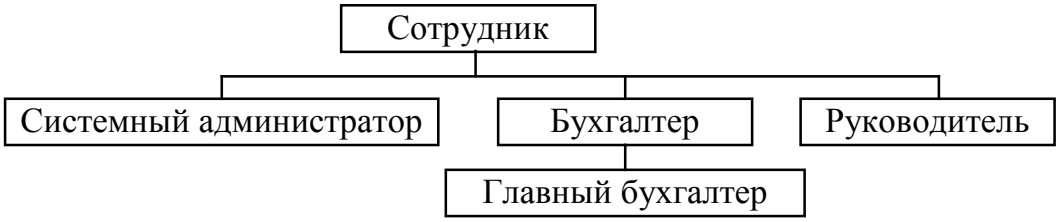


Рисунок 3 — Иерархия ролей

При использовании ролей вводится статическое и динамическое разделение обязанностей. Статическое разделение налагает ограничения на приписывание пользователей ролям. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному

множеству других ролей. Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях.

При динамическом разделении обязанностей рассматриваются роли, одновременно активные для данного пользователя. Например, один пользователь может играть роль и кассира, и контролера, но не одновременно. Тем самым реализуется так называемое временное ограничение доверия, являющееся аспектом минимизации привилегий.

Для администрирования ролевого управления доступом используются три категории функций:

- административные (управление ролями);
- вспомогательные (обслуживание сеансов работы пользователей);
- информационные.

## Протоколирование и аудит

Под *протоколированием* понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

*Аудит* — это анализ накопленной информации, проводимый в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется *активным*.

Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей;
- обеспечение возможности реконструкции событий;
- обнаружение попыток нарушений информационной безопасности;
- накопление информации для выявления и анализа проблем.

При протоколировании важно выяснить, какие события следует регистрировать и с какой степенью детализации. Разумный подход применительно к операционным системам предлагается в «Оранжевой книге», где выделяются следующие события:

- вход в систему (успешный или нет);
- выход из системы;
- обращение к удаленной системе;
- операции с файлами;
- смена привилегий или иных атрибутов безопасности.

Рекомендуется также выборочное протоколирование.

При протоколировании события рекомендуется записывать:

- дату и время события;
- идентификатор пользователя;
- тип события;
- результат действия (успех или неудача);
- источник запроса;
- имена затронутых объектов;
- описание изменений, внесенных в базы данных защиты.

***Активный аудит***

Под *подозрительной активностью* понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно некоторым критериям). Задача активного аудита — оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее.

Для описания и выявления подозрительной активности можно применять *сигнатуры* и их обнаружение во входном потоке событий с помощью аппарата экспертных систем.

*Сигнатура атаки* — это совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию. Простейший пример сигнатуры — «три последовательные неудачные попытки входа в систему с одного терминала», пример реакции — блокирование терминала.

Нетипичное поведение выявляется статистическими методами. В простейшем случае применяют систему порогов, превышение которых является подозрительным. В более совершенных системах производится сопоставление долговременных характеристик работы (называемых долгосрочным профилем) с краткосрочными профилями.

Применительно к средствам активного аудита различают ошибки первого и второго рода: пропуск атак и ложные тревоги соответственно.

Достоинства сигнатурного метода — высокая производительность, малое число ошибок второго рода, обоснованность решений. Основной недостаток — неумение обнаруживать неизвестные атаки и вариации известных атак.

Основные достоинства статистического подхода — универсальность и обоснованность решений, потенциальная способность обнаруживать неизвестные атаки, то есть минимизация числа ошибок первого рода.

Минусы заключаются в относительно высокой доле ошибок второго рода, плохой работе в случае, когда неправомерное поведение является типичным, когда типичное поведение плавно меняется от легального к неправомерному, а также в случаях, когда типичного поведения нет.

## Шифрование

Криптографические методы защиты подробнее рассматриваются в разделе «Криптографические методы». Криптография используется для реализации, как минимум, трех сервисов безопасности [1][3]:

- аутентификация;
- шифрование;
- контроль целостности.

Шифрование — наиболее мощное средство обеспечения конфиденциальности. Оно лежит в основе многих программно-технических регуляторов безопасности и является последним защитным рубежом. Криптографические методы защиты информации играют глубоко инфраструктурную роль, оставаясь прозрачными для приложений и для пользователей. Типичное место этих сервисов безопасности — на сетевом и транспортном уровнях реализации стека сетевых протоколов.

Существует два основных метода шифрования: симметричный и асимметричный. В симметричном шифровании один и тот же *секретный* ключ используется для зашифрования и для расшифрования. На настоящий момент разработаны эффективные (быстрые и надежные) методы симметричного шифрования. Самым известным является алгоритм DES (Data Encryption Standard). Существует и российский стандарт — ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Схема симметричного шифрования приведена на рисунке 4.

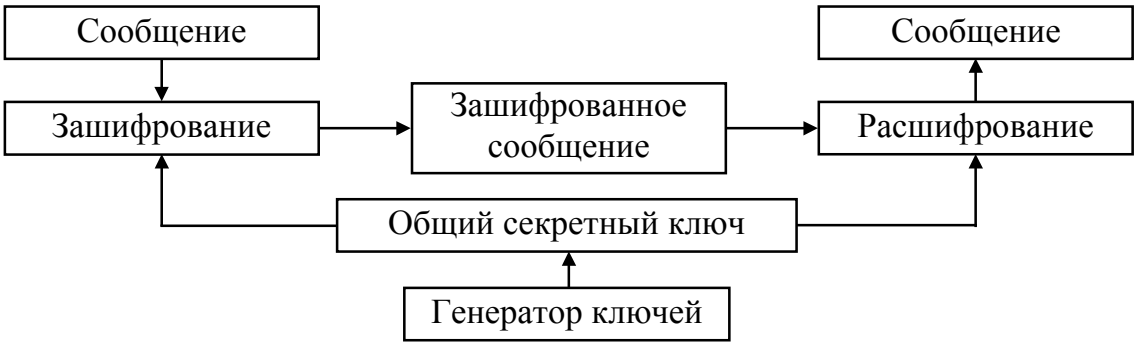


Рисунок 4 — Симметричное шифрование

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю.

С одной стороны, это создает новую *проблему распространения ключей*. С другой стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он может сгенерировать самостоятельно.

В асимметричном шифровании используется два ключа. Открытый (несекретный) ключ используется для зашифрования, а закрытый (секретный) ключ — для расшифрования. Самым известным методом симметричного шифрования является RSA (Rivest-Shamir-Adleman), основанный на операциях с очень большими простыми числами.

Схема асимметричного шифрования приведена на рисунке 5.

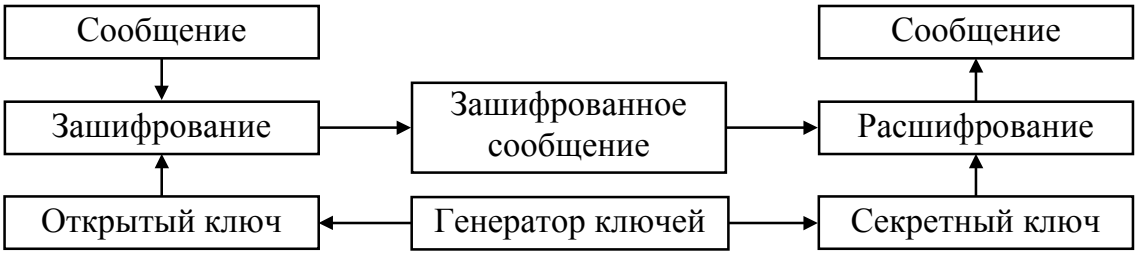


Рисунок 5 — Асимметричное шифрование

Недостатком асимметричного шифрования является низкое быстродействие (на 3 порядка медленнее симметричного шифрования). Эти два метода могут объединяться. Схема подобного эффективного шифрования показана на рисунке 6.

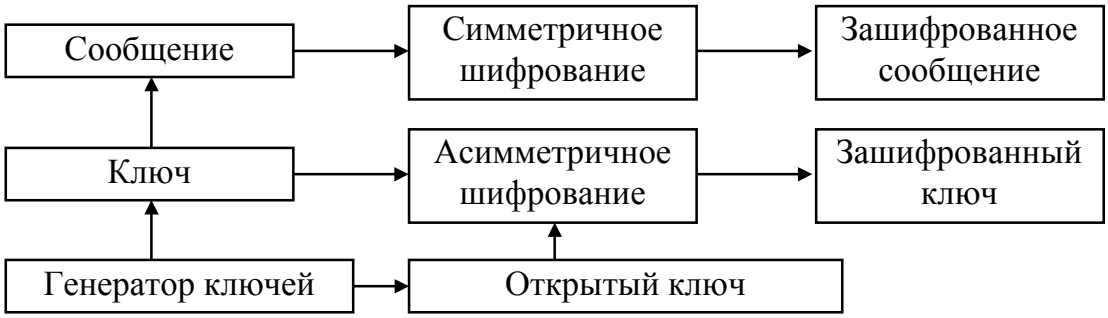


Рисунок 6 — Эффективное шифрование двумя методами

Для зашифрования сообщения используется уникальный для сеанса секретный ключ симметричного шифрования. Этот ключ шифруется методом асимметричного шифрования. Зашифрованные сообщение и ключ отправляются получателю. Получатель при помощи секретного ключа асимметричного шифрования сначала расшифровывает ключ, которым зашифровано сообщение, а затем расшифровывает сообщение.

Разработка методов асимметричного шифрования позволили решить важную проблему совместной выработки секретных ключей, используемых для обслуживания сеанса взаимодействия между отправителем и получателем. Для этой цели используется алгоритм Диффи-Хелмана.

Криптографические алгоритмы используются также для выработки псевдослучайных значений, которые необходимы для некоторых методов шифрования, а также для вычисления хеш-функций.

## Контроль целостности

Криптографический контроль целостности основан на использовании хэш-функций и электронных цифровых подписей (ЭЦП). С их помощью можно контролировать целостность как отдельных порций данных, так и их потоков, устанавливать подлинность источника данных и гарантировать неотказуемость (невозможность отказаться от совершенных действий).

Хеш-функция — это труднообратимое преобразование данных, основанное на методах симметричного шифрования. Эта односторонняя функция известна как отправителю, так и получателю сообщения.

Применение хеш-функции $h$ к некоторому сообщению T: $h$(T), вырабатывает блок данных $m$ фиксированной длины (например, 128 бит). Блок данных $m$ называют также *дайджестом* сообщения.

Пусть далее сообщение T передается получателю тем или иным образом. Обозначим полученное сообщение T'. Контроль целостности сообщения заключается в проверке равенства $m = h(\mathrm{T}')$.

Совпадение дайджестов для различных сообщений называется *коллизией*. Коллизии принципиально возможны, однако специально организовать коллизию за ограниченное время практически невозможно.

Электронная цифровая подпись вырабатывается на основе алгоритмов асимметричного шифрования. Обозначим E($m$) результат зашифрования с помощью открытого ключа, D($m$) — результат расшифрования с помощью секретного ключа. Для реализации ЭЦП должно выполняться равенство: E(D($m$)) = D(E($m$)) = $m$.

На рисунке 7 приведена схема использования ЭЦП.

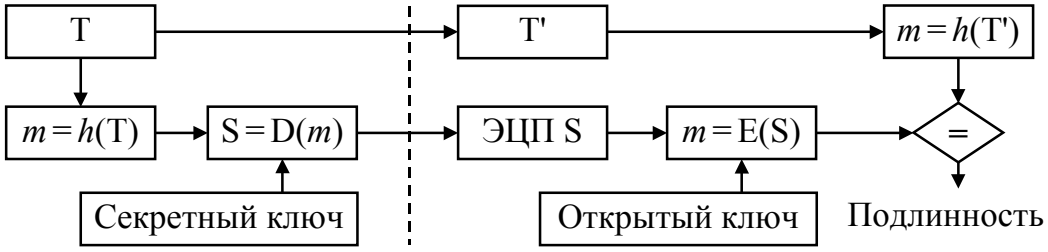


Рисунок 7 — Использование ЭЦП

Проверка подлинности сообщения T' осуществляется посредством вычисления дайджеста $m = h(\mathrm{T}')$ и его сравнения с результатом зашифрования ЭЦП открытым ключом: E(S) = $h$(T').

Для контроля целостности последовательности сообщений (то есть для защиты от кражи, дублирования и переупорядочения сообщений) применяют временные штампы и нумерацию элементов последовательности, при этом штампы и номера включают в подписываемый текст.

***Цифровые сертификаты***

При использовании асимметричных методов шифрования (в частности, ЭЦП) необходимо иметь гарантию подлинности пары (имя пользователя, открытый ключ пользователя). Для решения этой задачи в спецификациях X.509 вводятся понятия цифрового сертификата и удостоверяющего центра.

Удостоверяющий центр — это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится этими центрами в виде цифровых сертификатов, имеющих следующую структуру:

- порядковый номер сертификата;
- идентификатор алгоритма электронной подписи;
- имя удостоверяющего центра;
- срок годности;
- имя владельца сертификата;
- открытые ключи владельца сертификата;
- идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;
- электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат хеширования всей информации, хранящейся в сертификате).

Цифровые сертификаты обладают следующими свойствами:

- любой пользователь, знающий открытый ключ удостоверяющего центра, может узнать открытые ключи других клиентов центра и проверить целостность сертификата;
- никто, кроме удостоверяющего центра, не может модифицировать информацию о пользователе без нарушения целостности сертификата.

В спецификациях X.509 не описывается конкретная процедура генерации криптографических ключей и управления ими, однако даются некоторые общие рекомендации. В частности, оговаривается, что пары ключей могут порождаться любым из следующих способов:

- ключи может генерировать сам пользователь. В этом случае секретный ключ не попадает в руки третьих лиц, однако нужно решать задачу безопасной связи с удостоверяющим центром;
- ключи генерирует доверенное лицо. В этом случае приходится решать задачи безопасной доставки секретного ключа владельцу и предоставления доверенных данных для создания сертификата;
- ключи генерируются удостоверяющим центром. В этом случае остается только задача безопасной передачи ключей владельцу.

## Экранирование

В общем случае экран — это средство разграничения доступа между двумя множествами информационных сервисов (рисунок 8).

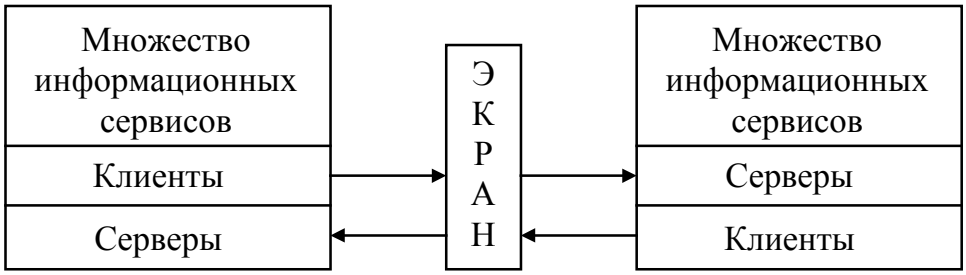


Рисунок 8 — Экран

Экран контролирует информационные потоки между этими множествами, при необходимости выполняя их фильтрацию и некоторые преобразования, а также протоколирование.

Экран удобно рассматривать как набор фильтров, каждый из которых, анализируя входной поток данных, либо пропускает его к следующему фильтру, либо задерживает, либо сразу «перебрасывает» за экран, либо отвечает отправителю запроса от имени адресата (рисунок 9).

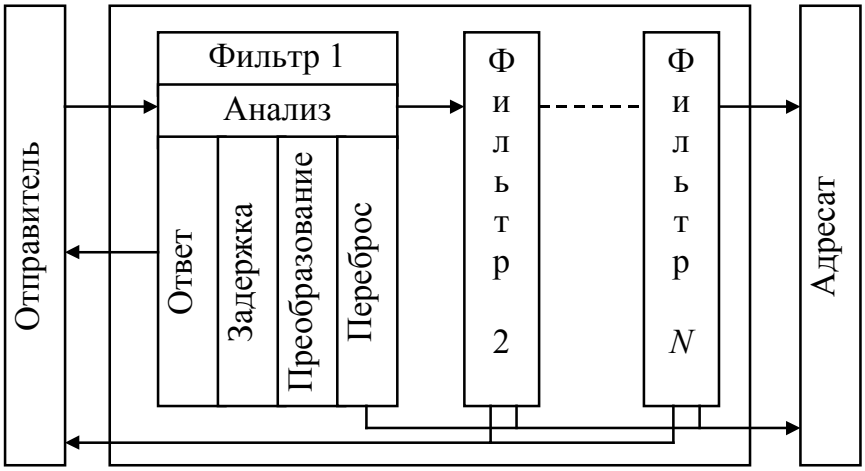


Рисунок 9 — Последовательность фильтров экрана

Обычно экран не является симметричным, для него определены понятия «внутри» и «снаружи». При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Так, межсетевые экраны (firewall) чаще всего устанавливают для защиты корпоративной сети организации от Интернет.

Экранирование помогает поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью.

Экранирование дает также возможность контролировать информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности в ИС организации.

Экранирование может быть частичным, защищающим только определенные информационные сервисы. Ограничивающий интерфейс также можно рассматривать как разновидность экранирования.

***Межсетевые экраны***

*Внешний* межсетевой экран (МЭ) располагается между защищаемой внутренней сетью и внешней средой (внешними сетями). *Внутренний* МЭ располагается между защищаемым сегментом корпоративной сети и другими ее сегментами.

Межсетевой экран — удобное место для встраивания средств активного аудита. На межсетевой экран целесообразно также возложить идентификацию и аутентификацию пользователей, нуждающихся в доступе к корпоративным ресурсам.

Для защиты внутренней сети организации часто используется двухкомпонентное экранирование (рисунок 10).


Рисунок 10 — Двухкомпонентное экранирование

Первичная фильтрация (например, блокирование пакетов протокола SNMP, опасного атаками на доступность) осуществляется граничным маршрутизатором, за которым располагается так называемая демилитаризованная зона (сеть с умеренным доверием безопасности) и основной МЭ, защищающий внутреннюю часть корпоративной сети.

Противоположностью составным корпоративным МЭ являются персональные межсетевые экраны и персональные экранирующие устройства. Первые являются программными продуктами, которые устанавливаются на персональные компьютеры и защищают только их. Вторые реализуются на отдельных устройствах и защищают небольшую локальную сеть, такую как сеть домашнего офиса.

***Классификация межсетевых экранов***

Межсетевые экраны принято классифицировать по уровню фильтрации в соответствии с семиуровневой эталонной моделью ISO/OSI — канальному, сетевому, транспортному или прикладному. Соответственно, говорят об экранирующих концентраторах, мостах и коммутаторах (на уровне 2), маршрутизаторах (уровень 3), о транспортном экранировании (уровень 4) и о прикладных экранах (уровень 7).

Экранирующие маршрутизаторы (и концентраторы) имеют дело с отдельными пакетами данных, поэтому иногда их называют пакетными фильтрами. Решение о том, пропустить или задержать данные, принимаются для каждого пакета независимо, на основании анализа адресов и других полей заголовков, а также порта.

Современные маршрутизаторы позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе, так и на выходе. В качестве пакетного фильтра может использоваться и универсальный компьютер с несколькими сетевыми картами.

Транспортное экранирование позволяет контролировать процесс установления виртуальных соединений и передачу информации по ним.

Межсетевой экран, функционирующий на прикладном уровне, способен обеспечить наиболее надежную защиту. Как правило, такой МЭ представляет собой универсальный компьютер, на котором функционируют экранирующие агенты, интерпретирующие протоколы прикладного уровня (HTTP, FTP, SMTP, telnet и т.д.) в той степени, которая необходима для обеспечения безопасности.

Помимо блокирования потоков данных, межсетевой экран может скрывать информацию о защищаемой сети, затрудняя действия потенциальных злоумышленников. Мощным методом сокрытия информации является трансляция «внутренних» сетевых адресов, которая попутно решает проблему расширения адресного пространства.

Дополнительные возможности межсетевых экранов:

- контроль информационного наполнения потоков (антивирусный контроль «на лету», верификация Java-апплетов, выявление ключевых слов в электронных сообщениях и т.п.);
- выполнение функций ПО промежуточного слоя.

Последний аспектов представляется важным, т.к. программное обеспечение промежуточного слоя может выполнять такие функции, как маршрутизация запросов и балансировка нагрузки. Это упрощает действия по обеспечению высокой доступности и позволяет осуществлять переключение на резервные мощности прозрачным для внешних пользователей образом.

**Анализ защищенности**

Данный сервис предназначен для выявления уязвимых мест с целью их оперативной ликвидации. Сам по себе этот сервис ни от чего не защищает, но помогает обнаружить и устранить пробелы в защите раньше, чем их сможет использовать злоумышленник. При этом имеются в виду «оперативные» бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий ПО.

Системы анализа защищенности, как и средства активного аудита, основаны на накоплении и использовании знаний о пробелах в защите. Ядром таких систем является база данных уязвимых мест, которая определяет доступный диапазон возможностей и требует практически постоянной актуализации.

Большинство систем анализа защищенности (XSpider, Internet Scanner, LanGuard, Nessus) обнаруживают уязвимости не только в операционных системах, но и в наиболее распространенном прикладном ПО.

Существуют два основных подхода, при помощи которых системы анализа защищенности обнаруживают уязвимости: *сканирование* и *зондирование* (имитация атаки). Из-за первого подхода данные системы называют «сканерами защищенности» или просто «сканерами».

При сканировании система анализа защищенности пытается определить наличие уязвимости по косвенным признакам, т.е. без фактического подтверждения ее наличия (посредством пассивного анализа). Данный подход является наиболее быстрым и простым в реализации.

При зондировании система анализа защищенности имитирует ту атаку, которая использует проверяемую уязвимость (активный анализ). Данный подход позволяет убедиться в наличии или отсутствии определенной уязвимости на анализируемом компьютере.

Эти два подхода реализуются в сканерах безопасности при помощи следующих методов:

- проверка заголовков (Banner check);
- активные зондирующие проверки (Active probing check);
- имитация атак (Exploit check).

Первый метод позволяет сделать вывод об уязвимости, опираясь на информацию в заголовке ответа на запрос сканера безопасности. Примером такой проверки может быть анализ заголовков почтовой программы Sendmail, в результате которого можно узнать ее версию и сделать вывод о наличии в ней уязвимости.

Активные зондирующие проверки сравнивают фрагменты сканируемого ПО с сигнатурой известной уязвимости. Разновидностями этого метода являются, например, проверки контрольных сумм или даты сканируемого программного обеспечения.

Имитация атак использует различные дефекты в программном обеспечении. При этом, как правило, нарушается нормальное функционирование сервисов тестируемой информационной системы, поэтому такое тестирование выполняется реже сканирования.

Контроль, обеспечиваемый системами анализа защищенности, носит запаздывающий характер — он не защищает от новых атак. Заметим, что подавляющее большинство атак возможны потому, что известные бреши в защите долгое время не устраняются.

## Обеспечение отказоустойчивости

В соответствии с ГОСТ 27.002, под отказом понимается событие, ведущее к нарушению работоспособности изделия. В контексте информационной безопасности под изделием следует понимать информационную систему или ее компонент.

Для оценки информационной системы с точки зрения надежности можно использовать следующие показатели:

- *эффективность услуг*; она может быть определена как максимальное время обслуживания запросов, количество одновременно обслуживаемых пользователей и т.п.

- *время недоступности*; определяется как максимальная продолжительность периода недоступности, а также суммарное время недоступности за определенный период (месяц, год).

Фактически требуется, чтобы информационная система почти всегда функционировала с заданной эффективностью. Для некоторых критически важных систем (например, систем управления) время недоступности должно быть практически нулевым. Для решения данной задачи создаются специальные отказоустойчивые системы, стоимость которых, как правило, относительно велика.

К подавляющему большинству коммерческих систем предъявляются менее жесткие ограничения, однако и здесь требования к надежности систем постоянно повышаются.

Среднее время наработки на отказ системы из $n$ компонентов можно оценить с помощью формулы:

$$T = \frac{1}{\lambda_1 + \ldots + \lambda_i + \ldots + \lambda_n},$$

$\lambda_i$ — интенсивность отказов компонента $i$ системы.

Полагая для простоты, что отказ одного компонента ведет к отказу всей системы, можно сделать вывод, что наработка на отказ всей системы определяется компонентом, интенсивность отказов которого существенно больше, чем интенсивность отказов других компонентов.

Надежность системы определяется не только временем наработки на отказ, но также и временем неработоспособности компонента в случае его отказа, поэтому требуется минимизировать это время.

При разработке мер обеспечения высокой эффективности информационных сервисов рекомендуется руководствоваться следующими архитектурными принципами:

- апробированность всех процессов и составных частей ИС;
- унификация процессов и составных частей;
- управляемость процессов, контроль состояния частей;
- автоматизация процессов;
- модульность архитектуры;
- ориентация на простоту решений.

Основным средством повышения отказоустойчивости является внесение избыточности в конфигурацию аппаратных и программных средств, поддерживающей инфраструктуры и персонала, резервирование технических средств и тиражирование информационных ресурсов.

Меры по обеспечению отказоустойчивости можно разделить на локальные и распределенные. Локальные меры направлены на повышение «живучести» отдельных компьютерных систем. Типичные примеры таких мер — использование кластерных конфигураций в качестве платформы критичных серверов или «горячее» резервирование активного сетевого оборудования с автоматическим переключением на резерв.

Распределенные меры обеспечения отказоустойчивости направлены на поддержание работоспособности организации в целом.

Информационные системы обычно находятся в постоянном развитии. Это требует непрерывного контроля за соответствием средств обеспечения отказоустойчивости текущему состоянию аппаратных и программных ресурсов системы. Если аппаратуру можно считать относительно статичной составляющей, то программное обеспечение и данные являются динамически развивающейся частью, требующей постоянного резервирования (тиражирования).

Выделяют следующие классы тиражирования:

- Симметричное и асимметричное. Тиражирование называется симметричным, если все серверы, предоставляющие данный сервис, могут изменять принадлежащую им информацию и передавать изменения другим серверам.
- Синхронное и асинхронное. Тиражирование называется синхронным, если изменение передается всем экземплярам сервиса в рамках одной распределенной транзакции.
- Осуществляемое средствами сервиса или внешними средствами.

## Обеспечение безопасного восстановления

Меры по обеспечению безопасного восстановления направлены на снижение сроков диагностирования и устранения отказов и их последствий. Для обеспечения безопасного восстановления рекомендуется соблюдать следующие архитектурные принципы:

- ориентация на построение информационной системы из унифицированных компонентов с целью упрощения замены отказавших частей;
- ориентация на решения модульной структуры с возможностью автоматического обнаружения отказов, динамического переконфигурирования аппаратных и программных средств и замены отказавших компонентов в «горячем» режиме.

Динамическое переконфигурирование преследует две цели:

- изоляция отказавших компонентов;
- сохранение работоспособности сервисов.

Средства повышения обслуживаемости системы в целом:

- программирование реакции на отказ; в простейшем случае отправляется сообщение системному администратору; в более сложном случае выполняется «мягкое» выключение (или переключение) сервиса;
- возможность удаленного выполнения административных действий;
- централизованное распространение и конфигурирование программного обеспечения, управление компонентами информационной системы и диагностирование;
- организация консультационной службы для пользователей.

## Туннелирование

Суть туннелирования состоит в том, чтобы «упаковать» передаваемую порцию данных, вместе со служебными полями, в некоторый «конверт». В качестве синонимов термина «туннелирование» могут использоваться «конвертование» и «обертывание».

Туннелирование может применяться для нескольких целей:

- передачи через сеть пакетов, принадлежащих протоколу, который в данной сети не поддерживается (например, передача пакетов IPv6 через устаревшие сети, поддерживающие только IPv4);
- обеспечения слабой формы конфиденциальности (в первую очередь конфиденциальности трафика) за счет сокрытия истинных адресов и другой служебной информации;
- обеспечения конфиденциальности и целостности передаваемых данных при использовании вместе с криптографическими сервисами.

Туннелирование может применяться на сетевом и прикладном уровнях. Например, стандартизовано туннелирование для IP и двойное конвертование для почты X.400.

Комбинация туннелирования и шифрования на выделенных шлюзах и экранирования на маршрутизаторах поставщиков сетевых услуг позволяет реализовать такое важное в современных условиях защитное средство, как виртуальные частные сети. Подобные сети, наложенные поверх Интернет, дешевле и безопаснее, чем собственные сети организации, построенные на выделенных каналах.

Концами туннелей, реализующих виртуальные частные сети, целесообразно сделать межсетевые экраны, обслуживающие подключение организаций к внешним сетям (рисунок 11).


Рисунок 11

В таком случае туннелирование и шифрование являются дополнительными преобразованиями, выполняемыми в процессе фильтрации сетевого трафика наряду с трансляцией адресов. Концами туннелей могут быть межсетевые экраны мобильных компьютеров сотрудников.

## Управление

Управление является инфраструктурным сервисом, обеспечивающим нормальную работу компонентов и средств безопасности. Сложность современных систем такова, что без правильно организованного управления они постепенно деградируют как в плане эффективности, так и в плане защищенности.

Согласно стандарту X.700, управление подразделяется на:

- мониторинг компонентов;
- контроль (выдачу и реализацию управляющих воздействий);
- координацию работы компонентов системы.

Системы управления должны:

- позволять администраторам планировать, организовывать, контролировать и учитывать использование информационных сервисов;
- давать возможность отвечать на изменение требований;
- обеспечивать предсказуемое поведение информационных сервисов;
- обеспечивать защиту информации.

В X.700 выделяется пять функциональных областей управления:

- управление конфигурацией;

- управление отказами;
- управление производительностью;
- управление безопасностью;
- управление учетной информацией.

В стандартах семейства X.700 вводится понятие управляемого объекта как совокупности характеристик компонента системы, важных с точки зрения управления. К таким характеристикам относятся:

- атрибуты объекта;
- допустимые операции;
- извещения, которые объект может генерировать;
- связи с другими управляемыми объектами.

Согласно рекомендациям X.701, системы управления распределенными ИС строятся в архитектуре менеджер-агент. Менеджер выдает агентам команды на управляющие воздействия и получает извещения. Агент выполняет управляющие действия и генерирует извещения от имени объекта.

Ключом к распределенному, масштабируемому управлению большими системами является многоуровневая архитектура менеджер-агент, в которой элементы промежуточных уровней по отношению к вышестоящим элементам являются агентами, а по отношению к нижестоящим — менеджерами.

Логически связанной с многоуровневой архитектурой является концепция доверенного управления. При доверенном управлении менеджер промежуточного уровня может управлять объектами, использующими собственные протоколы, в то время как «наверху» опираются исключительно на стандартные средства. Обязательным элементом при любом числе архитектурных уровней является управляющая консоль.

Ключевую роль играет модель управляющей информации. Она описывается рекомендациями X.720. Модель является объектно-ориентированной с поддержкой инкапсуляции и наследования. Дополнительно вводится понятие пакета как совокупности атрибутов, операций, извещений и соответствующего поведения.

Класс объектов определяется позицией в дереве наследования, набором включенных пакетов и внешним интерфейсом, то есть видимыми снаружи атрибутами, операциями, извещениями и демонстрируемым поведением.

Концептуально важным является понятие «проактивного», то есть упреждающего управления. Упреждающее управление основано на предсказании поведения системы на основе текущих данных и ранее накопленной информации.

## Криптографические методы

Классическая криптография занимается исследованием систем *засекреченной связи*. Под системой засекреченной связи понимается система передачи информации, в которой смысл передаваемой информации скрывается с помощью криптографических преобразований.

Криптографические методы и средства в целях защиты электронной информации могут использоваться для:

- идентификации и аутентификации;
- шифрования данных, хранящихся в виде файлов;
- шифрования всего информационного трафика или отдельных сообщений, передаваемых через открытые каналы связи;
- контроля целостности программного обеспечения при помощи криптостойких контрольных сумм;
- обеспечения целостности и достоверности передаваемой информации при помощи электронной цифровой подписи (ЭЦП);
- обеспечения юридической значимости электронных платежных документов при помощи ЭЦП;
- обеспечения неотслеживаемости действий клиента в электронных платежных системах, использующих понятие электронных денег;
- обеспечения неотказуемости (невозможности отказаться от совершенных действий).

Для реализации многих методов криптографической защиты требуются криптографические протоколы (то есть последовательности действий субъектов или объектов для достижения заданной цели). Криптографические протоколы используются, например, для:

- обмена ключевой информацией;
- аутентификации сторон, устанавливающих связь;
- авторизации пользователей информационных систем и служб.

### Основные понятия криптографии

Введем несколько понятий, используемых в криптографии.

Будем называть *открытым* сообщением (или открытым текстом) текст, предназначенный для передачи по открытым (незащищенным) каналам связи. Соответственно, *закрытым* сообщением (открытым текстом, шифртекстом) будем называть результат применения криптографического преобразования к некоторому открытому тексту.

Заметим, что под текстом в общем случае следует понимать набор символов над некоторым заданным алфавитом. На практике текст может представлять собой поток битов, файл, сетевой фрейм и т.п.

*Зашифрование* — это процесс криптографического преобразования множества открытых сообщений в множество закрытых сообщений.

*Расшифрование* — процесс криптографического преобразования закрытых сообщений в открытые.

*Ключ* — элемент криптографического преобразования, применяемый для зашифрования отдельного сообщения. Ключ обеспечивает выбор одного варианта преобразования из множества возможных. Множество всех возможных ключей называют *пространством ключей*.

*Криптосистема* — программная (программно-аппаратная) система, осуществляющая криптографическое преобразование. Она состоит из пространства ключей, множеств открытых и закрытых текстов, а также алгоритмов зашифрования и расшифрования.

*Дешифрование* — процесс нахождения открытого сообщения, соответствующего заданному закрытому сообщению при неизвестном криптографическом преобразовании.

*Криптоанализ* — раздел прикладной математики, изучающий методы, алгоритмы, а также программные и аппаратные средства анализа криптосистем с целью их раскрытия.

Способность криптосистемы противостоять атакам с целью извлечения открытых текстов, алгоритмов шифрования и пространства ключей называется ее *стойкостью* (или *криптостойкостью*).

Теоретически возможно создание *абсолютно стойкого* алгоритма шифрования. Клод Шеннон показал, что абсолютно стойким будет являться алгоритм, в котором:

- длина открытого сообщения и ключа одинаковы;
- ключ используется только один раз;
- выбор ключа осуществляется равновероятным образом.

На практике создание абсолютно стойких криптосистем невозможно в силу ряда причин. Например, для выполнения первого и второго условия требуется наличие неограниченного количества ключей достаточно большой длины. Выбор ключа равновероятным образом также является возможным только теоретически.

В качестве примера рассмотрим шифрование потока битов.

*Гамма шифра* — псевдослучайная двоичная последовательность, используемая для зашифрования и расшифрования.

*Гаммирование* — процесс наложения по определенному закону гаммы шифра на открытый текст.

В первой строчке показан поток шифруемых битов, во второй — некоторая случайная последовательность. Для зашифрования используется побитовое сложение по модулю 2 (операция XOR):

```
1 1 0 0 1 1 0 0 1 1 1 1 . . . — открытый входной поток
1 0 1 0 0 0 1 1 1 0 0 1 . . . — гамма шифра
0 1 1 0 1 1 1 1 0 1 1 0 . . . — закрытый выходной поток
```

Для расшифрования полученного в третьей строчке потока вновь требуется гамма шифра, использованная при зашифровании. Если мы можем воспроизвести эту последовательность во время расшифрования, то она не является псевдослучайной.

Кроме того, успешные атаки на алгоритмы шифрования возможны вследствие того, что в исторически сложившихся языках существуют *статистические структуры*. Например, некоторые символы и их комбинации чаще других встречаются в текстах (в естественной речи). Некоторые слова присутствуют во всех сообщениях определенного назначения. Это дает возможность криптоанализа посредством определенных статистических методов.

Для скрытия подобной статистической зависимости в закрытых текстах при зашифровании используются *диффузия* (рассеивание) и *конфузия* (запутывание и перемешивание).

*Рассеивание* заключается в распространении влияния одного символа открытого текста на множество символов закрытого текста.

*Запутывание* заключается в распространении влияния одного символа ключа (гаммы шифра) на множество символов закрытого текста.

*Перемешивание* заключается в распространении статистических последовательностей открытого текста по всему пространству возможных закрытых текстов.

Рассмотрим пример. Пусть шифрование осуществляется посредством инвертирования байтов B, то есть выполнения операции 255–B.

Пусть открытый текст «this is an apple». В следующей таблице приведены коды символов и результаты зашифрования:

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| t | h | i | s | | i | s | | a | n | | a | p | p | l | e |
| 116 | 104 | 105 | 115 | 032 | 105 | 115 | 032 | 097 | 110 | 032 | 097 | 112 | 112 | 108 | 101 |
| 139 | 151 | 150 | 140 | 223 | 150 | 140 | 223 | 158 | 145 | 223 | 158 | 143 | 143 | 147 | 154 |
| ‹ | — | – | Œ | ß | – | Œ | ß | ž | ‘ | ß | ž | ▯ | ▯ | “ | š |

В последней строке таблицы приведен вид зашифрованных байтов с использованием кодировки ANSI. Анализируя таблицу, можно заметить, что одним и тем же символам открытого текста соответствуют одни и те же символы закрытого текста. Если, например, нам известно, что открытый текст содержит слово this или is (что весьма вероятно), то, анализируя разности кодов закрытого текста и сравнивая их с разностями кодов открытого текста (например, слова this), можно легко установить алгоритм, использованный для зашифрования.

Для скрытия статистической зависимости между кодами открытого текста поступим следующим образом. Будем рассматривать текст в виде блоков из восьми последовательных байт.

Запишем биты первого байта в биты 7 первых восьми байт закрытого текста, биты второго байта в биты 6 восьми байт закрытого текста и т.д. В результате зашифрования получим:

| t | h | i | s | | i | s | | a | n | | a | p | p | l | e |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 116 | 104 | 105 | 115 | 032 | 105 | 115 | 032 | 097 | 110 | 032 | 097 | 112 | 112 | 108 | 101 |
| 000 | 246 | 255 | 146 | 100 | 128 | 018 | 054 | 000 | 223 | 255 | 012 | 066 | 067 | 064 | 145 |
| | ö | · | ’ | d | € | | 6 | | ß | · | | B | C | @ | ‘ |

Очевидно, что статистическую зависимость в этом закрытом тексте не так легко обнаружить, как в предыдущем примере. Приведенный алгоритм является обратимым — с его помощью можно расшифровать закрытый текст (что возможно не для всех алгоритмов). Заметим, что данные примеры приведены исключительно для пояснения и имеют лишь косвенное отношения к реальным алгоритмам шифрования.

*Безопасность*, обеспечиваемая алгоритмом шифрования, зависит от многих факторов.

Во-первых, криптографический алгоритм должен быть достаточно сильным, чтобы передаваемое зашифрованное сообщение невозможно было расшифровать без ключа, используя только различные статистические закономерности зашифрованного сообщения или какие-либо другие способы его анализа.

Во-вторых, безопасность передаваемого сообщения должна зависеть от секретности ключа, а не от секретности алгоритма. Криптоалгоритм должен исключать наличие слабых мест, при которых плохо скрыта взаимосвязь между открытыми и закрытыми сообщениями. К тому же при выполнении этого условия производители могут создавать дешевые аппаратные чипы и свободно распространяемые программы, реализующие данный алгоритм шифрования.

В-третьих, алгоритм должен быть таким, чтобы нельзя было узнать ключ, зная достаточно много пар (закрытый текст, открытый текст), полученных при зашифровании с использованием данного ключа.

Если говорить об алгоритмах, используемых для защиты электронной информации, то эти алгоритмы не являются секретными и всегда точно известно, где и какой алгоритм используется. Защитные свойства этих алгоритмов определяются секретностью ключа и невозможностью подобрать его за ограниченное время.

В классической криптографии (или в исторической криптографии) зачастую используются алгоритмы шифрования, которые являются секретом для потенциального противника. Все они со временем раскрываются (посредством криптоанализа или иных методов), однако при этом появляются новые, более изощренные.

## Операции и алгоритмы криптографии

В криптографии используются два вида преобразований: *замена* (*подстановка*) и *перестановка*. При замене символы открытого текста заменяются символами закрытого текста. Перестановка заключается в перемешивании символов.

Можно говорить о перестановочных алгоритмах шифрования, об алгоритмах замены, а также о комбинациях этих алгоритмов. В классической криптографии выделяют четыре типа шифров замены.

1) *Шифры простой замены*. Один символ открытого текста заменяется одним символом закрытого текста.

2) *Шифры сложной замены*. Один символ открытого текста заменяется одним или несколькими символами закрытого текста.

3) *Шифры блочной замены*. Один блок символов открытого текста заменяется на блок символов закрытого текста.

4) *Полиалфавитные шифры замены*. К открытому тексту применяется несколько шифров простой замены.

В качестве примера рассмотрим несколько известных шифров.

В шифрах перестановки для зашифрования используется таблица, в которой номер ячейки соответствует номеру символа открытого текста, а значение в ячейке — номеру символа в закрытом тексте. Пример использования таблицы перестановки (первая строка — открытый текст, последняя строка — закрытый текст):

| | | | | | | |
|---|---|---|---|---|---|---|
| С | е | м | е | с | т | р |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 6 | 4 | 1 | 5 | 7 | 3 |
| е | т | е | С | с | р | т |

Простым и самым древним шифром замены является шифр, который использовал Юлий Гай Цезарь. В шифре *Цезаря* каждая буква алфавита заменяется буквой, находящейся на три позиции дальше. Этот алгоритм шифрования выражается следующими формулами:

$C_i = (P_i + k) \bmod N$,

$P_i = (C_i - k) \bmod N$,

$C_i$ — символ закрытого текста, $P_i$ — символ открытого текста, $N = 32$ (число букв в кириллическом алфавите), $k = 3$.

В шифре *Плейфейера* замене подвергаются комбинации из двух или более символов.

В шифре *Хилла* каждые $m$ последовательных символов открытого текста заменяются на $m$ символов закрытого текста в соответствии с некоторой системой линейных уравнений.

Например, при $m = 3$ используется система:

$C_1 = (k_{11}P_1 + k_{12}P_2 + k_{13}P_3) \bmod N,$
$C_2 = (k_{21}P_1 + k_{22}P_2 + k_{23}P_3) \bmod N,$
$C_3 = (k_{31}P_1 + k_{32}P_2 + k_{33}P_3) \bmod N.$

В шифре *Виженера* используется таблица размером N×N, N — число букв алфавита. Первая строка содержит буквы алфавита в прямом порядке. Каждая последующая строка циклически сдвинута на одну букву влево или вправо (приведена только часть таблицы):

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

При зашифровании под каждой буквой открытого текста записывается буква ключа (при необходимости ключ циклически повторяется). Буква закрытого текста находится в таблице на пересечении столбца, определяемого буквой открытого текста и строки, определяемой буквой ключа. При расшифровании под буквами закрытого текста записывают буквы ключа. В строке таблицы, соответствующей букве ключа, ищется буква закрытого текста. Буква первой строки над найденной буквой закрытого текста является буквой открытого текста.

Пусть открытый текст «КОРОНА», а ключ — «БРОСОК», тогда закрытый текст будет «ЛЮЮЯЫК»:

| | | | | | |
|---|---|---|---|---|---|
| К | О | Р | О | Н | А |
| Б | Р | О | С | О | К |
| Л | Ю | Ю | Я | Ы | К |

При зашифровании буквы «К» буква «Л» находится на пересечении столбца «К» и строки «Б». При расшифровании буква «К» находится в первой строке в столбце, в котором буква «Л» находится в строке «Б».

Упомянутые шифры представляют только исторический интерес, так как они никаким образом не могут быть использованы для защиты электронной информации.

Современные алгоритмы шифрования используют однократные или многократные преобразования символов или блоков символов с применением таких простых операций, как сложение по модулю 2 (обозначается $\oplus$) или 32, инверсия (not), циклический сдвиг и перестановки.

Операция сложения по модулю 2 и инверсия обладают свойством *идемпотентности* — двукратное применение этих операций возвращает первоначальное значение: $(b \oplus k) \oplus k = b$. Это позволяет применять одни и те же преобразования при зашифровании и расшифровании. Используются также труднообратимые математические функции.

## Классификация криптоалгоритмов

На рисунке 12 приведена классификация современных алгоритмов, используемых при шифровании электронной информации [3][5].

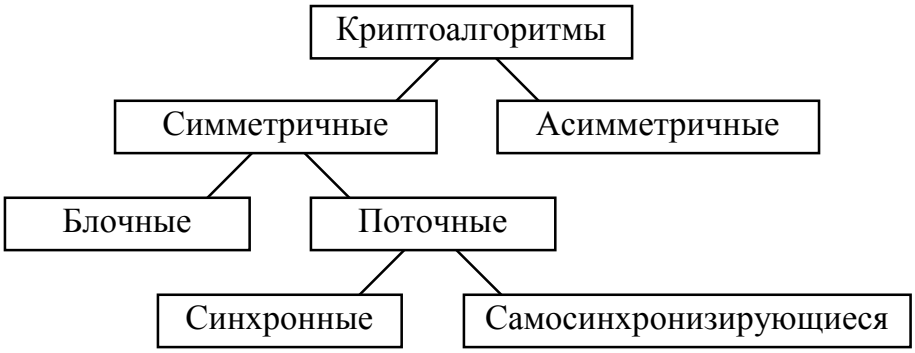


Рисунок 12 — Классификация криптоалгоритмов

Все алгоритмы шифрования делятся на две группы: симметричные и асимметричные. В симметричных алгоритмах для зашифрования и расшифрования используется один и тот же секретный ключ. В асимметричных алгоритмах для зашифрования используется открытый (несекретный) ключ, а для расшифрования — закрытый (секретный) ключ.

Симметричные и асимметричные алгоритмы шифрования появились относительно недавно (наиболее известные алгоритм симметричного шифрования DES и алгоритм асимметричного шифрования RSA появились примерно в 1977 г.).

В *блочных* алгоритмах открытый текст разбивается на блоки фиксированного размера (например, в DES размер блока равен 64 битам). При необходимости текст дополняется незначащими символами до получения длины, кратной размеру блока. Размер ключа в блочных алгоритмах также фиксирован. В принципе, размер ключа в этом случае определяет стойкость алгоритма к подбору ключа методом «грубой силы». Блочные алгоритмы являются также *симметричными* — для зашифрования и расшифрования в них используется один и тот же алгоритм.

В *поточных* алгоритмах каждый отдельный символ открытого текста зашифровывается независимо от других и расшифровывается таким же образом. Можно сказать, что каждый символ открытого текста при поточном шифровании подвергается собственному преобразованию (хотя количество преобразований символа не так уж и велико). Используемая при поточном шифровании гамма шифра вырабатывается на основе секретного ключа. Стойкость поточного алгоритма зависит от того, насколько выработанная гамма шифра обладает свойством равновероятности появления очередного символа гаммы. Гамму шифра нельзя использовать более одного раза, иначе ее можно будет вычислить.

С поточными алгоритмами связана проблема синхронизации на передающей и приемной сторонах (определения момента начала применения гаммы шифра). Различают два метода синхронизации шифраторов:

- *синхронные* шифраторы; они синхронизируют свою работу при начале сеанса шифрования;
- *самосинхронизирующиеся* шифраторы; они обладают свойством восстанавливать синхронизацию при пропуске символа.

Недостатком синхронных шифраторов является необходимость повторной синхронизации при разрыве связи. Недостатком самосинхронизирующихся шифраторов является разрастание ошибок расшифрования.

Рассматривая возможности применения блочных и поточных алгоритмов шифрования, можно отметить, что блочные алгоритмы больше подходят для шифрования файлов данных, а также пакетов, передаваемых по каналам связи. Поточные алгоритмы используются для шифрования потоков данных непосредственно во время их передачи.

Завершая обзор алгоритмов шифрования, отметим еще один современный метод скрытия информации.

*Стеганография* применяется для скрытия факта передачи секретных сообщений в другие сообщения, при этом скрывается даже само существование секрета. Отправитель может написать ничего не значащее сообщение и на том же листке бумаги скрыть секретное.

В настоящее время сообщения скрывают в битовых графических изображениях. При этом младший бит каждого пикселя заменяется битом сообщения. В результате этого преобразования изображение картинки изменяется совершенно незаметно для глаза. Картинка размером 800×600 пикселей позволяет записать таким образом текст длиной 60000 байт. Как уже было сказано, при этом невозможно установить даже сам факт записи в картинку какого-либо сообщения.

Заметим, что стеганография на битовых картинках применяется не только для записи секретных сообщений, но и для их подписи.

## Алгоритм DES

DES (Data Encryption Standard) является блочным алгоритмом шифрования, построенным на основе сети Фейштеля или, иначе, SP-сети (от *substitution* (подстановка) и *permutation* (перестановка)). Алгоритм разработан Х. Фейштелем и другими сотрудниками фирмы IBM.

Зашифрование и расшифрование текста производится блоками размером 64 бита на ключе размером 56 бит (фактически ключ имеет размер 64 бита, но каждый восьмой бит не используется). Над каждым блоком выполняется 16 преобразований, называемых *раундами*. Схема выполнения одного раунда приведена на рисунке 13.

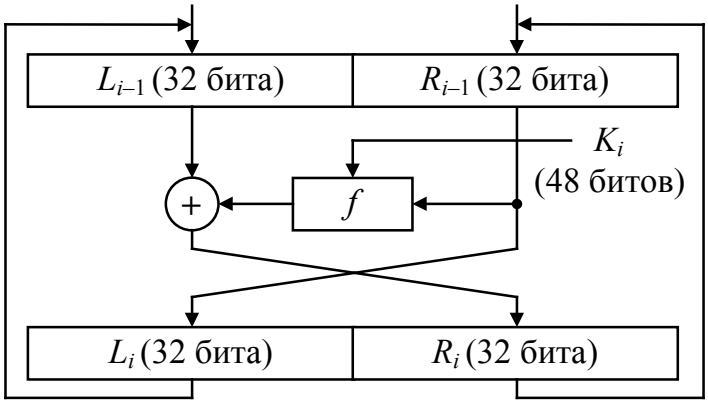


Рисунок 13 — Схема одного раунда

Блоки разбиваются на левую $L$ и правую $R$ ветки размером по 32 бита. Правая ветка предыдущего раунда $R_{i-1}$ становится левой веткой текущего раунда. Левая ветка предыдущего раунда $L_{i-1}$ складывается по модулю 2 с результатом преобразования правой ветки $R_{i-1}$, выполняемого при помощи *функции шифрования f*, в которой задействован также раундовый ключ $K_i$.

Математическая запись преобразований раунда имеет вид:

$L_i = R_{i-1}$ ,

$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ .

В некоторых вариантах алгоритма перед началом выполнения раундов выполняется начальная перестановка битов блока в соответствии с таблицей А.1 (приложение А). В таблице показан порядок битов исходного блока (первым битом результирующего блока становится бит 58 исходного блока, вторым битом — бит 50 и т.д.).

Если выполняется начальная перестановка, то после завершения раундов выполняется также завершающая (обратная) перестановка в соответствии с таблицей А.2, при этом в последнем раунде не выполняется обмен левой и правой ветвей (он задается таблицей завершающей перестановки).

Основные преобразования задает функция шифрования *f*. Схематически эта функция изображена на рисунке 14.

На вход функции шифрования поступает правая ветка предыдущего раунда $R_{i-1}$ размером 32 бита. Поскольку раундовый ключ $K_i$ состоит из 48 битов, ветка $R_{i-1}$ расширяется до 48 бит при помощи таблицы перестановки А.3. Биты ветки переставляются в порядке, заданном этой таблицей (при этом половина битов записываются дважды).

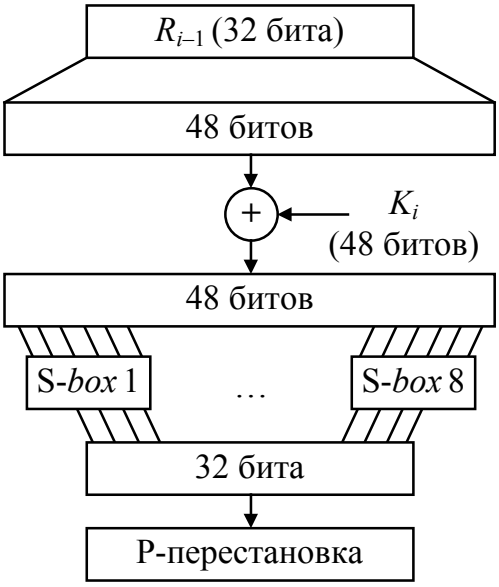


Рисунок 14 — Схема функции шифрования

Полученный блок из 48 битов складывается по модулю 2 с раундовым ключом $K_i$, после чего результат сжимается до 32 битов при помощи восьми таблиц замены, называемых S-*box* (S-блок). S-блоки выполняют единственные нелинейные преобразования в алгоритме и задают его аналитическую сложность. S-блоки приведены в таблице А.4.

Преобразования с помощью S-блоков выполняются следующим образом. Последовательность из 48 битов разбивается на 8 частей. Обозначим отдельную часть (состоящую из шести битов) как S.

Каждый из S-блоков преобразует шесть битов S в четыре бита.

S-блок задается как таблица размером 4×16. Для определения номера строки S-блока используются биты 1 и 6 последовательности S, а номер столбца определяется внутренними битами S (битами 2-5). В соответствующей ячейке таблицы S-блока записан код из четырех битов, который и является результатом преобразования S (при этом каждая строка S-блока определяет все 16 комбинаций из четырех битов).

Полученные восемь последовательностей по четыре бита объединяются (конкатенируются) в одну последовательность из 32-х битов, и выполняется P-перестановка битов в соответствии с таблицей А.5.

Рассмотрим, как формируется раундовый ключ $K_i$.

Вообще говоря, ключ шифрования имеет длину 8 знаков (64 бита), но при этом старшие биты байтов не используются. Иначе говоря, ключ задается значениями первой половины таблицы ASCII и предполагает использование букв только латинского алфавита. При этом фактически задействуется только 56 битов.

Перед началом преобразований из 64 битов ключа выбираются и переставляются 56 битов в соответствии с таблицей А.6, в которой пропущен каждый восьмой бит (старшие биты байтов).

Полученный результат делится на две равные части по 28 битов.

Далее в каждом раунде выполняются следующие операции.

1) Каждая из частей ключа независимо друг от друга циклически сдвигаются влево на количество бит, зависящее от номера раунда. Число сдвигов указано в таблице А.7 (первая строка в ней — номер раунда).

2) Из полученной общей последовательности в 56 битов выбираются и переставляются 48 битов в соответствии с таблицей А.8 (в ней пропущены биты 8, 18, 22, 25, 35, 38, 43 и 54). Результирующая последовательность из 48 битов и есть раундовый ключ $K_i$ (рисунок 15).

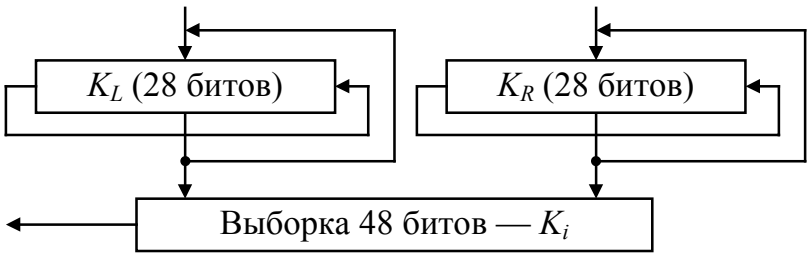


Рисунок 15 — Преобразования ключа в раунде

Общее число сдвигов половинок ключа равно 28, то есть после выполнения 16 раундов ключ возвращается в начальное состояние и его можно повторно использовать для зашифрования или расшифрования.

Расшифрование выполняется при помощи этого же алгоритма. При этом используются раундовые ключи в обратном порядке.

Достоинствами алгоритма DES являются высокое быстродействие и простая аппаратная реализация. Его встраивают, например, в интеллектуальные карты.

Недостатки алгоритма шифрования DES:

1) наличие слабых ключей, которые при работе алгоритма приводят к небольшому количеству раундовых комбинаций;

2) небольшая длина ключа, позволяющая раскрыть его на современном компьютере методом прямого перебора;

3) статические подстановки в S-блоках позволяют в конечном итоге проводить атаки на алгоритм.

## Алгоритм RSA

Для реализации алгоритмов асимметричного шифрования используются односторонние функции. *Односторонней* называется отображение $f(x)$: $X \to Y$, $x \in X$, при этом вычисление обратного отображения является сложной задачей. Эта задача называется трудновычисляемой, если нет алгоритма ее решения за полиномиальное время. Стойкость современных асимметричных алгоритмов базируется на двух математических проблемах, которые являются на данном этапе трудновычисляемыми даже для метода «грубой силы»:

- дискретное логарифмирование в конечных полях;
- факторизация больших чисел.

Алгоритм RSA (авторы Rivest, Shamir, Adleman) является самым распространенным алгоритмом асимметричного шифрования. Его можно применять для зашифрования и расшифрования, обмена ключами, а также для генерации и проверки электронной цифровой подписи.

### *Генерация ключей*

Участники информационного обмена независимо генерируют пару ключей (открытый и закрытый) при помощи следующей процедуры.

1. Выбираются два больших простых целых числа $p$ и $q$ приблизительно одинакового размера. Следует учитывать, что увеличение порядка чисел ведет, с одной стороны, к замедлению операций, а с другой — к увеличению стойкости алгоритма. Приблизительный порядок чисел — 150-200 десятичных знаков (примерно $2^{512}$).

2. Вычисляется модуль системы

$n = p \cdot q$

и функция Эйлера

$\varphi(n) = (p-1)(q-1)$.

3. Выбирается достаточно большое число $e$, удовлетворяющее условию $1 < e < \varphi(n)$, взаимно простое с $\varphi(n)$ (НОД($e$, $\varphi(n)$) = 1).

4. При помощи расширенного алгоритма Евклида вычисляется достаточно большое число $d$, отвечающее условию

$e \cdot d = 1 \pmod{\varphi(n)}$,

$1 < d < \varphi(n)$.

Пара ($e$, $n$) является открытым ключом, а пара ($d$, $n$) — закрытым.

### *Зашифрование и расшифрование*

Шифруются блоки (числа) $m$, размер которых определяется числом $k$, соответствующим неравенству $10^{k-1} < n < 10^k$.

Зашифрование производится по формуле: $c = m^e \bmod n$.

Расшифрование производится по формуле: $m = c^d \bmod n$.

## Алгоритм обмена ключа Диффи-Хеллмана

Цель алгоритма состоит в том, чтобы два участника могли безопасно обменяться ключом, который в дальнейшем может использоваться в каком-либо алгоритме симметричного шифрования. Данный алгоритм может применяться только для обмена ключами.

Алгоритм основан на трудности вычислений дискретных логарифмов. Дискретный логарифм определяется следующим образом. Вводится понятие примитивного корня простого числа $Q$ как числа, чьи степени создают целые числа от 1 до $Q$–1. Это означает, что если $A$ является примитивным корнем простого числа $Q$, тогда числа

$A \bmod Q, A^2 \bmod Q, \ldots, A^{Q-1} \bmod Q$

являются различными и состоят из целых от 1 до $Q$–1 с некоторыми перестановками. В этом случае для любого целого $Y < Q$ и примитивного корня $A$ простого числа $Q$ можно найти единственную экспоненту X, такую, что $Y = A^X \bmod Q$, $0 \le X \le Q$-1.

Экспонента $Y$ называется дискретным логарифмом или индексом $Y$ по основанию $A \bmod Q$.

Предполагается, что существуют два известных всем числа: простое число $Q$ и целое $A$, которое является примитивным корнем $Q$. Предположим, что пользователи $I$ и $J$ хотят обменяться ключом для алгоритма симметричного шифрования. Пользователь $I$ выбирает случайное число $X_i < Q$ и вычисляет $Y_i = A^{Xi} \bmod Q$. Аналогично пользователь $J$ независимо выбирает случайное целое число $X_j < Q$ и вычисляет $Y_i = A^{Xj} \bmod Q$. Каждая сторона держит значение $X$ в секрете и делает значение $Y$ доступным для другой стороны. Теперь пользователь $I$ вычисляет ключ как $K = (Y_j)^{Xi} \bmod Q$, и пользователь $J$ вычисляет ключ как $K = (Y_i)^{Xj} \bmod Q$. В результате оба получат одно и то же значение:

$$
\begin{aligned}
K &= (Y_j)^{Xi} \bmod Q \\
&= (A^{Xj} \bmod Q)^{Xi} \bmod Q \\
&= A^{Xj\ Xi} \bmod Q \\
&= (A^{Xj})^{Xj} \bmod Q \\
&= (A^{Xi} \bmod Q)^{Xj} \bmod Q \\
&= (Y_i)^{Xj} \bmod Q.
\end{aligned}
$$

Безопасность обмена ключа в алгоритме Диффи-Хеллмана вытекает из того факта, что, хотя относительно легко вычислить экспоненты по модулю простого числа, очень трудно вычислить дискретные логарифмы. Для больших простых чисел задача считается неразрешимой.

По современным оценкам теории чисел при $A \approx 2^{664}$ и $N \approx 2^{664}$ решение задачи дискретного логарифмирования потребует $10^{26}$ операций, т.е. эта задача имеет в $10^3$ раз большую степень сложности, чем задача разложения на множители.

## Сетевые (удаленные) атаки

Особенностью сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними осуществляется физически при помощи сетевых соединений, а программно — при помощи механизмов сообщений. К сетевым системам применим специфичный вид атак, обусловленных распределенным характером ресурсов и информации, и называемых сетевыми или удаленными атаками.

Под удаленной атакой будем понимать информационное разрушающее воздействие на распределенную вычислительную систему (РВС), осуществляемое программно по каналам связи.

### Классификация удаленных атак

Существует следующая классификация удаленных атак на РВС [4].

1) По характеру воздействия:

- пассивные атаки (класс 1.1);
- активные атаки (класс 1.2).

Пассивным называют воздействие, которое не оказывает непосредственного влияния на работу системы, но нарушает ее политику безопасности. Активное воздействие нарушает нормальное функционирование системы и также нарушает политику безопасности. Активное воздействие потенциально можно обнаружить.

2) По цели воздействия:

- нарушение конфиденциальности информации (класс 2.1)
- нарушение целостности информации (класс 2.2)
- нарушение работоспособности (доступности) системы (класс 2.3)

Этот классификационный признак является прямой проекцией трех основных элементов информационной безопасности.

Нарушение конфиденциальности является целью практически любой удаленной атаки. При этом атака может быть пассивной. Примером подобной атаки является пассивное прослушивание.

Целостность информации нарушается, когда злоумышленник имеет возможность либо полностью контролировать информационный поток, либо передавать сообщения от имени другого объекта, при этом атака является активным воздействием. Примером такой атаки является типовая атака «Ложный объект РВС».

Другой целью удаленной атаки может являться нарушение работоспособности атакуемой системы таким образом, чтобы доступ к ресурсам этой системы для легальных пользователей стал невозможен или затруднен. В этом случае обычно не предполагается несанкционированный доступ к информации. Примером является типовая атака «Отказ в обслуживании».

3) По условию начала различают три вида атак:

- атака по запросу от атакуемого объекта (класс 3.1). В этом случае атакующий ожидает передачи от потенциальной цели атаки запроса определенного типа, который является условием начала осуществления воздействия. Примером таких запросов в сети Интернет являются DNS- и ARP-запросы. Этот тип удаленных атак наиболее характерен для распределенных ВС.

- атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2). В этом случае атакующий осуществляет постоянное наблюдение за системой, являющейся целью атаки, и при возникновении определенного события в этой системе начинает воздействие.

- безусловная атака (класс 3.3). Инициатором является атакующий.

4) По наличию обратной связи с атакуемым объектом:

- с обратной связью (класс 4.1);
- без обратной связи (класс 4.2).

Удаленная атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ, а, следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему реагировать на изменения, происходящие на атакуемом объекте.

Атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны.

5) По расположению субъекта атаки относительно атакуемого объекта:

- внутрисегментное (класс 5.1);
- межсегментное (класс 5.2).

Этот классификационный признак позволяет судить о «степени удаленности» атаки. Отметим, что межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная.

6) По уровню эталонной модели ISO/OSI, на котором осуществляется воздействие, различают атаки на уровнях:

- физический (класс 6.1);
- канальный (класс 6.2);
- сетевой (класс 6.3);
- транспортный (класс 6.4);
- сеансовый (класс 6.5);
- представительный (класс 6.6);
- прикладной (класс 6.7).

## Типовые удаленные атаки

### *Анализ сетевого трафика*

Заключается в прослушивании канала связи. Анализ сетевого трафика позволяет, во-первых, изучить логику работы РВС, то есть получить взаимно однозначное соответствие событий, происходящих в системе, и команд, пересылаемых друг другу ее объектами, в момент появления этих событий. Это достигается путем перехвата и анализа пакетов обмена на канальном уровне. Знание логики работы распределенной ВС позволяет на практике моделировать и осуществлять типовые удаленные атаки, рассмотренные далее.

Во-вторых, анализ сетевого трафика позволяет перехватить поток данных, которыми обмениваются объекты распределенной ВС. Таким образом, удаленная атака данного типа заключается в получении на удаленном объекте несанкционированного доступа к информации, которой обмениваются два сетевых абонента. Отметим, что при этом отсутствует возможность модификации трафика и сам анализ возможен только внутри одного сегмента сети. Примером перехваченной информации могут служить имя и пароль пользователя.

Атака относится к классам 1.1, 2.1, 3.3, 4.2, 5.1, 6.2.

### *Подмена доверенного объекта или субъекта РВС*

В том случае, когда РВС использует нестойкие алгоритмы идентификации удаленных объектов, то оказывается возможной типовая удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта РВС. При этом существуют две разновидности данной типовой удаленной атаки:

- атака при установленном виртуальном канале,
- атака без установленного виртуального канала.

В случае установленного виртуального соединения атака будет заключаться в присвоении прав доверенного субъекта взаимодействия, легально подключившегося к объекту системы, что позволит атакующему вести сеанс работы с объектом РВС от имени доверенного субъекта.

Реализация удаленных атак данного типа обычно состоит в передаче пакетов обмена с атакующего объекта на цель атаки от имени доверенного субъекта взаимодействия. Для осуществления атаки данного типа необходимо преодолеть систему идентификации и аутентификации сообщений, которая может использовать контрольную сумму, вычисляемую с помощью открытого ключа, динамически выработанного при установлении канала, случайные многобитные счетчики пакетов и сетевые адреса станций.

Атака без установленного виртуального соединения заключается в передаче служебных сообщений от имени сетевых управляющих устройств, например, от имени маршрутизаторов. Посылка ложных управляющих сообщений может привести к серьезным нарушениям работы РВС (например, к изменению ее конфигурации).

Атака относится к классам 1.2, 2, 3.2, 4, 5, 6.2, 6.3, 6.4.

***Ложный объект РВС***

Существуют две принципиально разные причины, обуславливающие появление типовой удаленной атаки «Ложный объект РВС».

**Навязывание ложного маршрута**

Для обеспечения эффективной и оптимальной маршрутизации в РВС применяются управляющие протоколы, позволяющие маршрутизаторам обмениваться информацией друг с другом:

RIP, Routing Internet Protocol, OSPF, Open Shortest Path First,

уведомлять хосты о новом маршруте:

ICMP, Internet Control Message Protocol,

удаленно управлять маршрутизаторами:

SNMP, Simple Network Management Protocol.

Эти протоколы позволяют удаленно изменять маршрутизацию в сети Интернет, то есть являются протоколами управления сетью.

Реализация данной типовой удаленной атаки состоит в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации.

Для изменения маршрутизации атакующему необходимо послать по сети определенные данными протоколами управления сетью специальные служебные сообщения от имени сетевых управляющих устройств (например, маршрутизаторов). В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются два объекта распределенной ВС, и атака перейдет во вторую стадию, связанную с приемом, анализом и передачей сообщений, получаемых от дезинформированных объектов РВС.

Атака относится к классам 1.2, 2, 3.3, 4, 5, 6.2, 6.3, 6.4.

**Использование недостатков алгоритмов удаленного поиска**

Часто оказывается, что удаленные объекты РВС изначально не имеют достаточно информации, необходимой для адресации сообщений. Такой информацией являются, например, адрес сетевого адаптера или IP-адрес. Для получения этой информации в РВС используются алгоритмы удаленного поиска, заключающиеся в передаче по сети специ

ального вида поисковых запросов, и в ожидании ответов на запрос с искомой информацией. Примерами могут служить DNS- и ARP-запросы.

При этом существует потенциальная возможность на атакующем объекте перехватить посланный запрос и послать на него ложный ответ, где указать данные, использование которых приведет к адресации на атакующий ложный объект. В дальнейшем весь поток информации между субъектом и объектом взаимодействия будет проходить через ложный объект РВС.

Другой вариант внедрения в РВС ложного объекта использует недостатки алгоритма удаленного поиска и состоит в периодической передаче на атакуемый объект заранее подготовленного ложного ответа без приема поискового запроса. При этом атакующий может спровоцировать атакуемый объект на передачу поискового запроса, и его ложный ответ будет иметь успех.

Атака относится к классам 1.2, 2.1, 2.2, 3.1, 3.3, 4.1, 5, 6.2, 6.3, 6.4.

***Отказ в обслуживании***

Обычно в вычислительных сетях возможность предоставления удаленного доступа реализуется следующим образом: на объекте РВС в сетевой ОС запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т.п.), предоставляющих удаленный доступ к ресурсам данного объекта.

Задача сервера состоит в том, чтобы, находясь в памяти операционной системы объекта РВС, постоянно ожидать получения запроса на подключение от удаленного объекта. В случае получения подобного запроса сервер должен по возможности передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет (подключение к серверу специально описано очень схематично).

По аналогичной схеме происходит создание виртуального канала связи, по которому обычно взаимодействуют объекты РВС. В этом случае непосредственно ядро сетевой ОС обрабатывает приходящие извне запросы на создание виртуального канала и передает их в соответствии с идентификатором запроса (порт или сокет) прикладному процессу, которым является соответствующий сервер.

Сетевая операционная система способна иметь только ограниченное число открытых виртуальных соединений и отвечать лишь на ограниченное число запросов. Эти ограничения зависят от различных параметров системы в целом, основными из которых являются быстродействие ЭВМ, объем оперативной памяти, пропускная способность канала связи.

Основная проблема состоит в том, что при отсутствии статической ключевой информации в РВС идентификация запроса возможна только

по адресу его отправителя. Если в РВС не предусмотрено средств аутентификации адреса отправителя, то есть инфраструктура РВС позволяет с одного объекта системы передавать на другой атакуемый объект бесконечное число анонимных запросов на подключение от имени других объектов, то в этом случае будет иметь успех типовая удаленная атака «Отказ в обслуживании» (Denial of Service — DoS). Результат применения этой атаки — нарушение на атакованном объекте работоспособности соответствующей службы, то есть невозможность получения удаленного доступа с других объектов РВС.

Вторая разновидность этой типовой удаленной атаки состоит в передаче с одного адреса такого количества запросов на атакуемый объект, какое позволит трафик (направленный «шторм» запросов). В этом случае, если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом этой атаки может являться как переполнение очереди запросов и отказа одной из телекоммуникационных служб, так и полная остановка компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Третьей разновидностью атаки «Отказ в обслуживании» является передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы и т.п.

Атака относится к классам 1.2, 2.3, 3.3, 4.2, 4, 6.2, 6.3, 6.4, 6.7.

## Примеры сетевых атак

### *Ложный ARP-сервер Интернет (ARP- spoofing)*

Данная атака относится к типу «Ложный объект РВС». Она возможна вследствие необходимости определять аппаратный адрес некоторого хоста сети по его IP-адресу. Как известно, стек протоколов ISO/OSI формирует вложенную структуру заголовков, в которой IP-адрес хоста оказывается вложенным в аппаратный адрес (точнее, пакет сетевого уровня вложен в пакет канального уровня, рисунок 16).

| |
|---|
| *Ethernet-заголовок* |
| *IP-заголовок* |
| *TCP-заголовок* |
| *Данные* |

Рисунок 16 — Структура TCP-пакета

Первоначально хост может не иметь информации об аппаратных адресах других хостов, в том числе маршрутизатора. Эта стандартная проблема решается с помощью алгоритмов удаленного поиска. В сети Интернет используется протокол ARP (Address Resolution Protocol).

При первом обращении к сетевым ресурсам хост отправляет широковещательный ARP-запрос, в котором указывает IP-адрес маршрутизатора и просит сообщить его аппаратный адрес (MAC-адрес, Media Access Control). Этот запрос получат все хосты в пределах данного сегмента сети, в том числе и маршрутизатор. Получив запрос, маршрутизатор вносит запись о запросившем хосте в ARP-таблицу и отправляет ответ, в котором сообщает свой аппаратный адрес. Получив ответ, запрашивающий хост вносит MAC-адрес маршрутизатора в свою ARP-таблицу.

Атака осуществляется следующим образом (рисунок 17).

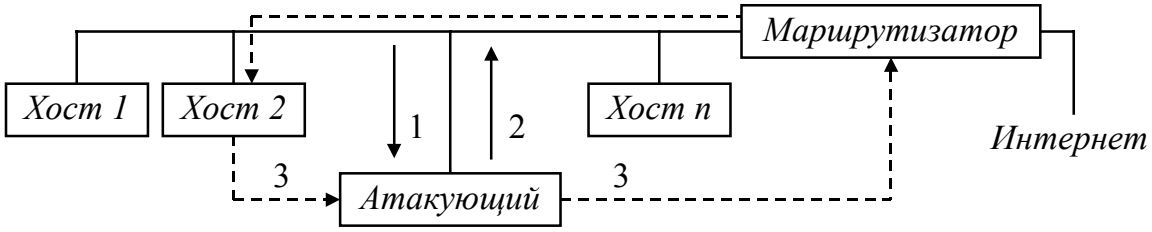


Рисунок 17 — Схема ложного ARP-сервера

1) Атакующий прослушивает сеть в ожидании широковещательного ARP-запроса.

2) Получив запрос, атакующий посылает запросившему ложный ответ, сообщая свой MAC-адрес. В результате запрашивающий хост запишет в свою ARP-таблицу MAC-адрес атакующего в качестве адреса маршрутизатора.

3) Атакующий, выдавая себя таким образом за маршрутизатор, получает возможность контролировать поток информации, которым атакуемый хост обменивается с маршрутизатором.

Заметим, что маршрутизатор, получив широковещательный запрос на разрешение сетевого адреса, связывает IP-адрес атакуемого хоста с его MAC-адресом. Поэтому пакет на IP-адрес атакуемого хоста будет направлен маршрутизатором не на ложный объект, а на атакуемый хост. Однако атакующий может получить полный контроль, если ему удастся подменить запись IP-адреса атакуемого на свой MAC-адрес в ARP-таблице маршрутизатора (что в принципе возможно).

В заключение отметим, что данная атака осуществима практически во всех современных операционных системах, а причина ее успеха кроется в особенностях среды Ethernet. Эта атака может быть осуществлена только в пределах сегмента сети.

***Перехват TCP-сеанса (TCP-hijacking)***

Для идентификации TCP-пакетов в TCP-заголовке используются два 32-разрядных идентификатора, играющие также роль счетчика пакетов: Sequence Number и Acknowledgement Number. Кроме этого, заголовок содержит битовое поле Control Bits, содержащее следующие команды:

URG (Urgent Pointer field significant),
ACK (Acknowledgement field significant),
PSH (Push Function),
RST (Reset the connection),
SYN (Synchronize sequence numbers),
FIN (No more data from sender).

Схема создания TCP-соединения показана на рисунке 18.

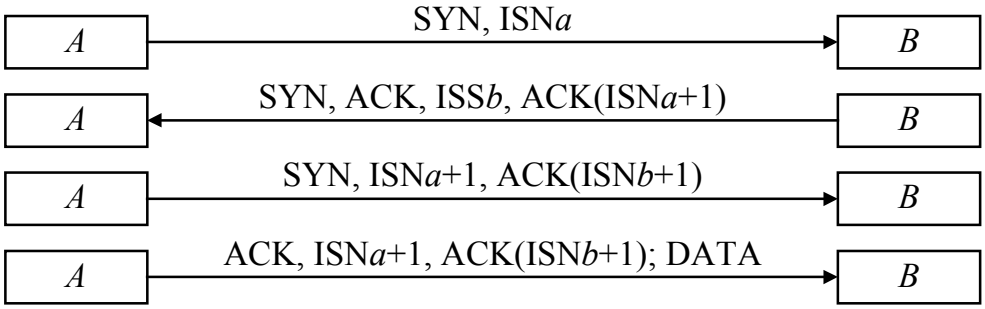


Рисунок 18 — Установление TCP-соединения

Сначала хост *A* посылает TCP-пакет, в заголовке которого установлен бит синхронизации SYN, в поле Sequence Number задано начальное значение, равное ISN*a* (Initial Sequence Number). Хост *B* отвечает пакетом, в заголовке которого установлены SYN и ACK, в поле Sequence Number — собственное начальное значение Sequence Number, равное ISN*b*, а в поле Acknowledgement Number — значение ISN*a*+1.

Хост *A*, завершая этот обмен (называемый handshake) посылает пакет, в заголовке которого установлен бит ACK, поле Sequence Number содержит ISN*a*+1, а поле Acknowledgement Number — ISN*b*+1. Далее хост *A* посылает пакеты данных по установленному соединению.

Для осуществления атаки необходимо знать текущие идентификаторы соединения ISN*a* и ISN*b*. При нахождении атакующего в одном сегменте с целью атаки эти значения узнаются посредством анализа сетевого трафика. При нахождении атакующего в другом сегменте задача не является тривиальной, однако подобрать значения принципиально возможно вследствие того, что начальные значения счетчиков генерируются операционными системами или соответствующими сетевыми службами на основе некоторых простых правил.

Для реализации атаки хост злоумышленника посылает пакеты хосту *A* с полем Sequence Number, равным ISN*x*. Целью является заполнить очередь запросов и вывести хост *A* из строя на некоторое время.

Затем атакующий устанавливает соединение с хостом B, используя ISN*x*. Хост B отвечает хосту A соответствующим пакетом. Атакующий, используя предсказание значения ISN*b*, возможно, после нескольких попыток, посылает на хост B пакет подтверждения установления соединения, в результате чего хост B считает, что он установил соединение с хостом A.

Наиболее известной осуществленной атакой с перехватом TCP-соединения является инцидент, произошедший 12 декабря 1994 года в суперкомпьютерном центре Сан-Диего (США), когда атакующий, небезызвестный Кевин Митник, осуществил данную схему атаки.

***Направленный шторм ложных TCP-запросов***

На каждый полученный TCP-запрос на установление соединения операционная система должна сгенерировать начальное значение ISN и отослать его в ответ на запросивший хост. При этом, так как в сети Интернет стандарта IPv4 не предусмотрен контроль за IP-адресом отправителя, невозможно ограничить число возможных запросов в единицу времени от одного хоста. Поэтому возможно осуществление типовой удаленной атаки «Отказ в обслуживании» (DoS).

Атака заключается в передаче на атакуемый хост как можно большего числа ложных TCP-запросов на создание соединения от имени любого хоста сети. Эффективность данной атаки тем выше, чем больше пропускная способность канала связи и тем меньше, чем больше вычислительная мощность атакуемого компьютера.

## Список литературы

1. В. А. Галатенко. Основы информационной безопасности. Интернет университет информационных технологий. Электронный ресурс:
«http://www.intuit.ru/department/security/secbasics/».
Проверено 12.03.2008.

2. В. А. Галатенко. Стандарты информационной безопасности. Интернет университет информационных технологий. Электронный ресурс:
«http://www.intuit.ru/department/security/secst/».
Проверено 12.03.2008.

3. О. Р. Лапонина. Криптографические основы безопасности. Интернет университет информационных технологий. Электронный ресурс:
«http://www.intuit.ru/department/security/networksec/».
Проверено 12.03.2008.

4. И. Д. Медведовский и др. Атака из Internet / И. Д. Медведовский, П. В. Семьянов, Д. Г. Леонов, А. В. Лукацкий — М.: СОЛОН-Р, 2002, 368 с. (Серия «Аспекты защиты»).

5. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. — М.: ДМК, 2000 — 448 с., ил.

6. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб: Наука и техника , 2004. — 384 с.

7. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Издательство «Феникс», 2008. — 254 с.

8. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. учреждений высш. проф. образования. М.: Издательский центр «Академия», 2013. — 336 с.

9. Кондаков В.В., Краснобородько А.А. Информационная безопасность систем физической защиты, учета и контроля ядерных материалов: Учебное пособие. М.: МИФИ, 2008. — 48 с.

10. ФСТЭК России. Руководящий документ (30 марта 1992 г.). «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

11. ФСТЭК России. Руководящий документ (30 марта 1992 г.). «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

12. ФСТЭК России. Руководящий документ (25 июля 1997 г.) «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

# Приложение А — Таблицы алгоритма DES

**Таблица А.1 — Начальная перестановка**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 | 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 36 | 22 | 14 | 6 | 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

**Таблица А.2 — Завершающая перестановка**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 | 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 | 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 | 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 | 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

**Таблица А.3 — Перестановка расширения**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 | 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 | 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 | 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 | 28 | 29 | 30 | 31 | 32 | 1 |

**Таблица А.4 — Подстановки в S-блоках**

**S-блок 1**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

**S-блок 2**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |

**S-блок 3**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |

**S-блок 4**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |

**S-блок 5**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 6 | 8 | 6 |
| 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |

**S-блок 6**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |

**S-блок 7**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 6 | 11 | 13 | в | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |

**S-блок 8**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

**Таблица А.5 — Перестановка в Р-блоке**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 | 1 | 15 | 23 | 26 | 5 | 18 | 31 | 16 |
| 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 | 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

**Таблица А.6 — Перестановка для начальной выборки ключа**

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | 28 | 20 | 12 | 4 |

**Таблица А.7 — Количество сдвигов ключа раунда**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

**Таблица А.8 — Перестановка для выборки ключа раунда**

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 | 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 | 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 | 46 | 42 | 50 | 36 | 29 | 32 |

Для заметок

Владимир Вадимович Пономарев

Методы и средства защиты информации

Оригинал-макет подготовлен автором 01.01.2011

ОТИ НИЯУ МИФИ