СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Обеспечение информационной безопасности является одной из основных проблем, с которой сталкивается современное общество. Причиной ее обострения в наши дни стало широкомасштабное использование автоматизированных средств накопления, хранения, обработки и передачи информации.

Проблема обеспечения информационной безопасности широка и многогранна. За внешней тривиальностью, заключающейся в обеспечении трех составляющих информационной безопасности — доступности, целостности и конфиденциальности информации, — скрывается значительный перечень мероприятий: от общих решений, принимаемых в интересах всего общества и государства, до частных решений в рамках отдельно взятых компаний. Развитие современного общества напрямую связано с ростом производства, потребления и накопления информации во всех отраслях человеческой деятельности. Информационные потоки в обществе увеличиваются с каждым днем, и этот процесс носит лавинообразный характер.

По своему значению для развития общества информация приравнивается к важнейшим ресурсам наряду с сырьем и энергией. В развитых странах большинство работающих заняты не в сфере производства, а в той или иной степени занимаются обработкой информации.

Следует отметить и новую тенденцию, заключающуюся во все большей информационной зависимости общества в целом и отдельного человека в частности. Именно поэтому в последнее время появились такие категории, как «информационная политика», «информационная безопасность», «информационная война», и целый ряд других новых понятий, в той или иной мере связанных с информацией.

Сегодня в нашей стране в целом сформирована единая политика в сфере обеспечения информационной безопасности. Для этого принят ряд основополагающих законов и разработаны ключевые оценочные стандарты средств автоматизированной обработки, хранения, отображения и обмена информацией. Об особом внимании государства к вопросам информационной безопасности говорит недавнее принятие новой Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646.

Опыт ведущих развитых стран показывает, что по мере все большей автоматизации и информатизации общественной жизни проблема информационной безопасности будет все больше обостряться. Наличие проблем с обеспечением защищенности информации и поддерживающей ее инфраструктуры на сегодняшний день сдерживает развитие таких перспективных экономических направлений, как электронная коммерция,

электронный бизнес, безбумажный документооборот и другие, которые могут реально повысить эффективность функционирования целых отраслей производства и сферы сервисных услуг.

В нашей стране все более востребованными становятся услуги специалистов, занимающихся вопросами защиты информации. На этом фоне появляются крупные компании, оказывающие подобные услуги, разрабатывающие специализированные аппаратно-программные комплексы защиты информации, что дополнительно подтверждает актуальность проблемы обеспечения информационной безопасности.

В связи с этим можно отметить, что современный человек, хоть как-то связанный с информационными технологиями и средствами автоматизации обработки информации, должен иметь представление об основных источниках и угрозах информационной безопасности и, самое главное, должен знать основные приемы безопасной работы. Именно с этой точки зрения излагается материал данной книги.

Если изучение представленных материалов сформирует у читателей устойчивое представление о проблеме обеспечения информационной безопасности, источниках и причинах инцидентов, а также способах защиты, то авторы будут считать свою цель в значительной степени достигнутой.

В *первой главе* книги даются базовые понятия, связанные с определением информации, ее мерами и фазами обращения в информационной системе, поскольку прежде, чем говорить о методах защиты информации и информационной безопасности, необходимо определить: «что есть информация?». Таким образом, первая глава — это фактически повторение тех вопросов, с которыми учащиеся уже должны быть знакомы из курса «Информатика».

Во *второй главе* книги рассмотрены нормативно-правовые основы обеспечения информационной безопасности. Существенное внимание уделено основополагающим нормативным документам, определяющим порядок использования различных категорий информации, а также ответственность за соответствующие нарушения в информационной сфере. Кроме этого, в этой же главе изложены общие подходы к обеспечению информационной безопасности на административном уровне, дано понятие политики безопасности и ее содержание, проанализированы основные угрозы информационной безопасности в контексте ее составляющих.

Отдельно во второй главе рассматриваются вопросы анализа и оценки рисков, а также управления событиями и инцидентами информационной безопасности. Именно процессы управления инцидентами позволяют определить конкретные уязвимости системы защиты информации, обнаружить следы атак и вторжений в информационную среду компании, что в свою очередь дает сведения о слабостях в существующей системе защиты.

Одним из механизмов обеспечения информационной безопасности является создание центров обеспечения информационной безопасности (SOC). Одно из определений SOC гласит, что SOC — это команда, состоящая, в основном, из аналитиков в сфере информационной безопасности, задачами которой является обнаружение, анализ, реагирование, предоставление отчетов и предотвращение инцидентов информационной безопасности.

Однако SOC это не только люди. Это взаимосвязь процессов, технологий и людей, выполняющих определенные функции. Этим вопросам также уделено внимание во второй главе книги.

Третья глава посвящена проблемам защиты информационных систем от вредоносных программ. В соответствии с современной классификацией вредоносных программ в разделе изложены основные способы противодействия проникновению вредоносных программ в компьютеры пользователей. Наиболее надежную защиту от вредоносных программ может обеспечить только комплекс разнообразных мер защиты, включающий организационные мероприятия, регламентирующие использование компьютера, безопасное администрирование компьютерной системы, применение программных средств защиты, соблюдение правил «техники безопасности» при работе в интернете, в том числе при использовании электронной почты, а также при копировании данных и инсталляции программ. Цель данной главы — сформировать представление о том, что, помимо установки на компьютере хорошей антивирусной программы, крайне желательно предпринимать дополнительные меры по выявлению и нейтрализации вредоносных программ.

Особенности обеспечения информационной безопасности в компьютерных сетях и облачных сервисах рассматриваются в *четвертой главе*. С появлением сетевых информационных систем проблема обеспечения информационной безопасности стала приобретать новые черты, поскольку наряду с локальными угрозами, осуществляемыми в пределах одного узла, к сетевым информационным системам применим специфический вид угроз, обусловленный распределенностью сетевых и информационных ресурсов в пространстве. Это так называемые сетевые или удаленные угрозы. Они отличаются, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого узла, и, во-вторых, тем, что атаке может подвергаться не конкретный узел, а информация, передаваемая по сетевым каналам. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения, и, соответственно, обеспечение безопасности вычислительных сетей с точки зрения противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что если в локальных вычисли-

тельных сетях наиболее частыми являются угрозы конфиденциальности и целостности информации, то в территориально распределенных сетях на первое место выходит угроза нарушения доступности информации. Отдельно в данной главе уделяется внимание вопросам обеспечения безопасности облачных сервисов, поскольку на сегодняшний день это одна из наиболее стремительно развивающихся технологий, предполагающая передачу части объектов информационной инфраструктуры на обслуживание сторонней организации, что несет дополнительные риски информационной безопасности.

В *пятой главе* описаны наиболее значимые механизмы защиты вычислительных систем от несанкционированных действий как преднамеренного, так и непреднамеренного характера, такие как аутентификация, аудит, шифрование, межсетевое экранирование, VPN и др.

Шестая глава посвящена вопросам криптографической защиты информации. В настоящее время исключительное значение в разных областях приобрели вопросы, связанные с сохранением и передачей конфиденциальной информации. Возникающие при этом задачи решает криптография — наука о методах преобразования информации в целях ее защиты от незаконных пользователей.

Значение криптографии выходит далеко за рамки обеспечения секретности данных. По мере все большей автоматизации передачи и обработки информации и интенсификации информационных потоков ее методы приобретают уникальное значение. Заметим, что в главе, посвященной вопросам криптографической защиты информации, авторы попытались донести до читателей суть основополагающих разделов криптографии от классических шифров до современных симметричных и асимметричных систем шифрования, а также методов управления криптографическими ключами. Кроме того, здесь же рассматриваются вопросы, связанные с процессами постановки и проверки электронной подписи.

Последняя глава книги затрагивает вопросы связанные с экономической эффективностью систем информационной безопасности, поскольку одна из основных задач специалиста в области защиты информации — доказать эффективность такой системы и показать руководству компании целесообразность инвестиций в информационную безопасность.

Для повышения качества проверки знаний в книге предусмотрены две формы контроля. Во-первых, в конце каждой главы приводятся контрольные тестовые задания, охватывающие основные вопросы раздела. Во-вторых, приведены три варианта тестовых контрольных заданий, охватывающих весь курс.

Глава 1. ИНФОРМАЦИЯ, ЕЕ ВИДЫ И ФОРМЫ ПРЕДСТАВЛЕНИЯ

1.1. Виды информации и формы представления информации в информационных системах

Прежде чем мы будем говорить о методах защиты информации и информационной безопасности, необходимо определить «что есть информация?». Сразу заметим, что здесь не существует всеобъемлющего определения.

Термин *информация* происходит от латинского слова *informatio* — разъяснение, изложение, осведомленность. Энциклопедический словарь (М.: Сов. энциклопедия, 1990) определяет информацию в исторической эволюции: первоначально это сведения, передаваемые людьми устным, письменным или другим способом (с помощью условных сигналов, технических средств и прочее); с середины XX в. — общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, обмен сигналами в животном и растительном мире (передача признаков от клетки к клетке, от организма к организму).

Философский подход использует свое понятие: *информация* — это взаимодействие, отражение, познание.

Толковый словарь русского языка Ожегова приводит два определения:

1. *Информация* — сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством.

2. *Информация* — сообщения, осведомляющие о положении дел, о состоянии чего-нибудь.

Согласно экономическому словарю *информация* (лат. *informatio* — осведомлять) — 1) любое сообщение о чем-либо; 2) сведения, данные, значения экономических показателей, являющиеся объектами хранения, обработки и передачи и используемые в процессе анализа и выработки экономических решений в управлении; 3) один из видов ресурсов, используемых в экономических процессах, получение которого требует затрат времени и других видов ресурсов, в связи с чем эти затраты следует включать в издержки производства и обращения; 4) одна из трех фундаментальных субстанций (вещество, энергия, информация), составляющих сущность мироздания и охватывающих любой продукт мыслительной деятельности, прежде всего — знания, образы.

Клод Элвуд Шеннон

По К.Э. Шеннону[1] *информация* — уменьшение неопределенности наших знаний.

В Российском законодательстве[2] вводится свое определение информации: *информация* — сведения (сообщения, данные) независимо от формы их представления.

Этот список определений далеко не полный, и подводя итог относительно понятия «информация», можно сказать, что информацию нельзя считать лишь техническим термином, это фундаментальная философская категория, которой присущи такие свойства, как запоминаемость, передаваемость, преобразуемость, воспроизводимость, стираемость.

В рамках научных представлений информация является первичным и неопределяемым понятием и предполагает наличие материального носителя информации, источника информации, передатчика информации, приемника и канала связи между источником и приемником. Понятие информации используется во всех сферах: науке, технике, культуре, социологии и повседневной жизни.

Каким же определением воспользоваться нам, рассматривая вопросы обеспечения информационной безопасности и защиты информации? Остановимся на том, что предлагает нам законодательство:

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

Информация — специфический атрибут реального мира, представляющий собой его объективное отражение в виде совокупности сигналов и проявляющийся при взаимодействии с приемником информации, позволяющим выделять, регистрировать эти сигналы из окружающего мира и по тому или иному критерию их идентифицировать. Причем сведения могут быть представлены в самом разнообразном виде. Информацию классифицируют по способу восприятия, по форме представления и по общественному значению.

---

[1] Клод Элвуд Шеннон является основателем теории информации, нашедшей применение в современных высокотехнологических системах связи. Статьи Шеннона «Математическая теория связи» и «Теория связи в секретных системах» считаются основополагающими для теории информации и криптографии.

[2] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 25.11.2017) «Об информации, информационых технологиях и о защите информации». Ст. 2.

Рассмотрим первоначально классификацию информации **по способу ее восприятия**.

У человека пять органов чувств:

- *зрение* — визуально люди различают цвета, воспринимают зрительную информацию, к которой относятся и текстовая, и числовая, и графическая;
- *слух* дает возможность воспринимать аудиальную информацию: речь, музыку, звуковые сигналы и шумы;
- *обоняние* дает возможность воспринимать информацию о запахах окружающего мира;
- *вкус* — вкусовые рецепторы языка дают возможность получить информацию о том, каков предмет на вкус: горький, кислый, сладкий, соленый;
- *осязание* — тактильно можно получить информацию о температуре предмета, о качестве его поверхности.

Таким образом, человек получает информацию о внешнем мире с помощью своих органов чувств. Практически около 90 % информации человек получает при помощи органов зрения, примерно 9 % — при помощи органов слуха и только 1 % — при помощи остальных органов чувств (обоняния, вкуса, осязания). Следует отметить также, что органы чувств человека получили название *анализаторов*, поскольку именно посредством этих органов информацию получает головной мозг.

Средства вычислительной техники, обеспечивающие передачу, хранение и обработку информации, приспособлены, в первую очередь, для обработки текстовой, числовой, графической, аудио- и видеоинформации.

Рассмотрим далее классификацию информации **по форме ее представления**, ограничиваясь только теми ее видами, которые используются в средствах вычислительной техники.

Текстовая информация, например текст в книге, компьютерный текст. При устном сообщении информация может быть представлена только в словесной, текстовой форме.

Числовая информация, например различного рода числовые таблицы, массивы цифровых данных и прочее. В чистом виде числовая информация встречается достаточно редко, чаще используется комбинированная форма представления информации.

Графическая информация, например рисунки, схемы, чертежи, фотографии. Такая форма представления информации наиболее доступна, так как сразу передает необходимый образ, а числовая и словесная требуют мысленного воссоздания образа.

Музыкальная (звуковая) информация, например аудиофайлы, воспроизводимые с использованием средств вычислительной техники, аналоговых или цифровых аудиоустройств.

В настоящее время большое значение приобретает комбинированная форма представления информации, так называемая мультимедийная форма: цветная графика сочетается в этих системах со звуком и текстом, с движущимися изображениями и трехмерными образами.

По общественному значению информация может быть:

– личной (знания, опыт, интуиция, умения);
– общественной, т.е. сведения, получаемые из средств массовой информации, кроме того, это опыт всего человечества, исторические, национальные и культурные традиции;
– обыденная (та, которой мы обмениваемся в процессе общения);
– эстетическая (например, музыка, театр, изобразительное искусство);
– специальная (например, научная, техническая).

С определением информации связаны такие понятия, как сигнал, сообщение и данные.

Сигнал (от лат. *signum* — знак) представляет собой любой процесс, несущий информацию.

Канал связи — среда (пространство), в которой проявляется сигнал.

Сообщение — это информация, представленная в определенной форме и предназначенная для передачи.

Данные — это информация, представленная в формализованном виде и предназначенная для обработки ее техническими средствами, например средствами вычислительной техники.

Применительно к компьютерной обработке данных под сообщением понимают некоторую последовательность символических обозначений (букв, цифр, закодированных графических образов и звуков и т.п.), несущих смысловую нагрузку и представленных в понятном компьютеру виде.

При передаче сообщения от источника к приемнику необходима некоторая материальная субстанция — *носитель информации*. Сообщение, передаваемое посредством носителя, представляет собой сигнал. В общем случае сигнал — это изменяющийся во времени физический процесс. Та из характеристик процесса, которая используется для представления сообщения, называется параметром сигнала.

Если параметр сигнала принимает последовательное во времени конечное число значений, сигнал называется дискретным, а сообщение, передаваемое с помощью таких сигналов, — дискретным сообщением. Если же источник вырабатывает непрерывное сообщение (параметр сигнала — непрерывная функция от времени), то соответствующее сообщение называется непрерывным сообщением.

Сигнал называется непрерывным, если его параметр в заданных пределах может принимать любые промежуточные значения. Сигнал называется дискретным, если его параметр в заданных пределах может принимать отдельные фиксированные значения. Следует различать непрерывность или дискретность сигнала по уровню и во времени.

На рис. 1.1 графически изображены:

а) непрерывный по уровню и во времени сигнал $x_{нн}$;
б) дискретный по уровню и непрерывный во времени сигнал $x_{дн}$;
в) непрерывный по уровню и дискретный во времени сигнал $x_{нд}$;
г) дискретный по уровню и во времени сигнал $x_{дд}$.

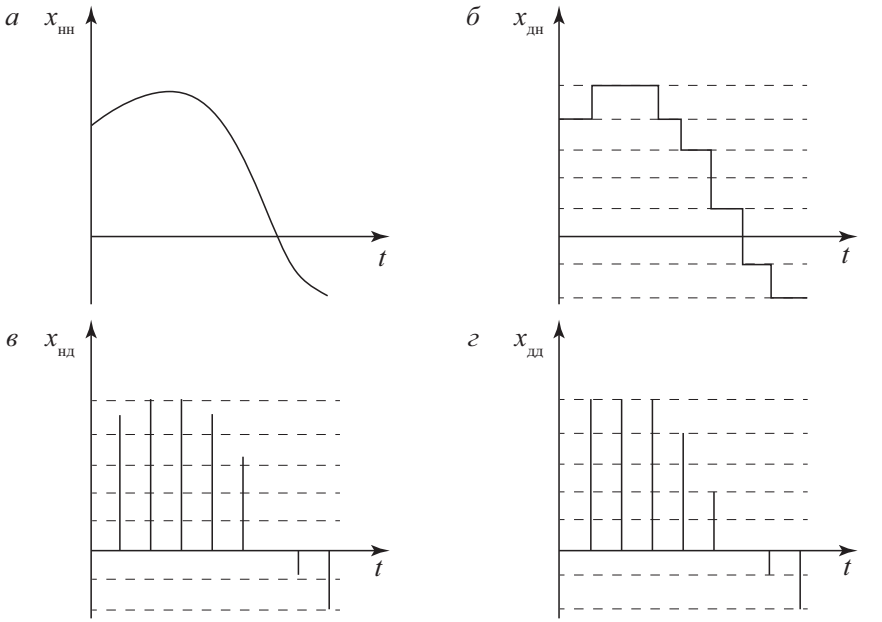


Рис. 1.1. Виды информационных сигналов

Непрерывное сообщение может быть представлено непрерывной функцией, заданной на некотором интервале. Непрерывное сообщение можно преобразовать в дискретное (такая процедура называется дискретизацией). Из бесконечного множества значений параметра сигнала выбирается их определенное число, которое приближенно может характеризовать остальные значения. Для этого область определения функции разбивается на отрезки равной длины и на каждом из этих отрезков значение функции принимается постоянным и равным, например, среднему значению на этом отрезке. В итоге получим конечное множество чисел. Временная дискретизация сигнала представлена на рис. 1.2.

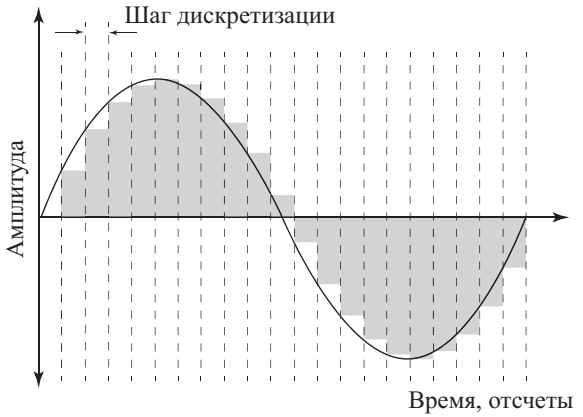


Рис. 1.2. Временная дискретизация сигнала

Таким образом, любое непрерывное сообщение может быть представлено как дискретное, иначе говоря, последовательностью знаков некоторого алфавита.

Возможность дискретизации непрерывного сигнала с любой желаемой точностью, причем для возрастания точности достаточно уменьшить шаг дискретизации, принципиально важна с точки зрения обработки информации в средствах вычислительной техники.

1.2. Фазы обращения информации. Меры информации

Введем ряд понятий, необходимых для дальнейшего рассмотрения вопросов, связанных с процессами хранения, передачи и преобразования информации.

Если процесс обработки информации формализуем, он может выполняться техническими средствами, например с помощью средств вычислительной техники, в связи с чем появилось понятие «данные».

Данные можно определить, как сведения, представленные в формализованной форме (например, закодированные), записанные на те или иные носители и допускающие обработку с помощью технических средств. Фазы обращения информации в информационной системе представлены рис. 1.3.

Восприятие состоит в том, что формулируется образ объекта, производится его опознание и оценка. В результате восприятия получают сигнал в форме, удобной для передачи.

Подготовка включает нормализацию, квантование, кодирование и прочее.

Рис. 1.3. Фазы обращения информации в информационной системе

Передача информации состоит в переносе ее на расстояние посредством сигналов различной физической природы, например по электрическим, оптическим, акустическим, механическим и прочим каналам.

Обработка заключается в решении задач, связанных с преобразованием информации, независимо от их функционального назначения, например, обработка с использованием вычислительных средств.

Хранение предполагает использование того или иного носителя информации, например магнитных носителей.

Представление информации требуется, как правило, тогда, когда в цикле участвует человек, т.е. осуществляется представление информации в форме, приемлемой для восприятия.

Заметим, что не все информационные системы замкнуты, как это показано на рис. 1.3. Существуют разомкнутые системы, где информация передается от источника к приемнику.

При реализации информационных процессов всегда происходит перенос информации в пространстве и времени от источника информации к приемнику. При этом для передачи информации используют различные символы, например естественного или некоего формального языка, позволяющие выразить ее в форме сообщения.

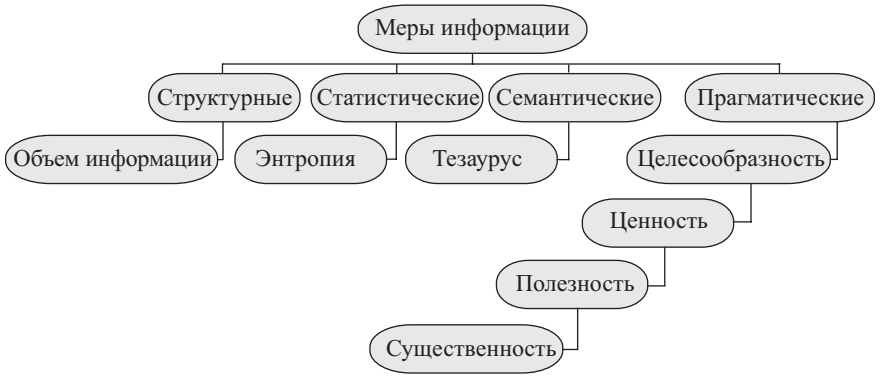


Рис. 1.4. Меры информации

Важнейшим вопросом теории информации является установление *меры количества* и *качества информации*. Информационные меры отвечают трем основным направлениям в теории информации: *структурному, статистическому* и *семантическому.* Кроме того, рассматривается *прагматический аспект*, т.е. отношения между сообщением и получателем — потребительское содержание сообщения, его отношение к получателю.

На рис. 1.4 представлена классификация мер информации.

Структурный подход рассматривает дискретное строение массивов информации и их измерение простым подсчетом информационных элементов (квантов). К наиболее часто употребляемым структурным мерам относится *объем данных*.

Объем данных в сообщении измеряется количеством символов (разрядов). В различных системах счисления один разряд имеет различный вес и, соответственно, меняется единица измерения данных:

– в двоичной системе счисления единица измерения *бит* (*binary digit* — двоичный разряд):

1 байт = 8 бит.

1 Кб = 1024 байт (2^{10} байт).

1 Мб = 1024 Кб (2^{10} Кб).

1 Гб = 1024 Мб (2^{10} Мб).

1 Тб = 1024 Гб (2^{10} Гб);

– в десятичной системе счисления единица измерения *дит* (десятичный разряд).

Пример

Сообщение в двоичной системе счисления в виде восьмиразрядного двоичного кода 11011001 имеет объем данных V= 8 бит.

Сообщение в десятичной системе счисления в виде шестиразрядного числа 678905 имеет объем данных V = 6 дит.

Структурная оценка не связана с содержательной стороной информации, а оперирует с обезличенной информацией, не выражающей смыслового отношения к объекту. В связи с этим данная мера дает возможность оценки информационных потоков в таких разных по своей природе объектах, как системы связи, вычислительные системы, системы управления, нервная система живого организма и др.

Статистический подход оперирует понятием *энтропия.* Количество информации на статистическом уровне невозможно определить без рассмотрения понятия неопределенности состояния системы — *энтропии системы*. Действительно, получение информации о какой-либо системе всегда связано с изменением степени неосведомленности получателя о состоянии этой системы.

Энтропия (от греч. ἐντροπία — превращение, обращение) представляет собой меру неопределенности и в теории информации характеризует способность источника отдавать информацию.

Существование неопределенности связано с участием вероятностей в осуществлении событий. Устранение неопределенности есть увеличение вероятности наступления того, что задано как цель. Поэтому вероятности должны участвовать в математической формулировке величины устраненной неопределенности.

Первая удачная попытка реализовать определение информации на такой основе была предпринята в 1928 г. Л. Хартли и получила развитие в работах Клода Шеннона[1].

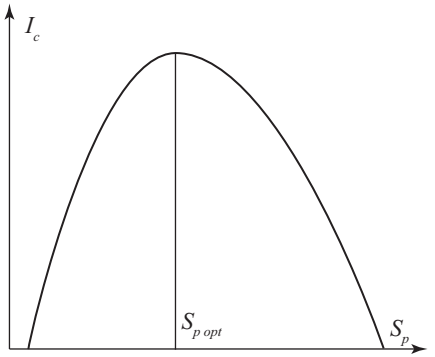
Семантический подход предполагает анализ отношения между знаками и обозначаемыми ими предметами, действиями, качествами, т.е. смысловое содержание сообщения, его отношение к источнику информации.

Для измерения смыслового содержания информации, т.е. ее количества на семантическом уровне, наибольшее признание получила *тезаурусная мера*, которая связывает семантические свойства информации со способностью пользователя принимать поступившее сообщение. Для этого используется понятие «тезаурус пользователя».

Тезаурус — это совокупность сведений, которыми располагает пользователь или система.

Максимальное количество семантической информации I_c потребитель приобретает при согласовании ее смыслового содержания S со своим тезаурусом S_p ($S_p = S_{p\,\mathrm{opt}}$), когда поступающая информация понятна пользователю и несет ему ранее неизвестные, т.е. отсутствующие в его тезаурусе сведения.

[1] *Шеннон К.* Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер. с англ.; под ред. Р.Л. Добрушина и О.Б. Лупанова. М.: ИЛ, 1963.



В зависимости от соотношений между смысловым содержанием информации S и тезаурусом пользователя S_p изменяется количество семантической информации I_c, воспринимаемой пользователем и включаемой им в дальнейшем в свой тезаурус.

Рассмотрим два предельных случая:

– при $S_p = 0$ пользователь не воспринимает, не понимает поступающую информацию;

– при $S_p \to \infty$ пользователь все знает, и поступающая информация ему не нужна.

Рис. 1.5. Зависимость количества семантической информации, воспринимаемой потребителем, от его тезауруса $I_c = f(S_p)$

Следовательно, количество семантической информации в сообщении, количество новых знаний, получаемых пользователем, является величиной относительной. Одно и тоже сообщение может иметь смысловое содержание для компетентного пользователя и быть бессмысленным для пользователя некомпетентного. При оценке семантического или содержательного аспекта информации необходимо стремиться к согласованию величин S и S_p.

Прагматический подход рассматривает отношения между сообщением и получателем, т.е. потребительское содержание сообщения, его отношение к получателю. На прагматическом уровне интересуют последствия от получения и использования данной информации потребителем. Проблемы этого уровня связаны с определением ценности и полезности информации для потребителя. Основная сложность здесь состоит в том, что целесообразность, ценность, полезность и существенность информации может быть совершенно различной для различных получателей и, кроме того, она зависит от ряда факторов, таких, например, как своевременность ее доставки и использования.

Контрольные задания к главе 1

1. Информацию, изложенную на доступном для получателя языке, называют:

   1) полной;
   2) полезной;
   3) актуальной;
   4) достоверной;
   5) понятной.

2. Информацию, не зависящую от личного мнения или суждения, называют:

   1) достоверной;
   2) актуальной;
   3) объективной;
   4) полной;
   5) понятной.

3. Информацию, отражающую истинное положение вещей, называют:

   1) полной;
   2) полезной;
   3) актуальной;
   4) достоверной;
   5) понятной.

4. Информацию, существенную и важную в настоящий момент, называют:

   1) полной;
   2) полезной;
   3) актуальной;
   4) достоверной;
   5) понятной.

5. Наибольший объем информации человек получает при помощи:

   1) органов слуха;
   2) органов зрения;
   3) органов осязания;
   4) органов обоняния;
   5) вкусовых рецепторов.

6. Тактильную информацию человек получает посредством:

   1) специальных приборов;
   2) термометра;
   3) барометра;
   4) органов осязания;
   5) органов слуха.

7. Сигнал называют аналоговым, если

   1) он может принимать конечное число конкретных значений;
   2) он непрерывно изменяется по амплитуде во времени;
   3) он несет текстовую информацию;
   4) он несет какую-либо информацию;
   5) это цифровой сигнал.

8. Сигнал называют дискретным, если

   1) он может принимать конечное число конкретных значений;
   2) он непрерывно изменяется по амплитуде во времени;
   3) он несет текстовую информацию;
   4) он несет какую-либо информацию;
   5) это цифровой сигнал.

9. Преобразование непрерывных изображений и звука в набор дискретных значений в форме кодов называют

   1) кодированием;
   2) дискретизацией;
   3) декодированием;
   4) информатизацией.

10. Во внутренней памяти компьютера представление информации

   1) непрерывно;
   2) дискретно;
   3) частично дискретно, частично непрерывно;
   4) осуществляется в виде символов и графиков.

11. Аналоговым сигналом является:

   1) сигнал светофора;
   2) сигнал SOS;
   3) сигнал маяка;
   4) электрокардиограмма;
   5) дорожный знак.

12. Дискретный сигнал формирует:

   1) барометр;
   2) термометр;
   3) спидометр;
   4) светофор.

13. Измерение температуры представляет собой процесс:

   1) хранения информации;
   2) передачи информации;
   3) получения информации;
   4) защиты информации;
   5) использования информации.

14. Перевод текста с английского языка на русский можно назвать процессом:

   1) хранения информации;
   2) передачи информации;
   3) получения информации;
   4) защиты информации;
   5) обработки информации.

15. Обмен информацией — это

   1) выполнение домашней работы;
   2) просмотр телепрограммы;
   3) наблюдение за поведением рыб в аквариуме;
   4) разговор по телефону.

16. К формальным языкам можно отнести

   1) английский язык;
   2) язык программирования;
   3) язык жестов;
   4) русский язык;
   5) китайский язык.

17. Основное отличие формальных языков от естественных:

   1) в наличии строгих правил грамматики и синтаксиса;
   2) количество знаков в каждом слове не превосходит некоторого фиксированного числа;
   3) каждое слово имеет не более двух значений;
   4) каждое слово имеет только один смысл;
   5) каждое слово имеет только один смысл и существуют строгие правила грамматики и синтаксиса.

18. Двоичное число 10001_2 соответствует десятичному числу

   1) 11_{10};
   2) 17_{10};
   3) 256_{10};
   4) 1001_{10};
   5) 10001_{10}.

19. Число 24_8 соответствует числу

   1) 10110_{16};
   2) 20_{16};
   3) 76_{16};
   4) BF_{16};
   5) 14_{16}.

20. Какое число лишнее?

   1) FF_{16};
   2) 226_{10};
   3) 377_8;
   4) 11111111_2.

21. Укажите самое большое число:

   1) 144_{16};
   2) 144_{10};
   3) 144_8;
   4) 144_6.

22. За единицу количества информации принимается:
    1) байт;
    2) бит;
    3) бод;
    4) дит.
23. В какой из последовательностей единицы измерения указаны в порядке возрастания?
    1) гигабайт, килобайт, мегабайт, байт;
    2) гигабайт, мегабайт, килобайт, байт;
    3) мегабайт, килобайт, байт, гигабайт;
    4) байт, килобайт, мегабайт, гигабайт.

Ответы на тестовое задание к главе 1

Номер вопроса	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Правильный ответ	5	3	4	3	2	4	2	1	2	2	4	4

Номер вопроса	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**
Правильный ответ	3	5	4	2	5	2	5	2	1	2	4

Глава 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

2.1. Понятия «информационная безопасность» и «защита информации»

Ответив на вопрос «что есть информация?», перейдем к понятиям «информационная безопасность» и «защита информации». Прежде всего выясним, являются ли они синонимами, поскольку в литературе эти понятия употребляются не всегда корректно.

Информационная безопасность (англ. *information security*) — защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность[1].

С понятием «информационная безопасность» в разных контекстах связаны различные определения. Так, в Законе РФ «Об участии в международном информационном обмене» информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. Подобное же определение дается и в Доктрине информационной безопасности Российской Федерации[2], где указывается, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Оба эти определения рассматривают информационную безопасность в национальных масштабах и поэтому имеют очень широкое приложение.

Наряду с этим характерно, что применительно к различным сферам деятельности, так или иначе связанным с информационными технологиями, понятие «информационная безопасность» принимает более конкретные очертания.

Информационная безопасность организации — состояние защищенности интересов организации в условиях угроз в информационной

[1] ГОСТ Р ИСО/МЭК 27011–2012 Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002.

[2] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).

сфере. Защищенность достигается обеспечением совокупности свойств информационной безопасности — конфиденциальности, целостности, доступности информационных активов и инфраструктуры организации. Приоритетность свойств информационной безопасности определяется значимостью информационных активов для интересов (целей) организации[1].

Необходимо иметь в виду, что при рассмотрении проблемы информационной безопасности нарушитель необязательно является злоумышленником. Нарушителем информационной безопасности может быть сотрудник, нарушивший режим информационной безопасности или условия внешней среды. Например, высокая температура, может привести к сбоям в работе технических средств хранения информации и т.д.

Защита информации (ЗИ) — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию[2].

Таким образом, мы ответили на поставленный выше вопрос — термины «информационная безопасность» и «защита информации» не являются синонимами, о чем следует помнить при их употреблении.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий — области, развивающейся беспрецедентно высокими темпами. В области информационной безопасности важны не столько отдельные решения (правовые акты или программно-технические средства защиты), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.

В ряде случаев понятие «информационная безопасность» подменяется термином «компьютерная безопасность» или «кибербезопасность». В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры — только одна из составляющих информационных систем. Иными словами, информационная безопасность отличается от кибербезопасности тем, что стремится обеспечить безопасность данных в любой форме, тогда как понятие «кибербезопасность» применимо только к цифровым данным и средствам их передачи, обработки и хранения.

[1] ГОСТ Р 53114–2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

[2] ГОСТ Р 50922–2006 Защита информации. Основные термины и опередедения.

Несмотря на это, в рамках изучаемого курса основное внимание будет уделяться рассмотрению вопросов, связанных с обеспечением режима информационной безопасности применительно к вычислительным системам.

2.2. Составляющие информационной безопасности

Как уже было отмечено ранее, информационная безопасность — многогранная область деятельности, в которой успех может принести только системный подход.

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач:

1) обеспечением доступности информации;
2) обеспечением целостности информации;
3) обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности, кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность.

Доступность информации

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления производством, транспортом и т.п. Менее драматичные, но также весьма неприятные последствия — и материальные, и моральные — может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей, например продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть «Интернет» и т.п.

Доступность — это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени. Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Получение прогноза погоды на вчерашний день также не имеет никакого смысла, поскольку это событие уже наступило. В этом контексте весьма уместным является выражение «дорога ложка к обеду».

Целостность информации

Целостность информации условно подразделяется на статическую и динамическую. *Статическая* целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. *Динамическая* целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например анализ потока сообщений для выявления некорректных действий, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т.д.

Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно так же неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Целостность — гарантия того, что информация сейчас существует в ее исходном виде, т.е. при ее хранении или передаче не было произведено несанкционированных изменений.

Конфиденциальность информации

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, персональные данные сотрудников и др. Например, применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями. Во-первых, сведения о технических каналах утечки информации зачастую являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные и технические проблемы.

Конфиденциальность — гарантия доступности конкретной информации только тем, для кого она предназначена.

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности — к фальсификации информации и, наконец, нарушение конфиденциальности — к раскрытию информации ограниченного доступа.

Как уже отмечалось, выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме этого, нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке, уничтожению данных (нарушение доступности информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

2.3. Уровни формирования режима информационной безопасности

Задачи информационной безопасности общества

Анализ основ информационной безопасности показал, что обеспечение режима информационной безопасности является задачей комплексной. С одной стороны, информационная безопасность предполагает, как минимум, обеспечение трех ее составляющих — доступность, целостность и конфиденциальность данных. С другой стороны, информацией и информационными системами в буквальном смысле «пронизаны» все сферы общественной деятельности, и влияние информации на общество все нарастает, поэтому обеспечение информационной безопасности требует комплексного подхода.

В этой связи закономерным является рассмотрение проблемы обеспечения информационной безопасности на нескольких уровнях, которые в совокупности обеспечивали бы защиту информации и информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений.

Рассматривая проблему информационной безопасности в широком смысле, можно отметить, что в этом случае речь идет об информационной безопасности всего общества и его жизнедеятельности, при этом на информационную безопасность возлагается задача по минимизации всех отрицательных последствий от всеобщей информатизации и содействия развитию всего общества при использовании информации как ресурса его развития.

Основными задачами информационной безопасности в широком смысле являются:

– защита государственной тайны, т.е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
– защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
– защита прав предпринимателей при осуществлении ими коммерческой деятельности;
– защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Рассматривая проблему информационной безопасности в узком смысле, отметим, что в этом случае речь идет о совокупности методов и средств защиты информации и ее материальных носителей, направленных на обеспечение целостности, конфиденциальности и доступности информации.

Исходя из этого, выделим следующие задачи информационной безопасности:

– защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
– защита технических и программных средств информатизации от преднамеренных воздействий.

Заметим, что понятие «компьютерная безопасность», которому посвящена большая часть данного курса, как раз подходит под определение информационной безопасности в узком смысле, но не является полным ее содержанием, поскольку информационные системы и материальные носители информации связаны не только с компьютерами.

Уровни формирования режима информационной безопасности

С учетом изложенного выделим три уровня формирования режима информационной безопасности:

– законодательно-правовой;
– административный (организационный);
– программно-технический.

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности. Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений. К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированными в законодательном порядке, т.е. в виде свода правил и предписаний. Тем не менее, эти нормы большей частью не являются обязательными, как законодательные меры.

Административный уровень включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации. Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный. Физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам, соответственно, к нему относятся технические средства, реализуемые в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решетки и т.д.).

Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу. К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по ключу и т.д. К программным средствам защиты, образующим программный подуровень, относится специальное программное обеспечение, используемое для защиты информации, например антивирусный пакет и т.д.

Подчеркнем, что формирование режима информационной безопасности является сложной системной задачей, решение которой в разных странах различается по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и экономику, развитие производственной базы, общей культуры общества и, наконец, традиций и норм поведения.

2.4. Нормативно-правовые основы информационной безопасности в Российской Федерации

Правовые основы информационной безопасности общества

Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

Законодательная база в сфере информационной безопасности включает пакет федеральных законов, указов Президента РФ, постановлений Правительства РФ, межведомственных руководящих документов и стандартов.

Основополагающими документами по информационной безопасности в РФ являются Конституция РФ[1] и Доктрина информационной безопасности Российской Федерации.

В Конституции РФ гарантируется «тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» (ч. 2 ст. 23), а также «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (ч. 4 ст. 29). Кроме этого, Конституцией РФ «гарантируется свобода массовой информации» (ч. 5 ст. 29), т.е. массовая информация должна быть доступна гражданам.

Базовым документом по информационной безопасности в России является Доктрина информационной безопасности РФ. Она представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации. Доктрина информационной безопасности РФ представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Под информационной сферой в ней понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

[1] Конституция Российской Федерации принята всенародным голосованием 12.12.1993 (с учетом поправок, внесенных законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).

Основные законодательные акты Российской Федерации в области информационной безопасности и защиты информации

1. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В Законе определены следующие основные понятия:

– *государственная тайна* — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

– *носители сведений, составляющих государственную тайну* — материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;

– *система защиты государственной тайны* — совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;

– *доступ к сведениям, составляющим государственную тайну* — санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

– *гриф секретности* — реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;

– *средства защиты информации* — 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.

2. Закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» является одним из базовых законов в области защиты информации, который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Этот закон регулирует отношения, возникающие при:
– осуществлении права на поиск, получение, передачу, производство и распространение информации;
– применении информационных технологий;
– обеспечении защиты информации.

3. В 2001 г., после ратификации Конвенции «О защите физических лиц при автоматизированной обработке персональных данных» Совета Европы, в России появляется Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональный данных», целью которого стало обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. В данном Федеральном законе вводится определение персональных данных как «любой информации, относящейся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)».

В связи с этим на практике возникают вопросы. Например, означает ли такое широкое определение, что даже фамилия лица без его имени и отчества подлежит защите на основании Закона о персональных данных? Или все-таки Закон о персональных данных защищает только совокупность данных, позволяющих идентифицировать конкретное физическое лицо? Если обратиться к судебной практике, то помимо фамилии, имени и отчества к персональным данным также относятся: год, месяц, место и дата рождения, адрес, семейное, имущественное, социальное положения, профессия, образование, доходы и т.д. Вместе с тем суд подчеркивает, что не каждый из этих элементов сам по себе подпадает под защиту Федерального закона № 152-ФЗ, а только если они в отдельности или в совокупности помогают идентифицировать конкретное лицо.

4. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» принят взамен действовавшего ранее Федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи». Федеральный закон № 63-ФЗ принят в целях регулирования отношений в следующих областях: совершение гражданско-правовых сделок; оказание государственных и муниципальных услуг; исполнение государственных и муниципальных функций; совершение иных юридически значимых действий. Закон должен обеспечить сохранение подлинности и достоверности электронных документов и информации, заверенных электронной подписью подписанта, при соблюдении требований, указанных в нем. Также обмен документами, которые подписаны электронно, позволяет одновременно решить проблему медленного процесса документообмена в бумажном формате и утраты бумажного документа, потери его физических и информационных свойств с течением времени.

Мы привели здесь только основные законодательные акты в сфере информационной безопасности. Работа по созданию нормативной базы предусматривает разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроля за исполнением указанных документов. Необходимо отметить, что такая работа в последнее время ведется практически непрерывно, поскольку сфера информационных технологий развивается стремительно, соответственно появляются новые формы информационных отношений, существование которых должно быть определено законодательно.

Ответственность за нарушения в сфере информационной безопасности

Немаловажная роль в системе правового регулирования информационных отношений отводится ответственности субъектов за нарушения в сфере информационной безопасности.

Основными документами в этом направлении являются:
– Уголовный кодекс Российской Федерации;
– Кодекс Российской Федерации об административных правонарушениях.

В принятом в 1996 г. Уголовном кодексе Российской Федерации как наиболее сильнодействующем законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности вопросам безопасности информации посвящены следующие главы и статьи:
– Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.
– Статья 140. Отказ в предоставлении гражданину информации.
– Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.
– Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей.
– Статья 283. Разглашение государственной тайны.
– Статья 284. Утрата документов, содержащих государственную тайну.

Особое внимание уделяется компьютерным преступлениям, ответственность за которые предусмотрена в специальной главе 28 «Преступления в сфере компьютерной информации». Глава 28 включает следующие статьи:

Статья 272. Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы

ЭВМ или их сети, — наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, — наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или другого дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, — наказывается лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.
2. Те же деяния, повлекшие по неосторожности тяжкие последствия, — наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, — наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.
2. То же деяние, повлекшее по неосторожности тяжкие последствия, — наказывается лишением свободы на срок до четырех лет.

2.5. Стандарты информационной безопасности

Требования безопасности к информационным системам

Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» был издан 1 декабря 1999 г. (соответствующий ему национальный стандарт ГОСТ Р ИСО/МЭК 15408-2012) и относится к оценочным стандартам. Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран. Он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Именно поэтому этот стандарт очень часто называют «Общими критериями».

«Общие критерии» являются метастандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.

Как и «Оранжевая книга»[1], «Общие критерии» содержат два основных вида требований безопасности:

- *функциональные требования* — соответствуют активному аспекту защиты — предъявляемые к функциям безопасности и реализующим их механизмам;
- *требования доверия* — соответствуют пассивному аспекту — предъявляемые к технологии и процессу разработки и эксплуатации.

В отличие от «Оранжевой книги», «Общие критерии» не содержат предопределенных «классов безопасности». Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

Очень важно, что безопасность в «Общих критериях» рассматривается не статично, а в привязке к жизненному циклу объекта оценки.

Угрозы безопасности в стандарте характеризуются следующими параметрами:

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

Принцип иерархии: класс — семейство — компонент — элемент

Для структуризации пространства требований, в «Общих критериях» введена иерархия класс — семейство — компонент — элемент.

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

Семейства в пределах класса различаются по строгости и другим тонкостям требований.

Компонент — минимальный набор требований, фигурирующий как целое.

Элемент — неделимое требование.

Между компонентами могут существовать зависимости, которые возникают, когда компонент сам по себе недостаточен для достижения цели безопасности.

---

[1] Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации в области информационной безопасности во многих странах, стал стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем». Данный труд, называемый чаще всего по цвету обложки «Оранжевой книгой», был впервые опубликован в августе 1983 г.

Подобный принцип организации защиты напоминает принцип программирования с использованием библиотек, в которых содержатся стандартные (часто используемые) функции, из комбинаций которых формируется алгоритм решения.

«Общие критерии» позволяют с помощью подобных библиотек (компонент) формировать два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты представляет собой типовой набор требований, которым должны удовлетворять продукты и/или 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.

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, т.е. подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Функциональные требования

Все *функциональные требования* объединены в группы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в «Общих критериях» представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это гораздо больше, чем число аналогичных понятий в «Оранжевой книге».

«Общие критерии» включают следующие классы функциональных требований:

1) идентификация и аутентификация;
2) защита данных пользователя;
3) защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
4) управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
5) аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
6) доступ к объекту оценки;
7) приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);

8) использование ресурсов (требования к доступности информации);
9) криптографическая поддержка (управление ключами);
10) связь (аутентификация сторон, участвующих в обмене данными);
11) доверенный маршрут/канал (для связи с сервисами безопасности).

Рассмотрим, например, содержание одного из классов.

Класс функциональных требований «Использование ресурсов» включает три семейства:

1. *Отказоустойчивость.* Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В стандарте различаются активная и пассивная отказоустойчивости. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

2. *Обслуживание по приоритетам.* Выполнение этих требований позволяет управлять использованием ресурсов так, что низко приоритетные операции не могут помешать высоко приоритетным.

3. *Распределение ресурсов.* Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

Аналогично и другие классы включают наборы семейств требований, которые используются для формулировки требований к системе безопасности.

Требования доверия

Вторая форма требований безопасности в «Общих критериях» — требования доверия безопасности. Установление доверия безопасности основывается на активном исследовании объекта оценки. Форма представления требований доверия та же, что и для функциональных требований (класс — семейство — компонент).

Всего в «Общих критериях» 10 классов, 44 семейства, 93 компонента требований доверия безопасности.

Классы требований доверия безопасности:

1) разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
2) поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
3) тестирование;
4) оценка уязвимостей (включая оценку стойкости функций безопасности);
5) поставка и эксплуатация;
6) управление конфигурацией;
7) руководства (требования к эксплуатационной документации);

8) поддержка доверия (для поддержки этапов жизненного цикла после сертификации);

9) оценка профиля защиты;

10) оценка задания по безопасности.

Применительно к требованиям доверия (для функциональных требований не предусмотрены) в «Общих критериях» введены оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Степень доверия возрастает от первого к седьмому уровню. Так, оценочный уровень доверия 1 (начальный) применяется, когда угрозы не рассматриваются как серьезные, а оценочный уровень 7 применяется к ситуациям чрезвычайно высокого риска.

Стандарты информационной безопасности распределенных систем

Сервисы безопасности в вычислительных сетях. В настоящее время с развитием вычислительных сетей и в особенности глобальной сети «Интернет» вопросы безопасности распределенных систем приобрели особую значимость. Важность этого вопроса косвенно подчеркивается появлением чуть позже «Оранжевой книги» стандарта, получившего название «Рекомендации X.800», который достаточно полно трактовал вопросы информационной безопасности распределенных систем, т.е. вычислительных сетей.

«Рекомендации X.800» выделяют следующие сервисы (функции) безопасности и исполняемые ими роли:

1. *Аутентификация*. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и периодически во время сеанса. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

2. *Управление доступом*. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

3. *Конфиденциальность данных*. Обеспечивает защиту от несанкционированного получения информации. Отдельно выделяется *конфиденциальность трафика* — это защита информации, которую можно получить, анализируя сетевые потоки данных.

4. *Целостность данных* подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры — с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

5. *Неотказуемость* (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки.

Механизмы безопасности. В X.800 определены следующие сетевые механизмы безопасности:

– шифрование;
– электронная цифровая подпись;
– механизм управления доступом;
– механизм контроля целостности данных;
– механизм аутентификации;
– механизм дополнения трафика;
– механизм управления маршрутизацией;
– механизм нотаризации (заверения).

Таблица 2.1 иллюстрирует, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для реализации той или иной функции.

Таблица 2.1

Взаимосвязь функций и механизмов безопасности

Функции	Механизмы							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+	–	–	+	–	–	–
Аутентификация источника	+	+	–	–	–	–	–	–
Управление доступом	–	–	+	–	–	–	–	–
Конфиденциальность	+	–	+	–	–	–	+	–
Избирательная конфиденциальность	+	–	–	–	–	–	–	–
Конфиденциальность трафика	+	–	–	–	–	+	+	–
Целостность соединения	+	–	–	+	–	–	–	–
Целостность вне соединения	+	+	–	+	–	–	–	–
Неотказуемость	–	+	–	+	–	–	–	+

«+» механизм используется для реализации данной функции безопасности;
«–» механизм не используется для реализации данной функции безопасности.

Так, например, «Конфиденциальность трафика» обеспечивается «Шифрованием», «Дополнением трафика» и «Управлением маршрутизацией».

Администрирование средств безопасности. В рекомендациях X.800 рассматривается понятие «*администрирование средств безопасности*», которое включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Например, распространение криптографических ключей.

Согласно рекомендациям X.800 усилия администратора средств безопасности должны распределяться по трем направлениям:

– администрирование информационной системы в целом;
– администрирование сервисов безопасности;
– администрирование механизмов безопасности.

Администрирование информационной системы в целом включает обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Администрирование механизмов безопасности включает:

– управление криптографическими ключами (генерация и распределение);
– управление шифрованием (установка и синхронизация криптографических параметров);
– администрирование управления доступом (распределение информации, необходимой для управления — паролей, списков доступа и т.п.);
– управление аутентификацией (распределение информации, необходимой для аутентификации — паролей, ключей и т.п.);
– управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений — частоту отправки, размер и т.п.);
– управление маршрутизацией (выделение доверенных путей);
– управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

В 1987 г. Национальным центром компьютерной безопасности США была опубликована интерпретация «Оранжевой книги» для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Интерпретация отличается от самой «Оранжевой книги» учетом динамичности сетевых конфигураций. В интерпретациях предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети.

Среди защитных механизмов в сетевых конфигурациях на первое место выдвигается *криптография*, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.

В интерпретациях «Оранжевой книги» впервые систематически рассматривается вопрос обеспечения доступности информации.

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 обслуживании пользователей.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

– внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.);
– наличие средств реконфигурирования для изоляции и/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.

Стандарты информационной безопасности в Российской Федерации

Федеральная служба по техническому и экспортному контролю (ФСТЭК). В Российской Федерации информационная безопасность обеспечивается соблюдением указов Президента, Федеральных законов, постановлений Правительства Российской Федерации, руководящих документов Федеральной службы по техническому и экспортному контролю (до 16 августа 2004 г. ФСТЭК называлась Государственной технической комиссией при Президенте РФ, а в августе в рамках

административной реформы комиссия была переименована в Федеральную службу и подчинена Министерству обороны) и других нормативных документов.

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю», ФСТЭК является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

– обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;
– противодействия иностранным техническим разведкам на территории Российской Федерации;
– обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;
– защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
– осуществления экспортного контроля.

Стандарты информационной безопасности. В России в последние годы активно ведется работа по стандартизации в области информационной безопасности. Принят ряд стандартов, регламентирующих деятельность по управлению рисками информационной безопасности и системе управления информационной безопасностью (СУИБ). Перечислим лишь наиболее значимые из них.

ГОСТ Р ИСО/МЭК 13335-1–2006 «Информационная технология. Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий». Данный документ представляет собой руководство по управлению безопасностью информационных и телекоммуникационных технологий (ИТТ), устанавливает концепцию и модели, лежащие в основе базового понимания безопасности ИТТ, и раскрывает общие вопросы управления, которые важны для успешного планирования, реализации и поддержки безопасности ИТТ.

ГОСТ Р 51897–2011 «Менеджмент риска. Термины и определения». Содержит определения основных терминов в области менеджмента риска.

ГОСТ Р ИСО/МЭК 27000 (семейство стандартов), основанный и соответствующий семейству международных стандартов на системы управления информационной безопасностью ISO/IEC 27000. Эти стандарты определяют требования к системам управления информационной безопасностью, управлению рисками, метрики и измерения, а также руководство по внедрению. В семействе ISO 27000 четыре вида групп стандартов:

– стандарты для обзора и введения в терминологию;
– стандарты, которые определяют обязательные требования к СУИБ;
– стандарты, определяющие требования и рекомендации для аудита СУИБ;
– стандарты, предлагающие лучшие практики внедрения, развития и совершенствования СУИБ.

Перечислим наиболее значимые стандарты семейства ISO 27000:

Стандарты для обзора и введения в терминологию

ISO/IEC 27000:2016 «Информационные технологии. Средства обеспечения безопасности. Системы менеджмента информационной безопасности. Обзор и словарь».

Стандарты, которые определяют обязательные требования к СУИБ

ISO/IEC 27001:2005 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Это основной стандарт пакета. Он определяет требования к разработке, внедрению, поддержке и улучшению систем менеджмента информационной безопасности.

Стандарты, определяющие требования и рекомендации для аудита СУИБ

ISO/IEC 27006:2011 «Информационные технологии. Средства обеспечения безопасности. Требования для органов, выполняющих аудит и сертификацию систем менеджмента информационной безопасности». Этот стандарт расширяет требования стандарта ISO 17021 специально для органов, проводящих аудит и сертификацию СУИБ;

ISO/IEC 27007:2011 «Информационные технологии. Средства обеспечения безопасности. Руководящие указания для аудита систем менеджмента информационной безопасности». Стандарт ISO 27007 предлагает рекомендации по проведению аудитов СУИБ со стороны сертификационных организаций. Он полезен для аудиторов этих организаций;

ISO/IECTR 27008:2011«Информационныетехнологии. Методы обеспечения безопасности — Руководство для аудиторов по мерам и средствам обеспечения информационной безопасности». Данный стандарт, как и ISO 27007, является дополнительным стандартом к ISO 19011:2011 специально для СУИБ. Он специализирован для аудита средств управления информационной безопасностью в организации.

Стандарты, предлагающие лучшие практики внедрения, развития и совершенствования СУИБ

ISO/IEC 27002:2005 «Информационные технологии. Средства обеспечения. Свод практики для менеджмента информационной безопасности». Стандарт дает указания для разработки, внедрения, поддержки и совершенствования СУИБ;

ISO/IEC 27003:2010 «Информационные технологии. Руководство по осуществлению системы менеджмента информационной безопасности». Стандарт дает указания и методику для процессов разработки и внедрения СУИБ;

ISO/IEC 27004:2009 «Информационные технологии. Средства обеспечения безопасности. Измерения менеджмента информационной безопасности». Стандарт является руководством для выбора, проектирования, управления и улучшения средств и методов измерения эффективности и результативности системы;

ISO/IEC 27005:2011 «Информационные технологии. Методы защиты. Менеджмент рисков информационной безопасности». Этот стандарт является одним из самых важных в группе;

ISO/IEC 27011:2016 «Информационная технология. Методы и средства обеспечения безопасности. Практическое руководство по контролю за информационной безопасностью организаций, предлагающих телекоммуникационные услуги, на основе ISO/ IEC 27002». Это специализированное руководство по СУИБ в телекоммуникационных организациях;

ISO/IEC 27035:2016 «Информационные технологии — Методы обеспечения защиты. Управление инцидентами по информационной безопасности».

Отметим, что стандартизация в области информационной безопасности необходима и профессионалам, и потребителям продуктов и услуг ИБ, так как позволяет установить оптимальный уровень упорядочения и унификации, обеспечить взаимозаменяемость продуктов информационной безопасности, а также возможность ознакомления с результатами, полученными в разных странах и организациях. Для профессионалов это экономия времени на поиск эффективных и зарекомендовавших себя решений, а для потребителя — гарантия получения результата ожидаемого качества.

2.6. Административный уровень обеспечения информационной безопасности

Цели, задачи и содержание административного уровня

Административный уровень является промежуточным между законодательно-правовым и программно-техническим уровнями формирования режима информационной безопасности. Законы и стандарты в области информационной безопасности являются лишь отправным нормативным базисом информационной безопасности. Основой практического построения комплексной системы безопасности является административный уровень, определяющий главные направления работы по защите информационных систем.

Задачей административного уровня является разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.

Существенно, что именно на административном уровне определяются механизмы защиты, которые составляют третий уровень информационной безопасности — программно-технический.

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения в конкретных условиях функционирования информационной системы.

Содержанием административного уровня являются следующие мероприятия:

- разработка политики информационной безопасности;
- проведение анализа угроз и оценки рисков;
- выбор механизмов и средств обеспечения информационной безопасности.

Разработка политики информационной безопасности

Разработка политики безопасности ведется для конкретных условий функционирования информационной системы. Как правило, речь идет о политике безопасности организации, предприятия или учебного заведения. С учетом этого рассмотрим следующее определение политики безопасности.

Политика безопасности — это комплекс предупредительных мер по обеспечению информационной безопасности организации.

Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме того, политика безопасности

включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Основные направления разработки политики безопасности:

– определение объема и требуемого уровня защиты данных;
– определение ролей субъектов информационных отношений.

Результатом разработки политики безопасности является комплексный документ, представляющий собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности. Этот документ является методологической основой практических мер по обеспечению информационной безопасности и включает следующие группы сведений:

– основные положения информационной безопасности организации;
– область применения политики безопасности;
– цели и задачи обеспечения информационной безопасности организации;
– распределение ролей и ответственности субъектов информационных отношений организации и их общие обязанности.

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

При описании области применения политики безопасности перечисляются компоненты автоматизированной системы обработки, хранения и передачи информации, подлежащие защите.

Цели, задачи, критерии оценки информационной безопасности определяются функциональным назначением организации. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных и т.д.

Политика безопасности затрагивает всех субъектов информационных отношений в организации, поэтому на этапе разработки политики безопасности очень важно разграничить права и обязанности, связанные с их непосредственной деятельностью. С точки зрения обеспечения информационной безопасности разграничение прав и обязанностей целесообразно провести по следующим группам (ролям):

– специалист по информационной безопасности;
– владелец информации;
– поставщики аппаратного и программного обеспечения;
– менеджер отдела;
– операторы;
– аудиторы.

В зависимости от размеров организации, степени развитости ее информационной системы некоторые из перечисленных ролей могут отсутствовать вообще, а некоторые могут совмещаться одним и тем же физическим лицом.

Специалист по информационной безопасности (начальник службы безопасности, администратор по безопасности) играет основную роль в разработке и соблюдении политики безопасности предприятия. Он проводит оценку и переоценку рисков, выявляет уязвимости системы безопасности по всем направлениям (аппаратные средства, программное обеспечение и т.д.).

Владелец информации — лицо, непосредственно владеющее информацией и работающее с ней. В большинстве случае именно владелец информации может определить ее ценность и конфиденциальность.

Поставщики аппаратного и программного обеспечения обычно являются сторонними лицами, которые несут ответственность за поддержание должного уровня информационной безопасности в поставляемых им продуктах.

Администратор сети — лицо, занимающееся обеспечением функционирования информационной сети организации, поддержанием сетевых сервисов, разграничением прав доступа к ресурсам сети на основании соответствующей политики безопасности.

Менеджер отдела является промежуточным звеном между операторами и специалистами по информационной безопасности. Его задача — своевременно и качественно информировать подчиненный ему персонал обо всех требованиях службы безопасности и следить за их выполнением на рабочих местах. Менеджеры должны доводить до подчиненных все аспекты политики безопасности, которые непосредственно их касаются.

Операторы обрабатывают информацию, поэтому должны знать класс конфиденциальности информации и уметь оценивать ущерб, который будет нанесен организации при ее раскрытии.

Аудиторы — внешние специалисты по безопасности, нанимаемые организацией для периодической проверки функционирования всей системы безопасности предприятия.

Анализ угроз информационной безопасности

Анализ и выявление угроз информационной безопасности является второй важной функцией административного уровня обеспечения информационной безопасности. Во многом структура разрабатываемой системы защиты и состав механизмов ее реализации определяются потенциальными угрозами, выявленными на этом этапе.

Угроза безопасности информации — это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками.

Чаще всего возможность реализации угрозы является следствием наличия уязвимых мест в информационной системе. Это могут быть, например, неконтролируемый доступ к персональным компьютерам или нелицензионное программное обеспечение (к сожалению, даже лицензионное программное обеспечение не лишено уязвимостей).

Уязвимость информационной системы — это свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

История развития информационных систем показывает, что новые уязвимые места появляются постоянно. С такой же регулярностью, но с небольшим отставанием, появляются и средства защиты. В этой связи эффективным является способ упреждающей защиты, заключающийся в разработке механизмов защиты от возможных, предполагаемых и потенциальных угроз.

Отметим, что некоторые угрозы нельзя считать следствием целенаправленных действий злоумышленников. Существуют угрозы, вызванные случайными ошибками или техногенными явлениями.

Знание возможных угроз информационной безопасности, а также уязвимых мест системы защиты необходимо для того, чтобы выбрать наиболее экономичные и эффективные средства обеспечения безопасности.

Угрозы информационной безопасности классифицируются по нескольким признакам:

– *по составляющим информационной безопасности* (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;
– *по компонентам информационных систем*, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
– *по характеру воздействия* (случайные или преднамеренные, действия природного или техногенного характера);
– *по расположению источника угроз* (внутри или вне рассматриваемой информационной системы).

Отправной точкой при анализе угроз информационной безопасности является определение составляющей информационной безопасности, которая может быть нарушена той или иной угрозой: конфиденциальность, целостность или доступность.

Рис. 2.1. Классификация угроз информационной безопасности

На рис. 2.1 показано, что все виды угроз, классифицируемые по другим признакам, могут воздействовать на все составляющие информационной безопасности.

Рассмотрим классификацию угроз информационной безопасности по характеру воздействия.

Опыт проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах жизненного цикла системы.

Причинами *случайных воздействий* при эксплуатации могут быть:

– аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
– отказы и сбои аппаратуры;
– ошибки в программном обеспечении;
– ошибки в работе персонала;
– помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия — это целенаправленные действия злоумышленника. В качестве злоумышленника могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами**,** например:

– недовольством служащего служебным положением;
– любопытством;
– конкурентной борьбой;
– уязвленным самолюбием и т.д.

Угрозы, классифицируемые по расположению источника угроз, бывают *внутренние* и *внешние*. Внешние угрозы обусловлены применением вычислительных сетей и созданием на их основе информационных систем. Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.

Основные угрозы нарушения доступности информации

Наиболее опасными с точки зрения размера ущерба и частоты реализации являются *непреднамеренные ошибки* пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Эффективным способом борьбы с непреднамеренными случайными ошибками является максимальная автоматизация и строгий контроль.

Угрозы доступности информации можно рассматривать по компонентам автоматизированной информационной системы, на которые нацелены угрозы:

– отказ пользователей;
– внутренний отказ информационной системы;
– отказ поддерживающей инфраструктуры.

Применительно к пользователям характерны следующие угрозы:

– нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности);
– невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
– невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

– отступление (случайное или умышленное) от установленных правил эксплуатации;
– выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала;
– ошибки при конфигурировании системы;
– отказы программного и аппаратного обеспечения;
– разрушение данных;
– разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рассматриваются следующие угрозы:

– нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
– разрушение или повреждение помещений;
– невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности.

Опасными являются и *стихийные бедствия* — пожары, наводнения, землетрясения, ураганы. По статистике, на долю этих источников угроз с учетом перебоев электропитания приходится более 10 % потерь, нанесенных информационным системам.

Одним из опаснейших способов нарушения доступности и в целом информационной безопасности является внедрение в атакуемые системы *вредоносного программного обеспечения*.

Целями такого программного обеспечения являются:

– внедрение другого вредоносного программного обеспечения;
– получение контроля над атакуемой системой;
– агрессивное потребление ресурсов;
– изменение или разрушение программ и/или данных.

К сожалению, количество вредоносного программного обеспечения постоянно увеличивается. Вирусы и троянские программы считают уже на десятки тысяч, а базы данных антивирусных программ обновляются практически ежедневно, несмотря на постоянно внедряемые методы «универсального» детектирования (т.е. детектирования не конкретных вариантов отдельно взятого вируса, а всего семейства или даже целого класса вредоносных программ).

Подробный анализ данного класса угроз будет дан в последующих разделах.

Основные угрозы нарушения целостности информации

На втором месте по размерам ущерба, после непреднамеренных ошибок и упущений, стоят *кражи* и *подлоги*.

С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

– ввести неверные данные;
– модифицировать данные.

Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. С этой угрозой связано понятие «аутентичность», т.е. возможность подтверждения (доказательства) авторства того или иного документа или действия.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение рассмотренного выше вредоносного программного обеспечения — пример подобного нарушения.

Угрозами динамической целостности являются дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Основные угрозы нарушения конфиденциальности информации

Конфиденциальную информацию условно можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер, например, при работе с несколькими информационными системами возникает необходимость запоминания нескольких паролей. В таких случаях чаще всего пользуются записными книжками, листками, которые зачастую находятся рядом с компьютером и т.д. Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую — и не может быть обеспечена) необходимая защита. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным *перехват данных*. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна — осуществить доступ к данным в тот момент, когда они наименее защищены.

Перехват данных — очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например, на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных.

К существенным угрозам, от которых трудно защищаться, можно отнести *злоупотребление полномочиями*. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример — нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

2.7. Анализ и оценка рисков информационной безопасности

Анализ информационного риска — это систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации.

Общие понятия и терминология

Под риском понимают возможность наступления некоторого неблагоприятного события, влекущего за собой различного рода потери.

> **Риск информационной безопасности** (*information security risk*) — возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Различают базовый и полный анализ рисков информационной безопасности.

Базовый анализ рисков — анализ рисков, проводимый в соответствии с требованиями базового уровня защищенности. Прикладные методы анализа рисков, ориентированные на данный уровень, обычно дают качественные оценки и не оценивают эффективность контрмер. Методы данного класса применяются в случаях, когда к информационной системе не предъявляются повышенные требования в области информационной безопасности (ИБ).

Полный анализ рисков — анализ рисков для информационных систем, предъявляющих повышенные требования в области ИБ. Он включает в себя определение ценности информационных ресурсов, оценку угроз и уязвимостей, выбор адекватных контрмер, оценку их эффективности.

Управление рисками информационной безопасности

Важным этапом в сфере обеспечения информационной безопасности является процесс управления (менеджмента) рисками ИБ. *Процесс управления рисками* — это скоординированные действия по управлению и контролю организации в отношении риска. Управление рисками включает в себя *оценку риска*, *обработку риска*, *принятие риска* и *сообщение о риске* (рис. 2.2).

Управление рисками информационной безопасности — непрерывный процесс. В рамках данного процесса следует устанавливать контекст, оценивать и обрабатывать риски, используя для реализации рекомендации и решения плана обработки рисков. До принятия решения о том, что и когда должно быть сделано для снижения риска до приемлемого уровня, в рамках менеджмента риска анализируется, что может произойти и какими могут быть возможные последствия.

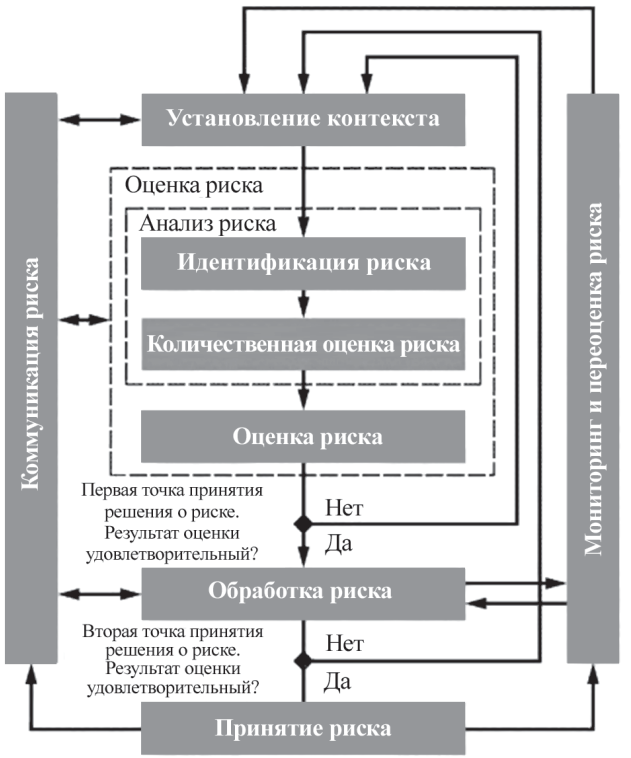


Рис. 2.2. Процесс менеджмента риска информационной безопасности (ГОСТ Р ИСО/МЭК 27005–2010)

Цель процесса оценивания рисков состоит в определении характеристик рисков по отношению к информационной системе и ее ресурсам (активам). На основе полученных данных могут быть выбраны необходимые средства защиты. При оценивании рисков учитываются многие факторы: ценность ресурсов, значимость угроз, уязвимостей, эффективность имеющихся и планируемых средств защиты и многое другое.

Менеджмент риска ИБ должен способствовать:

– идентификации рисков;
– оценке рисков, исходя из последствий их реализации для бизнеса и вероятности их возникновения;
– осознанию и информированию о вероятности и последствиях рисков;
– установлению приоритетов в рамках обработки рисков;
– установлению приоритетов мероприятий по снижению имеющихся рисков;

– привлечению причастных сторон к принятию решений о менеджменте риска и подержанию их информированности о состоянии менеджмента риска;
– эффективности проводимого мониторинга обработки рисков;
– проведению регулярного мониторинга и пересмотра процесса менеджмента риска;
– сбору информации для совершенствования менеджмента риска;
– подготовке менеджеров и персонала по вопросам менеджмента рисков и необходмых действий, предпринимаемых для их уменьшения.

Для решения задач управления рисками ИБ наиболее часто используются следующие методики и программные комплексы: OCTAVE, CRAMM, FRAP, RiskWatch, Microsoft Security Assessment Tool (MSAT), CORAS. Анализ перечисленных методик рассмотрен в работе[1], а подробное описание работы с программным инструментарием в учебном пособии[2]. Все известные методики анализа рисков ИБ можно классифицировать следующим образом:

– методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»), к таким методикам, в частности, относится FRAP;
– количественные методики (риск оценивается через числовое значение, например, размер ожидаемых годовых потерь), к этому классу относится методика RiskWatch;
– методики, использующие смешанные оценки (такой подход используется в методиках CRAMM и MSAT).

Для обработки риска ИБ входными данными являются сведения о перечне рисков с назначенными приоритетами в соответствии с критериями оценки рисков, касающимися сценариев инцидентов, которые приводят к этим рискам. Для обработки риска имеются четыре варианта: *снижение риска*, *сохранение риска*, *предотвращение риска* и *перенос риска* (рис. 2.3).

При *снижении риска* уровень риска должен быть снижен путем выбора меры и средства контроля и управления так, чтобы остаточный риск мог быть повторно оценен как допустимый. Решение *сохранить риск*, не предпринимая дальнейшего действия, следует принимать в зависимости от оценки риска. *Предотвращение риска* — отказ от деятельности или условия, вызывающего конкретный риск. *Перенос риска* — разделение с другой стороной бремени потерь или выгод от риска.

---

[1] *Баранова Е.К., Бабаш А.В.* Информационная безопасность и защита информации. Учеб. пособие. 4-е изд., перераб. и доп. М.: РИОР: ИНФРА-М, 2018.

[2] *Баранова Е.К., Бабаш А.В.* Моделирование системы защиты информации. Практикум: Учеб. пособие. 2-е изд., перераб. и доп. М.: РИОР: ИНФРА-М, 2016.

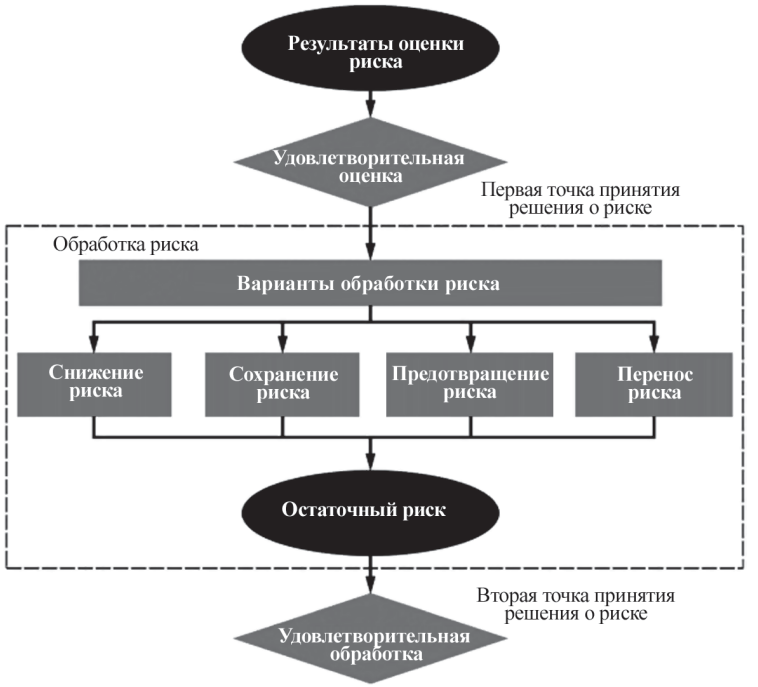


Рис. 2.3. Деятельность по обработке риска (ГОСТ Р ИСО/МЭК 27005–2010)

Варианты обработки риска должны выбираться исходя из результатов оценки риска, предполагаемой стоимости реализации этих вариантов и их ожидаемой эффективности. Должны реализовываться такие варианты, при которых значительное снижение риска может быть достигнуто при относительно небольших затратах. Четыре варианта обработки риска не являются взаимоисключающими. В отдельных случаях организация может получить значительную выгоду от объединения вариантов, таких как снижение риска, уменьшение последствий и перенос или сохранение любого остаточного риска.

2.8. Управление инцидентами информационной безопасности

Процесс управления инцидентами информационной безопасности

Информационная безопасность любой организации в первую очередь направлена на уменьшение рисков, связанных с информационными ресурсами. Конечным результатом обеспечения ИБ является предотвращение или минимизация ущерба от вероятных угроз или

инцидентов ИБ и, таким образом, получение выигрыша для всего бизнес-процесса организации. Для достижения данного результата в организациях, как правило, создаются подразделения информационной безопасности, которые занимаются защитой информационных ресурсов. Однако не стоит забывать о том, что вероятность возникновения инцидентов ИБ существует всегда, и даже самый совершенный комплекс мер по защите информации не может гарантировать возникновение в информационной среде событий, потенциально несущих угрозу всему бизнес-процессу. Неготовность организации к пониманию этого вопроса и своевременному его решению может сильно «ударить» по бизнесу и существенно повысить величину причиненного ущерба. У организаций, которые понимают степень важности этой проблемы, возникают вопросы, связанные с ИБ, а именно:

– с чего стоит начинать процесс управления инцидентами?
– как обеспечить взаимодействие между структурными подразделениями организации и оценивать эффективность их работы?

Для решения этих вопросов руководителям организаций и специалистам по обеспечению ИБ разумно реализовать комплексный подход к решению следующих задач:

1) определение, оповещение и регистрация инцидентов ИБ;
2) реагирование на инциденты ИБ и применение превентивных мер защиты для устранения причин потенциального ущерба;
3) расследование или анализ инцидентов с целью предотвращения повторного их проявления.

Решить эти задачи можно путем разработки и реализации эффективного процесса управления инцидентами. Тема управления инцидентами информационной безопасности на сегодняшний день является одной из наиболее обсуждаемых и актуальных для организаций. Это связанно с тем, что управление инцидентами ИБ является важнейшим процессом развития и совершенствования всей системы управления информационной безопасности (СУИБ).

В рамках управления инцидентами ИБ различают два взаимосвязанных понятия — это *событие ИБ* и, собственно, сам *инцидент ИБ*.

Событие ИБ — это идентифицированный случай состояния системы или сети, который указывает на возможное нарушение политики информационной безопасности или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности[1].

[1] ГОСТ Р ИСО/МЭК ТО 18044–2007. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

Событие представляет собой логическую связь между действием, объектом, на который направленно данное действие, и результатом действия. Иногда возникающие события являются частью шагов, предпринимаемых злоумышленником для получения какого-либо несанкционированного результата. Эти события можно рассматривать как часть инцидента ИБ. Если событие возникает вновь и может нанести ущерб организации, то такое событие нужно считать инцидентом ИБ.

Инцидент ИБ — это возникновение одного или нескольких нежелательных или непредвиденных событий ИБ, в результате которых велика вероятность компрометации бизнес-процессов и угрозы ИБ для организации[1].

Управление инцидентами — это процесс, который отвечает за управление жизненным циклом всех инцидентов. Основная цель управления инцидентами — это скорейшее возобновление прерванной работы информационной системы. Кроме того, процесс управления инцидентами должен осуществлять точную регистрацию всех инцидентов для оценки и совершенствования процесса управления и предоставления необходимой информации для других процессов. В общем виде процесс управления инцидентами представлен на рис. 2.4.

Рис. 2.4. Процесс управления инцидентами ИБ

Именно процесс управления инцидентами ИБ позволяет определить конкретные уязвимости ИБ организации, обнаружить следы атак и вторжений в информационную среду компании, что, в свою очередь, дает информацию о слабостях в системе защиты информации. Таким образом, управление инцидентами ИБ позволяет оценить эффективность

[1] ГОСТ Р ИСО/МЭК ТО 18044–2007.

СУИБ, определить ключевые роли персонала в результате возникновения нештатных ситуаций и, главное, за минимальный промежуток времени принять необходимые меры для восстановления полноценной работы компании.

Организация центра управления событиями информационной безопасности

В настоящее время особое внимание уделяется организации центра управления событиями информационной безопасности (Security Operations Center, SOC), который представляет собой комплекс процессов и программно-аппаратных средств, предназначенных для централизованного сбора и анализа информации о событиях и инцидентах ИБ, поступающих из различных источников IT-инфраструктуры, и своевременное реагирование на них.

Одним из наиболее популярных решений последних лет для контроля и выявления инцидентов является SIEM-система (Security Information and Event Management). Популярность SIEM прежде всего обусловлена значительным объемом задач, которые можно решить с помощью SIEM-системы:

- сконцентрировать инциденты, фиксируемые другими системами самостоятельно, в рамках единого ядра инцидент-менеджмента;
- получить удобный инструмент для поиска необходимых событий, разбора инцидентов, хранения собранных данных о событиях и инцидентах ИБ;
- выявлять статистические отклонения и медленно развивающиеся инциденты за счет анализа больших интервалов и объемов информации с конкретных средств защиты;
- сопоставлять и коррелировать данные из разных систем и, как следствие, строить сложные цепочки сценариев по обнаружению инцидентов.

Принцип работы SIEM заключается в том, что система собирает информацию, анализирует «на лету» и генерирует предупреждающее сообщение, записывает информацию в базы данных, анализирует поведение на основании предыдущих наблюдений, а также генерирует предупреждающее сообщение.

На рис. 2.5 представлено содержание основных механизмов функционирования SIEM-системы в виде трех уровней иерархии: *сбор данных*; *управление данными*; *анализ данных о событиях и инцидентах ИБ*.

Раскроем содержание основных механизмов функционирования SIEM-системы.

Нормализация означает приведение форматов записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки.

Рис. 2.5. Обобщенная иерархическая модель SIEM-системы

Фильтрация событий безопасности заключается в удалении избыточных событий из поступающих в систему потоков. *Классификация* позволяет для атрибутов событий безопасности определить их принадлежность определенным классам. *Агрегация* объединяет события, схожие по определенным признакам. *Корреляция* выявляет взаимосвязи между разнородными событиями, что позволяет обнаруживать атаки, а также нарушения критериев и политик безопасности. *Приоритизация* определяет значимость и критичность событий безопасности на основании правил, определенных в системе.

Анализ событий, инцидентов и их последствий включает процедуры моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров нарушителей, оценки риска, прогнозирования событий и инцидентов. *Генерация отчетов и предупреждений* означает формирование, передачу, отображение и/или печать результатов функционирования. *Принятие решений* определяет выработку мер по реконфигурированию средств защиты с целью предотвращения атак или восстановления безопасности инфраструктуры. *Визуализация* предполагает представление в графическом виде данных, характеризующих результаты анализа событий безопасности и состояние защищаемой системы и ее элементов.

SIEM-система является ядром любого SOC. Можно выделить несколько предпосылок для создания SOC — центра управления событиями информационной безопасности:

– постоянно развивающаяся IT-инфраструктура;
– большое количество активных средств защиты информации;
– отсутствие единой картины происходящего в IT-инфраструктуре;
– невозможность оценить эффективность текущих мер защиты информации;

– невозможность своевременного реагирования на инциденты ИБ;
– отсутствие сквозного процесса между IT, ИБ и бизнесом;
– необходимость выполнения требований стандартов.

Система управления (мониторинга) событиями ИБ реализует комплексный подход к решению задач сбора, анализа, корреляции и контроля событий ИБ, поступающих от различных средств защиты.

SOC — это не только и не столько технические средства, это прежде всего команда, задача которой обнаруживать, анализировать, реагировать, уведомлять о возникновении и предотвращать инциденты ИБ. Чтобы персонал, вооруженный техническими средствами, понимал свои задачи, имел четкие инструкции и KPI (Key Performance Indicators — ключевые показатели эффективности), мог эффективно взаимодействовать внутри SOC и со смежными подразделениями, необходимо выстроить целый ряд процессов в зоне ответственности SOC, направленных на повышение защищенности IT-инфраструктуры.

Базовые компоненты SOC представлены на рис. 2.6.

Как видно из представленной схемы, SOC — это не только люди. Это взаимосвязь процессов, технологий и людей, выполняющих определенные функции.

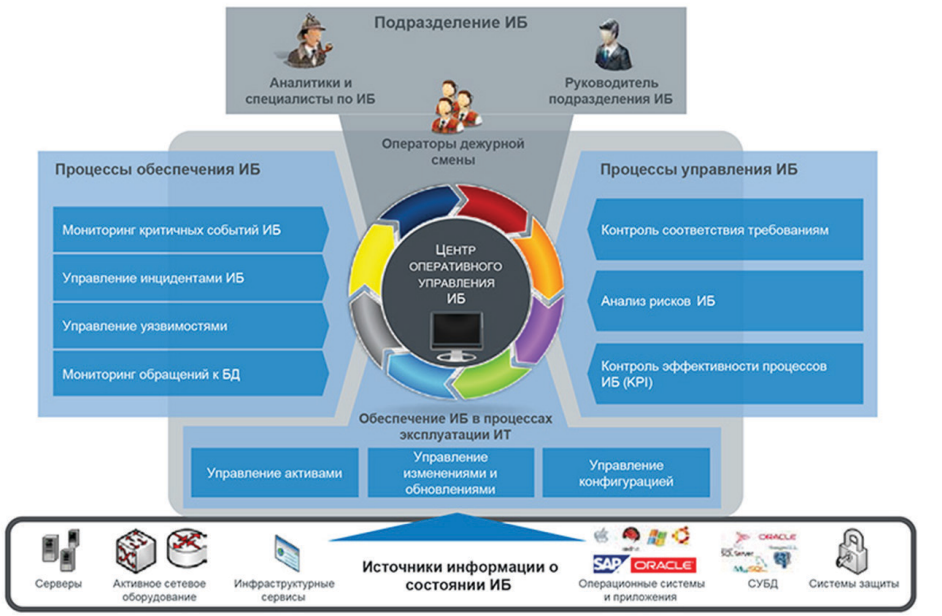


Рис. 2.6. Базовые компоненты SOC

Контрольные задания к главе 2

1. Угроза информационной безопасности — это:

1) чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий;
2) незаконное подключение к линиям связи;
3) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения информационной безопасности;
4) дистанционное преодоление систем защиты.

2. Любое действие или последовательность действий, использующих уязвимости

1) информационной системы и приводящих к нарушению политики безопасности — это:
2) вирус;
3) атака;
4) угроза;
5) взлом;
6) нападение.

3. Из приведенного ниже списка выберите понятия, не являющиеся принципами:

1) обеспечения ИБ:
2) системность;
3) комплексность;
4) шифрование информации;
5) разумная достаточность;
6) засекречивание данных;
7) открытость алгоритмов.

4. Как можно классифицировать атаки с точки зрения расположения источника угроз?

1) локальные;
2) удаленные;
3) пассивные;
4) активные.

5. Атаки, результатом воздействия которых является нарушение деятельности — это:

1) информационной системы, называются:
2) локальные;
3) удаленные;
4) пассивные;
5) активные.

6. Атаки, ориентированные на получение информации из системы, не нарушая функционирование информационной системы:

1) локальные;
2) удаленные;
3) пассивные;
4) активные.

7. Ориентирование на весь набор средств защиты данных — программные, технические, правовые, организационные и т.д. — является характеристикой следующего принципа обеспечения информационной безопасности:

1) комплексности;
2) разумной достаточности;
3) системности;
4) гибкости управления;
5) непрерывности защиты.

8. Комплекс мероприятий по обеспечению информационной безопасности должен быть непрерывен во времени и пространстве — это принцип:

1) комплексности;
2) разумной достаточности;
3) системности;
4) гибкости управления;
5) непрерывности защиты.

9. Какой принцип подразумевает нахождение компромисса между затратами на защиту информационных объектов и возможными потерями при реализации информационных угроз?

1) комплексности;
2) разумной достаточности;
3) системности;
4) гибкости управления;
5) непрерывности защиты.

10. Изменение применяемых средств, оперативное включение или исключение используемых средств защиты данных, добавление новых механизмов защиты определяют принцип:

1) комплексности;
2) разумной достаточности;
3) системности;
4) гибкости управления;
5) непрерывности защиты.

11. Что понимают под термином «информационная безопасность»?

1) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений;
2) комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты;
3) комплекс взаимно координируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации;
4) средства защиты аппаратной и программной составляющей систем обработки информации.

12. Защита информации — это:

1) защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
2) комплекс мероприятий, направленных на обеспечение информационной безопасности;
3) обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление;
4) защита государственной тайны, т.е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения.

13. Какие базовые свойства информации и систем ее обработки информационная система не должна обеспечивать?

1) доступность;
2) конфиденциальность;
3) целостность;
4) динамичность.

14. Что такое сервис безопасности?

1) сервис, который обеспечивает задаваемую политикой безопасность систем и/или передаваемых данных, либо определяет осуществление атаки;
2) гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена;
3) система формирования режима информационной безопасности;
4) сервис защиты технических и программных средств информатизации от преднамеренных воздействий.

15. Попытка реализации угрозы называется:

1) атакой;
2) любопытством;
3) методом воздействия;
4) источником угрозы.

16. Какие из ниже перечисленных примеров нарушения целостности информации являются статическими?

1) дублирование данных, несанкционированное изменение данных, ввод неверных данных, внесение дополнительных пакетов в сетевой трафик;
2) дублирование данных, нарушение атомарности транзакций, несанкционированное изменение данных, ввод неверных данных;
3) ввод неверных данных, несанкционированное изменение данных, изменение программного модуля вирусом;
4) нарушение атомарности транзакций, дублирование данных, внесение дополнительных пакетов в сетевой трафик.

17. Какие из перечисленных документов можно отнести к основным правовым актам в области информационной безопасности?

1) Уголовый кодекс РФ;
2) Конституция РФ;
3) Трудовой кодекс РФ;
4) Доктрина информационной безопасности РФ.

18. Какие существуют группы мер законодательного уровня, обеспечивающие правовую поддержку мероприятий информационной безопасности?

1) меры, направленные на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям ИБ;
2) меры по распространению и разработке средств, помогающих создавать компьютерные вирусы, с целью создания антивирусов;
3) направляющие и координирующие меры, способствующие повышению уровня знаний в области ИБ, помогающие в разработке и распространении средств обеспечения безопасности.

19. Какие статьи Уголовного кодекса РФ не посвящены вопросам безопасности информации?

1) статья 138;
2) статья 140;
3) статья 284;
4) статья 237;
5) статья 183;
6) статья 283;
7) Статья 290.

20. Содержанием административного уровня обеспечения информационной безопасности не являются следующие мероприятия?

1) проведение аудита информационной безопасности;
2) разработка политики информационной безопасности;
3) проведение анализа угроз и оценки рисков;
4) выбор механизмов и средств обеспечения информационной безопасности.

Ответы на тестовое задание к главе 2

Номер вопроса	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Правильный ответ	3	2	3, 5	1, 2	4	3	1	5	2	4

Номер вопроса	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
Правильный ответ	1	2	4	1	1	3	1, 2, 4	1, 3	7	1

Глава 3. ВРЕДОНОСНЫЕ ПРОГРАММЫ И ЗАЩИТА ОТ НИХ

3.1. Классификация вредоносного программного обеспечения

Вредоносные программы — одна из главных угроз информационной безопасности. Это связано с масштабностью распространения данного явления и, как следствие, огромного ущерба, наносимого информационным системам.

Вредоносные программы создаются специально для несанкционированного уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К данной категории относятся вирусы и черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников.

Современное вредоносное ПО — это практически незаметный для обычного пользователя «враг», который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей. Необходимость борьбы с вредоносными программами обусловлена возможностью нарушения ими всех составляющих информационной безопасности. «Компьютерные вирусы, черви, троянские программы, спам, сетевые атаки и прочие нежелательные компьютерные явления давно перестали быть чем-то необычным, приводящим пользователя или системного администратора в шоковое состояние. Заражение вирусом или троянской программой — весьма частая ситуация как для тех, кто небрежно относится к элементарным правилам компьютерной гигиены, так и для профессиональных системных администраторов, отвечающих за бесперебойную работу корпоративных сетей. Обыденным также стал электронный спам, давно количественно перекрывший поток «легальных» писем»[1].

Термин *«компьютерный вирус»* впервые был введен в середине 1980-х гг. на одной из конференций по безопасности информации, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла. Согласно современной классификации используется более широкое понятие — *«вредоносные программы»*, включающее компьютерные вирусы, сетевые черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников.

---

[1] *Касперский Е.* Компьютерное зловредство. СПб: Питер, 2009.

Вредоносная программа — программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы[1].

Трудность, возникающая при попытках сформулировать строгое определение вируса, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и др.) либо присущи другим программам, которые никакого отношения не имеют к вирусам, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения).

Компьютерный вирус — вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы[2].

Несмотря на все усилия разработчиков антивирусного программного обеспечения, до сих пор отсутствуют достаточно надежные антивирусные средства, и, скорее всего, противостояние «вирусописателей» и их оппонентов будет постоянным.

Исходя из этого, необходимо понимать, что нет достаточных программных и аппаратных средств защиты от вирусов, а надежная защита от вирусов может быть обеспечена комплексным применением этих средств и, что немаловажно, соблюдением элементарной «компьютерной гигиены».

К вредоносному программному обеспечению относятся *сетевые черви*, *классические файловые вирусы*, *троянские программы*, *хакерские утилиты* и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам сети[3].

Сетевые черви представляют собой программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

– проникновения на удаленные устройства (компьютеры, мобильные телефоны);
– запуска своей копии на удаленном устройстве;
– дальнейшего перехода на другие устройства в сети.

[1] ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

[2] Там же.

[3] *Касперский Е.* Компьютерное зловредство. СПб: Питер, 2009.

Путями распространения большинства известных червей являются:

– вложение в электронное письмо;
– ссылка в ICQ- и IRC-сообщениях на зараженный файл, расположенный на каком-либо веб- или FTP-ресурсе;
– файл в каталоге обмена P2P и пр.

Некоторые черви распространяются в виде сетевых пакетов и проникают непосредственно в память компьютера и там самостоятельно активизируют свой код. Это так называемые «бесфайловые» или «пакетные» черви.

Классические компьютерные вирусы — это программы, распространяющие свои копии по ресурсам локального компьютера с целью:

– последующего запуска своего кода при каких-либо действиях пользователя;
– дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевые сервисы для проникновения в другие компьютеры. Копия вируса попадает на удаленные компьютеры только в тех случаях, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

– при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
– вирус скопировал себя на съемный носитель и заразил файлы на нем;
– пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например шпионскую процедуру или троянский компонент уничтожения информации на диске.

Следует отметить, что в последнее время классические вирусы встречаются крайне редко. Однако заражение файлов вирусными методами периодически встречается в современных сетевых червях и троянских программах, написанных в криминальных целях. Такие черви и троянские программы при заражении компьютера внедряют свой код в файлы операционной системы и/или приложений для того, чтобы этот код было сложнее обнаружить и удалить из системы. В этих случаях используются технологии классических компьютерных вирусов.

Троянские программы — это вредоносные программы, созданные для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители данной категории не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения. Основным признаком, по которому различают типы троянских программ, является

их не санкционированные пользователем действия — те, которые они производят на зараженном компьютере. Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособности зараженного компьютера: например, троянские программы, разработанные для массированных распределенных атак на удаленные ресурсы сети или для рассылки спама.

Хакерские утилиты и прочие вредоносные программы включают:

- утилиты, автоматизирующие создание вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносных программ;
- хакерские утилиты, скрывающие код зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному компьютеру или удаленным компьютерам сети.

Компьютерные вирусы, черви, троянские программы существуют для десятков операционных систем и приложений. В то же время имеется огромное количество других операционных систем и приложений, для которых вредоносные программы пока не обнаружены. Что является причиной существования вредных программ в одних системах и отсутствия их в других?

Причиной появления подобных программ в конкретной операционной системе или приложении является одновременное выполнение следующих условий:

- *популярность*, широкое распространение данной системы;
- *документированность* — наличие разнообразной и достаточно полной документации по системе;
- *незащищенность* системы или существование известных уязвимостей в ее безопасности и приложениях.

Каждое перечисленное условие является необходимым, а выполнение всех условий одновременно является достаточным для появления разнообразных вредоносных программ.

Условие популярности системы необходимо для того, чтобы она попалась на глаза хотя бы одному компьютерному хулигану или хакеру. Если система существует в единичных экземплярах, то вероятность ее злонамеренного использования близка к нулю. Если же производитель системы добился ее массового распространения, то очевидно, что рано или поздно хакеры и вирусописатели попытаются воспользоваться ею в своих интересах.

Напрашивается естественный вывод: чем популярнее операционная система или приложение, тем чаще она будет являться жертвой вирусной атаки. Практика это подтверждает — распределение количества вредоносного программного обеспечения для Windows, Linux и MacOS практически совпадает с долями рынка, которые занимают эти операционные системы.

Наличие полной документации необходимо для существования вирусов по естественной причине: создание программ (включая вирусные) невозможно без технического описания использования сервисов операционной системы и правил написания приложений. Например, у обычных мобильных телефонов конца прошлого и начала нынешнего столетия подобная информация была закрыта — ни компании производители программных продуктов, ни хакеры не имели возможности разрабатывать программы для данных устройств. У телефонов с поддержкой Java и «умных» телефонов есть документация по разработке приложений — и, как следствие, появляются и вредоносные программы, разработанные специально для телефонов данных типов.

Уязвимостями называют «дыры» в программном обеспечении, как программистские (ошибки в коде программы, позволяющие вирусу «пролезть в дыру» и захватить контроль над системой), так и логические (возможность проникновения в систему легальными, иногда даже документированными методами). Если в операционной системе или в ее приложениях существуют известные уязвимости, то такая система открыта для вирусов, какой бы защищенной она ни была.

Под *защищенностью* системы понимаются архитектурные решения, которые не позволяют новому (неизвестному) приложению получить полный или достаточно широкий доступ к файлам на диске (включая другие приложения) и потенциально опасным сервисам системы. Подобное ограничение фактически блокирует любую вирусную активность, но при этом, естественно, накладывает существенные ограничения на возможности обычных программ.

3.2. Антивирусные программы

Особенности работы антивирусных программ

Наиболее эффективным способом борьбы с вредоносными программами является использование антивирусного программного обеспечения.

Антивирусная программа — программа, предназначенная для поиска, обнаружения, классификации и удаления вредоносных программ.

Вместе с тем необходимо признать, что не существует антивирусов, гарантирующих стопроцентную защиту, поскольку на любой алгоритм антивируса всегда можно предложить новый алгоритм вируса, невидимого для этого антивируса.

При работе с антивирусными программами необходимо знать некоторые понятия:

«Ложное срабатывание» — детектирование вируса в незараженном объекте (файле, секторе или системной памяти).

«Пропуск вируса» — недетектирование вируса в зараженном объекте.

«Сканирование по запросу» — поиск вирусов по запросу пользователя. В этом режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.

«Сканирование на лету» — постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т.п.). В этом режиме антивирус постоянно активен, он присутствует в памяти «резидентно» и проверяет объекты без запроса пользователя.

Методы защиты от вредоносных программ

Основной метод борьбы с вредоносными программами, как и в медицине, — своевременная профилактика. Компьютерная профилактика предполагает соблюдение правил «компьютерной гигиены», позволяющих значительно снизить вероятность заражения и потери каких-либо данных. Уяснение и строгое следование основным правилам поведения при использовании индивидуального компьютера и в сети является важным методом защиты от компьютерных злоумышленников. Всего есть три основных правила, которые верны как для индивидуальных, так и для корпоративных пользователей.

Обязательное использование антивирусной защиты. Если вы не являетесь экспертом в области компьютерной безопасности, то лучше всего вас защитит надежная антивирусная защита и защита от сетевых атак (сетевой экран) — доверьте свою безопасность профессионалам. Большинство современных антивирусных программ защищают от самых разнообразных компьютерных угроз — от вирусов, червей, троянских программ и рекламных систем. Интегрированные решения по безопасности также ставят фильтр против спама, сетевых атак, посещения нежелательных и опасных интернет-ресурсов и т.д.

Не следует доверять всей поступающей на компьютер информации — электронным письмам, ссылкам на веб-сайты, сообщениям на интернет-пейджеры. Категорически не следует открывать файлы и ссылки, приходящие из неизвестного источника. Риск заражения снижается

также при помощи организационных мер. К таким мерам относятся различные ограничения в работе пользователей, как индивидуальных, так и корпоративных, например:

- запрет на использование интернет-пейджеров;
- доступ только к ограниченному числу веб-страниц;
- физическое отключение внутренней сети предприятия от интернета и использование для выхода в интернет выделенных компьютеров и т.д.

К сожалению, жесткие ограничительные меры могут конфликтовать с пожеланиями каждого конкретного пользователя или с бизнес-процессами предприятия, в таких случаях необходимо искать баланс, причем в каждом отдельно взятом случае этот баланс может быть различным.

Следует обращать достаточно внимания на информацию от антивирусных компаний и от экспертов по компьютерной безопасности. Обычно они своевременно сообщают о новых видах интернет-мошенничества, новых вирусных угрозах, эпидемиях и т.п. — уделяйте больше внимания подобной информации.

Факторы, определяющие качество антивирусных программ

Качество антивирусной программы определяется несколькими факторами. Перечислим их по степени важности:

- надежность и удобство работы — отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки;
- качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц, упакованных и архивированных файлов, отсутствие «ложных срабатываний», возможность лечения зараженных объектов;
- существование версий антивируса под основные популярные платформы (Windows, Linux и т.д.);
- возможность сканирования «на лету»;
- существование серверных версий с возможностью администрирования сети;
- скорость работы.

В настоящее время, когда написание вирусов и охота за конфиденциальной информацией вышли на профессиональный уровень, вопрос качественной защиты данных чрезвычайно актуален. Как уже указывалось, легче предупредить опасность, чем бороться с негативными последствиями, поэтому использование антивирусного программного обеспечения — одна из составляющих информационной безопасности.

Контрольные задания к главе 3

1. К признакам вредоносных программ можно отнести следующее:
   1) скрытие своего присутствия в компьютерной системе;
   2) реализацию самодублирования, ассоциации своего кода с другими программами, перенос своего кода в не занимаемые ранее области памяти компьютера;
   3) искажение кода других программ в оперативной памяти компьютера;
   4) сохранение данных из оперативной памяти других процессов в других областях памяти компьютера;
   5) искажение, блокирование, подмену сохраняемых или передаваемых данных, полученных в результате работы других программ или уже находящихся во внешней памяти компьютера;
   6) неверное информирование пользователя о действиях, якобы выполняемых программой;
   7) приведенный выше список является исчерпывающим.
2. Компьютерный вирус — это
   1) вредоносная программа, созданная для похищении конфиденциальной информации;
   2) вредоносная программа, способная создавать свои копии;
   3) вредоносная программа для шифровании пользовательской информации с последующим шантажом и требованием выкупа;
   4) вредоносная программа для искажение кода других программ в оперативной памяти компьютера.
3. Примерами противодействия вредоносных программ установленному у пользователя антивирусному программному обеспечению являются:
   1) принудительная остановка работы антивирусного ПО;
   2) изменение настроек системы защиты для облегчения внедрения и функционирования вредоносной программы;
   3) предупреждения об обнаруженной вредоносной программе;
   4) скрытие своего присутствия в системе (так называемые «руткиты»);
   5) приведенный выше список является исчерпывающим.
4. Классификация компьютерных вирусов по способу распространения в системе:
   1) файловые вирусы, загрузочные вирусы, комбинированные вирусы;
   2) активные, пассивные;
   3) резидентные, нерезидентные;
   4) безвредные вирусы, неопасные вирусы, опасные и очень опасные вирусы;
   5) вирусы-спутники, паразитические вирусы, вирусы-невидимки (стелс-вирусы), вирусы-призраки (полиморфные вирусы).
5. Классификация компьютерных вирусов по способу заражения других объектов системы:
   1) файловые вирусы, загрузочные вирусы, комбинированные вирусы;
   2) активные, пассивные;
   3) резидентные, нерезидентные;
   4) безвредные вирусы, неопасные вирусы, опасные и очень опасные вирусы;
   5) вирусы-спутники, паразитические вирусы, вирусы-невидимки (стелс-вирусы), вирусы-призраки (полиморфные вирусы).
6. Классификация компьютерных вирусов по деструктивным возможностям:
   1) файловые вирусы, загрузочные вирусы, комбинированные вирусы;
   2) активные, пассивные;
   3) резидентные, нерезидентные;
   4) безвредные вирусы, неопасные вирусы, опасные и очень опасные вирусы;
   5) вирусы-спутники, паразитические вирусы, вирусы-невидимки (стелс-вирусы), вирусы-призраки (полиморфные вирусы).
7. Классификация компьютерных вирусов по особенностям реализуемого алгоритма:
   1) файловые вирусы, загрузочные вирусы, комбинированные вирусы;
   2) активные, пассивные;
   3) резидентные, нерезидентные;
   4) безвредные вирусы, неопасные вирусы, опасные и очень опасные вирусы;
   5) вирусы-спутники, паразитические вирусы, вирусы-невидимки (стелс-вирусы), вирусы-призраки (полиморфные вирусы).
8. Простейший макровирус в документе Microsoft Word заражает остальные файлы документов следующим образом:
   1) при открытии зараженного документа управление получает содержащийся в нем макрос с кодом вируса;
   2) вирус помещает в файл шаблонов другие макросы со своим кодом (например, FileOpen, FileSaveAs и FileSave);
   3) простейший макровирус не способен в документе Microsoft Word заражать остальные файлы документов.

9. Программная закладка — это

1) внешняя или внутренняя по отношению к атакуемой компьютерной системе программа, обладающая определенными разрушительными функциями;
2) программа перехвата паролей пользователей компьютерной системы;
3) условно опасные программы, которые разрабатываются легальными производителями, но содержат потенциально опасные функции, которые могут быть использованы нарушителем.

10. «Троянская» программа — это

1) вредоносная программа, созданная для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей;
2) программа перехвата паролей пользователей компьютерной системы;
3) вредоносная программа, способная создавать свои копии.

11. Причины появления вредоносных программ для конкретных операционных систем заключаются:

1) в слабостях архитектурного решения операционной системы;
2) в популярности, документированности, незащищенности и широком распространении операционной системы;
3) в отсутствии открытой документации по архитектуре операционной системы.

12. Подберите слово к данному определению:

_____ — это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

1) троянская программа;
2) стелс-вирус;
3) программный вирус;
4) логическая бомба.

13. Подберите слово к данному определению:

_____ — это достаточно трудно обнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода.

1) полиморфик-вирусы;

2) стелс-вирусы;
3) макровирусы;
4) конструкторы вирусов.

14. Что из перечисленного не относится к вредоносным программам?

1) логическая бомба;
2) «троянский конь»;
3) макровирус;
4) конструкторы вирусов;

15. Какой из вирусов при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них?

1) нерезидентный вирус;
2) файловый вирус;
3) резидентный вирус;
4) загрузочный вирус.

16. Полиморфные генераторы — это

1) исполняемые модули в составе компьютерных вирусов, главной функцией которых является шифрование тела вируса случайным ключом;
2) исполняемые модули в составе компьютерных вирусов, задача которых поиск новых вирусов;
3) исполняемые модули в составе компьютерных вирусов, задача которых размножение вируса.

17. Главной функцией полиморфных генераторов является:

1) поиск новых вирусов;
2) удаление антивирусной программы;
3) шифрование тела вируса;
4) размножение вируса.

18. Конструктор вирусов — это

1) утилита, предназначенная для изготовления новых компьютерных вирусов;
2) утилита, предназначенная для удаления антивирусной программы;
3) исполняемый модуль в составе компьютерных вирусов, задача которого поиск новых вирусов.

19. Сканирование «на лету» — это

1) детектирование вируса в незараженном объекте;
2) постоянная проверка на вирусы объектов, к которым происходит обращение;
3) поиск вирусов по запросу пользователя.

20. Самошифрование и полиморфичность используются для:
    1) саморазмножения вируса;
    2) максимального усложнения процедуры обнаружения вируса;
    3) расшифровки тел вируса;
    4) для скрытия действий антивирусной программы.

Ответы на тестовое задание к главе 3

Номер вопроса	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Правильный ответ	7	2	5	1	3	4	5	1, 2	1, 3	1

Номер вопроса	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
Правильный ответ	2	3	1	4	3	1	3	1	2	2

Глава 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ И ОБЛАЧНЫХ СЕРВИСОВ

4.1. Особенности обеспечения информационной безопасности в компьютерных сетях

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т.п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые или удаленные угрозы. Они характерны, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных сетей с точки зрения противостояния удаленным атакам приобретает первостепенное значение.

> **Удаленная угроза —** потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемое программно по каналам связи.

Это определение охватывает обе особенности сетевых систем — распределенность компьютеров и распределенность информации. Поэтому при рассмотрении вопросов информационной безопасности вычислительных сетей рассматриваются два подвида удаленных угроз — это удаленные угрозы на инфраструктуру и протоколы сети и удаленные угрозы на телекоммуникационные службы. Первые используют уязвимости в сетевых протоколах и инфраструктуре сети, а вторые — уязвимости в телекоммуникационных службах.

При рассмотрении вопросов, связанных с информационной безопасностью, в современных вычислительных сетях необходимо учитывать следующие факторы:

– глобальную связанность;
– разнородность корпоративных информационных систем;
– распространение технологии «клиент/сервер».

Применительно к системам связи глобальная связанность означает, что речь идет о защите сетей, пользующихся внешними сервисами, основанными, например, на протоколах TCP/IP, и предоставляющих аналогичные сервисы вовне. Весьма вероятно, что внешние сервисы находятся в других странах, поэтому от средств защиты в данном случае требуется следование стандартам, признанным на международном уровне.

Из факта глобальной связанности вытекает также меньшая эффективность мер физической защиты, общее усложнение проблем, связанных с защитой от несанкционированного доступа, необходимость привлечения для их решения новых программно-технических средств, например, межсетевых экранов.

Разнородность аппаратных и программных платформ требует от изготовителей средств защиты соблюдения определенной технологической дисциплины. Важны не только чисто защитные характеристики, но и возможность встраивания этих систем в современные корпоративные информационные структуры.

Корпоративные информационные системы оказываются разнородными еще в одном важном отношении — в разных частях этих систем хранятся и обрабатываются данные разной степени важности и конфиденциальности.

Использование технологии «клиент/сервер» с точки зрения информационной безопасности имеет следующие особенности:

– каждый сервис имеет свою трактовку главных аспектов информационной безопасности (доступности, целостности, конфиденциальности);
– каждый сервис имеет свою трактовку понятий субъекта и объекта;
– каждый сервис имеет специфические угрозы;
– каждый сервис нужно по-своему администрировать;
– средства безопасности в каждый сервис нужно встраивать по-особому.

Особенности вычислительных сетей, и в первую очередь глобальных, предопределяют необходимость использования специфических методов и средств защиты, например:

– защита подключений к внешним сетям;
– защита корпоративных потоков данных, передаваемых по открытым сетям;
– защита потоков данных между клиентами и серверами;
– обеспечение безопасности распределенной программной среды;
– защита важнейших сервисов (в первую очередь Web-сервиса);
– аутентификация в открытых сетях.

4.2. Сетевые модели передачи данных

Понятие протокола передачи данных

Обмен информацией между узлами сети на больших расстояниях всегда казался более важной задачей, чем локальный обмен. Поэтому ему уделялось больше внимания и, соответственно, велось большее финансирование во многих странах. Один из немногих открытых проектов по исследованию вычислительных сетей, финансировавшийся военным ведомством США, известен под названием сеть ARPA (Advanced Research Projects Agency). С самого начала в рамках этого проекта велись работы по объединению ресурсов вычислительных машин различного типа. В 1960–1970-е гг. многие результаты, полученные при эксплуатации сети ARPA, были опубликованы в открытой печати. Это обстоятельство, а также тот факт, что почти все страны занялись практически слепым копированием не только аппаратной архитектуры американских машин, но и базового программного обеспечения, обусловили сильное влияние сети ARPA на многие другие сети. Именно поэтому принято считать, что сеть ARPA является предшественницей знаменитой всемирной компьютерной сети «Интернет».

Основной задачей сетевой общественности явилась разработка протоколов обмена информацией. Эта задача совершенно справедливо представлялась важнейшей, поскольку настоятельно требовалось заставить «понимать» друг друга компьютеры, обладавшие различной архитектурой и программным обеспечением. Первоначально разработчики многочисленных корпоративных сетей договаривались о внутренних протоколах информационного обмена в своих сетях. Но уже в 70-е гг. специалистам стало ясно, что необходима и неизбежна стандартизация. В эти годы шел бурный процесс создания многочисленных национальных и международных комитетов и комиссий по стандартизации программных и аппаратных средств в области вычислительной техники и информационного обмена.

В общем случае протокол сетевого обмена информацией можно определить как перечень форматов передаваемых блоков данных, а также правил их обработки и соответствующих действий. Другими словами, протокол обмена данными — это подробная инструкция о том, какого типа информация передается по сети, в каком порядке обрабатываются данные, а также набор правил обработки этих данных.

Сообщения могут проходить довольно сложный путь по сетям, стоять в очередях на передачу или обработку, в том числе не доходить до адресата, о чем отправитель также должен быть уведомлен специальным сообщением.

Первоначально вычислительные сети были сетями коммутации сообщений. Это было оправдано, пока сообщения были сравнительно короткими. Но параллельно с этим всегда существовали задачи передачи

на расстояние больших массивов информации. Решение этой задачи в сетях с коммутацией сообщений является неэффективным, поскольку длины сообщений имеют большой разброс — от очень коротких до очень длинных. В связи с этим было предложено разбивать длинные сообщения на части — пакеты, и передавать сообщения не целиком, а пакетами, вставляя в промежутках пакеты других сообщений. На месте назначения сообщения собираются из пакетов. Короткие сообщения при этом были вырожденным случаем пакета, равного сообщению.

В настоящее время почти все сети в мире являются сетями коммутации пакетов.

Принципы организации обмена данными в вычислительных сетях

Существуют два принципа организации обмена данными в сетях:
- установление виртуального соединения с подтверждением приема каждого пакета;
- передача датаграмм (datagram).

Установление виртуального соединения или создание виртуального канала является более надежным способом обмена информацией. Поэтому он более предпочтителен при передаче данных на большие расстояния и/или по физическим каналам, в которых возможны помехи. При виртуальном соединении пункт приема информации уведомляет отправителя о правильном или неправильном приеме каждого пакета. Если какой-то пакет принят неправильно, отправитель повторяет его передачу. Так длится до тех пор, пока все сообщение не будет успешно передано. На время передачи информации между двумя пунктами коммутируется канал, подобный каналу при телефонном разговоре. Виртуальным его называют потому, что в отличие от телефонного коммутированного канала обмен информацией может идти по различным физическим путям даже в процессе передачи одного сообщения.

При передаче датаграмм, каждая содержит в своем заголовке полный адрес места назначения и поэтому является полностью независимой от других датаграмм. В общем случае датаграммы, даже являясь частями одного и того же сообщения, могут быть доставлены получателю по различным маршрутам. О получении всего сообщения целиком должна уведомить целевая программа.

Модель взаимодействия открытых систем OSI/ISO. Стек протоколов TCP/IP

В конце 1980-х гг. наблюдался подлинный бум, вызванный разработкой Международной организацией по стандартизации (ISO, International Standard Organization) модели взаимодействия открытых систем OSI (Open Systems Interconnection). OSI/ISO определяет различные уровни

взаимодействия систем в сетях с коммутацией пакетов, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.

Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена сообщениями участвуют две стороны, т.е. в данном случае необходимо организовать согласованную работу двух «иерархий», функционирующих на разных узлах. Оба участника сетевого обмена должны принять множество соглашений. Например, они должны согласовать уровни и форму электрических сигналов, способ определения длины сообщений, договориться о методах контроля достоверности и т.п. Другими словами, соглашения должны быть приняты для всех уровней, начиная от самого низкого — уровня передачи битов — до самого высокого, реализующего сервис для пользователей сети. Сравнительная схема уровневых моделей протоколов OSI/ISO и TCP/IP представлена на рис. 4.1.

7	Прикладной уровень	4	Прикладной уровень
6	Представительный уровень		
5	Сеансовый уровень		
4	Транспортный уровень	3	Транспортный уровень
3	Сетевой уровень	2	Межсетевой уровень
2	Канальный уровень	1	Доступа к среда передачи данных
1	Физический уровень		

Рис. 4.1. Сравнительная схема уровневых моделей протоколов OSI/ISO и TCP/IP

За время развития вычислительных сетей было предложено и реализовано множество протоколов обмена данными, самыми удачными из которых явились семейство протоколов TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/межсетевой протокол).

TCP/IP — это набор протоколов, состоящий из следующих основных компонентов:
- *межсетевой протокол* (Internet Protocol), обеспечивающий адресацию в сетях (IP-адресацию);
- *межсетевой протокол управления сообщениями* (Internet Control Message Protocol — ICMP), который обеспечивает низкоуровневую поддержку протокола IP, включая такие функции, как сообщения об ошибках, квитанции, содействие в маршрутизации и т.п.;
- *протокол разрешения адресов* (Address Resolution Protocol — ARP), выполняющий преобразование логических сетевых адресов в аппаратные, а также обратный ему RARP (Reverse ARP);
- *протокол пользовательских датаграмм* (User Datagramm Protocol — UDP);
- *протокол управления передачей* (Transmission Control Protocol — TCP).

Протокол UDP обеспечивает передачу пакетов без проверки доставки, в то время как протокол TCP требует установления виртуального канала и, соответственно, подтверждения доставки пакета с повтором в случае ошибки.

Этот набор протоколов образует самую распространенную модель сетевого обмена данными, получившую название — TCP/IP.

Прикладной уровень определяет способ общения пользовательских приложений. В системах «клиент–сервер» приложение-клиент должно знать, как посылать запрос, а приложение-сервер должно знать, как ответить на запрос. Этот уровень обеспечивает такие протоколы, как HTTP, FTP, Telnet.

Транспортный уровень позволяет сетевым приложениям получать сообщения по строго определенным каналам с конкретными параметрами.

На *межсетевом уровне* определяются адреса включенных в сеть компьютеров, выделяются логические сети и подсети, реализуется маршрутизация между ними.

На *уровне доступа к среде передачи данных* определяется адресация физических интерфейсов сетевых устройств. К этому уровню относятся программы управления физическими сетевыми устройствами, так называемые драйверы.

Как уже отмечалось ранее, в сетях с коммутацией пакетов, а модель TCP/IP относится к таким, для передачи по сети сообщение, сформированное на уровне приложений, разбивается на пакеты. Пакет — это часть сообщения с добавленным заголовком пакета. При продвижении пакета данных по уровням сверху вниз каждый новый уровень добавляет к пакету свою служебную информацию в виде заголовка и, возможно, трейлера (информации, помещаемой в конец сообщения). Эта операция называется *инкапсуляцией данных* верхнего уровня в пакете нижнего уровня, рис. 4.2. Служебная информация предназначается для объекта того же уровня на удаленном компьютере, ее формат и интерпретация определяются протоколом данного уровня.

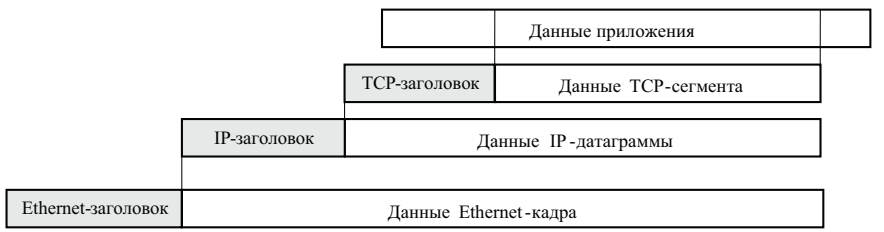


Рис. 4.2. Инкапсуляция данных в стеке TCP/IP

На транспортном уровне к полезной информации добавляется заголовок — служебная информация. Для сетевого уровня полезной информацией является уже пакет транспортного уровня. Далее добавляется заголовок сетевого уровня. Полученный блок данных называется IP-пакетом. Полезной нагрузкой для канального уровня является уже IP-пакет. Здесь перед передачей по каналу к нему добавляются собственный заголовок и еще трейлер. Получившийся блок называется кадром. Он и передается по сети. Переданный по сети кадр в пункте назначения преобразуется в обратном порядке, проходя по уровням модели снизу вверх.

Адресация в сетях TCP/IP

Одной из главных проблем построения глобальных сетей является проблема адресации. С одной стороны, постоянное расширение глобальной сети «Интернет» привело к нехватке уникальных адресов для вновь подключаемых узлов. С другой стороны, система адресации в таких сетях должна быть защищена от возможного вмешательства злоумышленников, связанного с подменой адресов и реализацией обходных маршрутов передачи сообщений.

Адресация современного интернета основана на протоколе IP (Internet Protocol), история которого неразрывно связана с транспортным протоколом TCP.

Концепция протокола IP представляет сеть как множество узлов (хостов), подключенных к некоторой интерсети. Интерсеть, в свою очередь, рассматривается как совокупность физических сетей, связанных маршрутизаторами. Физические объекты (хосты, маршрутизаторы, подсети) идентифицируются при помощи специальных IP-адресов. Каждый IP-адрес представляет собой 32-битовый идентификатор. Принято записывать IP-адреса в виде 4 десятичных чисел, разделенных точками.

Для этого 32-битовый IP-адрес разбивается на четыре группы по 8 бит (1 байт), после чего каждый байт двоичного слова преобразовывается в десятичное число по известным правилам. Например, IP-адрес:

10010011 10000111 00001110 11100101

преобразовывается указанным способом к следующему виду:

147.135.14.229

Каждый адрес является совокупностью двух идентификаторов: сети — NetID, и хоста — HostID. Все возможные адреса разделены на 5 классов, схема которых приведена на рис. 4.3.

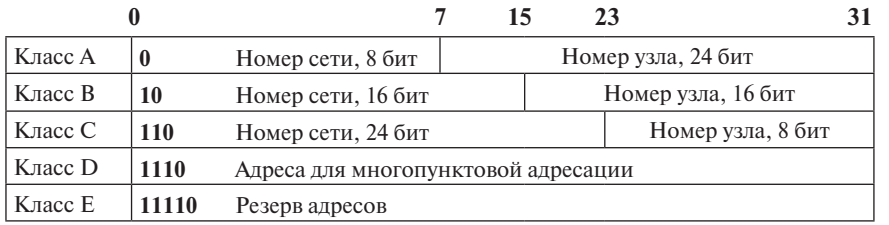


Рис. 4.3. Классы адресов вычислительных сетей

Из рис. 4.3 видно, что классы сетей определяют как возможное количество этих сетей, так и число хостов в них.

– *Класс A*: 0. Если первый бит в адресе — 0, значит, адрес относится к диапазону A (это адреса от 0.0.0.0 до 127.255.255.255).
– *Класс B*: 10. К этому классу относятся все адреса от 128.0.0.0 до 191.255.255.255. Это адреса, первый бит которых представлен единицей, а второй — нулем.
– *Класс C*: 110. Это адреса от 192.0.0.0 до 223.255.255.255. Их первые два бита представлены единицей, а третий — нулем.
– *Класс D*: 1110. Первые три бита этого класса представлены единицей. Это адреса в диапазоне от 224.0.0.0 до 239.255.255.255.
– *Класс E*: 1111. Это адреса в диапазоне от 224.0.0.0 до 239.255.255.255. Этот класс включает в себя все адреса, которые начинаются с 1111.

Очевидно, что количество доступных адресов сетей и хостов в классовой модели ограничено, поэтому кроме рассмотренной системы адресации со временем стала использоваться бесклассовая адресация CIDR (Classless Inter-Domain Routing), которая была разработана в качестве альтернативы традиционной классовой модели. С помощью CIDR существует возможность добавить спецификацию самого IP-адреса в число значимых битов, составляющих часть маршрутизации или сети. Например, выразить связь IP-адреса 192.168.0.15 с сетевой маской 255.255.255.0 можно с помощью CIDR-нотации 192.168.0.15/24. Это означает, что первые 24 бита указанного IP-адреса считаются значимыми для сетевой маршрутизации. CIDR можно использовать для обозначения «суперсетей» с более широким диапазоном адресов.

4.3. Классификация удаленных угроз в вычислительных сетях

Удаленные угрозы, или в данном случае будем говорить об атаках, классифицируют по следующим признакам (см. табл. 4.1).

По характеру воздействия:

– пассивные (класс 1.1);
– активные (класс 1.2).

Пассивным воздействием на распределенную вычислительную систему называется воздействие, которое не оказывает непосредственного влияния на работу системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на работу сети приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия в вычислительных сетях является прослушивание канала связи в сети.

Под активным воздействием на вычислительную сеть понимается воздействие, оказывающее непосредственное влияние на работу сети (изменение конфигурации, нарушение работоспособности и т.д.) и нарушающее принятую в ней политику безопасности. Практически все типы удаленных угроз являются активными воздействиями. Это связано с тем, что в самой природе разрушающего воздействия содержится активное начало. Очевидной особенностью активного воздействия по сравнению с пассивным является принципиальная возможность его обнаружения, так как в результате его осуществления в системе происходят определенные изменения. В отличие от активного, при пассивном воздействии не остается никаких следов (просмотр чужого сообщения ничего не меняет).

Таблица 4.1

Классификация удаленных атак

Типовая удаленная атака	Характер воздействия		Цель воздействия			Условие начала			Наличие обратной связи		Расположение субъекта атаки		Уровень модели OSI						
Класс воздействия	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	5.1	5.2	6.1	6.2	6.3	6.4	6.5	6.6	6.7
Анализ сетевого трафика	+	–	+	–	–	–	–	+	–	+	+	–	–	+	–	–	–	–	–
Подмена доверенного объекта сети	–	+	+	+	–	–	+	–	+	+	+	+	–	–	+	+	–	–	–
Ложный объект сети	–	+	+	+	+	–	–	+	+	+	+	+	–	–	+	–	–	–	–
Отказ в обслуживании	–	+	–	–	+	–	–	+	–	+	+	+	–	+	+	+	+	+	+

По цели воздействия:

– нарушение конфиденциальности информации (класс 2.1);
– нарушение целостности информации (класс 2.2);
– нарушение доступности информации (работоспособности системы) (класс 2.3).

Одна из основных целей злоумышленников — получение несанкционированного доступа к информации. Существуют две принципиальные возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности.

Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, очевидно, что искажение информации ведет к нарушению ее целостности. Данное информационное разрушающее воздействие представляет собой яркий пример активного воздействия. Примером удаленной угрозы, цель которой — нарушение целостности информации, может служить типовая удаленная атака «ложный объект распределенной вычислительной сети».

Принципиально другая цель преследуется злоумышленником при реализации угрозы для нарушения работоспособности сети. В этом случае не предполагается получение несанкционированного доступа к информации. Его основная цель — добиться, чтобы узел сети или какой-то из сервисов, поддерживаемый им, вышел из строя и для всех остальных объектов сети доступ к ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить типовая удаленная атака «отказ в обслуживании».

По условию начала осуществления воздействия. В вычислительных сетях можно выделить три вида условий начала осуществления удаленной атаки:

– атака по запросу от атакуемого объекта (класс 3.1);
– атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2);
– безусловная атака (класс 3.3).

В первом случае злоумышленик ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в сети «Интернет» служат DNS-запросы. Отметим, что данный тип удаленных атак наиболее характерен для распределенных вычислительных сетей.

Во втором случае злоумышленник осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сам атакуемый объект.

Реализация третьего вида атаки не связана ни с какими событиями и реализуется безусловно по отношению к цели атаки, т.е. атака осуществляется немедленно.

По наличию обратной связи с атакуемым объектом:

– с обратной связью (класс 4.1);
– без обратной связи (однонаправленная атака) (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 адекватно реагировать на все изменения, происходящие на атакуемом объекте.

В отличие от атак с обратной связью удаленным 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. Подобную удаленную атаку можно называть однонаправленной удаленной атакой. Примером однонаправленных атак является типовая удаленная атака «отказ в обслуживании».

По расположению субъекта атаки относительно атакуемого объекта:

– внутрисегментные (класс 5.1);
– межсегментные (класс 5.2).

Рассмотрим ряд определений, связанных с данным типом атак:

Субъект атаки (или источник атаки) — это атакующая программа или злоумышленник, непосредственно осуществляющие воздействие.

Маршрутизатор (router) — устройство, обеспечивающее маршрутизацию пакетов обмена в глобальной сети.

Подсеть (subnetwork) — совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, минуя маршрутизатор.

Сегмент сети — физическое объединение хостов. Например, сегмент сети образуют совокупность хостов, подключенных к серверу по схеме «общая шина». При такой схеме подключения каждый хост имеет возможность подвергать анализу любой пакет в своем сегменте.

С точки зрения удаленной атаки чрезвычайно важно, как по отношению друг к другу располагаются субъект и объект атаки, т.е. в одном или в разных сегментах они находятся. В случае внутрисегментной атаки, как следует из названия, субъект и объект атаки находятся в одном сегменте. При межсегментной атаке субъект и объект атаки находятся в разных сегментах.

Данный классификационный признак позволяет судить о так называемой «степени удаленности» атаки.

Важно отметить, что межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект ее и непосредственно атакующий

могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по локализации субъекта атаки.

По уровню модели ISO/OSI, на котором осуществляется воздействие:
– 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).

4.4. Угрозы информационной безопасности в облачных сервисах

Основные характеристики и модели облачных сервисов

Облачный сервис — это интернет-сервис, предполагающий передачу части объектов ИТ-инфраструктуры на обслуживание сторонней организации (так называемый аутсорсинг). Наиболее корректное определение понятию «облачные вычисления» дали американские специалисты Питер Мелл и Тим Гранс: облачные вычисления, по их версии, — это «модель предоставления удобного сетевого доступа в режиме “по требованию” к коллективно используемому набору настраиваемых ресурсов (например, сетей, серверов, хранилищ данных, приложений и/или сервисов), которые пользователь может оперативно задействовать под свои задачи и высвобождать при сведении к минимуму числа взаимодействий с поставщиком услуги или собственных управленческих усилий»[1].

Облачное хранилище данных (cloud storage) — модель онлайн-хранилища, в котором данные хранятся на многочисленных распределенных в сети серверах, предоставляемых в пользование клиенам, как правило, третьей стороной.

С точки зрения принадлежности облачной инфраструктуры различают четыре разновидности.

1. *Частное облако* — облачная инфраструктура, которая принадлежит непосредственно одной организации. Это не просто набор виртуальных машин, но и система мониторинга и управления. Она служит для анализа эффективности, корректности и оптимальности процессов, протекающих в частном облаке.

[1] Ссылка на оригинальный текст: https://csrc.nist.gov/publications/detail/sp/800-145/final.

2. *Публичное облако* — облачная инфраструктура, которая принадлежит множеству компаний. Наибольшее количество вопросов по информационной безопасности возникает именно в нем. Проверка безопасности устройств конечных пользователей становится одной из приоритетных задач в обеспечении ИБ публичного облака.

3. *Общественное облако* — облачная инфраструктура с общими серверами, которые открыты доступу по общедоступной сети. К примеру, общественным облаком является iCloud Apple или Google Drive.

4. *Гибридное облако* — это сочетание двух и более видов облаков (частного, публичного, общественного).

В настоящее время выделяют следующие модели облачных сервисов.

SaaS (*Software-as-a-Service*) — модель продажи программного обеспечения, при которой поставщик разрабатывает веб-приложение и самостоятельно управляет им, предоставляя заказчикам доступ к программному обеспечению через интернет.

Database-as-a-service (*DBaaS, «база данных как сервис»*) — облачный подход к хранению и управлению структурированными данными. Суть концепции *DBaaS* в том, что пользователю не нужно устанавливать и поддерживать базу данных, ему достаточно произвести запрос и получить по нему базу данных. Для ее создания используются ресурсы частного, публичного или гибридного облака.

Desktop-as-a-Service (DaaS) — модель распространения и эксплуатации программного обеспечения, получившая известность в начале 2000-х гг. и являющаяся логическим продолжением *SaaS*. При предоставлении услуги *DaaS* клиенты получают полностью готовое к работе («под ключ») стандартизированное виртуальное рабочее место, которое каждый пользователь имеет возможность дополнительно настраивать под свои задачи. Таким образом, пользователь получает доступ не к отдельной программе, а к необходимому для полноценной работы программному комплексу. Физически доступ к рабочему месту пользователь может получить через локальную сеть или интернет. В качестве терминала может использоваться персональный компьютер или ноутбук, нетбук и даже смартфон.

PaaS (Platform-as-a-Service, платформа как услуга) — это модель предоставления облачных вычислений, при которой потребитель получает доступ к использованию информационно-технологических платформ, таких как ОС, СУБД, связующему ПО, средствам тестирования и разработки, размещенным у облачного провайдера.

IaaS (*Infrastructure-as-a-Service*) — инфраструктура как услуга предоставляет возможность использования облачной инфраструктуры для самостоятельного управления ресурсами обработки, хранения, сетями и другими фундаментальными вычислительными ресурсами. Например, потребитель может устанавливать и запускать произвольное программное обеспечение, которое может включать в себя операционные системы, платформенное и прикладное программное обеспечение.

Угрозы безопасности различных моделей облачных сервисов

Наиболее уязвимыми с точки зрения информационной безопасности считаются модели PaaS и IaaS, где пользователям предоставляется больший контроль над инфраструктурой облака, а также больший набор предоставляемых услуг.

Группы угроз безопасности для модели PaaS.

Атаки на отказ в обслуживании. DDoS-атаки.

Для PaaS эти атаки нацелены не на банальное «затопление» сервера запросами, а на использовние конкретной бреши в платформе. В этом случае атака может содержать небольшой поток данных, но приводить к плачевным результатам: зацикливанию платформ, замедлению обработки обычных запросов или даже выводу из строя некоторых важных для системы элементов.

Атаки на API-платформы.

Пользователь часто не знает, на какой именно операционной системе и базе данных работает платформа, хакеры, могут атаковать не саму платформу, а через нее — базовые компоненты. Опасность таких атак зависит от набора интерфейсов, которые предоставляет платформа для приложений, поскольку именно через них хакеры, в конце концов, и нападут на операционную систему или базу данных.

Атаки на передаваемые данные.

Данного типа атаки подразумевают, что злоумышленник будет совершать нападение на сети между клиентом и провайдером. Атаки являются потенциально опасными, так как клиент при работе с облаком зачастую передает конфиденциальную информацию.

SQL-инъекции и XSS-нападения.

SQL-инъекции — это методика, при которой взломщик создает или изменяет текущие SQL-запросы для отображения скрытых данных, их изменения или даже выполнения опасных команд операционной системы на сервере баз данных. Атака выполняется на базе приложения, строящего SQL-запросы из пользовательского ввода и статических параметров.

XSS — это уязвимость на сервере, позволяющая внедрить в генерируемую скриптами на сервере HTML-страницу произвольный код путем передачи его в качестве значения нефильтруемой переменной. Любой метод атак для определенной XSS-уязвимости представляет собой некий контейнер, в котором код будет подан жертве.

Распространение вредоносных программ.

Для этого типа атак используют популярные платформы CMS (Content Management System). Делается это так: взламывается сервер со свободно распространяемой CMS и в нее инсталлируется модуль, который вставляет в коды страниц ссылки на вредоносные ресурсы. Есть также модули для удаленного исполнения любых команд на сервере, которые могут быть встроены, например, в тему сайта.

Атаки на клиента.

Здесь рассматриваются такие атаки, как Cross Sit Scripting, «угон» паролей, перехваты веб-сессий, «человек посредине» и др. Провайдерам облачных технологий требуется организовать доверительные отношения пользователь — облачный провайдер. Для этого необходимо прибегнуть к более надежной аутентификации пользователя на сервере предоставления услуг.

Группы угроз безопасности для модели IaaS.

Атаки на клиента.

Так как уязвимости модели PaaS, через которые совершаются атаки этого типа, присутствуют и в модели IaaS, то важность защиты от них не стоит упускать.

Функциональные атаки на элементы облака.

Облако представляет собой многослойную структуру, где прочность общей защиты системы равна прочности защиты самого слабого элемента. Другими словами, к примеру, успешная атака на межсетевой экран или proxy-сервер, стоящий на границе облака и выходом в интернет, заблокирует доступ ко всем ресурсам, тем не менее, связи внутри него будут сохраняться.

Атаки с использованием смежной уязвимости.

В любой модели облачного сервиса существует угроза уязвимости через общие ресурсы. Если ключевой компонент совместно используемой технологии будет взломан, то это подвергнет риску не только пострадавшего заказчика.

Традиционные атаки на ПО.

К таким атакам можно отнести атаки на уязвимости операционной системы, модульные компоненты, сетевые протоколы и др.

Атаки на виртуальную инфраструктуру.

К этому типу относятся атаки на виртуальную машину; на хост виртуализации; на сервер управления виртуальными машинами; на ресурсы хоста виртуализации.

Атаки на системы управления.

Большое количество виртуальных машин, используемых в облаках, требует наличия систем управления, способных надежно контролировать создание, перенос и утилизацию виртуальных машин. Вмешательство в системы управления может привести к появлению виртуальных машин-«невидимок», способных блокировать одни виртуальные машины и поставлять другие. Все это позволяет злоумышленникам получать информацию из облака или захватывать его части или все облако целиком.

Заметим, для того чтобы обеспечить полную и грамотную защиту от угроз информационной безопасности в облачных сервисах, следует применять комплексный подход к построению системы обеспечения

информационной безопасности (СОИБ). В этом случае необходимо последовательно решить следующие задачи:

– оценка текущего состояния информационной безопасности;
– определение желаемого (целевого) состояния информационной безопасности;
– формирование дорожной карты мероприятий, направленных на преодоление существующего разрыва и достижение желаемого (целевого) состояния информационной безопасности.

Работа в облаках обладает огромным потенциалом для компаний. Зачастую применение облачных вычислений — наилучший способ решения корпоративных задач, на которые не хватает мощности собственной ИТ-инфраструктуры. Помимо существенной экономической выгоды, важным аргументом использования этой технологии для многих компаний может стать возможность доступа к данным из любой точки планеты. Несмотря на все плюсы облачных сервисов, большинство компаний боятся их использовать по причине недоработки в области информационной безопасности. Как видим, информация, находящаяся в облачных сервисах, может подвергнуться атаке посредством уязвимостей как непосредственно облачной системы, так и решений, нацеленных на управление сервисами.

Контрольные задания к главе 4

1. Компьютерная сеть — это:
   1) группа установленных рядом вычислительных машин, объединенных с помощью средств сопряжения и выполняющих единый информационно-вычислительный процесс;
   2) система, обеспечивающая обмен данными между вычислительными устройствами (компьютеры, серверы, маршрутизаторы и другое оборудование);
   3) совокупность сервера и рабочих станций, соединенных с помощью коаксиального или оптоволоконного кабеля.
2. Абонент сети — это:
   1) аппаратура, выполняющая обработку данных на независимых компьютерах;
   2) объекты, генерирующие или потребляющие информацию;
   3) аппаратура для получения информации от сервера.
3. Станция — это:
   1) средство сопряжения с компьютером;
   2) аппаратура для подключения к глобальной сети;
   3) аппаратура, передающая и принимающая информацию.

4. Физическая передающая среда — это:
   1) линии связи, пространство для распространения сигналов, аппаратура передачи данных;
   2) мультиплексор передачи данных;
   3) витая пара проводов, коаксиальный кабель, оптоволоконный кабель.
5. Существуют три режима передачи данных в сети:
   1) симплексный, прямой, обратный;
   2) симплексный, полудуплексный, дуплексный;
   3) последовательный, параллельный, многопроцессорный.
6. Наиболее распространенным кодом передачи данных по каналам связи является:
   1) код КОИ-7;
   2) код ASCII;
   3) код ПД-6.
7. Для сопряжения компьютера с одним каналом связи используется:
   1) адаптер;
   2) концентратор;
   3) повторитель.
8. Для сопряжения компьютера с несколькими каналами связи используется:
   1) сетевой адаптер;
   2) мультиплексор передачи данных;
   3) модем.
9. Количество уровней модели взаимодействия открытых систем OSI/ISO:
   1) семь;
   2) четыре;
   3) шесть.
10. Протокол компьютерной сети — это:
    1) программа для связи абонентов;
    2) набор правил, обусловливающий порядок обмена информацией в сети;
    3) программа, позволяющая преобразовывать информацию в коды ASCII.
11. Телекоммуникационные сети по их размерам подразделяются на:
    1) локальные, региональные, глобальные;
    2) терминальные, административные, смешанные;
    3) цифровые, коммерческие, корпоративные.

12. Альтернативой классовой адресации в телекоммуникационных сетях является:

1) бесклассовая адресация CIDR;
2) уникальная адресация отдельных узлов;
3) многопунктовая адресация.

13. IP — это:

1) уникальный сетевой адрес узла в компьютерной сети, построенной на основе стека протоколов TCP/IP;
2) сетевой адрес в модели OSI/ISO;
3) стек протоколов.

14. Телекоммуникационные сети по признаку «топология» подразделяются на:

1) реальные, виртуальные;
2) типа «звезда», «шина», «кольцо»;
3) проводные, беспроводные.

15. Инкапсуляция данных — это:

1) добавление к пакету дополнительных пользовательских данных;
2) добавление к пакету служебной информации в виде заголовка и трейлера;
3) подсчет контрольной суммы в пакете данных.

16. Протокол UDP:

1) обеспечивает передачу пакетов без проверки доставки;
2) обеспечивает передачу пакетов с квинтированием;
3) является протоколом межсетевого уровня.

17. Наиболее распространенной операционной системой для локальных вычислительных сетей является:

1) NetWare;
2) Linux;
3) Windows.

18. Межсетевой протокол управления сообщениями в стеке TCP/IP —

1) TCP;
2) IP;
3) ICMP.

19. По характеру воздействия угрозы в телекоммуникационных сетях делятся на:

1) преднамеренные и случайные;
2) пассивные и активные;
3) программные и аппаратные.

20. Аппаратное обеспечение локальных вычислительных сетей включает:

1) рабочие станции, коммуникационное оборудование;
2) рабочие станции, сервер, коммуникационное оборудование;
3) коммуникационное оборудование, сервер.

21. Удаленная угроза — это:

1) активное воздействие на вычислительную сеть;
2) пассивное воздействие на вычислительную сеть;
3) потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемое программно по каналам связи.

22. Архитектура «клиент-сервер» — это:

1) сетевая архитектура, в которой задания или сетевая нагрузка распределены между поставщиками и заказчиками услуг;
2) сетевая архитектура, использующая протоколы стека TCP/IP;
3) архитектура программ, позволяющих просматривать информацию, содержащуюся на конкретном сервере в сети «Интернет».

23. Наиболее эффективными средствами контроля данных в сети являются:

1) организация надежной и эффективной системы архивации;
2) использование зеркальных дисков;
3) организация надежной системы идентификации и аутентификации пользователей.

24. Наиболее эффективными средствами защиты от вредоносного программного обеспечения являются:

1) антивирусные программы;
2) аппаратные средства;
3) организационные мероприятия.

25. Облачный сервис — это:

1) интернет-сервис, предполагающий передачу части объектов ИТ-инфраструктуры на обслуживание сторонней организации;
2) сервис для подключения к сети «Интернет»;
3) поставщик услуг сети «Интернет».

Ответы на тестовое задание к главе 4

Номер вопроса	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Правильный ответ	2	2	3	1	2	1, 2	1	2	1	2	1	1	1

Номер вопроса	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
Правильный ответ	2	2	1	1	3	2	2	3	1	3	1	1

Глава 5. МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Идентификация и аутентификация

Идентификация и аутентификации применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы). Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой. Наличие процедур аутентификации и/или идентификации пользователей является обязательным условием любой защищенной системы, поскольку все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами информационных систем.

Дадим определения этих понятий.

Идентификация — присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) — проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

При построении систем идентификации и аутентификации возникает проблема выбора идентификатора, на основе которого осуществляются процедуры идентификации и аутентификации пользователя. В качестве идентификаторов обычно используют:

– набор символов (пароль, секретный ключ, персональный идентификатор и т.п.), который пользователь запоминает (для их запоминания могут использоваться специальные средства хранения — электронные ключи);
– физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т.п.) или особенности поведения (особенности работы на клавиатуре и т.п.).

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

5.2. Разграничение доступа

Методы разграничения доступа

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов информационной системы.

Обычно полномочия субъекта представляются *списком ресурсов*, доступным пользователю и *правами по доступу* к каждому ресурсу из списка.

Существуют следующие методы разграничения доступа:

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

Суть метода разграничения доступа по спискам состоит в задании соответствий: для каждого пользователя задается список ресурсов и права доступа к ним или для каждого ресурса определяется список пользователей и права доступа к этим ресурсам. С помощью списков возможно установление прав с точностью до каждого пользователя. Возможен вариант добавления прав или явного запрета доступа. Метод доступа по спискам используется в подсистемах безопасности операционных систем и систем управления базами данных.

При использовании матрицы установления полномочий применяется матрица доступа (таблица полномочий). В матрице доступа в строках записываются идентификаторы субъектов, которые имеют доступ в компьютерную систему, а в столбцах — объекты (ресурсы) компьютерной системы. В каждой ячейке матрицы может содержаться имя и размер ресурса, право доступа (чтение, запись и др.), ссылка на другую информационную структуру, которая уточняет права доступа, ссылка на программу, которая управляет правами доступа и др. Данный метод является достаточно удобным, так как вся информация о полномочиях сохраняется в единой таблице. Недостаток матрицы — ее возможная громоздкость.

Разграничение по степени секретности разделяется на несколько уровней. Полномочия каждого пользователя могут быть заданы

в соответствии с максимальным уровнем секретности, к которому он допущен. При разграничении по категориям задается и контролируется ранг категории пользователей. Таким образом, все ресурсы компьютерной системы разделены по уровням важности, причем каждому уровню соответствует категория пользователей.

Парольное разграничение использует методы доступа субъектов к объектам с помощью пароля. Постоянное использование паролей приводит к неудобствам для пользователей и временным задержкам. По этой причине методы парольного разграничения используются в исключительных ситуациях.

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

Требования к разграничению доступа

Согласно ГОСТ Р 50739-95[1] «Средства вычислительной техники. Защита от несанкционированного доступа к информации» требования к разграничению доступа включают, в том числе:

– дискретизационный принцип контроля доступа;
– мандатный принцип контроля доступа.

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

Мандатный принцип контроля доступа основан на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

5.3. Регистрация и аудит

Регистрация является еще одним механизмом обеспечения защищенности информационной системы.

Регистрация основана на подотчетности системы обеспечения безопасности, фиксирующий все события, касающиеся безопасности.

[1] Настоящий стандарт устанавливает единые функциональные требования к защите средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к информации, к составу документации на эти средства, а также номенклатуру показателей защищенности СВТ, описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации.

Механизм регистрации фиксирует все события, касающиеся безопасности, такие как:

– вход и выход субъектов доступа;
– запуск и завершение программ;
– выдача печатных документов;
– попытки доступа к защищаемым ресурсам;
– изменение полномочий субъектов доступа;
– изменение статуса объектов доступа и т.д.

Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей и т.д.

Аудит — это анализ накопленной информации, проводимый оперативно в реальном времени или периодически.

Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация механизмов регистрации и аудита позволяет решать следующие задачи обеспечения информационной безопасности:

– обеспечение подотчетности пользователей и администраторов;
– обеспечение возможности реконструкции последовательности событий;
– обнаружение попыток нарушений информационной безопасности;
– предоставление информации для выявления и анализа проблем.

Механизмы регистрации и аудита являются сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям — за возможные критические ошибки.

5.4. Межсетевое экранирование

Одним из эффективных механизмом обеспечения информационной безопасности в распределенных вычислительных сетях является экранирование, выполняющее функции разграничения информационных потоков на границе защищаемой сети.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет *межсетевой экран* или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих

из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны классифицируются по следующим признакам:

– по месту расположения в сети — на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;
– по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI (табл. 5.1). Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Межсетевые экраны разделяют на четыре типа:

– межсетевые экраны с фильтрацией пакетов;
– шлюзы сеансового уровня;
– шлюзы прикладного уровня;
– межсетевые экраны экспертного уровня.

Таблица 5.1

Типы межсетевых экранов и уровни модели OSI/ISO

№ п/п	Уровень модели OSI/ISO	Протокол	Тип межсетевого экрана
1	Прикладной	Telnet, FTP, DNS, NFS, SMTP, HTTP	Шлюз прикладного уровня. Межсетевой экран экспертного уровня
2	Представления данных		
3	Сеансовый	TCP, UDP	Шлюз сеансового уровня
4	Транспортный	TCP, UDP	
5	Сетевой	IP, ICMP	Межсетевой экран с фильтрацией пакетов
6	Канальный	ARP, RAP	
7	Физический	Ethernet	

Межсетевые экраны с фильтрацией пакетов представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их со сконфигурированной таблицей правил. Эти межсетевые экраны просты в использовании, дешевы, оказывают минимальное влияние на производительность вычислительной системы. Основным недостатком является их уязвимость при подмене адресов IP. Кроме

того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

Шлюзы сеансового уровня контролируют допустимость сеанса связи. Они следят за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т.е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функцию трансляции сетевых адресов, которая скрывает внутренние IP-адреса, тем самым исключая подмену IP-адреса. Однако в таких межсетевых экранах отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

Шлюзы прикладного уровня проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип межсетевого экрана, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб сети «Интернет» (HTTP, FTP, Telnet и т.д.) и служат для проверки сетевых пакетов на наличие достоверных данных.

Шлюзы прикладного уровня снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в интернете при работе по низкоскоростным каналам, но существенно при работе во внутренней сети.

Межсетевые экраны экспертного уровня сочетают в себе элементы всех трех описанных выше категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Межсетевые экраны экспертного уровня также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И, наконец, брандмауэры экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

Вместо применения связанных с приложениями программ-посредников брандмауэры экспертного уровня используют специальные алгоритмы распознавания и обработки данных на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что теоретически должно обеспечить более эффективную фильтрацию пакетов.

5.5. Технология виртуальных частных сетей (VPN)

Технология виртуальных частных сетей (VPN — Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

– шифрования на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);
– экранирования (с использованием межсетевых экранов);
– туннелирования.

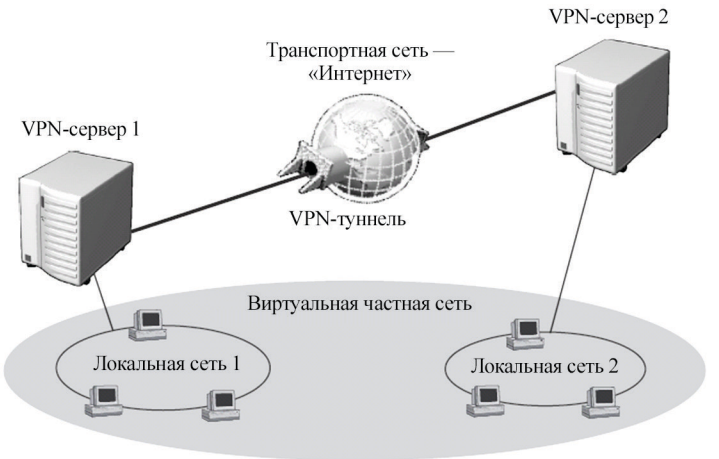


Рис. 5.1. Технология VPN

Сущность технологии VPN заключается в следующем (рис. 5.1).

На все компьютеры, имеющие выход в интернет (вместо интернета может быть и любая другая сеть общего пользования), устанавливается VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям.

Перед отправкой IP-пакета VPN-агент выполняет следующие операции:

– анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут поддерживать одновременно несколько алгоритмов шифрования и контроля целостности). Пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;
– вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;
– пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);
– формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для внешней атаки информация, например внутренние IP-адреса сети, в этом случае недоступна.

При получении IP-пакета выполняются обратные действия:

– из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается (то же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком);
– согласно настройкам выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);
– после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является лишь настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется «туннелем», а технология его создания называется «туннелированием»). Вся информация передается по туннелю в зашифрованном виде.

Одной из обязательных функций VPN-агентов является фильтрация пакетов. Фильтрация пакетов реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать шлюзы безопасности (рис. 5.2).

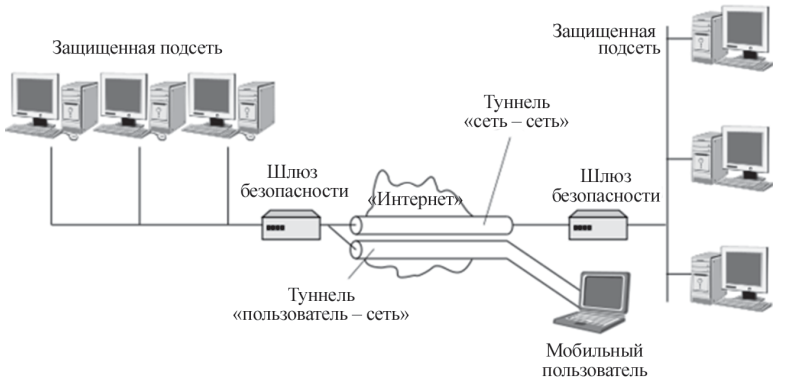


Рис. 5.2. Пример туннелирования в VPN

Контрольные задания к главе 5

1. К числу сервисов безопасности можно отнести:
   1) идентификацию и аутентификацию;
   2) шифрование и расшифровывание;
   3) отключение безопасного восстановления.

2. Система обеспечения безопасности информации (СОБИ) для каждой организации представляет собой различный набор решений, который...
   1) является стандартным и обязательным в каждой, независимо от статуса и сферы деятельности, организации;
   2) не является стандартным и различен в зависимости от бизнес-задач, решаемых информационной системой;
   3) в большинстве организаций является стандартным, однако более крупные предприятия имеют возможность незначительно уклоняться от стандартного шаблона;

3. Назовите действие, позволяющее субъекту указать свое имя в информационной системе:
   1) аутентификация;
   2) экранирование;
   3) идентификация.

4. Что из перечисленного нельзя отнести к мерам по обеспечению надежности парольной защиты?
   1) автоматическое сохранение пароля при вводе без дополнительного запроса;
   2) наложение технических ограничений (длина пароля, алфавит пароля);
   3) управление сроком действия пароля, его периодическая смена.

5. Для чего предназначена схема Kerberos?
   1) для решения задачи аутентификации в открытой сети с использованием третьей доверенной стороны;
   2) для использования программных средств генерации паролей;
   3) для передачи секретных ключей, используемых в процессе шифрования, через сеть.

6. Какие биометрические данные не могут использоваться при идентификации/аутентификации пользователей?
   1) отпечатки пальцев;
   2) походка;
   3) сетчатка и роговица глаза.

7. Для обеспечения большей надежности паролей можно применять:
   1) единый пароль для всех пользователей внутри сети;
   2) одноразовый пароль;
   3) пароль, содержащий стандартную информацию о пользователе.

8. Идентификация — это:
   1) проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности;
   2) присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным;
   3) гарантирование того, что информация остается неизменной, корректной и аутентичной;
   4) гарантирование того, что авторизованные пользователи могут иметь доступ и работать с информационными активами, ресурсами и системами, которые им необходимы, при этом обеспечивается требуемая производительность.

9. Аутентификация — это:
   1) проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности;
   2) присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным;
   3) гарантирование того, что информация остается неизменной, корректной и аутентичной;
   4) гарантирование того, что авторизованные пользователи могут иметь доступ и работать с информационными активами, ресурсами и системами, которые им необходимы, при этом обеспечивается требуемая производительность.

10. Авторизация — это:
   1) присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным;
   2) предоставление определенному лицу или группе лиц прав на выполнение определенных действий, а также процесс подтверждения данных прав при попытке выполнения этих действий;

3) гарантирование того, что авторизованные пользователи могут иметь доступ и работать с информационными активами, ресурсами и системами, которые им необходимы, при этом обеспечивается требуемая производительность.

11. Под сертификацией средств защиты информации по требованиям безопасности информации понимается:

1) деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации;
2) управление системой защиты информации информационной системы;
3) контроль (мониторинг) обеспечения уровня защищенности информации, содержащейся в информационной системе.

12. Уязвимость — это:

1) недостаток в системе, используя который, можно нарушить порядок ее функционирования и вызвать неправильную работу системы;
2) физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности защищаемой информации при ее обработке;
3) субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

13. Виртуальные частные сети (VPN) являются комбинацией нескольких самостоятельных механизмов безопасности:

1) шифрования на выделенных шлюзах, экранирования, туннелирования;
2) аутентификации, идентификации, регистрации и учета;
3) аутентификации и отключения опасного соединения.

14. В состав обязательных функций VPN-агентов входит:

1) контроль целостности передаваемых пакетов с помощью контрольных сумм;
2) фильтрация передаваемых пакетов;
3) создание виртуальных каналов (туннелей) между защищаемыми локальными сетями или компьютерами.

15. Подберите слово к данному определению:

_____ — программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее и обеспечивает защиту информационной системы посредством фильтрации информации.

1) межсетевой экран;
2) криптоалгоритм;
3) сервер удаленного доступа;
4) криптосистема.

16. Идентификация и аутентификации применяются:

1) для регистрации событий безопасности;
2) для выявления попыток несанкционированного доступа;
3) для обеспечения целостности данных;
4) для ограничения доступа случайных и незаконных субъектов информационной системы к ее объектам.

17. Постоянные пароли относятся к:

1) статической аутентификации;
2) временной аутентификации;
3) устойчивой аутентификации;
4) постоянной аутентификации.

18. Реализация механизмов регистрации и аудита не позволяет решать следующие задачи обеспечения информационной безопасности:

1) обеспечение подотчетности пользователей и администраторов;
2) обеспечение возможности реконструкции последовательности событий;
3) обеспечение аудита информационной системы;
4) обнаружение попыток нарушений информационной безопасности;
5) предоставление информации для выявления и анализа проблем.

19. К методам разграничения доступа не относятся:

1) разграничение доступа по степени осведомленности пользователей;
2) разграничение доступа по спискам;
3) использование матрицы установления полномочий;
4) разграничение доступа по уровням секретности и категориям;
5) парольное разграничение доступа.

20. Полномочия субъекта информационной системы представляются:

1) списком ресурсов и правами по доступу к каждому ресурсу из списка;
2) матрицей прав доступа к ресурсам информационной системы;
3) категориями ресурсов информационной системы.

Ответы на тестовое задание к главе 5

Номер вопроса	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Правильный ответ	1	2	3	1	1	2	2	2	1	2

Номер вопроса	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
Правильный ответ	1	1	1	2, 3	1	4	1	3	1	1, 2

ГЛАВА 6. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. Классические шифры

Наука, занимающаяся вопросами безопасной связи, называется *криптологией* (*kryptos* — тайный, *logos* — наука). Она в свою очередь разделяется на два направления *криптографию* и *криптоанализ*.

Джон Валлис

Термин *криптография* (тайнопись) ввел Джон Валлис (1616–1703), английский математик, один из основателей и первых членов Лондонского королевского общества, профессор геометрии Оксфордского университета (1649 г.)

Криптография (др.-греч. κρυπτός — скрытый, γράφω — пишу) — наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров. Она занимается поиском математических методов преобразования информации.

Криптоанализ — раздел, посвященный исследованию возможности чтения сообщений без знания ключей. Он связан непосредственно со взломом шифров. Специалисты, занимающиеся криптоанализом и исследованием шифров, называются криптоаналитиками.

Шифр — совокупность обратимых преобразований множества открытых текстов (исходного сообщения) на множество зашифрованных текстов, проводимых с целью их защиты. Конкретный вид преобразования определяется с помощью ключа шифрования.

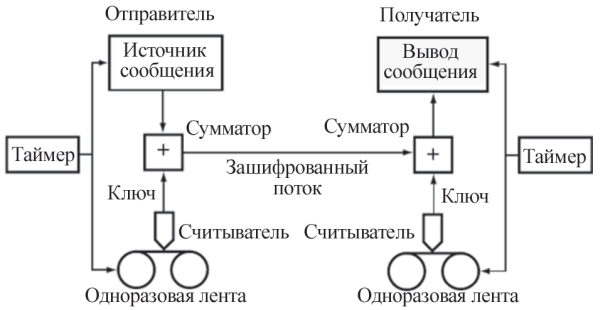


Рис. 6.1. Гилберт Вернам и его схема телеграфной шифровальной машины, использующей одноразовую гамму

В истории криптографии можно выделить три основных периода. Первый, наиболее продолжительный, — это эпоха «ручной криптографии». Ее начало теряется в глубокой древности, а окончание приходится на 30-е гг. XX в. Криптография прошла путь от магического искусства до вполне прозаической прикладной специальности чиновников дипломатических и военных ведомств.

Второй период — создание и широкое внедрение в практику сначала механических затем электромеханических и электронных устройств шифрования, организация целых сетей засекреченной связи. Его началом можно считать разработку Гилбертом Вернамом в 1917 г. схемы телеграфной шифровальной машин, использующей одноразовую гамму (рис. 6.1).

К середине 70-х гг. с развитием разветвленных коммерческих сетей связи, электронной почты и глобальных информационных систем на первый план вышли новые проблемы — проблемы снабжения ключами и проблемы подтверждения подлинности.

В 1976 г. американские ученые Уитфилд Диффи и Мартин Хеллман предложили два новых принципа организации засекреченной связи без предварительного снабжения абонентов секретными ключами шифрования — принцип так называемого открытого ключа шифрования и принцип открытого распределения ключей. Этот момент можно считать началом нового периода в развитии криптографии. В настоящее время данное направление современной криптографии очень интенсивно развивается.

Потребность шифровать и передавать шифрованные сообщения возникла очень давно. Так еще в V–VI вв. до н.э. греки применяли специальное шифрующее устройство. По описанию Плутарха оно состояло из двух цилиндрических стержней одинаковой длины и толщины. Один оставляли себе, а другой отдавали отъезжающему. Эти стержни называли сциталами (рис. 6.2). При необходимости передачи сообщения длинную ленту папируса наматывали на сциталу, не оставляя на ней никакого промежутка.

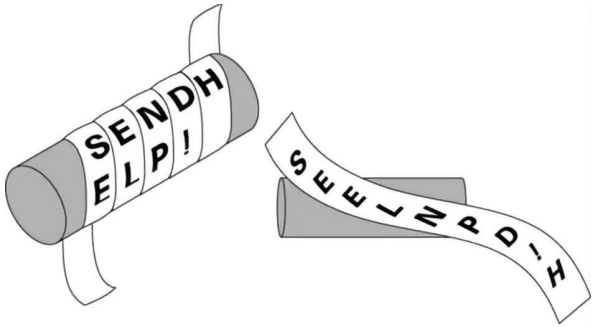


Рис. 6.2. Сцитала (от греч., σκυτάλη — жезл)

Затем, оставляя папирус на сцитале, записывали на нем все, что необходимо, а написав, снимали папирус и без стержня отправляли адресату. Так как буквы оказывались разбросанными в беспорядке, то прочитать сообщение мог только тот, кто имел свою сциталу такой же длины и толщины, намотав на нее папирус.

Квадрат Полибия[1]. В Древней Греции (II в. до н.э.) был известен шифр, называемый «квадрат Полибия». Это устройство представляло собой квадрат 5×5, столбцы и строки которого нумеровали цифрами от 1 до 5. В каждую клетку записывалась одна буква (в греческом варианте одна клетка оказывалась пустой, а в латинском — в одну клетку помещали две буквы I, J). В результате каждой букве отвечала пара чисел по номеру строки и столбца.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

13 34 22 24 44 34 15 42 22 34 43 45 32

Cogito ergo sum — лат. «Я мыслю, следовательно, существую».
Р. Декарт

Шифр Цезаря. В I в. Гай Юлий Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) — на пятую (E), наконец последнюю — на третью.

Шифр Цезаря относится к так называемому классу *моноалфавитных подстановок* и имеет множество модификаций.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC

YHQL YLGL YLFL
Veni vidi vici – «Пришел, увидел, победил»
Ю. Цезарь.
Донесение Сенату о победе над понтийским царем.

[1] Полибий (200–120 гг. до н.э.) — древнегреческий историк.

Джероламо Кардано

Решетка Кардано[1]**.** Широко известны шифры, принадлежащие к классу «*перестановка*», в частности решетка Кардано. Это прямоугольная карточка с отверстиями, чаще всего квадратная, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. Число строк и столбцов на карточке четно. Карточка сделана так, что при последовательном ее поворачивании каждая клетка лежащего под ней листа окажется занятой. Карточку поворачивают сначала вдоль вертикальной оси симметрии на 180°, а затем вдоль горизонтальной оси также на 180°. И вновь повторяют ту же процедуру (рис. 6.3).

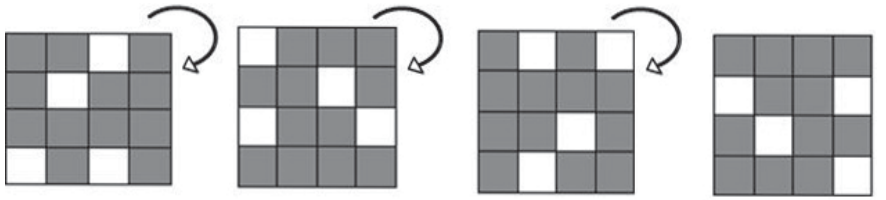


Рис. 6.3. Решетка Кардано

Диск Альберти. Итальянец Леон Баттист Альберти (XVI в.) впервые выдвинул идею «двойного шифрования» — текст, полученный в результате первого шифрования, подвергался повторному зашифрованию. В трактате Альберти был приведен его собственный шифр, который он назвал «шифром, достойным королей». Он утверждал, что этот шифр недешифруем. Реализация шифра осуществлялась с помощью шифровального диска, положившего начало целой серии *многоалфавитных подстановок*. Устройство представляло собой пару дисков — внешний, неподвижный (на нем были нанесены буквы в естественном порядке и цифры от 1 до 4) и внутренний — подвижный — на нем буквы были переставлены. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замену ее на соответствующую (стоящую под ней) букву шифрованного текста. После шифрования нескольких слов внутренний диск сдвигался на один шаг. Ключом данного шифра являлся порядок расположения букв на внутреннем диске и его начальное положение относительно внешнего диска (рис. 6.4).

[1] Кардано Джероламо (1501–1576) — итальянский математик, философ и врач.

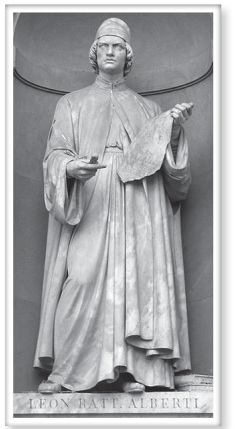


Рис. 6.4. Диск Альберти. Статуя Альберти в коллонаде Уффици (Флоренция)

Заметим также, что одна из первых в Европе книг, посвященных криптоанализу «Трактат о шифрах» (1466 г.), написана Леоном Баттиста Альберти — итальянским ученым, гуманистом, писателем, одним из зачинателей новой европейской архитектуры и ведущим теоретиком искусства эпохи Возрождения. Своей работой он внес существенный вклад в развитие криптографии.

Таблица Виженера[1]**.** Неудобство рассмотренных выше шрифтов моноалфавитных подстановок очевидно, так как в случае использования стандартного алфавита, таблица частот встречаемости букв алфавита позволяет определить один или несколько символов, а этого иногда достаточно для вскрытия шифра (например, эпизоды, описанные в художественной литературе: «Пляшущие человечки» Конан Дойля или «Золотой жук» Эдгара По). Поэтому использовались различные приемы для того чтобы затруднить дешифрование, например, таблица Виженера, которая представляет собой квадратную матрицу с числом строк и столбцов равным количеству букв алфавита.

Для шифрования по этой схеме используется таблица, где первая строка состоит из букв исходного алфавита (в примере приводится кириллическая таблица для шифра Виженера), а каждая последующая строка представляет собой циклический сдвиг предыдущей на одну позицию.

[1] Блез де Виженер (1523–1596) — французский дипломат, криптограф и алхимик, написал большой труд о шифрах. Квадратный шифр Виженера на протяжении почти 400 лет не был дешифрован, считался недешифруемым шифром.

м о н а с т ы р ь м о н а с т ы р ь м о н
р а с к и н у л о с ь м о р е ш и р о к о

э о я к щ а п ы й ю й щ о в ч ф ш л ь ш ы

Таблица Виженера (для кириллического алфавита)

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯ
БВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯА
ВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБ
ГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВ
ДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯФБВГ
ЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯФБВГД
ЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯФБВГДЕ
ЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖ
ИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗ
ЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИ
КЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙ
ЛМНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙК
МНОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛ
НОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМ
ОПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМН
ПРСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНО
РСТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОП
СТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПР
ТУФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРС
УФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТ
ФХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУ
ХЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФ
ЦЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХ
ЧШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦ
ШЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧ
ЩЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШ
ЬЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩ
ЫЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬ
ЭЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧЩШЬЫ
ЮЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭ
ЯАБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЭЮ

Пароль или лозунг с повторениями выписывается буква к букве под исходным сообщением. Каждая буква зашифрованного текста берется из таблицы на пересечении соответствующей буквы исходного текста, и столбца, соответствующего текущей букве лозунга. Подобный шифр

получил название многоалфавитной замены. Кроме непосредственного увеличения стойкости шифр Виженера привнес в криптографию две качественно новых идеи. Во-первых, процесс шифрования стал зависеть, в первую очередь, от небольшого неизвестного третьей стороне слова-лозунга. Во-вторых, сама таблица, использованная Виженером, несет по своей сути первые намеки на идею цифрового шифрования. Если все буквы исходного алфавита пронумеровать по порядку от 0 до N (где N — число символов в алфавите), то процедура шифрования по такой таблице превратится в обычную операцию сложения по модулю N.

Чтобы зашифровать какое-либо сообщение выбирают слово-лозунг (например, «монастырь») и надписывают его над сообщением с необходимым повторением. Заметим, что в качестве лозунга подойдет любая последовательность неповторяющихся символов исходного алфавита, однако осмысленная последовательность лучше для запоминания лозунга. Для получения шифрованного текста находят очередной символ лозунга, начиная с первого в вертикальном алфавите, и ему соответствующий знак сообщения — в горизонтальном алфавите. На пересечении выделенных столбца и строки находят первую букву шифра. Очевидно, что ключом к такому шифру является используемый лозунг.

Одноразовый шифровальный блокнот. Примером нераскрываемого шифра может служить так называемый *одноразовый шифровальный блокнот* — шифр, в основе которого лежит та же идея, что в шифре Цезаря. Назовем расширенным алфавитом множество букв алфавита и знаков препинания { . , : ; ! ? () — “ <пробел>}, число символов расширенного кириллического алфавита в данном варианте будет равно 44. Пронумеруем символы расширенного алфавита числами от 0 до 43. Тогда любой передаваемый текст можно рассматривать как последовательность $\{a_n\}$ чисел множества $A = \{0, 1, 2, ..., 43\}$.

Предположим, что имеем *ключ* — случайную последовательность $\{c_n\}$ чисел из множества A той же длины, что и передаваемый текст. Складывая по модулю[1] 44 число из передаваемого текста a_n с соответствующим числом из множества ключа c_n:

$$a_n + c_n \equiv b_n \pmod{44},$$

получим последовательность $\{b_n\}$ знаков шифрованного текста. Чтобы получить передаваемый текст, можно воспользоваться тем же ключом:

$$a_n \equiv b_n - c_n \pmod{44}, \text{ если } b_n - c_n < 0, \text{ то } a_n = b_n - c_n + 44.$$

[1] Напомним, что результатом модульной операции является остаток от целочисленного деления, например, если мы делим 11 на 3, то целых частей у нас получается 3, (так как 3 × 3 = 9), в остатке будет 2, это число и будет результатом деления по модулю, т.е. 11 mod 3 = 2.

Процесс шифрования можно описать следующим образом. У двух абонентов, находящихся в секретной переписке, имеются два одинаковых блокнота. В каждом из них на нескольких листах напечатана случайная последовательность чисел множества А. Отправитель свой текст шифрует указанным выше способом при помощи первой страницы блокнота. Зашифровав сообщение, он уничтожает использованную страницу и отправляет текст сообщения второму абоненту, получатель шифрованного текста расшифровывает его и также уничтожает использованный лист блокнота. Нетрудно видеть, что одноразовый шифр не раскрываем в принципе, так как символ в тексте может быть заменен любым другим символом и этот выбор совершенно случаен.

Шифрование методом перестановки символов. Суть этого метода заключается в том, что символы текста переставляются по определенным правилам, при этом используются только символы исходного (незашифрованного) текста. Перестановки в классической криптографии обычно получаются в результате записи исходного текста и чтения шифрованного текста по разным путям геометрической фигуры. Простейшим примером перестановки является запись исходного текста по строкам некоторой матрицы и чтение его по столбцам этой матрицы (табл. 6.1). Последовательность заполнения строк и чтения столбцов может быть любой и задается ключом. Например, для матрицы размером 8×8 (длина блока 64 символа) возможно $1{,}6 \cdot 10^9$ ключей, что позволяет на современных компьютерах путем перебора дешифровать заданный текст. Однако для матрицы размером 16×16 (длина блока 256 символов) имеется $1{,}4 \cdot 10^{26}$ ключей, и перебор их с помощью современных вычислительных средств весьма затруднителен.

Таблица 6.1

Пример шифрования методом перестановки

1	И	Е	—	П
2	Е	Р	Е	С
3	О	В	А	Н
4	Т	А	Н	О
5	Ш	И	Ф	Р
6	В	К	О	Й
k_1/k_2	1	2	3	4

Пример

Исходный текст: ШИФРОВАНИЕ_ПЕРЕСТАНОВКОЙ
Ключи: k_1 {5-3-1-2-4-6}; k_2 {4-2-3-1}.
Запись по строкам производится в соответствии с ключом k_1.
Чтение по столбцам в соответствии с ключом k_2.
Шифртекст: ПСНОРЙЕРВАИК_ЕАНФОИЕОТШВ

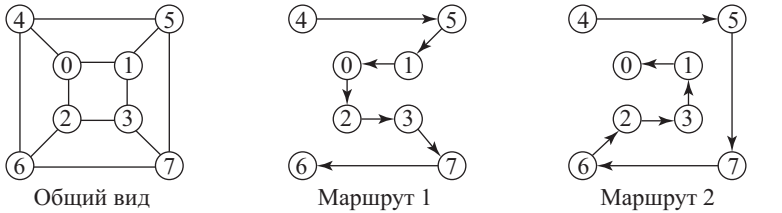


Рис. 6.5. Перестановки с использованием гамильтоновых путей на графе

Примером применения метода перестановки может быть также восьмиэлементная таблица (или граф), обладающая совокупностью маршрутов, носящих название маршрутов Гамильтона. Последовательность заполнения таблицы каждый раз соответствует нумерации ее элементов. Если длина шифруемого текста не кратна числу элементов, то при последнем заполнении в свободные элементы заносится произвольный символ. Выборка из таблицы для каждого заполнения может выполняться по своему маршруту, при этом маршруты могут использоваться как последовательно, так и в порядке, задаваемом ключом. Наиболее сложные перестановки осуществляются по гамильтоновым путям, которых в графе может быть несколько. Гамильтонов путь — путь, содержащий каждую вершину графа ровно один раз. Необходимо отметить, что, например, для графа на рис. 6.5 из восьми вершин можно предложить несколько маршрутов записи открытого текста и несколько гамильтоновых путей для чтения криптограмм.

Для методов перестановки характерны простота алгоритма, возможность программной реализации, но достаточно низкий уровень защиты, так как при большой длине исходного текста в его зашифрованном варианте проявляются статистические закономерности ключа, что и позволяет его быстро раскрыть.

Многоалфавитные методы шифрования. Многоалфавитное шифрование (многоалфавитная замена) заключается в том, что для последовательных символов шифруемого текста используются одноалфавитные методы с различными ключами. Например, первый символ заменяется по методу Цезаря со смещением 14, второй — со смещением 10, и так далее до конца заданного ключа. Затем процедура продолжается периодически. Более общей является ситуация, когда используется не шифр Цезаря, а последовательность произвольных подстановок, соответствующих одноалфавитным методам.

Более наглядным примером подобного шифрования является *метод гаммирования*. Данный способ преобразования заключается в том, что символы закрываемого текста последовательно складываются с символами некоторой специальной последовательности, именуемой гаммой. Такое преобразование иногда называют наложением гаммы на открытый текст.

Символы закрываемого текста и гаммы заменяются цифровыми эквивалентами, а затем складываются по модулю k, где k — количество символов алфавита:

$$T_ш = (T_о \oplus T_г) \bmod k ,$$

где $T_ш$ — шифртекст; $T_о$ — открытый текст; $T_г$ — гамма.

Символы текста и гаммы представляются в двоичных кодах, а затем каждая пара двоичных разрядов складывается по модулю 2.

Стойкость шифрования методом гаммирования определяется, главным образом, качеством гаммы, которое определяется двумя характеристиками: длиною периода и случайностью распределения символов по периоду. Длиною периода гаммы называется минимальное количество символов, после которого последовательность начинает повторяться. Случайность распределения символов по периоду означает отсутствие закономерностей между появлением различных символов в пределах периода.

Основные требования,
которые предъявляются к методам шифрования

1. Сложность и трудоемкость процедур шифрования и расшифрования должны определяться в зависимости от степени секретности защищаемых данных.
2. Надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику известен способ закрытия.
3. Способ закрытия и набор используемых служебных данных (ключевых установок) не должны быть слишком сложными. Затраты на защитные преобразования должны быть приемлемые при заданном уровне сохранности информации.
4. Выполнение процедур прямого и обратного преобразования должно быть формальным и как можно проще.
5. Процедуры прямого и обратного преобразования не должны зависеть от длины сообщения.
6. Ошибки, возникающие в процессе преобразования, не должны распространяться по системе и вызывать потерю информации. Из-за появления ошибок передачи зашифрованного сообщения по каналам связи не должна исключаться возможность надежной расшифровки текста на приемном конце.
7. Избыточность сообщений, вносимая закрытием, должна быть как можно меньшей.
8. Объем ключа не должен затруднять его запоминание и пересылку.

6.2. Особенности построения блочных шифров

Современные алгоритмы шифрования возникли на базе развития и совершенствования классических шифров, путем устранения имеющихся у них криптографических слабостей. Большинство современных шифров можно рассматривать как усиление и модернизацию известных с древних времен шифров простой замены, перестановки, о которых мы говорили в предыдущих разделах этой главы.

Очевидна возможность дешифрования шифра простой замены в случае, если достаточно велико соотношение между объемом материала и размером алфавита открытого и шифрованного текстов. Однако шифр простой замены сложно вскрыть, если это соотношение мало, например в случае, когда шифруются тексты единичной длины (одна буква). Отсюда и вытекает подход к усилению шифра простой замены — разрабатывают шифры, для которых это соотношение чрезвычайно мало. Делают это двумя способами: увеличивают алфавит либо максимально уменьшают объем сообщения, шифруемого с помощью одной и той же замены.

Первый путь (увеличение алфавита) реализован в шифрах многозначной замены, в кодах и современных блочных шифрах. По второму пути (уменьшение числа знаков, шифруемых по одной замене) пошли при создании поточных шифров замены.

Шифры многозначной замены. Шифр многозначной замены может быть задан в табл. 6.2.

Таблица 6.2

Пример задания шифра многозначной замены

А	Б	В	Г	Д	...
$а_1$	$б_1$	$в_1$	$г_1$	$д_1$	...
$а_2$	$б_2$	$в_2$	$г_2$	$д_2$	...
$а_3$	$б_3$	$в_3$	$г_3$	$д_3$	...
$а_4$	...	...	...	...	...
...	...	...	...	...	...

Здесь каждой букве отвечает несколько символов шифртекста, следовательно, алфавит шифртекста больше алфавита открытого текста. Шифровальщик, зашифровывая открытый текст, должен выбрать для каждой буквы одно из обозначений, например, А зашифровывается в $а_1$, или в $а_2$, или в $а_3$ и т.д. Такой подход при грамотном использовании может значительно повысить криптостойкость шифра.

Коды. Идея увеличения алфавита открытого текста реализована в кодах. Код представляет собой два словаря. Первый словарь предназначен для зашифрования, а второй — для расшифрования. В словаре для зашифрования в алфавитном порядке выписаны символы алфавита

открытого текста: отдельные буквы, слова, целые предложения и для каждого символа указано его кодообозначение. При шифровании шифровальщик каждый символ (или слово, предложение) заменяет с помощью первого словаря на кодообозначение. Это преобразование неоднозначно. Слово можно заменить по буквам или попытаться подобрать кодообозначение для целого слова или фразы. При расшифровании используется второй словарь, в котором в алфавитном порядке записаны кодообозначения, и расшифрование сводится к замене их на символы открытого текста. Словарь может состоять из тысяч, десятков тысяч слов. Дешифровать код достаточно сложно. Для этого необходимо набрать достаточное количество материала. Коды находят определенное применение, например, есть военно-морские коды, дипломатические коды и т.п. Недостаток этой системы шифрования заключается в том, что каждый код — это две книги, их надо напечатать без ошибок, разослать всем участникам закрытой связи. Если одна такая книга попадет злоумышленнику, то код надо срочно менять, система инерционная.

Промежуточным вариантом между простой заменой и кодом является блочный шифр. В нем текст делится на блоки и проводится простая замена блоков. Когда длина блока достаточно велика, таблица замены становится необозримой и саму замену приходится задавать не таблицей, а некоторым алгоритмом преобразования.

Блочный шифр «два квадрата». Блочные шифры, в которых заменялись пары букв, применяли во время Второй мировой войны немцы в низовых линиях связи. При шифровании открытый текст разбивался на блоки по две буквы, например:

КР ИП ТО ГР АФ ИЯ

Ключом являлись два квадрата, в которых записывался алфавит в произвольном порядке.

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

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

Первая буква выбиралась в левом квадрате, вторая — в правом. Мысленно строился прямоугольник, и в шифртекст включались буквы из незанятых его углов. Так, в примере на место К ставилась буква из соответствующего незанятого угла прямоугольника второго квадрата Ж, а вместо Р ставилась Ф. Если буквы оказывались в одной строке, то буква заменялась на букву той же позиции, но из другого квадрата. Так,

в примере вместо И ставилась буква этого же столбца второго квадрата К, а вместо П — соответствующая буква первого квадрата З. Таким образом, слово криптография после зашифрования имело бы вид:

ЖФКЗФБЕРРУЩР

Советским криптографам в годы Второй мировой войны шифры типа «два квадрата» удавалось дешифровывать, но это требовало значительных усилий и опыта.

Преимуществами данных шифров перед кодами были достаточная простота и быстрота зашифрования и расшифрования, отсутствие потребности в словарях, простота в смене ключевых квадратов.

Сеть Фейстеля. Блочные шифры — это шифры простой замены с большим алфавитом «открытого текста». Многие блочные шифры используют в своем построении так называемую идею Хорста Фейстеля состоящую в реализации многих «раундов» шифрования, каждый из которых реализуется криптосхемой.

Хорст Фейстель
(1915–1990)
В 1971 г. запатентовал два устройства, реализовавшие различные алгоритмы шифрования, известные под общим названием «Люцифер».
Одно из устройств использовало конструкцию, впоследствии названную сетью Фейстеля.

Сеть Фейстеля имеет следующую структуру. Входной блок делится на несколько равной длины подблоков, называемых ветвями. В случае если блок имеет длину 64 бита, используются две ветви по 32 бита каждая. Каждая ветвь обрабатывается независимо от другой, после чего осуществляется циклический сдвиг всех ветвей влево. Такое преобразование выполняется несколько циклов или раундов.

В случае двух ветвей каждый раунд имеет структуру, показанную на рис. 6.6.

Функция F называется образующей. Каждый раунд состоит из вычисления функции F для одной ветви и побитового выполнения операции XOR результата *F* с другой ветвью.

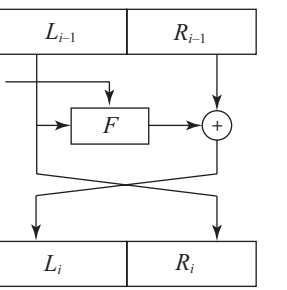


Рис. 6.6. I-й раунд сети Фейстеля

После этого ветви меняются местами. Считается, что оптимальное число раундов — от 8 до 32.

Важно то, что увеличение количества раундов значительно увеличивает криптостойкость алгоритма. Возможно, эта особенность и повлияла на столь активное распространение сети Фейстеля, так как для большей криптостойкости достаточно просто увеличить количество раундов, не изменяя сам алгоритм.

Сеть Фейстеля является обратимой даже в том случае, если функция F не является таковой, так как для расшифрования не требуется вычислять обратную функцию F^{-1}. Для расшифрования используется тот же алгоритм, но на вход подается зашифрованный текст и ключи используются в обратном порядке.

В настоящее время все чаще используются различные разновидности сети Фейстеля для 128-битного блока с четырьмя ветвями. Увеличение количества ветвей, а не размерности каждой ветви связано с тем, что наиболее популярными до сих пор остаются процессоры с 32-разрядными словами, следовательно, оперировать 32-разрядными словами эффективнее, чем с 64-разрядными.

На основе различных модицикаций сети Фейстеля построены многие современные алгоритмы симметричного шифрования: DES, ГОСТ 28147–89, Blowfish, RC5, FEAL и ряд других. Во многих блочных шифрах на основе сети Фейстеля были найдены те или иные уязвимости, однако в ряде случаев эти уязвимости являются чисто теоретическими и при нынешней производительности компьютеров использовать их на практике для взлома невозможно.

6.3. Симметричные криптосистемы

Симметричные криптосистемы (с секретным ключом — secret key systems) построены на основе сохранения в тайне ключа шифрования. Процессы зашифрования и расшифрования используют один и тот же ключ. Секретность ключа является постулатом. Основная проблема при применении симметричных криптосистем для связи заключается в сложности передачи обоим сторонам секретного ключа. Однако данные системы обладают высоким быстродействием. Раскрытие ключа злоумышленником грозит раскрытием только той информации, что была зашифрована на этом ключе. Старый американский и российский стандарты шифрования DES и ГОСТ 28.147–89, а также новый американский стандарт AES Rijndael являются представителями симметричных криптосистем.

Симметричные криптосистемы, также симметричное шифрование, симметричные шифры (symmetric-key algorithm) — способ шифрования, в котором для зашифрования и расшифрования применяется один и тот же криптографический секретный ключ.

Симметричные криптосистемы в настоящее время принято подразделять на блочные и поточные.

Блочные криптосистемы разбивают текст сообщения на отдельные блоки и затем осуществляют преобразование этих блоков с использованием ключа.

Поточные криптосистемы работают несколько иначе. На основе ключа системы вырабатывается некая последовательность — так называемая гамма, которая затем используется для зашифрования (расшифрования) текста сообщения. Таким образом, преобразование текста осуществляется как бы потоком по мере выработки гаммы.

Общая структура использования симметричной криптосистемы представлена на рис. 6.7.

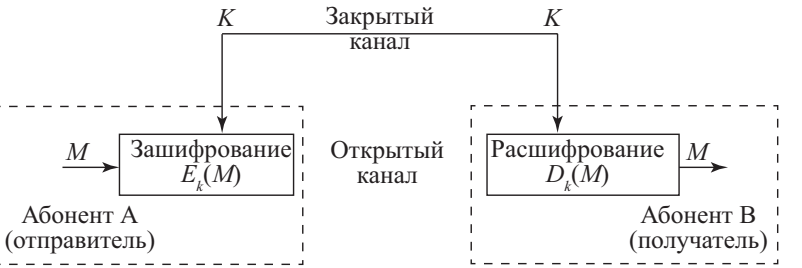


Рис. 6.7. Структура симметричной криптосистемы:
M — открытый текст; K — секретный ключ, передаваемый по закрытому каналу; $E_k(M)$ — операция зашифрования; $D_k(M)$ — операция расшифрования

Теоретическая база для построения стойких симметричных шифров была разработана в середине прошлого века известным американским ученым Клодом Элвудом Шенонном, знаменитым также своими основополагающими трудами в области теории информации. В частности, в его работе «Теория связи в секретных системах»[1] был предложен математический аппарат для построения стойких шифров, а также сформулированы основные принципы обеспечения криптостойкости симметричных шифров — рассеивание и перемешивание:

- *рассеивание* (diffusion) — изменение любого знака открытого текста или ключа влияет на большое число знаков шифртекста, что скрывает статистические свойства открытого текста;
- *перемешивание* (confusion) — использование преобразований, затрудняющих получение статистических зависимостей между шифротектстом и открытым текстом.

[1] *Шеннон К.* Теория связи в секретных системах // В кн.: Шеннон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963. 333 с.

Практически все современные блочные шифры являются композиционными, т.е. состоят из композиции простых преобразований. Само по себе преобразование может и не обеспечивать нужных свойств, но их цепочка позволяет получить необходимый результат.

При поточном шифровании каждый символ исходного текста может представляться в битовой форме, т.е. в двоичном виде. Далее каждый бит полученной последовательности можно преобразовать по определенному правилу. В качестве такого правила преобразования часто используют побитовое сложение исходного текста с некоторой секретной битовой последовательностью. Секретная последовательность битов играет роль ключа зашифрования в симметричных потоковых шифрах. Сама по себе операция побитового сложения называется также операцией сложения по модулю два, операцией «исключающего ИЛИ» или XOR.

Напомним, что выполнение операции XOR осуществляется по следующему правилу:

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

Для расшифрования необходимо выполнить обратную процедуру. Перевести криптограмму в двоичный вид и сложить побитово с той же самой секретной последовательностью, которая использовалась для зашифрования.

Основу большинства потоковых шифров составляет генератор псевдослучайных последовательностей. Задача такого генератора состоит в создании битовой последовательности, которую называют ключевой гаммой шифра. Такая гамма используется в операции побитового сложения с исходным текстом. Собственно ключом шифрования в таком случае является начальное состояние (и, возможно, структура генератора). Очевидно, что тот, кто знает алгоритм генерации последовательностей и начальные входные данные для работы алгоритма, сможет воспроизвести всю гамму.

Основной характеристикой таких потоковых шифров является криптографическая стойкость генератора псевдослучайных последовательностей. Генератор должен обеспечивать следующие важные свойства:

– создавать последовательности битов, по своим статистическим характеристикам близкие к случайным равновероятным последовательностям;
– обеспечивать генерацию достаточно длинных неповторяющихся последовательностей;
– обладать достаточной скоростью для работы в реальном времени.

Первое из этих свойств необходимо для того, чтобы злоумышленник не мог угадать ключевую гамму шифра. Второе свойство обеспечивает устойчивость метода шифрования к различным атакам. Последнее свойство позволяет на практике использовать потоковые шифры в реальном режиме времени.

Далее рассмотрим подробно работу симметричной криптосистемы на примере алгоритма DES.

Блочный шифр DES

Стандарт шифрования данных DES (Data Encryption Standard) был опубликован в 1977 г. Национальным бюро стандартов США (National Bureau of Standards, NBS). Стандарт DES был предназначен для защиты от несанкционированного доступа к важной, но несекретной информации в государственных и коммерческих организациях США. Долгое время DES являлся самым распространенным алгоритмом, используемым в системах защиты коммерческой информации. В конце 1996 г. Национальным институтом стандартов США (NIST) был объявлен конкурс на создание нового общенационального стандарта шифрования, который должен был прийти на замену DES. В настоящее время в качестве американского стандарта блочного шифрования AES (Advanced Encryption Standard) испльзуется алгоритм Rijndael.

DES осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит (остальные 8 бит — проверочные для контроля на четность). Расшифрование в DES является операцией, обратной шифрованию, и выполняется путем повторения операций шифрования в обратной последовательности. Обобщенная схема процесса шифрования в алгоритме DES представлена на рис. 6.8. Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и, наконец, в конечной перестановке битов.

Следует сразу отметить, что все приводимые далее таблицы являются стандартными и должны включаться в реализацию алгоритма DES в неизменном виде. Все перестановки и коды в таблицах подобраны разработчиками таким образом, чтобы максимально затруднить процесс дешифровки путем подбора ключа.

При описании алгоритма DES (рис. 6.9) применены следующие обозначения:

L и R — последовательности битов (левая (left) и правая (right));

LR — конкатенация последовательностей L и R, т.е. такая последовательность битов, длина которой равна сумме длин L и R; в последовательности LR биты последовательности L следуют за битами последовательности R;

$\oplus$ — операция побитового сложения по модулю 2.

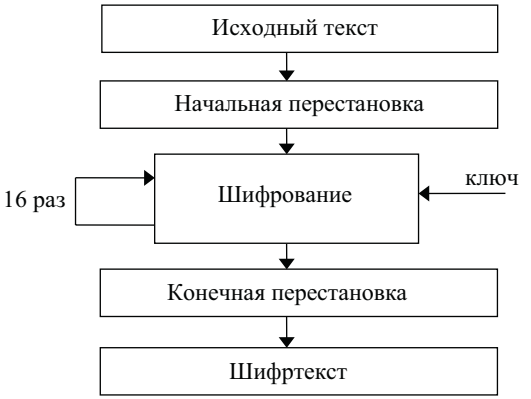


Рис. 6.8. Обобщенная схема шифрования в алгоритме DES

Пусть из файла исходного текста считан очередной 64-битовый (8-байтовый) блок T. Этот блок T преобразуется с помощью *матрицы начальной перестановки P* (табл. 6.3).

Таблица 6.3

Матрица начальной перестановки P

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	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

Биты входного блока T (64 бита) переставляются в соответствии с матрицей P: бит 58 входного блока T становится битом 1, бит 50 — битом 2 и т.д. Эту перестановку можно описать выражением $T_0 = \mathrm{P(T)}$. Полученная последовательность битов T_0 разделяется на две последовательности: L_0 — левые или старшие биты, R_0 — правые или младшие биты, каждая из которых содержит 32 бита.

Биты входного блока T (64 бита) переставляются в соответствии с матрицей P: бит 58 входного блока T становится битом 1, бит 50 — битом 2 и т.д. Эту перестановку можно описать выражением $T_0 = P(T)$. Полученная последовательность битов T_0 разделяется на две последовательности: L_0 — левые или старшие биты, R_0 — правые или младшие биты, каждая из которых содержит 32 бита.

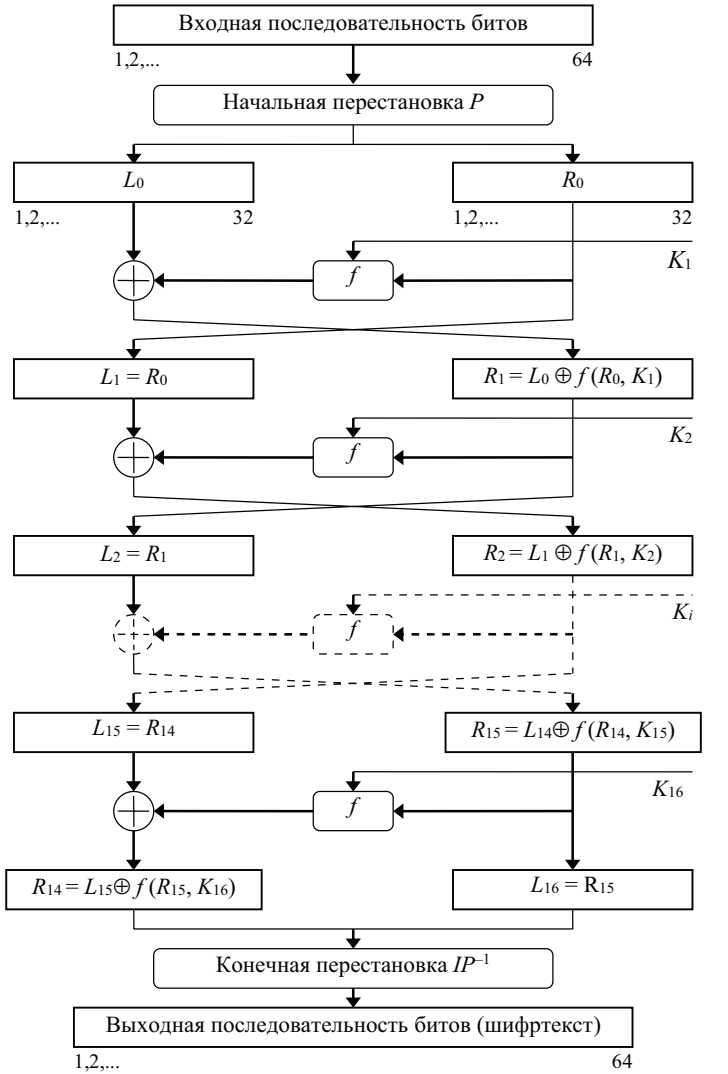


Рис. 6.9. Структура алгоритма DES

Затем выполняется итеративный процесс шифрования, состоящий из 16 шагов (циклов). Пусть T_i — результат i-й итерации: $T_i = L_i R_i$, где $L_i = t_1 t_2 \ldots t_{32}$ (первые 32 бита); $R_i = t_{33} t_{34} \ldots t_{64}$ (последние 32 бита). Тогда результат i-й итерации описывается следующими формулами:

$L_i = R_{i-1}$, $i \in \{1, 2, \ldots, 16\}$;
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, $i \in \{1, 2, \ldots, 16\}$.

Функция f называется функцией шифрования. Ее аргументами являются последовательность R_{i-1}, получаемая на предыдущем шаге итерации, и 48-битовый ключ K_i, который является результатом преобразования 64-битового ключа шифра K. Подробнее функция шифрования f и алгоритм получения ключа K_i описаны ниже.

На последнем шаге итерации получают последовательности R_{16} и L_{16} (без перестановки местами), которые конкатенируются в 64-битовую последовательность $R_{16}L_{16}$.

По окончании шифрования осуществляется восстановление позиций битов с помощью матрицы обратной перестановки P^{-1} (табл. 6.4).

Таблица 6.4

Матрица обратной перестановки P^{-1}

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

Пример того, как соотносятся элементы первой строки матрицы P^{-1} с элементами матрицы P, приведен в табл. 6.5.

Таблица 6.5

Связь элементов матриц

Элемент матрицы IP^{-1}	Элемент матрицы IP
40	01
8	02
48	03
16	04
56	05
...	...

Процесс расшифрования данных является инверсным по отношению к процессу шифрования. Все действия должны быть выполнены в обратном порядке. Это означает, что расшифровываемые данные сначала переставляются в соответствии с матрицей P^{-1}, а затем над последовательностью битов $R_{16}L_{16}$ выполняются те же действия, что и в процессе шифрования, но в обратном порядке.

Итеративный процесс расшифрования может быть описан следующими формулами:

$R_{i-1} = L_i$, $i \in \{1, 2, ..., 16\}$;
$L_{i-1} = R_i \oplus f(L_i, K_i)$, $i \in \{1, 2, ..., 16\}$.

Таким образом, для процесса расшифрования с переставленным входным блоком $R_{16}L_{16}$ на первой итерации используется ключ K_{16}, на второй итерации — K_{15} и т.д. На 16-й итерации используется ключ K_1. На последнем шаге итерации будут получены последовательности L_0 и R_0, которые конкатенируются в 64-битовую последовательность L_0R_0. Затем в этой последовательности 64 бита переставляются в соответствии с матрицей P. Результат такого преобразования — исходная последовательность битов (расшифрованное 64-битовое значение).

Теперь рассмотрим, что скрывается под преобразованием, обозначенным буквой f. Схема вычисления функции шифрования $f(R_{i-1}, K_i)$ показана на рис. 6.10.

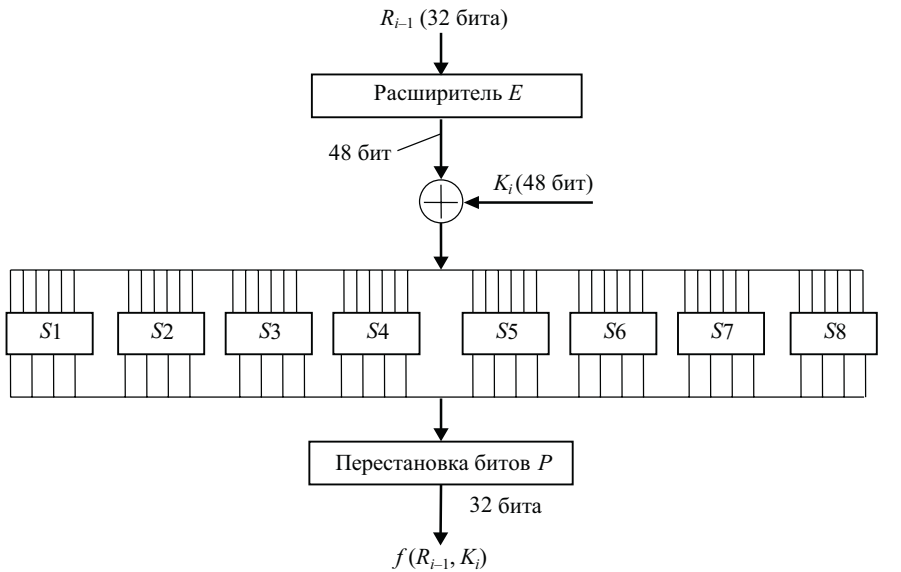


Рис. 6.10. Схема вычисления функции шифрования f

Для вычисления значения функции f используются:
– функция E (расширение 32 бит до 48);
– функция $S_1, S_2, ..., S_8$ (преобразование 6-битового числа в 4-битовое);
– функция P (перестановка битов в 32-битовой последовательности).

Приведем определения этих функций.

Аргументами функции шифрования f являются R_{i-1} (32 бита) и K_i (48 бит). Результат функции $E(R_{i-1})$ есть 48-битовое число. Функция расширения E, выполняющая расширение 32 бит до 48 (принимает блок из 32 бит и порождает блок из 48 бит), определяется в табл. 6.6.

Таблица 6.6

Функция расширения *E*

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

В соответствии с табл. 6.6 первые три бита $E(R_{i-1})$ — это биты 32, 1 и 2, а последние — 31, 32, 1. Полученный результат (обозначим его $E(R_{i-1})$) складывается по модулю 2 (операция XOR) с текущим значением ключа K_i и затем разбивается на восемь 6-битовых блоков B_1, B_2, ..., B_8:

$E(R_{i-1}) \oplus K_i = B_1 B_2 \ldots B_8$.

Далее каждый из этих блоков используется как номер элемента в функциях-матрицах S_1, S_2, ..., S_8, содержащих 4-битовые значения (табл. 6.7).

Следует отметить, что выбор элемента в матрице S_j осуществляется достаточно оригинальным образом. Пусть на вход матрицы S_j поступает 6-битовый блок $B_j = b_1b_2b_3b_4b_5b_6$, тогда двухбитовое число b_1b_6 указывает номер строки матрицы, а четырехбитовое число $b_2b_3b_4b_5$ — номер столбца. Например, если на вход матрицы S_1 поступает 6-битовый блок $B_1 = b_1b_2b_3b_4b_5b_6 = 100110$, то 2-битовое число $b_1b_6 = 10_{(2)} = 2_{(10)}$ указывает строку с номером 2 матрицы S_1, а 4-битовое число $b_2b_3b_4b_5 = 0011_{(2)} = 3_{(10)}$ указывает столбец с номером 3 матрицы S_1. Это означает, что в матрице S_1 блок $B_1 = 100110$ выбирает элемент на пересечении строки с номером 2 и столбца с номером 3, т.е. элемент $8_{(10)} = 1000_{(2)}$. Совокупность 6-битовых блоков B_1, B_2, ..., B_8 обеспечивает выбор четырехбитового элемента в каждой из матриц S_1, S_2, ..., S_8.

В результате получаем $S_1(B_1)\, S_2(B_2)\, S_3(B_3) \ldots S_8(B_8)$, т.е. 32-битовый блок (поскольку матрицы S_j содержат 4-битовые элементы). Этот 32-битовый блок преобразуется с помощью функции перестановки битов P (табл. 6.8).

Таким образом, функция шифрования

$f(R_{i-1}, K_i) = P(S_1(B_1), ..., S_8(B_8))$.

Как нетрудно заметить, на каждой итерации используется новое значение ключа K_i (длиной 48 бит). Новое значение ключа K_i вычисляется из начального ключа K (рис. 6.10). Ключ K представляет собой 64-битовый блок с 8 битами контроля по четности, расположенными в позициях 8, 16, 24, 32, 40, 48, 56, 64. Для удаления контрольных битов и подготовки ключа к работе используется функция G первоначальной подготовки ключа (табл. 6.9).

Таблица 6.7

Функции преобразования S_1, S_2, ..., S_8

	Номер столбца																
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	4	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	1	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Таблица 6.8

Функция *P* перестановки битов

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

Таблица 6.9

Функция *G* первоначальной подготовки ключа (переставленная выборка 1)

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

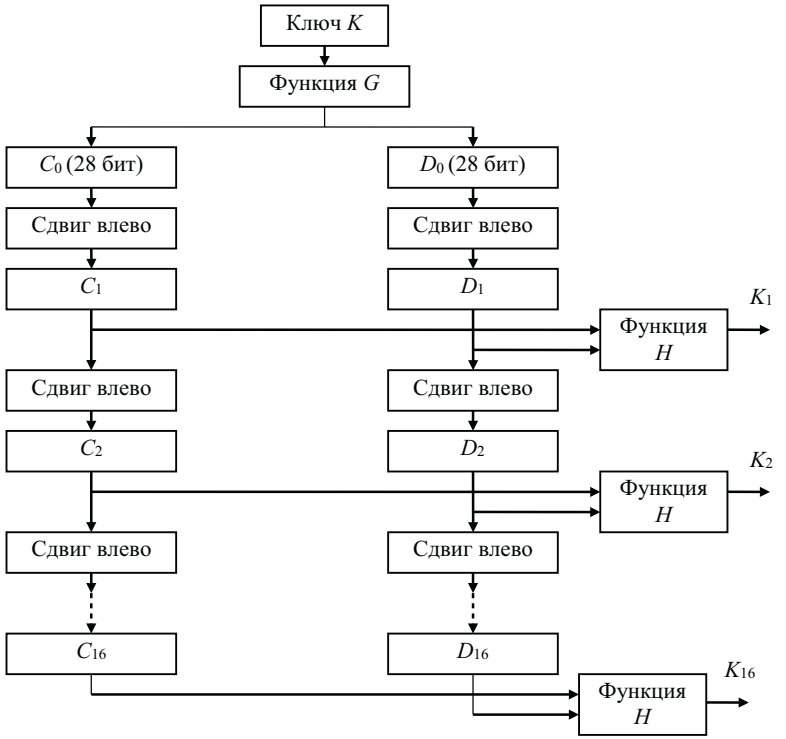


Рис. 6.11. Схема алгоритма вычисления ключей K_i

Таблица 6.9 разделена на две части. Результат преобразования $G(K)$ разбивается на две половины C_0 и D_0 по 28 бит каждая. Первые четыре строки матрицы G определяют, как выбираются биты последовательности C_0 (первым битом C_0 будет бит 57 ключа шифра, затем бит 49 и т.д., а последними битами — биты 44 и 36 ключа).

Следующие четыре строки матрицы G определяют, как выбираются биты последовательности D_0 (т.е. последовательность D_0 будет состоять из 63, 55, 47, ...,12, 4 битов ключа шифра).

Как видно из табл. 6.9, для генерации последовательностей C_0 и D_0 не используются биты 8, 16, 24, 32, 40, 48, 56 и 64 ключа шифра. Эти биты не влияют на шифрование и могут служить для других целей (например, для контроля по четности). Таким образом, в действительности ключ шифра является 56-битовым.

После определения C_0 и D_0 рекурсивно определяются C_i и D_i, $i \in \{1, 2, ..., 16\}$. Для этого применяются операции циклического сдвига влево на один или два бита в зависимости от номера шага итерации, как показано в табл. 6.10.

Таблица 6.10

Таблица сдвигов s_i для вычисления ключа

Номер итерации	Количество s_i сдвигов влево, бит	Номер итерации	Количество s_i сдвигов влево, бит
1	1	9	1
2	1	10	2
3	2	11	2
4	2	12	2
5	2	13	2
6	2	14	2
7	2	15	2
8	2	16	1

Операции сдвига выполняются для последовательностей C_i и D_i независимо. Например, последовательность C_3 получается посредством циклического сдвига влево на две позиции последовательности C_2, а последовательность D_3 — посредством сдвига влево на две позиции последовательности D_2, C_{16} и D_{16} получаются из C_{15} и D_{15} посредством сдвига влево на одну позицию.

Ключ K_i, определяемый на каждом шаге итерации, есть результат выбора конкретных битов из 56-битовой последовательности C_iD_i и их перестановки. Другими словами, ключ $K_i = H(C_iD_i)$, где функция H определяется матрицей, завершающей обработку ключа (табл. 6.11).

Таблица 6.11

Функция H завершающей обработки ключа (переставленная выборка 2)

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

Как следует из табл. 6.11, первым битом ключа K_i будет 14-й бит последовательности C_iD_i, вторым — 17-й бит, 47-м битом ключа K_i будет 29-й бит C_iD_i, а 48-м битом — 32-й бит C_iD_i.

Основные режимы работы алгоритма DES

Алгоритм DES вполне подходит как для шифрования, так и для аутентификации данных. Он позволяет непосредственно преобразовывать 64-битовый входной открытый текст в 64-битовый выходной шифрованный текст, однако данные редко ограничиваются 64 разрядами.

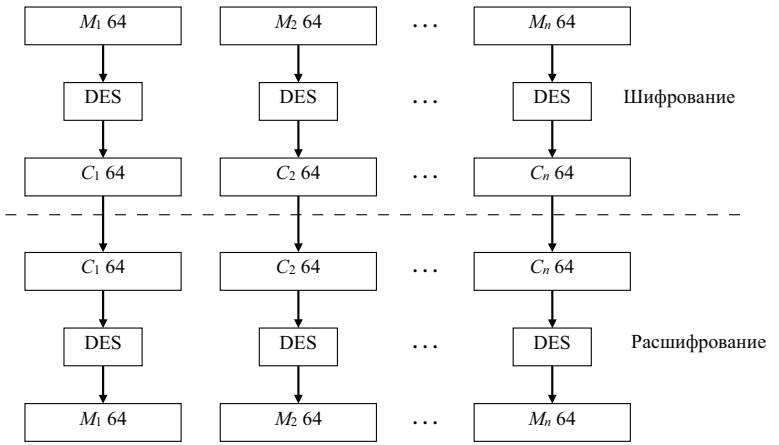


Рис. 6.12. Схема алгоритма DES в режиме электронной кодовой книги

Чтобы воспользоваться алгоритмом DES для решения разнообразных криптографических задач, разработаны четыре рабочих режима:

– электронная кодовая книга ECB (Electronic Code Book);
– сцепление блоков шифра CBC (Cipher Block Chaining);
– обратная связь по шифртексту CFB (Cipher Feed Back);
– обратная связь по выходу OFB (Output Feed Back).

Режим «Электронная кодовая книга». Длинный файл разбивают на 64-битовые отрезки (блоки) по 8 байтов. Каждый из этих блоков шифруют независимо с использованием одного и того же ключа шифрования (рис. 6.12).

Основное достоинство — простота реализации. Из-за фиксированного характера шифрования при ограниченной длине блока 64 бита возможно проведение криптоанализа «со словарем». Блок такого размера может повториться в сообщении вследствие большой избыточности в тексте на естественном языке. Это приводит к тому, что идентичные блоки открытого текста в сообщении будут представлены идентичными блоками шифртекста, что дает криптоаналитику некоторую информацию о содержании сообщения.

Режим «Сцепление блоков шифра». В этом режиме (рис. 6.13) исходный файл M разбивается на 64-битовые блоки: $M = M_1 M_2 ... M_n$. Первый блок M_1 складывается по модулю 2 с 64-битовым начальным вектором IV, который меняется ежедневно и держится в секрете. Полученная сумма затем шифруется с использованием ключа DES, известного и отправителю, и получателю информации. Полученный 64-битовый шифр C_1 складывается по модулю 2 со вторым блоком текста, результат шифруется и получается второй 64-битовый шифр C_2, и т.д. Процедура повторяется до тех пор, пока не будут обработаны все блоки текста.

Таким образом, для всех i из {1, ..., n} (n — число блоков) результат шифрования C_i определяется следующим образом:

$$C_i = \text{DES}\,(M_i \oplus C_{i-1}),$$

где C_0 = IV — начальное значение шифра, равное начальному вектору (вектору инициализации).

Очевидно, что последний 64-битовый блок шифртекста является функцией секретного ключа, начального вектора и каждого бита открытого текста независимо от его длины. Этот блок шифртекста называют *кодом аутентификации сообщения* (КАС).

Код КАС может быть легко проверен получателем, владеющим секретным ключом и начальным вектором, путем повторения процедуры, выполненной отправителем. Посторонний, однако, не может осуществить генерацию КАС, который воспринялся бы получателем как подлинный, чтобы добавить его к ложному сообщению, либо отделить КАС от истинного сообщения для использования его с измененным или ложным сообщением.

Достоинство данного режима в том, что он не позволяет накапливаться ошибкам при передаче. Блок M_i является функцией только C_{i-1} и C_i. Поэтому ошибка при передаче приведет к потере только двух блоков исходного текста.

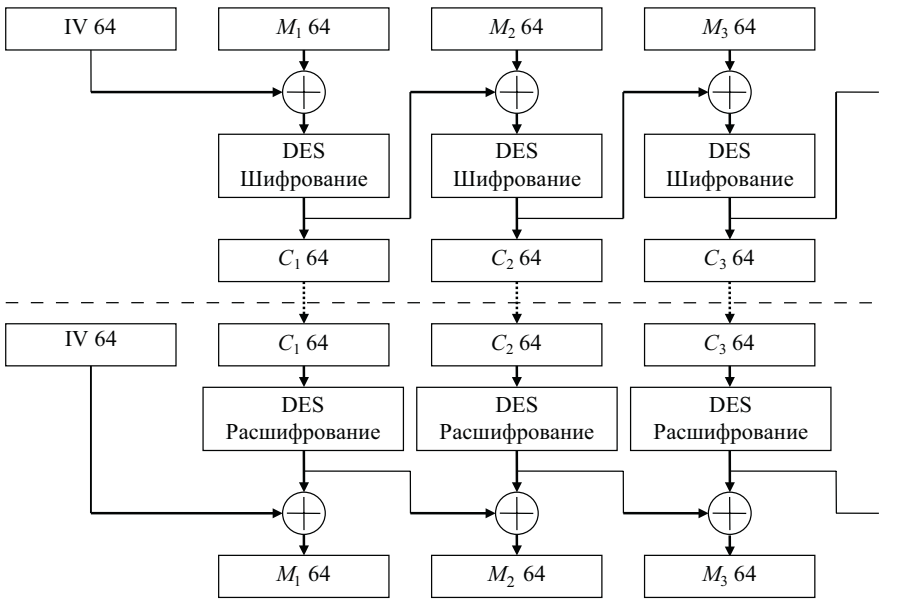


Рис. 6.13. Схема алгоритма DES в режиме сцепления блоков шифра

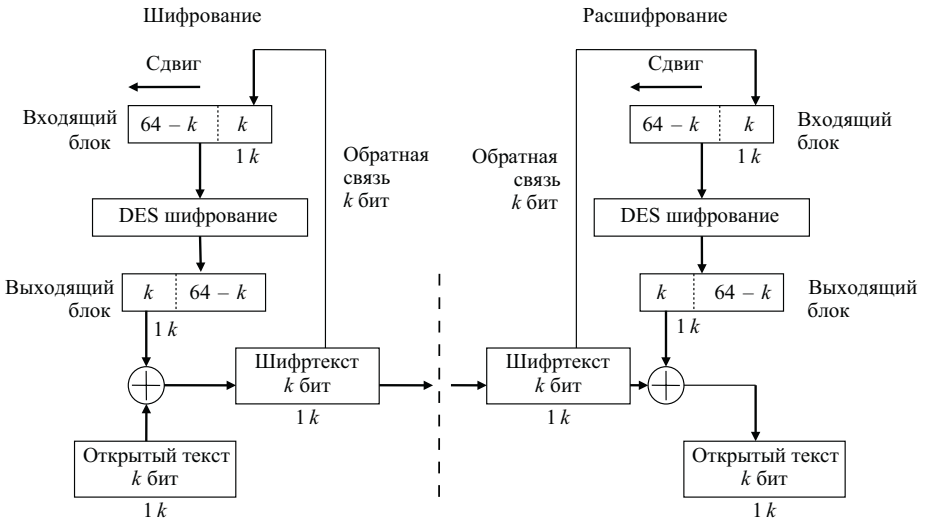


Рис. 6.14. Схема алгоритма DES в режиме обратной связи по шифртексту

Режим «Обратная связь по шифртексту». В этом режиме (рис. 6.14) размер блока длиной k битов может отличаться от 64 бит. Файл, подлежащий шифрованию (расшифрованию), считывается последовательными блоками длиной k битов, $k \leqslant 64$).

Входной блок (64-битовый регистр сдвига) вначале содержит вектор инициализации, выровненный по правому краю.

Предположим, что в результате разбиения на блоки мы получили n блоков длиной k битов каждый (остаток дописывается нулями или пробелами). Тогда для любого i из {1, ..., n} блок шифртекста получается по правилу

$$C_i = M_i \oplus P_{i-1},$$

где P_{i-1} обозначает k старших битов предыдущего зашифрованного блока.

Обновление сдвигового регистра осуществляется путем удаления его старших k битов и записи C_i в регистр. Восстановление зашифрованных данных также выполняется относительно просто: P_{i-1} и C_i вычисляются аналогичным образом и $M_i = C_i \oplus P_{i-1}$.

Режим «Обратная связь по выходу». Этот режим (рис. 6.15) тоже использует переменный размер блока и сдвиговый регистр, инициализируемый так же, как в режиме CFB, а именно — входной блок вначале содержит вектор инициализации IV, выровненный по правому краю. При этом для каждого сеанса шифрования данных необходимо использовать новое начальное состояние регистра, которое должно пересылаться по каналу открытым текстом.

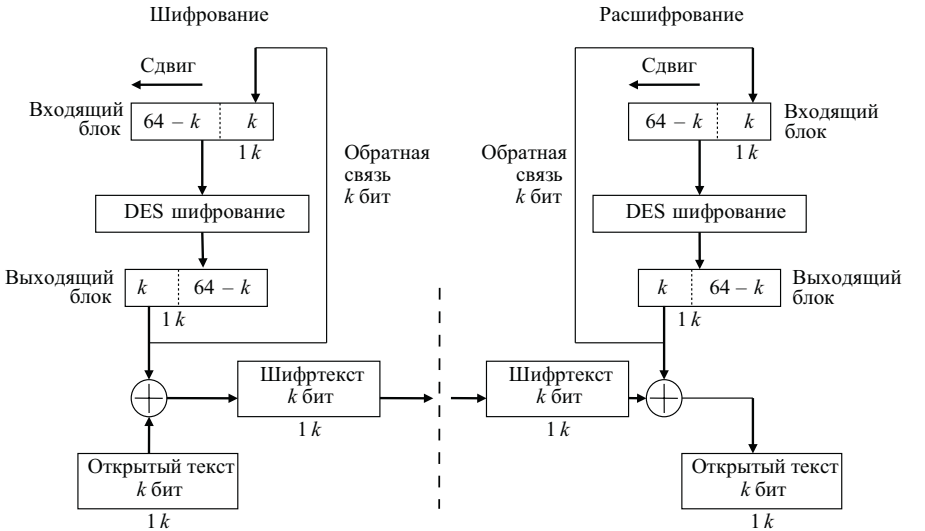


Рис. 6.15. Схема алгоритма DES в режиме обратной связи по выходу

Положим $M = M_1 M_2 \ldots M_n$. Для всех i из {1, ..., n}

$$C_i = M_i \oplus P_i,$$

где P_i — старшие k битов операции DES (C_{i-1}).

Отличие от режима обратной связи по шифртексту состоит в методе обновления сдвигового регистра. Это осуществляется путем отбрасывания старших k битов и дописывания справа P_i.

Каждому из рассмотренных режимов (ECB, CBC, CFB, OFB) свойственны свои достоинства и недостатки, что обусловливает области их применения. Режим ECB хорошо подходит для шифрования ключей, режим CFB, как правило, предназначается для шифрования отдельных символов, а режим OFB нередко применяется для шифрования в спутниковых системах связи.

Режимы CBC и CFB пригодны для аутентификации данных. Эти режимы позволяют использовать алгоритм DES для:

- интерактивного шифрования при обмене данными в телекоммуникационных сетях;
- шифрования криптографических ключей в практике автоматизированного распространения ключей;
- шифрования файлов, почтовых отправлений, данных спутников и других практических задач.

Другие симметричные криптоалгоритмы

ГОСТ 28147-89 (Россия). В нашей стране установлен единый алгоритм криптографического преобразования данных для систем обработки информации в телекоммуникационных сетях и отдельных вычислительных комплексах ГОСТ 28147-89[1]. Стандарт обязателен для организаций, предприятий и учреждений, применяющих криптографическую защиту данных.

Этот алгоритм криптографического преобразования данных предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации. Алгоритм шифрования данных представляет собой 64-битовый блочный алгоритм с 256-битовым ключом.

Сравнивая схемы DES и ГОСТ, следует заметить, что они во многом похожи, но есть и существенные различия:

– в ГОСТе проводится в два раза большее число итераций, определяющих криптографическую сложность результирующих преобразований;
– в ГОСТе существенно больше ключей ($2^{56} = 6{,}4 \cdot 10^{16}$ вариантов ключевых установок в DES и $2^{256} = 6{,}4 \cdot 10^{76}$ ключевых установок в ГОСТ).

Rijndael (Бельгия). Шифр разработали известные бельгийские криптографы Йон Дамен и Винсент Рэмен из Лувенского католического университета, являющегося одним из признанных центров академической криптографии не только Бельгии, но и всей Европы. Конструкция шифра в значительной степени опирается на идеи, воплощенные и проверенные в архитектуре шифра SQUARE, предыдущего детища этих же авторов, представленного в начале 1997 г. Как показали исследования, Rijndael может быть очень эффективно реализован на самых разных процессорах и чрезвычайно успешно противостоит известным криптоаналитическим атакам. Проблема с данным шифром — это как читать его название, составленное из фамилий криптографов. В соответствии с фламандскими традициями, «ij» читается как «э», а «ae» — как открытое «а». Так что «Rijndael» — это просто «Рэндал»...

В настоящее время именно Rijndael используется в качестве американского стандарта шифрования AES (Advanced Encryption Standard), заменив DES. AES — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит). AES получает все большее распространение, становясь фактически стандартом не только в США, но и системах независимых разработчиков. На AES переходят системы, в которых использовался DES или 3-DES[1]. AES поддерживается практически во всех современных утилитах предназначенных для шифрования данных, таких как Cryptainer, Visual AES и других. Также AES поддерживается в zip-архиваторах, в современных Wi-Fi-роутерах, в базах данных и во многих других приложениях

RC6 (США). Это быстрый, гибкий и необычно компактный алгоритм — сочетание мощи и простоты. «R» в его названии — Рональд Ривест, знаменитый соавтор в алгоритме RSA, один из сооснователей криптофирмы RSA Data Security и изобретатель широко используемых шифров RC2 и RC4, а также хеш-функций MD2, MD4 и MD5. Своими соавторами при создании криптоалгоритма RC6 Ривест называет команду криптографов исследовательского центра RSA Laboratories. По всеобщему признанию, шифр RC6 — это прямое эволюционное развитие предыдущего криптоалгоритм Ривеста под названием RC5, появившегося в 1995 г.

Twofish (США). Шифр основан на хорошо известном, популярном и широко используемом в интернете криптоалгоритме Blowfish, разработанном в 1993 г. Брюсом Шнайером, автором книги-бестселлера «Прикладная криптография»[2]. По оценкам специалистов, алгоритм Twofish эффективно реализуется на 32-битных микропроцессорах и 64-битных архитектурах, 8-битных смарт-картах.

6.4. Асимметричные криптосистемы

Криптосистема называется *асимметричной* (системой открытого шифрования, с открытым ключом, public key system), поскольку для зашифрования и расшифрования в ней используются разные преобразования (и, соответственно, ключи — открытый и секретный).

Для зашифрования информации используется открытый ключ, для расшифрования — секретный. Обобщенная схема асимметричной криптосистемы представлена на рис. 6.16.

Криптографическая система с открытым ключом (асимметричная криптосистема) — система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передается по открытому (т.е. незащищенному) каналу и используется для проверки ЭП и/или для шифрования сообщения.

[1] Российский ГОСТ 28147-89 с изначально более длинными ключами продержался дольше DES, но, естественно, пришло время модернизировать и его. Новые версии блочных шифров в РФ были опубликованы в 2015 г. и уже с 2016 г. начался перевод продуктов с использованием криптографии на новые стандарты.

[1] Алгоритм 3-DES построен на основе DES и обадает более высокой криптостойкостью.

[2] *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке «Си». М.: Триумф, 2002.

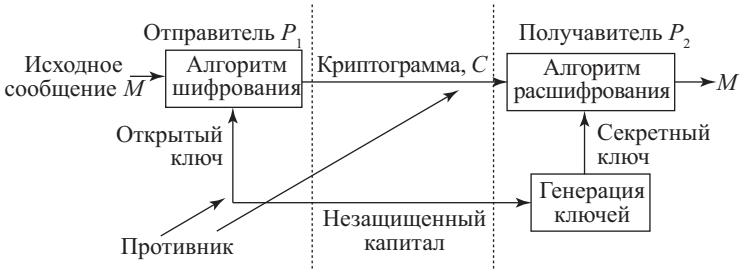


Рис. 6.16. Обобщенная схема асимметричной криптосистемы

Итак, в асимметричных криптосистемах (шифрах) участники обмена (отправитель, P_1 и получатель, P_2) используют два ключа — *секретный* и *открытый*. Открытый ключ публикуется в общедоступном месте, и каждый, кто захочет оправить сообщение получателю, может зашифровать текст открытым ключом. Расшифровать же сможет только получатель сообщения, владеющий секретным ключом. Таким образом, отпадает проблема передачи секретного ключа, как в симметричных системах. Однако, несмотря на все свои преимущества, эти криптосистемы достаточно трудоемки и медлительны. Стойкость асимметричных криптосистем базируется, в основном, на алгоритмической трудности решить за приемлемое время какую-либо математическую задачу. Если злоумышленнику удастся построить такой алгоритм, то дискредитирована будет вся система и все сообщения, зашифрованные с помощью этой системы. В этом состоит главная опасность асимметричных криптосистем в отличие от симметричных.

Для понимания криптопреобразований, которые используются в асимметричных системах, необходимо обратиться к основам модулярной арифметики.

Модулярная арифметика

Множество всех целых чисел с операциями сложения и умножения называют *кольцом целых чисел*.

Для любого целого $a > 0$ справедливо равенство $a = k \times n + r_a$, где k — целое число — частное от деления a на натуральное число n, r_a остаток от деления a на n. Величина r_a может принимать значения лишь из множества $Z/n = \{0, 1, 2, ..., (n - 1)\}$. Равенство $a = k \times n + r_a$ записывают в новом виде $a \equiv r_a \bmod n$ и читают так: «a сравнимо с r_a по модулю n». На множестве Z/n вводят операции сложения по модулю n, умножения по модулю n. Результатом сложения по модулю n чисел a, b является остаток r_{a+b} от деления (a + b) на n. Это записывают в виде $(a + b) = r_{a+b} \bmod n$. Аналогично вводится операция умножения по модулю n: $(ab) = r_{ab} \bmod n$. Напоминаем, что операции проводятся над возможными остатками — вычетами $\{0, 1, 2, ..., (n - 1)\}$ от деления на n целых неотрицательных чисел.

Пример

Для $n = 12$ полный набор вычетов: $Z/12 = \{0, 1, 2, \ldots, 11\}$, $2 + 5 = 7 \bmod 12$, $9 + 4 = 1 \bmod 12$, $11 + 11 = 10 \bmod 12$, $2 + 0 = 2 \bmod 12$, $2 \times 5 = 10 \bmod 12$, $9 \times 4 = 0 \bmod 12$, $11 \times 11 = 1 \bmod 12$.

Здесь и ниже индексы у остатков опускаются.

Множество $Z/n = \{0, 1, 2, ..., (n-1)\}$ с введенными операциями сложения и умножения по модулю n называют *кольцом целых по модулю n* (кольцом вычетов по модулю n).

Получение остатка $a \bmod n$ от деления на n произвольного целого числа a называют приведением по модулю n. Эта операция обладает хорошим свойством, называемым гомоморфизмом: мы можем либо сначала приводить числа по модулю n, а затем выполнять операции сложения и умножения, либо сначала выполнять операции, а затем приводить полученное число по модулю n. Более точно: приведение по модулю n является *гомоморфным отображением* кольца целых чисел в кольцо целых по модулю n.

Легко проверяется, что:

$(a + b) \bmod n = [a \pmod n + b \pmod n] \bmod n$,

$(a - b) \bmod n = [a \pmod n - b \pmod n] \bmod n$,

$(a \times b) \bmod n = [a \pmod n \times b \pmod n] \bmod n$,

$[a \times (b + c)] \bmod n = \{[a \times b \pmod n] + [a \times c \pmod n]\} \bmod n$.

Вычисление $a^x \bmod n$ — степени числа a по модулю n как следует из записи можно выполнить как ряд умножений и последним действием выполнить деление получая остаток. Можно вычислить эту степень быстрее, производя возведение в степень как ряд последовательных умножений совместно с приведением по модулю. Это особенно заметно, если работать с большими числами (200 бит и более).

Пример

Если нужно вычислить $a^8 \bmod n$, то выполняют три малых умножения и три малых приведения по модулю:

$((a^2 \bmod n)^2 \bmod n)^2 \bmod n$.

Тем же способом вычисляют

$a^{16} \bmod n = (((a^2 \bmod n)^2 \bmod n)^2 \bmod n)^2 \bmod n$.

Вычисление $a^x \bmod n$, где x не является степенью 2, лишь немного сложнее. Двоичная запись числа x позволяет представить число x как сумму степеней 2:

$x = 25_{(10)} \rightarrow 1\ 1\ 0\ 0\ 1_{(2)}$ — двоичное представление числа 25, поэтому

$25 = 2^4 + 2^3 + 2^0$.

Тогда

$a^{25} \bmod n = (a \times a^{24}) \bmod n = (a \times a^8 \times a^{16}) \bmod n =$

$= a \times ((a^2)^2)^2 \times (((a^2)^2)^2)^2 \bmod n = ((((a^2 \times a)^2)^2)^2 \times a) \bmod n$.

Алгоритм Евклида для нахождения наибольшего общего делителя (НОД). Целое число a делит без остатка другое целое число b, если и только если $b = k \times a$ для некоторого целого числа k (т.е. остаток отделения равен 0). В этом случае a называют *делителем числа b* или *множителем в разложении* числа b на множители.

Пусть a — целое число, большее 1. Тогда a является *простым числом*, если его единственными положительными делителями будут 1 и само a, в противном случае a называется *составным*. Любое целое $n > 1$ может быть представлено единственным образом с точностью до порядка сомножителей как произведение простых.

Существенный с точки зрения криптографии факт состоит в том, что не известно никакого эффективного алгоритма разложения чисел на множители. Более точно: криптографическая стойкость ряда шифров с открытым ключом держится именно на отсутствии эффективного алгоритма разложения чисел на множители (*алгоритма факторизации*).

Наибольший общий делитель чисел a и b, обозначаемый как НОД (a, b), или просто (a, b), — это наибольшее целое, делящее одновременно числа a и b. В эквивалентной форме (a, b) — это то единственное натуральное число, которое делит а и b и делится на любое целое, делящее и a и b. Если НОД $(a, b) = 1$, то целые a и b — *взаимно простые*.

Наибольший общий делитель может быть вычислен с помощью *алгоритма Евклида*. Опишем алгоритм Евклида для нахождения НОД (a, b). Введем обозначения: q_i — частное; r_i — остаток. Тогда алгоритм можно представить в виде следующей цепочки равенств:

$a = b \times q_1 + r_1,\ 0 < r_1 < b,$
$b = r_1 \times q_2 + r_2,\ 0 < r_2 < r_1,$
$r_1 = r_2 \times q_3 + r_3,\ 0 < r_3 < r_2,$
.....
$r_{k-2} = r_{k-1} \times q_k + r_k,\ 0 < r_k < r_{k-1},$
$r_{k-1} = r_k \times q_{k+1}.$

Остановка гарантируется, поскольку остатки r_i от делений образуют строго убывающую последовательность натуральных чисел. Из этой цепочки немедленно получаем, что r_k есть общий делитель чисел a и b и, более того, что любой общий делитель чисел a и b делит и r_k. Таким образом, r_k = НОД (a, b) или $r_k = (a, b)$.

Отметим, что при *операции умножения действительных чисел* нетрудно вычислить мультипликативную обратную величину a^{-1} для ненулевого числа a: $a^{-1} = \frac{1}{a}$ или $a \times a^{-1} = 1$. Например, мультипликативная обратная величина от числа 4 равна $\frac{1}{4}$, поскольку $4 \times \frac{1}{4} = 1$.

Обращаем особое внимание, что при операции умножения по модулю n в кольце $Z/n = \{0, 1, 2, ..., (n-1)\}$ вычисление обратной величины для $a \in Z/n$, т.е. величины x, для которой $a \times x \bmod n = 1$ является более сложной задачей.

Например, решение сравнения $4 \times x \equiv 1 \pmod 7$ эквивалентно нахождению таких значений x и k, что $4 \times x \equiv 7 \times k + 1$, где x и k — целые числа. Общая формулировка этой задачи — нахождение такого целого числа x, что $a \times x \bmod n = 1$, или $a^{-1} \oplus x \bmod n$.

Решение этой задачи иногда существует, но иногда его нет. Например, обратная величина для числа 5 по модулю 14 равна 3, поскольку $5 \times 3 = 15 \equiv 1 \pmod{14}$. С другой стороны, число 2 не имеет обратной величины по модулю 14. Вообще сравнение $a^{-1} \equiv x \pmod n$ имеет единственное решение, тогда и только тогда когда a и n — взаимно простые числа.

В этом случае говорят, что элемент a обратим и его обратный элемент a^{-1} равен x. Часто элемент a^{-1} обозначают через $\frac{1}{a}$. Но надо всегда понимать, что это целый положительный вычет по модулю n.

Множество всех обратимых элементов кольца Z/n называется *мультипликативной группой кольца вычетов* Z/n. Эту группу обозначают через G или $(Z/n)^*$. Оказывается, что элемент а из Z/n обратим, тогда и только тогда, когда он взаимно прост с n, $(a, n) = 1$.

Через $\varphi(n)$ обозначают, так называемую, функцию Эйлера. Значение $\varphi(n)$ от натурального числа n равно числу положительных целых чисел меньших n и взаимно простых с n. В связи с чем, число $|G|$ элементов в *мультипликативной группе вычетов кольца* Z/n равно $\varphi(n)$, $\varphi(n) = |G|$.

Пример

Пусть модуль $n = 10$. Полный набор вычетов по модулю $n = 10$ {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}. Из них только 1, 3, 7, 9 не имеют общего сомножителя с числом 10, т.е. обратимы, $\varphi(10) = 4$, $G = \{1, 3, 7, 9\}$, $|G| = 4$.

Для произведения простых чисел p, q:

$\varphi(p \times q) = (p - 1) \times (q - 1) = n$, $|G| = (p - 1) \times (q - 1)$

В табл. 6.12 приведены значения функции Эйлера для некоторых значений n.

Таблица 6.12

Модуль *n*	**Функция φ(*n*)**
n — простое	$n - 1$
n^2	$n \times (n-1)$
...	...
n^r	$n^{r-1} \times (n - 1)$
$n = p \times q$, (p, q — простые)	$(p - 1) \times (q - 1)$

Вычисления в конечных полях

Конечное поле $F(q)$ с конечным числом q элементов играет важную роль в криптографии. Примерами простейших конечных полей являются кольца вычетов по простому модулю Z/p. В общем случае число элементов конечного поля имеет вид

$$q = p^n,$$

где p — некоторое простое число и $n \geq 1$. Конечные поля называют *полями Галуа*[1] и обозначают $GF(p^n)$ или $GF(p)$ при $n = 1$. Многие криптосистемы шифров с открытым ключом базируются на полях Галуа $GF(p)$, где p — большое простое число.

Пример

Поле Галуа $GF(5)$ имеет элементы 0, 1, 2, 3, 4 и описывается следующими таблицами сложения (табл. 6.13) и умножения (табл. 6.14).

Таблица 6.13

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Таблица 6.14

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Если p — простое, то число $a \in \{1, ..., p - 1\}$ является взаимно простым с p, и поэтому обратный элемент a^{-1} существует. Тем самым однозначно определяется операция деления.

Обозначим через $GF^*(p)$ множество всех ненулевых элементов поля $GF(p)$. Некоторый элемент g из $GF^*(p)$ называют *образующим* или *порождающим элементом* $GF^*(p)$, если для всех a из $GF^*(p)$ найдется такое целое x, что $g^x = a \bmod p$.

Всего имеется $\varphi(p - 1)$ образующих элементов g. Число x называют *дискретным логарифмом элемента a* по основанию g и модулю p. Вычисление дискретных логарифмов (когда заданы g, a и p) примерно такая же труднорешаемая задача, как и задача разложения целого числа на множители. Криптографическая стойкость ряда шифров с открытым ключом держится именно на отсутствии эффективного алгоритма вычисления дискретных логарифмов.

Итак, ознакомившись с основами модулярной арифметики и элементами вычисления в конечных полях, можем перейти к рассмотрению алгоритмов асимметричного шифрования.

[1] Именуемые так в честь французского математика, основателя современной высшей алгебры Эвариста Галуа (1811–1832).

Алгоритм Диффи – Хеллмана

Мартин Хеллман (слева) и Уитфилд Диффи

В 1976 г. Мартин Хеллман (род. в 1945 г.) и Уитфилд Диффи (род. в 1944 г.) предложили на тот момент революционную концепцию криптографии с открытым ключом.

Алгоритм Диффи – Хеллмана использует функцию дискретного возведения в степень. Сначала генерируются два больших простых числа n и q. Эти два числа не обязательно хранить в секрете. Далее один из партнеров P_1 генерирует случайное число x и посылает другому участнику будущих обменов P_2 значение

$$A = q^x \bmod n.$$

По получении A партнер P_2 генерирует случайное число y и посылает участнику обмена P_1 вычисленное значение

$$B = q^y \bmod n.$$

Партнер P_1, получив B, вычисляет $K_x = B^x \bmod n$, а партнер P_2 вычисляет $K_y = A^y \bmod n$. Алгоритм гарантирует, что числа K_y и K_x равны и могут быть использованы в качестве секретного ключа для шифрования. Ведь даже перехватив числа A и B, трудно вычислить K_x или K_y. Схематично, работа алгоритма Диффи – Хеллмана представлена на рис. 6.17.

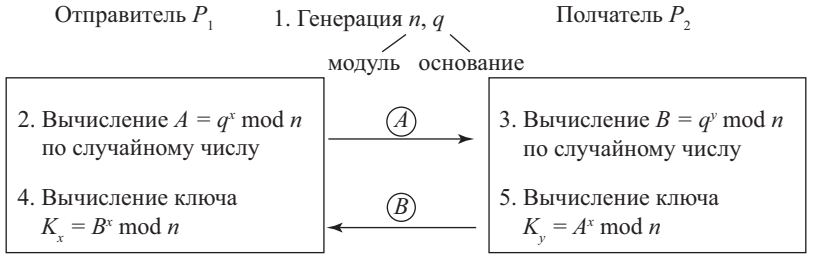


Рис. 6.17. Алгоритм Диффи – Хеллмана

Пример

Рассмотрим пример работы алгоритма Диффи – Хеллмана на небольших целых числах (в современных асимметричных криптосистемах длины чисел выбираются от 512 бит):

$n = 5$, $q = 7$, $x = 3$, $y = 2$;

$A = 7^3 \pmod 5 = 343 \pmod 5 = 3$; $\quad B = 7^2 \pmod 5 = 49 \pmod 5 = 4$;

$K_x = 4^3 \pmod 5 = 64 \pmod 5 = 4$; $\quad K_y = 3^2 \pmod 5 = 4$.

Алгоритм Диффи – Хеллмана, обеспечивая конфиденциальность передачи ключа, не может гарантировать того, что он прислан именно тем партнером, который предполагается. Для решения этой проблемы (аутентификации пользователя) был предложен протокол STS (station-to-station). Этот протокол для идентификации отправителя использует технику электронной подписи, о чем мы поговорим в следующей главе.

Алгоритм RSA

Р. Ривест, Э. Шамир, Л. Адлеман (слева направо)

Первое практическое воплощение принцип открытого шифрования получил в системе RSA, разработанной в 1977 г. в Массачусетском Технологическом Институте (США) и получившей свое название RSA от первых букв фамилий авторов: Рональд Ривест, Эди Шамир, Леонард Адлеман.

В криптосистеме RSA открытый ключ k_o, секретный ключ k_c, сообщение M и криптограмма C принадлежат кольцу целых чисел $Z/N = \{0, 1, 2, ..., N-1\}$ по модулю N, где $N = P \times Q$, P и Q — случайные большие *простые* числа.

Открытый ключ k_o выбирают случайным образом так, чтобы выполнялись условия:

$1 < k_o \le \varphi(N)$,
НОД $(k_o, \varphi(N)) = 1$,
$\varphi(N) = (P-1) \times (Q-1)$,

где $\varphi(N)$ — функция Эйлера — количество положительных целых чисел в интервале от 1 до N взаимно простых с N.

НОД $(k_o, \varphi(N)) = 1$, следовательно, используя алгоритм Евклида, вычисляется секретный ключ k_c, такой, что

$k_c \times k_o \equiv 1 \bmod \varphi(N)$.

Это можно осуществить, так как получатель знает пару простых чисел (P, Q) и может легко найти $\varphi(N)$. Открытый ключ k_o используют для зашифрования данных, а секретный ключ k_c — для расшифрования.

Криптограмма C определяется через пару (открытый ключ k_o, сообщение M)

$C = M^{ko} \pmod N$.

В качестве алгоритма быстрого вычисления значения C используют ряд последовательных возведений в квадрат целого M и умножений на M с приведением по модулю N.

Обращение функции $C = M^{ko} \pmod N$, т.е. определение значения M по известным значениям C, k_o и N, практически не осуществимо при $N \approx 2^{512}$.

Однако обратную задачу, т.е. задачу расшифрования криптограммы C, можно решить, используя пару (секретный ключ k_c, криптограмма C) по следующей формуле расшифрования:

$M = C^{kc} \pmod N$.

Открытый и шифрованный тексты эффективно вычисляются, если известны k_o и k_c при помощи алгоритма быстрого возведения в степень. Если искать секретный ключ k_c по известному открытому ключу k_o, то надо знать $\varphi(N)$.

Таким образом, получатель, который создает криптосистему, защищает два параметра:

1) секретный ключ k_c;

2) пару чисел (P, Q), произведение которых дает значение модуля N.

С другой стороны, получатель открывает значение модуля N и открытый ключ k_o, т.е. противнику могут быть известны лишь значения k_o и N. Если бы он смог разложить число N на множители P и Q, то он узнал бы тройку чисел $\{P, Q, k_o\}$, вычислил значение функции Эйлера $\varphi(N) = (P-1)(Q-1)$ и определил значение секретного ключа k_c. Однако, как уже отмечалось, разложение очень большого N на множители вычислительно не осуществимо (при условии, что длины выбранных P и Q составляют не менее 100 десятичных знаков). Для обеспечения максимальной безопасности выбирают P и Q равной длины и хранят в секрете.

Процедуры шифрования и расшифрования в криптосистеме RSA. Предположим, что пользователь A хочет передать пользователю B сообщение в зашифрованном виде, используя криптосистему RSA. В таком случае пользователь A выступает в роли отправителя сообщения, а пользователь B — в роли получателя. Как отмечалось выше, криптосистему RSA должен сформировать получатель сообщения, т.е. пользователь B. Рассмотрим последовательность действий пользователя B и пользователя A.

1. Пользователь B выбирает два произвольных больших простых числа P и Q (напомним, что в современных асимметричных криптосистемах длины чисел P и Q выбираются от 512 бит).

2. Пользователь B вычисляет значение модуля $N = P \times Q$.

3. Пользователь B вычисляет функцию Эйлера $\varphi(N) = (P-1)(Q-1)$ и выбирает случайным образом значение открытого ключа k_o с учетом выполнения условий: $1 < k_o \le \varphi(N)$, НОД $(k_o, \varphi(N)) = 1$.

4. Пользователь B вычисляет значение секретного ключа k_c, используя алгоритм Евклида при решении сравнения $k_c \equiv k_o^{-1} \pmod{\varphi(N)}$.

5. Пользователь B пересылает пользователю A пару чисел (N, k_o) по незащищенному каналу.

Если пользователь A хочет передать пользователю B сообщение M, он выполняет следующие шаги.

6. Пользователь A разбивает исходный открытый текст M на блоки, каждый из которых может быть представлен в виде числа $M_i \in \{0, 1, 2, ..., N-1\}$.

7. Пользователь A шифрует текст, представленный в виде последовательности чисел M_i по формуле $C_i = M_i^{ko} \pmod{N}$ и отправляет криптограмму $C_1, C_2, C_3, ..., C_i, ...$ пользователю B.

8. Пользователь B расшифровывает принятую криптограмму $C_1, C_2, C_3, ..., C_i, ...$, используя секретный ключ k_c, по формуле $M_i = C_i^{kc} \pmod{N}$.

В результате будет получена последовательность чисел M_i, которые представляют собой исходное сообщение M. Чтобы алгоритм RSA имел практическую ценность, необходимо иметь возможность без существенных затрат генерировать большие простые числа, уметь оперативно вычислять значения ключей k_o и k_c.

Пример

Рассмотрим пример работы алгоритма RSA на небольших целых числах (в современных асимметричных криптосистемах длины чисел выбираются от 512 бит):

1) пусть пользователь A выбирает $P = 3$, $Q = 11$;
2) тогда $N = P \times Q = 33$;
3) функция Эйлера: $\varphi(N) = (P-1) \times (Q-1) = 2 \times 10 = 20$, и значение открытого ключа можем выбрать $k_o = 7$ с учетом выполнения условий: $1 < k_o \le \varphi(N)$, НОД $(k_o, \varphi(N)) = 1$;
4) начение секретного ключа $k_c = 3$, вычислили из сравнения $k_c \times k_o \equiv 1 \pmod{\varphi(N)}$, так как $7 \times 3 \equiv 1 \pmod{20}$;
5) пара чисел $(N = 33, k_o = 7)$ по незащищенному каналу передается пользователю B;
6) пусть текст пользователя A для зашифрования имеет вид: $M_1 = 3$, $M_2 = 2$;
7) тогда исходя из процедуры шифрования:
   $C_i = M_i^{ko} \pmod{N}$, криптограмма будет иметь вид: (9,29)
   $C_1 = 3^7 \bmod 33 = 2187 \bmod 33 = 9$,
   $C_2 = 2^7 \bmod 33 = 128 \bmod 33 = 29$;
8) пользователь B, расшифровывая принятую криптограмму $C_1, C_2, C_3, ..., C_i, ...$, на секретном ключе $k_c = 3$, по формуле $M_i = C_i^{kc} \pmod{N}$:
   $M_1 = 9^3 \bmod 33 = 729 \bmod 33 = 3$,
   $M_2 = 29^3 \bmod 33 = 243899 \bmod 33 = 2$,
   востанавливает открытый текст (3,2).

Алгоритм Эль Гамаля

Тахер Эль Гамаль
(род. в 1955 г.)

Тахер Эль Гамаль египетский криптограф. В 1985 г. он опубликовал статью под названием «Криптосистема с открытым ключом и схема цифровой подписи на основе дискретных логарифмов», в которой представил свои разработки по созданию систем асимметричного шифрования и цифровой подписи, основанных на сложности проблемы дискретного логарифмирования.

Схема Эль Гамаля может быть использована как для шифрования, так и для электронных подписей. Безопасность схемы Эль Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

Для того чтобы генерировать пару ключей (открытый ключ – секретный ключ), сначала выбирают некоторое большое простое число P и большое целое число G, причем $G < P$. Числа P и G могут быть распространены среди группы пользователей.

Затем выбирают случайное целое число X, причем $X < P$. Число X является секретным ключом и должно храниться в секрете.

Далее вычисляют $Y = G^X \bmod P$. Число Y является открытым ключом.

Для того чтобы зашифровать сообщение M, выбирают случайное целое число K, $1 < K < (P-1)$, такое, что числа K и $(P-1)$ являются взаимно простыми.

Затем вычисляют

$a = G^K \bmod P$,
$b = Y^K M \bmod P$.

Пара чисел (a, b) является шифртекстом. Заметим, что длина шифртекста вдвое больше длины исходного открытого текста M.

Для того чтобы расшифровать шифртекст (a, b), вычисляют

$b \times a^{-X} = M \bmod P$.

Пример

1) выберем $P = 11$, $G = 2$ (помним, что в реальных криптосистемах с открытым ключом эти числа имеют длину порядка 512 бит), секретный ключ $X = 8$ выбрали исходя из условия $X < P$;
2) вычисляем
   $Y = G^X \bmod P = 2^8 \bmod 11 = 256 \bmod 11 = 3$,
   таким образом открытый ключ $Y = 3$;
3) пусть сообщение $M = 5$;
4) выберем некоторое случайное число $K = 9$ и убедимся, что НОД $(K, P-1) = 1$ — действительно, НОД (9, 10) = 1;

5) вычисляя пару чисел a и b:
$a = G^K \bmod P = 2^9 \bmod 11 = 512 \bmod 11 = 6$,
$b = Y^K M \bmod P = 3^9 \times 5 \bmod 11 = 19\,683 \times 5 \bmod 11 = 9$,
получим шифртекст $(a, b) = (6, 9)$;
6) выполним расшифрование этого шифртекста, используя секретный ключ X:
$M = b \times a^{-X} \bmod P = 9 \times 6^{-8} \bmod 11$,
выражение $9 \times 6^{-8} \bmod 11$ можно представить в виде: $6^8 \times M \equiv 9 \bmod 11$ или $1\,679\,616 \times M \equiv 9 \bmod 11$.
Решая данное сравнение, находим открытий текст: $M = 5$.

6.5. Электронная подпись

Обмен электронными документами по телекоммуникационным сетям существенно снижает затраты на обработку и хранение документов, ускоряется их поиск, однако при этом возникает проблема аутентификации, т.е. установления подлинности автора и отсутствия изменений в полученном документе.

При обработке документов в электронной форме непригодны традиционные способы установления подлинности по рукописной подписи и оттиску печати на бумажном документе, здесь принципиально новым решением является электронная подпись.

Электронная подпись (ЭЦП) — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию[1].

Первая схема электронной цифровой подписи[2] RSA была разработана еще в конце 1970-х гг., однако проблема подтверждения авторства стала актуальной настолько, что в 1990-х гг. потребовалось установление стандарта. Причиной послужило повсеместное расширение глобальной сети Интернет и массовое распространение электронной торговли и оказания услуг. Именно по указанной причине стандарты ЭЦП в России и США были приняты практически одновременно, в 1994 г.

Из предложенных схем ЭЦП наиболее удачными оказались RSA и схема Эль Гамаля. Первая из них была запатентована в США и в ряде других стран (патент на RSA прекратил свое действие не так давно).

[1] Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» , принятый взамен ранее действовавшего Федерального закона от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи».

[2] Согласно упомянутому Федеральному закону № 63-ФЗ понятия «электронная подпись» и «электронная цифровая подпись» считаются синонимами.

У второй схемы существует большое количество возможных модификаций, и все их запатентовать было весьма затруднительно. Именно по этой причине схема ЭЦП Эль Гамаля осталась по большей части свободной от патентов.

Процедуры постановки и проверки электронной подписи

ЭЦП используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. Функционально она аналогична обычной рукописной подписи и обладает основными ее достоинствами:
- удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
- не дает самому этому лицу возможность отказаться от обязательств, связанных с подписанным текстом;

и дополнительным свойством — гарантирует целостность подписанного текста.

ЭЦП представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом, и включает две процедуры:
- процедуру постановки подписи, в которой используется секретный ключ отправителя сообщения;
- процедуру проверки подписи, в которой используется открытый ключ отправителя.

Процедура постановки подписи

При формировании ЭЦП отправитель прежде всего вычисляет значение хэш-функции $m = H(M)$ подписываемого текста M. Вычисленное значения хэш-функции $H(M)$ представляет собой один короткий блок информации m, характеризующий весь текст M в целом. Затем значение m шифруется секретным ключом отправителя. Получаемая при этом пара чисел и представляет собой ЭЦП для данного текста M.

Процедура проверки подписи

При проверке ЭЦП получатель сообщения снова вычисляет хэш-функцию $m = H(M)$ принятого по каналу текста M, после чего при помощи открытого ключа отправителя проверяет, соответствует ли полученная подпись вычисленному значению m хэш-функции.

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа. Каждая подпись, как правило, содержит следующую информацию:
- дату подписи;
- срок окончания действия ключа данной подписи;
- информацию о лице, подписавшем текст;
- идентификатор подписавшего (имя открытого ключа);
- собственно цифровую подпись.

Однонаправленные хэш-функции

Обычно на практике хэш-функция сжимает подписываемый документ M до нескольких десятков или сотен бит. Хэш-функция $H(\cdot)$ принимает в качестве аргумента сообщение (документ) M произвольной длины и возвращает хэш-значение $H(M) = z$ фиксированной длины. Как было отмечено ранее, хэшированная информация является сжатым двоичным представлением основного сообщения произвольной длины. Напомним, что значение хэш-функции $H(M)$ сложным образом зависит от документа M и не позволяет восстановить сам документ M.

Хэш-функция должна удовлетворять целому ряду условий:

- хэш-функция должна быть чувствительна к всевозможным изменениям в тексте M, таким как вставки, выбросы, перестановки и т.п.;
- хэш-функция должна обладать свойством необратимости, т.е. задача подбора документа M', который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима;
- вероятность того, что значения хэш-функций двух различных документов (вне зависимости от их длин) совпадут, должна быть ничтожно мала.

Большинство хэш-функций строится на основе однонаправленной функции $f(\cdot)$, которая образует выходное значение длиной n при задании двух входных значений длиной n (рис. 6.18). Этими входами являются блок исходного текста M_i и хэш-значение R_{i-1} предыдущего блока текста:

$$R_i = f(M_i, R_{i-1}).$$

Хэш-значение, вычисляемое при вводе последнего блока текста, становится хэш-значением всего сообщения M.

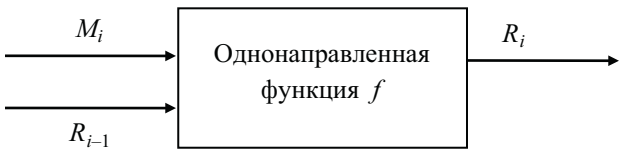


Рис. 6.18. Построение однонаправленной хэш-функции

В результате однонаправленная хэш-функция всегда формирует выход фиксированной длины n (независимо от длины входного текста).

Однонаправленные хэш-функции на основе симметричных блочных алгоритмов. Однонаправленную хэш-функцию можно построить, используя симметричный блочный алгоритм. Наиболее очевидный подход состоит в том, чтобы шифровать сообщение M посредством блочного алгоритма в специальных режимах CBC — сцепление блоков шифра или CFB — обратная связь по шифртексту с помощью фиксированного ключа и некоторого вектора инициализации. Последний блок шифртекста можно рассматривать в качестве хэш-значения сообщения M.

При таком подходе не всегда возможно построить безопасную однонаправленную хэш-функцию, но всегда можно получить код аутентификации сообщения MAC (Message Authentication Code).

Более безопасный вариант хэш-функции можно получить, используя блок сообщения в качестве ключа, предыдущее хэш-значение — в качестве входа, а текущее хэш-значение — в качестве выхода. Реальные хэш-функции проектируются еще более сложными. Длина блока обычно определяется длиной ключа, а длина хэш-значения совпадает с длиной блока.

Поскольку большинство блочных алгоритмов являются 64-битовыми, некоторые схемы хэширования проектируют так, чтобы хэш-значение имело длину, равную двойной длине блока.

Если принять, что получаемая хэш-функция корректна, безопасность схемы хэширования базируется на безопасности лежащего в ее основе блочного алгоритма. Схема хэширования, у которой длина хэш-значения равна длине блока, показана на рис. 6.19.

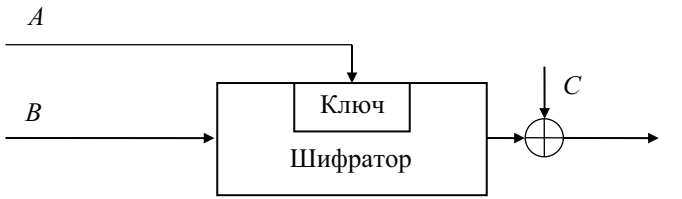


Рис. 6.19. Обобщенная схема формирования хэш-функции

Ее работа описывается выражениями:

$$R_0 = I_R,$$
$$R_i = E_A(B) \oplus C,$$

где I_R — некоторое случайное начальное значение; A, B и C могут принимать значения M_i, R_{i-1}, $(M_i \oplus R_{i-1})$ или быть константами; E_A — функция шифрования на ключе A.

Здесь сообщение M разбивается на блоки M_i принятой длины, которые обрабатываются поочередно. На рис. 6.20 приведены четые варианта реализации схем хэширования, у которых длина хэш-значения равна длине блока.

Алгоритм цифровой подписи RSA

Рассмотрим подробно процедуры постановки и проверки электронной подписи с использованием алгоритма RSA.

Сначала необходимо вычислить пару ключей (секретный ключ и открытый ключ). Для этого отправитель электронных документов вычисляет два больших простых числа P и Q, затем находит их произведение $N = P \times Q$ и значение функции Эйлера:

$$\varphi(N) = (P-1) \times (Q-1).$$

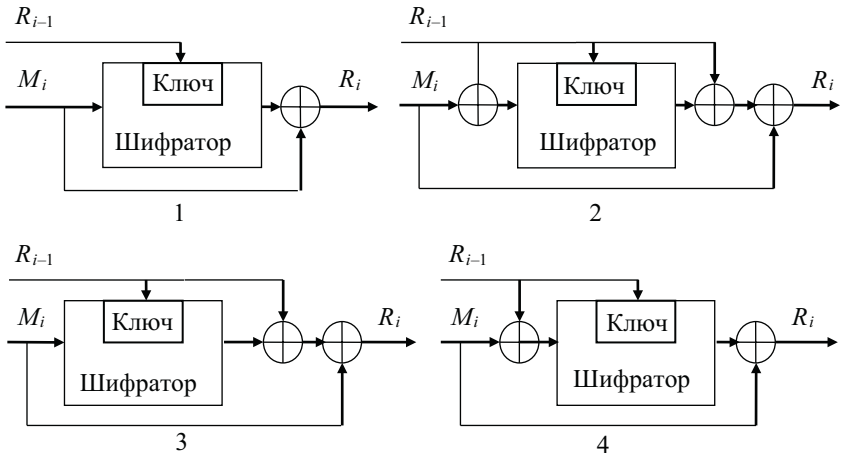


Рис. 6.20. Четыре схемы безопасного хэширования

Далее отправитель вычисляет число E из условий:

$E \le \varphi(N)$, НОД $(E, \varphi(N)) = 1$

и число D из условий:

$D < N$, $E \times D \equiv 1 \pmod{\varphi(N)}$.

Пара чисел (E, N) является открытым ключом. Эту пару чисел автор передает партнерам по переписке для проверки его цифровых подписей. Число D сохраняется отправителем как секретный ключ для подписывания. Обобщенная схема формирования и проверки цифровой подписи RSA показана на рис. 6.21.

Допустим, что отправитель хочет подписать сообщение M перед его отправкой. Сначала сообщение M (блок информации, файл, таблица) сжимают с помощью хэш-функции $H(\cdot)$ в целое число m:

$m = H(M)$.

Затем вычисляют цифровую подпись S под электронным документом M, используя хэш-значение m и секретный ключ D:

$S = m^D \pmod{N}$.

Пара (M, S) передается партнеру-получателю как электронный документ M, подписанный цифровой подписью S, причем подпись S сформирована обладателем секретного ключа D.

После приема пары (M, S) получатель вычисляет хэш-значение сообщения M двумя разными способами. Прежде всего он восстанавливает хэш-значение m', применяя криптографическое преобразование подписи S с использованием открытого ключа E:

$m' = S^E \pmod{N}$.

Кроме того, он находит результат хэширования принятого сообщения M с помощью такой же хэш-функции $H(\cdot)$: $m = H(M)$.

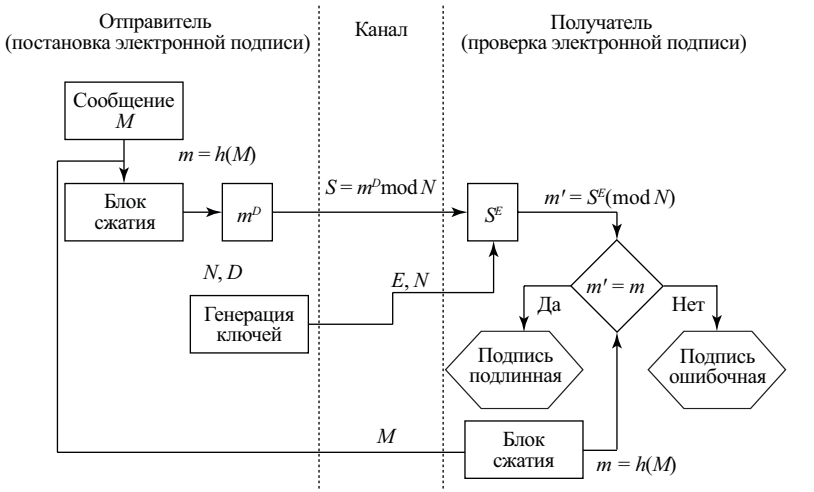


Рис. 6.21. Обобщенная схема формирования и проверки цифровой подписи RSA

Если соблюдается равенство вычисленных значений, т.е.

$S^E \pmod{N} = H(M)$,

то получатель признает пару (M, S) подлинной. Доказано, что только обладатель секретного ключа D может сформировать цифровую подпись S по документу M, а определить секретное число D по открытому числу E не легче, чем разложить модуль N на множители.

Кроме того, можно строго математически доказать, что результат проверки цифровой подписи S будет положительным только в том случае, если при вычислении S был использован секретный ключ D, соответствующий открытому ключу E. Поэтому открытый ключ E иногда называют «идентификатором» подписавшего.

6.6. Управление криптографическими ключами

Любой шифр использует ключи. В симметричной криптосистеме, как уже указывалось, отправитель и получатель сообщения используют один и тот же секретный ключ. Этот ключ должен быть неизвестен всем остальным и должен периодически обновляться одновременно у отправителя и получателя. Процесс распределения (рассылки) секретных ключей между участниками информационного обмена в симметричных криптосистемах имеет весьма сложный характер.

Асимметричная криптосистема предполагает использование двух ключей — открытого и секретного. Открытый ключ можно разглашать,

а личный надо хранить в тайне. При обмене сообщениями необходимо пересылать только открытый ключ. Важным требованием является обеспечение подлинности отправителя сообщения. Это достигается путем взаимной аутентификации участников информационного обмена.

Под ключевой информацией понимают совокупность всех действующих ключей в системах обработки информации. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации.

Управление ключами — информационный процесс, включающий реализацию следующих основных функций:

– генерация ключей;
– хранение ключей;
– распределение ключей.

Генерация и хранение ключей

Безопасность любого криптографического алгоритма определяется используемым криптографическим ключом. Добротные криптографические ключи должны иметь достаточную длину и случайные значения битов. Для получения ключей используются аппаратные и программные средства генерации случайных значений ключей. Как правило, применяют датчики псевдослучайных чисел.

Генерация сеансового ключа для симметричных криптосистем. Один из методов генерации сеансового ключа для симметричных криптосистем описан в стандарте ANSI X9.17. Он предполагает использование криптографического алгоритма DES (хотя можно применить и другие симметричные алгоритмы шифрования). Введем следующие обозначения:

$E_K(X)$ — результат шифрования алгоритмом DES значения X;

K — ключ, зарезервированный для генерации секретных ключей;

V_0 — секретное 64-битовое начальное число;

T — временная отметка.

Схема генерации случайного сеансового ключа R_i в соответствии со стандартом

ANSI X 9.17 показана на рис. 6.22.

Случайный ключ R_i генерируют, вычисляя значение

$$R_i = E_K(E_K(T_i) \oplus V_i).$$

Следующее значение V_{i+1} вычисляют так:

$$V_{i+1} = E_K(E_K(T_i) \oplus R_i).$$

Если необходим 128-битовый случайный ключ, генерируют пару ключей R_i, R_{i+1} и объединяют их вместе.

Если ключ не меняется регулярно, это может привести к его раскрытию и утечке информации. Регулярную замену ключа можно осуществить, используя процедуру модификации ключа.

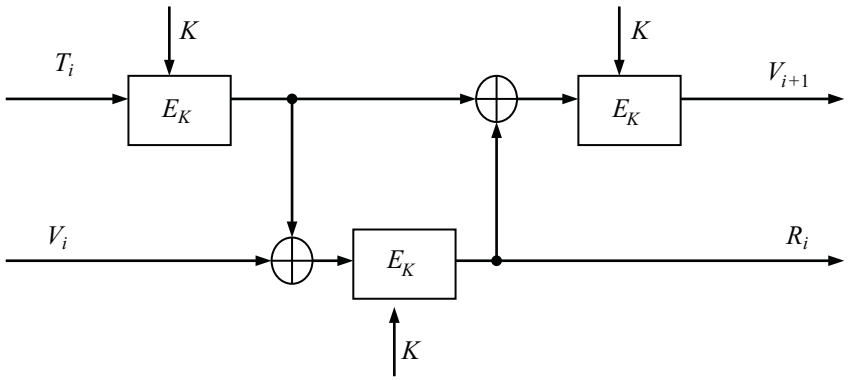


Рис. 6.22. Схема генерации случайного ключа R_i в соответствии со стандартом ANSI X9.17

Модификация ключа — это генерирование нового ключа из предыдущего значения ключа с помощью односторонней (однонаправленной) функции. Участники информационного обмена разделяют один и тот же ключ и одновременно вводят его значение в качестве аргумента в одностороннюю функцию, получая один и тот же результат. Затем они берут определенные биты из этих результатов, чтобы создать новое значение ключа.

Генерация ключей для асимметричных криптосистем с открытыми ключами много сложнее, потому что эти ключи, как уже указывалось ранее, должны обладать определенными математическими свойствами.

Хранение ключей. Под функцией хранения ключей понимают организацию их безопасного хранения, учета и удаления. Ключ является самым привлекательным для злоумышленника объектом, открывающим ему путь к конфиденциальной информации. Поэтому вопросам безопасного хранения ключей уделяют особое внимание. Секретные ключи никогда не должны записываться в явном виде на носителе, который может быть считан или скопирован.

Носители ключевой информации. Ключевой носитель может быть технически реализован различным образом на разных носителях информации.

Электронные пластиковые карты становятся в настоящее время наиболее распространенным и универсальным носителем конфиденциальной информации, который позволяет идентифицировать и аутентифицировать пользователей, хранить криптографические ключи, пароли и коды.

Интеллектуальные карты (смарт-карты), обладающие наибольшими возможностями, не только эффективно применяются для хранения ключевой информации, но и широко используются в электронных платежных системах, в комплексных решениях для медицины, транспорта, связи, образования и т.п.

Распределение ключей

Распределение ключей — самый ответственный процесс в управлении ключами. К нему предъявляются следующие требования:

– оперативность и точность распределения;
– скрытность распределяемых ключей.

Распределение ключей между пользователями компьютерной сети реализуется двумя способами:

– использованием одного или нескольких центров распределения ключей;
– прямым обменом сеансовыми ключами между пользователями сети.

Недостаток первого подхода состоит в том, что центру распределения ключей известно, кому и какие ключи распределены, и это позволяет читать все сообщения, передаваемые по сети. Возможные злоупотребления существенно влияют на защиту. При втором подходе проблема состоит в том, чтобы надежно удостоверить подлинность субъектов сети.

В обоих случаях должна быть обеспечена подлинность сеанса связи. Это можно осуществить, используя механизм запроса-ответа или механизм отметки времени.

Механизм запроса-ответа заключается в следующем. Пользователь *A* включает в посылаемое сообщение (запрос) для пользователя *B* непредсказуемый элемент (например, случайное число). При ответе пользователь *B* должен выполнить некоторую операцию с этим элементом (например, добавить единицу), что невозможно осуществить заранее, поскольку неизвестно, какое случайное число придет в запросе. После получения результата действий пользователя *B* (ответ) пользователь *A* может быть уверен, что сеанс является подлинным.

Механизм отметки времени предполагает фиксацию времени для каждого сообщения. Это позволяет каждому субъекту сети определить, насколько старо пришедшее сообщение, и отвергнуть его, если появится сомнение в его подлинности. При использовании отметок времени необходимо установить допустимый временной интервал задержки.

В обоих случаях для защиты элемента контроля используют шифрование, чтобы быть уверенным, что ответ отправлен не злоумышленником и не изменен штемпель отметки времени.

Задача распределения ключей сводится к построению протокола распределения ключей, обеспечивающего:

– взаимное подтверждение подлинности участников сеанса;
– подтверждение достоверности сеанса механизмом запроса-ответа или отметки времени;
– использование минимального числа сообщений при обмене ключами;
– возможность исключения злоупотреблений со стороны центра распределения ключей (вплоть до отказа от него).

В основу решения задачи распределения ключей целесообразно положить принцип отделения процедуры подтверждения подлинности партнеров от процедуры собственно распределения ключей. Цель такого подхода состоит в создании метода, при котором после установления подлинности участники сами формируют сеансовый ключ без участия центра распределения ключей с тем, чтобы распределитель ключей не имел возможности выявить содержание сообщений.

Распределение ключей с участием центра распределения ключей. При распределении ключей между участниками предстоящего информационного обмена должна быть гарантирована подлинность сеанса связи. Для взаимной проверки подлинности партнеров приемлема *модель рукопожатия*. В этом случае ни один из участников не будет получать никакой секретной информации во время процедуры установления подлинности.

Взаимное установление подлинности гарантирует вызов нужного субъекта с высокой степенью уверенности, что связь установлена с требуемым адресатом и никаких попыток подмены не было. Реальная процедура организации соединения между участниками информационного обмена включает как этап распределения, так и этап подтверждения подлинности партнеров.

При включении в процесс распределения ключей центра распределения ключей осуществляется его взаимодействие с одним или обоими участниками сеанса с целью распределения секретных или открытых ключей, предназначенных для использования в последующих сеансах связи.

Следующий этап — подтверждение подлинности участников — содержит обмен удостоверяющими сообщениями, чтобы иметь возможность выявить любую подмену или повтор одного из предыдущих вызовов.

Протокол аутентификации и распределения ключей для симметричных криптосистем

Рассмотрим в качестве примера протокол аутентификации и распределения ключей Kerberos (по-русски — Цербер). Протокол Kerberos спроектирован для работы в сетях TCP/IP и предполагает участие в аутентификации и распределении ключей третьей доверенной стороны. Kerberos обеспечивает надежную аутентификацию в сети, разрешая законному пользователю доступ к различным машинам в сети. Протокол Kerberos основывается на симметричных шифрах (реализован алгоритм DES, хотя возможно применение и других симметричных криптоалгоритмов). Kerberos вырабатывает отдельный секретный ключ для каждого субъекта сети, и знание такого секретного ключа равносильно доказательству подлинности субъекта сети.

В протоколе Kerberos участвуют две взаимодействующие стороны *A* и *B* и доверенный сервер KS (Kerberos Server). Стороны *A* и *B* каждая по отдельности разделяют свой секретный ключ с сервером KS. Доверенный сервер KS выполняет роль центра распределения ключей ЦРК.

Пусть сторона A хочет получить сеансовый ключ для информационного обмена со стороной B.

Сторона A инициирует фазу распределения ключей, посылая по сети серверу KS идентификаторы Id_A и Id_B:

$$A \rightarrow \text{KS}: Id_{\text{A}}, Id_{B}. \quad (1)$$

Сервер KS генерирует сообщение с временной отметкой T, сроком действия L, случайным сеансовым ключом K и идентификатором Id_{A}. Он шифрует это сообщение секретным ключом, который разделяет со стороной B.

Затем сервер KS берет временную отметку T, срок действия L, сеансовый ключ K, идентификатор Id_B стороны B и шифрует все это секретным ключом, который разделяет со стороной A. Оба эти зашифрованные сообщения он отправляет стороне A:

$$\text{KS} \rightarrow A: E_{\text{A}}(T, L, K, Id_B), E_B(T, L, K, Id_{\text{A}}). \quad (2)$$

Сторона A расшифровывает первое сообщение своим секретным ключом, проверяет отметку времени T, чтобы убедиться, что это сообщение не является повторением предыдущей процедуры распределения ключей.

Затем сторона A генерирует сообщение со своим идентификатором Id_{A} и отметкой времени T, шифрует его сеансовым ключом K и отправляет стороне B. Кроме того, A отправляет для B сообщение от KS, зашифрованное ключом стороны B:

$$A \rightarrow B: E_K(Id_A, T), E_B(T, L, K, Id_A). \quad (3)$$

Только сторона B может расшифровать сообщения (3). Сторона B получает отметку времени T, срок действия L, сеансовый ключ K и идентификатор Id_{A}. Затем сторона B расшифровывает сеансовым ключом K вторую часть сообщения (3). Совпадение значений T и Id_{A} в двух частях сообщения подтверждают подлинность A по отношению к B.

Для взаимного подтверждения подлинности сторона B создает сообщение, состоящее из отметки времени T плюс 1, шифрует его ключом K и отправляет стороне A:

$$B \rightarrow A: E_K(T+1). \quad (4)$$

Если после расшифрования сообщения (4) сторона A получает ожидаемый результат, она знает, что на другом конце линии связи находится действительно B.

Этот протокол успешно работает при условии, что часы каждого участника синхронизированы с часами сервера KS. Следует отметить, что в этом протоколе необходим обмен с KS для получения сеансового ключа каждый раз, когда A желает установить связь с B. Протокол обеспечивает надежное соединение объектов A и B при условии, что ни один из ключей не скомпрометирован и сервер KS защищен.

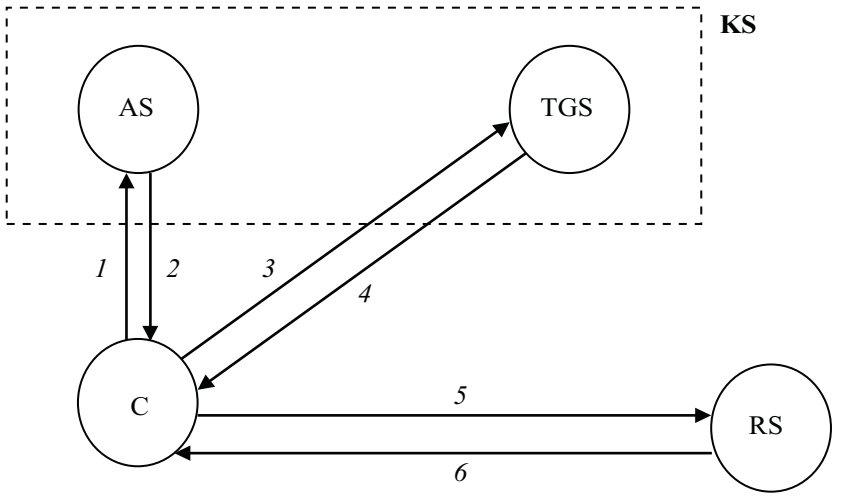


Рис. 6.23. Схема протокола Kerberos:
KS – сервер системы Kerberos; AS – сервер идентификации; TGS – сервер выдачи разрешений; RS – сервер информационных ресурсов; C – клиент системы Kerberos; *1* — запрос разрешить обратиться к TGS; *2* — разрешение обратиться к TGS; *3* – запрос на допуск к RS; *4* – разрешение на допуск к RS; *5* – запрос на получение информационного ресурса от RS; *6* – подтверждение подлинности сервера RS и предоставление ресурса

Система Kerberos обеспечивает защиту сети от несанкционированного доступа, базируясь исключительно на программных решениях, и предполагает многократное шифрование передаваемой по сети управляющей информации.

Система Kerberos имеет структуру типа клиент-сервер и состоит из клиентских частей C, установленных на все машины сети (рабочие станции пользователей и серверы), и Kerberos-сервера KS, располагающегося на каком-либо (не обязательно выделенном) компьютере.

Kerberos-сервер, в свою очередь, можно разделить на две части: сервер идентификации AS (Authentication Server) и сервер выдачи разрешений TGS (Ticket Granting Server). Информационными ресурсами, необходимыми клиентам C, управляет сервер информационных ресурсов RS (рис. 6.23).

Область действия системы Kerberos распространяется на тот участок сети, все пользователи которого зарегистрированы под своими именами и паролями в базе данных Kerberos-сервера.

Укрупненно процесс идентификации и аутентификации пользователя в системе Kerberos можно представить следующим образом. Пользователь (клиент) C, желая получить доступ к ресурсу сети, направляет запрос

серверу идентификации AS. Последний идентифицирует пользователя с помощью его имени и пароля и выдает разрешение на доступ к серверу выдачи разрешений TGS, который в свою очередь по запросу клиента C разрешает использование необходимых ресурсов сети с помощью целевого сервера информационных ресурсов RS.

Данная модель взаимодействия клиента с серверами может функционировать только при условии обеспечения конфиденциальности и целостности передаваемой управляющей информации. Без строгого обеспечения информационной безопасности клиент не может отправлять серверам AS, TGS и RS свои запросы и получать разрешения на доступ к обслуживанию в сети. Чтобы избежать возможности перехвата и несанкционированного использования информации, Kerberos применяет при передаче любой управляющей информации в сети сложную систему многократного шифрования с использованием комплекса секретных ключей (секретный ключ клиента, секретный ключ сервера, секретные сеансовые ключи, клиент-сервер).

6.7. Современные приложения криптографии

В современном мире значение криптографии выходит далеко за рамки обеспечения секретности данных. По мере все большей автоматизации передачи и обработки информации и интенсификации информационных потоков ее методы приобретают уникальное значение.

Отметим некоторые современные направления ее приложения:

– защита от несанкционированного чтения, или обеспечение конфиденциальности информации;
– защита от навязывания ложных сообщений, как умышленных, так и непреднамеренных;
– идентификация (*identification)* — некое описательное представление какого-либо субъекта;
– контроль целостности информации;
– аутентификация *(authentication)* — проверка подлинности;
– электронная подпись;
– системы тайного электронного голосования;
– электронная жеребьевка;
– защита документов и ценных бумаг от подделки.

Защита от несанкционированного чтения, или обеспечение конфиденциальности информации обеспечивается путем шифрования информации с использованием современных симметричных или асимметричных криптографических систем.

Защита от навязывания ложных сообщений может быть обеспечена с помощью так называемой имитозащиты. *Имитозащита* — защита от навязывания ложных сообщений путем формирования в зависимости от секретного ключа специальной дополнительной информации, называемой *имитовставкой*. Она передается вместе с криптограммой, причем могут использоваться два варианта: либо вычисление имитовставки по открытому тексту, либо по шифртексту. Чем больше длина имитовставки, тем меньше вероятность того, что искажение шифртекста не будет обнаружено получателем.

Идентификация законных пользователей заключается в распознавании пользователей, после чего им предоставляются определенные права доступа к ресурсам.

Контроль целостности информации — это обнаружение любых несанкционированных изменений информации, например данных или программ, хранящихся в компьютере. Имитозащита, в сущности, является частным случаем контроля целостности информации, передаваемой в виде шифртекста. В практических приложениях часто требуется удостовериться, что некоторые данные или программы не были изменены каким-либо несанкционированным способом, хотя сами данные не являются секретными и хранятся в открытом виде. Контроль целостности информации может быть основан и на использовании кодов для обнаружения и исправления ошибок, например таких, как *коды с проверкой на четность, коды Хэмминга, циклические коды*[1].

Аутентификация — установление санкционированным получателем того факта, что полученное сообщение послано санкционированным отправителем. Соблюдение заранее оговоренного *протокола* (набора правил и процедур) должно обеспечить максимальную вероятность этого факта. Очевидно, что при этом контролируется и целостность сообщения на возможность подмены или искажения. Принятый протокол должен обеспечить противодействие использованию потенциальным нарушителем ранее переданных сообщений. Это направление современной криптологии очень интенсивно развивается с момента открытия криптографии с открытым ключом (асимметричной или двухключевой криптографии) в середине 70-х гг. Если работа Шеннона «Теория связи в секретных системах» 1949 г.[2] заложила фундамент формирования криптологии как науки, то открытие двухключевой криптографии[3] ознаменовало собой ее переход в качественно новую фазу бурного развития, и послужило основой для наиболее полного решения проблем аутентификации информации и разработки систем *электронной подписи,* которые призваны придать юридическую силу документам и другим сообщениям, переданным электронным способом.

---

[1] Подробно об этих кодах можно прочесть в учебном пособии: *Баранова Е.К.* Основы информатики и защиты информации. М.: РИОР: ИНФРА-М. 2013.

[2] *Шеннон К.* Теория связи в секретных системах // В кн.: Шеннон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 333–402.

[3] *Диффи У., Хеллман М.* Защищенность и имитостойкость. Введение в криптографию // ТИИЭР. 1979. Т. 67. № 3. С. 71–109.

Электронная подпись основывается на двухключевых криптографических алгоритмах, в которых предусматривается использование открытого и секретного ключей. Такие криптоалгоритмы позволяют обеспечить строгую доказательность факта составления того или иного сообщения конкретными пользователями криптосистемы. Это основано на том, что только отправитель сообщения, который держит в секрете некоторую дополнительную информацию (секретный ключ), может составить сообщение со специфической внутренней структурой. То, что сообщение имеет структуру, сформированную с помощью секретного ключа, проверяется с помощью открытого ключа (процедура проверки электронной цифровой подписи). Вероятность того, что некоторое сообщение, составленное нарушителем, может быть принято за сообщение, подписанное каким-либо санкционированным пользователем для современных алгоритмов электронной подписи оценивается порядка 10^{-30}.

Открытый ключ формируется на основе секретного ключа или оба они вырабатываются одновременно по специальным процедурам, причем определение секретного ключа по открытому является *вычислительно сложной задачей,* т.е. задачей заведомо имеющей решение, но требующей для его нахождения выполнения чрезвычайно большого числа операций вычислителя (затраты времени на вычисления с привлечением самых современных средств могут достигать десятилетий).

Системы тайного электронного голосования строятся на базе двухключевых алгоритмов, которые используют механизм слепой подписи, т.е. возможность подписать сообщение без ознакомления с его содержанием. Такие системы имеют большие перспективы для совершенствования системы политического управления современного общества с развитой информационной инфраструктурой.

Электронная жеребьевка сводится, например, к реализации ниже приведенного алгоритма.

Абонент A выбирает случайное число x_a, двоичное представление которого имеет, например, 80 разрядов, вычисляет значение некоторой односторонней функции $y_a = F(x_a)$ и сообщает величину y_a абоненту B. Абонент B должен угадать, является ли число x_a четным или нечетным.

Поскольку используемая функция (известная и B) является односторонней, то B не может по значению y_a определить x_a, поэтому он должен угадывать четность. Пусть абонент B утверждает, что x_a является четным и сообщает об этом абоненту A.

Абонент A сообщает абоненту B число x_a.

Абонент B вычисляет значение $y = F(x_a)$, если $y = y_a$, то B убеждается, что его партнер действительно предоставил для проверки первоначально выбранное число.

Очевидно, вариантов электронной жеребьевки может быть предложено множество, а практическое использование ее приложимо к любым спортивным жеребьевкам, розыгрышам лотерей и пр.

Криптографическая защита документов и ценных бумаг от подделки является наиболее надежным современным способом пресечения их фальсифицирования. Криптографическая защита от подделки может осуществляться следующим образом. Считывается информация об уникальных особенностях данного носителя информации, формируется цифровой паспорт, включающий содержание документа и информацию о микроструктуре документа. Затем законный изготовитель документа, используя свой секретный ключ, вычисляет цифровую подпись паспорта и записывает на носителе паспорт и соответствующую ему цифровую подпись.

Проверка подлинности документа выполняется путем сканирования микроструктуры материального объекта, на котором сформирован документ, считывания записанной на нем информации и проверки цифровой подписи изготовителя документа по открытому ключу, который является общедоступным. Изготовление фальшивого документа на другом материальном объекте или модифицирование содержания документа и его цифрового паспорта практически неосуществимы без знания секретного ключа, с помощью которого формируется подпись. Любая подделка будет обнаружена путем считывания цифрового паспорта и цифровой подписи, сопоставления паспорта с содержанием документа и проверки подписи по открытому ключу.

Контрольные задания к главе 6

1. Всякий источник сообщений можно моделировать списком допустимых (т.е. встречающихся в каких-либо текстах) k-грамм при $k = 1, 2, 3, \ldots$. Какие из приведенных k-грамм не являются допустимыми в русском языке? (несколько верных ответов)

1) ШЕЕ;
2) ЖФ;
3) АУ;
4) ЮЪХ;
5) ЖЬН.

2. Криптограмма получена в результате простой замены:
ВГАДЮБКГЖЯАО МЮБ ЕДБЕБЗ ЛЖФАЮТ АЬЯБГЫЖРАА

Ключ-подстановка:

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

Восстановленный исходный текст:

1) КРИПТОЛОГИЯ ЭТО НАУКА О ЗАЩИТЕ ИНФОРМАЦИИ;
2) КРИПТОГРАФИЯ ЭТО СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ;
3) КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ.

3. Что означает термин «многократное шифрование» применительно к блочным шифрам?

1) повторное применение алгоритма шифрования к шифртексту с теми же ключами;
2) шифрование одного и того же блока открытого текста несколько раз с несколькими ключами;
3) увеличение числа этапов шифрования открытого текста.

4. Гаммирование чаще всего осуществляется: (несколько верных ответов)

1) по модулю 2, если открытый текст представляется в виде бинарной последовательности;
2) по модулю 256, если открытый текст представляется в виде последовательности байтов;
3) по модулю 16, если открытый текст представлен в цифровом виде;
4) по модулю 10, если открытый текст представлен в виде последовательности цифр, что иногда делается в ручных системах шифрования.

5. Основой построения большинства поточных шифров являются:

1) генераторы псевдослучайных чисел, в частности, различные комбинации регистров сдвига;
2) схемы суммирования по mod 16;
3) таблицы подстановок.

6. Зашифрованный методом перестановки открытый текст «Сертификаты ключей ЭЦП» при ключе длинной 7 и перестановке {4132756} имеет вид:

1) тСреиифыктал кйюечЦ Э П;
2) юклчТи ЭСЦ еиртфаикт ы;
3) чКилют рСекиафиЭтПы Ц.

7. Зашифруйте слово «выборочность» методом перестановки с ключом {3142}:

1) бвоычрнотоьс;
2) ыовбрчоонсьт;
3) ывброончотсь.

8. Зашифруйте открытый текст «field» методом Виженера; ключ — «moon», алфавит — латиница:

1) rwcup;
2) rwsyp;
3) rvsyp.

9. Частотный анализ может эффективно применяться для дешифрования шифров:

1) перестановки;
2) многоалфавитной замены;
3) простой замены.

10. Какие меры практической стойкости шифра относительно метода криптоанализа вы можете выделить (несколько верных ответов)?

1) вероятность дешифрования за время, не превосходящее T;
2) среднее время, необходимое для дешифрования шифра;
3) скорость дешифрования шифра.

11. Какие шифры можно называть имитостойкими?

1) шифры, обладающие свойством противостоять разрастанию ошибок при расшифровании текстов;
2) шифры, обладающие свойством противостоять попыткам навязывания ложной информации.

12. Какие шифры можно называть помехоустойчивыми?

1) шифры, обладающие свойством противостоять разрастанию ошибок при расшифровании текстов;
2) шифры, обладающие свойством противостоять попыткам навязывания ложной информации.

13. Разрастание числа ошибок означает, что:

1) ошибка в одной букве, допущенная при шифровании, приводит к большому числу ошибок в расшифрованном тексте;
2) ошибка в одной букве, допущенная при расшифровании, приводит к последующим ошибкам.

14. Шифр считается совершенным,

1) если он не поддается дешифрованию;
2) если положение противника, стремящегося к его дешифрованию, не облегчается в результате перехвата шифртекста;
3) если требуются большие затраты или мала вероятность успеха его дешифрования.

15. Шифр считается практически стойким,

1) если он не поддается дешифрованию;
2) если положение противника, стремящегося к его дешифрованию, не облегчается в результате перехвата шифртекста;
3) если требуются большие затраты или мала вероятность успеха его дешифрования.

16. Степень неоднозначности восстановления открытого текста при дешифровании:

1) возрастает при уменьшении материала;
2) снижается при уменьшении материала.

17. Какова длина ключа в отечественном стандарте симметричного шифрования?

1) 56 бит;
2) 124 бит;
3) 256 бит

18. Что позволяет предотвратить использование криптографических систем с открытым ключом?

1) отказ от информации;
2) передачу секретного ключа получателю;
3) передачу открытого ключа получателю;
4) использование алгоритмов асимметричного шифрования.

19. Ниже перечислены механизмы защиты АИС от несанкционированного доступа и взлома. Что здесь лишнее?

1) идентификация и аутентификация пользователей и субъектов доступа;
2) управление доступом;
3) обеспечение постоянного числа пользователей сети;
4) обеспечения целостности.

20. Какова длина блока алгоритма шифрования DES?

1) 16 бит;
2) 56 бит;
3) 64 бита;
4) 5 байт.

21. Сколько всего циклов выполняется при зашифровывании в алгоритме шифрования DES?

1) 10;
2) 14;
3) 16;
4) 20.

22. Какой алгоритм не используется при симметричном шифровании?

1) поточное шифрование;
2) шифрование методом гаммирования;
3) блочное шифрование;
4) алгоритм Эль-Гамаля.

23. Что является преимуществом симметричного шифрования?

1) скорость выполнения криптографических преобразований;
2) легкость внесения изменений в алгоритм шифрования;
3) секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
4) применение в системах аутентификации (электронная цифровая подпись).

24. Длина раундового ключа в отечественном стандарте симметричного шифрования:

1) 8 бит;
2) 32 бита;
3) 48 бит.

25. Как иначе называется асимметричное шифрование?

1) шифрование с закрытым ключом;
2) шифрование методом Бейтса;
3) шифрование с открытым ключом;
4) шифрование с переменным ключом.

26. Что является преимуществом асимметричного шифрования?

1) скорость выполнения криптографических преобразований;
2) легкость внесения изменений в алгоритм шифрования;
3) секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
4) применение в системах аутентификации (электронная цифровая подпись).

27. В асимметричных алгоритмах шифрования ключи зашифровывания и расшифровывания всегда:

1) разные, хотя и связанные между собой;
2) разные, никак не связанные между собой;
3) совпадают;
4) ключ зашифровывания представляет собой ключ расшифровывания, записанный в обратном порядке.

28. Безопасность системы RSA основана на:

1) трудности задачи разложения на простые множители;
2) комбинации символов, выбранных случайным образом;
3) использовании секретного ключа для шифрования;
4) использовании простого делителя в качестве открытого ключа.

29. Что лежит в основе криптографического контроля целостности?

1) правильная полная архивация;
2) хэш-функция;
3) кодовая защита;
4) биометрическая идентификация.

30. Хэш-функция используется для (несколько верных ответов):

1) создания сжатого образа сообщения, применяемого в ЭЦП;
2) быстрой передачи данных;
3) идентификации отправителя;
4) защиты пароля;
5) построения кода аутентификации сообщений.

31. Какую роль выполняет электронная цифровая подпись?

1) это информация о передаваемых данных;
2) роль обычной подписи в электронных документах;
3) содержит дополнительную информацию;
4) содержит обратный адрес.

32. При формировании цифровой подписи по классической схеме отправитель (несколько правильных ответов):

1) применяет к исходному тексту хэш-функцию;
2) применяет к исходному тексту идентификатор отправителя;
3) дополняет хэш-образ до длины, требуемой в алгоритме создания ЭЦП;
4) выполняет максимальное сжатие;
5) вычисляет ЭЦП по хэш-образу с использованием секретного ключа создания подписи.

Ответы на тестовое задание к главе 6

Номер вопроса	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Правильный ответ	4,5	2	2	1,2,4	1	1	1	2

Номер вопроса	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Правильный ответ	3	1,2	2	1	1	2	3	1

Номер вопроса	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
Правильный ответ	3	2	3	3	3	4	1	2

Номер вопроса	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**
Правильный ответ	3	3,4	1	1	2	1,4,5	2	1,3,5

Задачи к главе 6

Задача 1

Зашифруйте текст при помощи шифра простой замены, при имеющемся ключе шифрования.

Текст: «ВГАДЮБКГЖЯАО МЮБ ЕДБЕБЗ ЛЖФАЮТ АЬЯБГЫЖРАА»

Ключ-подстановка:

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

Решение:

Запишем **ключ-обратной подстановки** на основе ключа-подстановки:

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

При помощи этого ключа расшифровываем текст. В соответствии с ключом-обратной подстановки первая буква зашифрованного текста «В» перейдет в «К», «Г» перейдет в «Р» и т.д. В итоге получим **расшифрованный текст:**

«КРИПТОГРАФИЯ ЭТО СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ».

Задача 2

Зашифруйте текст при помощи шифра перестановки при имеющемся ключе.

Текст: «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА»

Ключ:

1	2	3	4	5	6
5	3	4	1	6	2

Решение:

Разделим текст в соответствии с длинной ключа и запишем в столбик

К	Р	И	П	Т	О
Г	Р	А	Ф	И	Ч
Е	С	К	А	Я	
З	А	Щ	И	Т	А

Затем поменяем столбцы местами в соответствии с ключом. Первый столбец станет пятым, второй — третьим и т.д. В итоге получим такую таблицу:

П	О	Р	И	К	Т
Ф	Ч	Р	А	Г	И
А		С	К	Е	Я
И	А	А	Щ	З	Т

Затем выпишем строки по порядку и получим **зашифрованный текст:**

«ПОРИКТФЧРАГИА СКЕЯИААЩЗТ».

Задача 3

Расшифруйте текст, зашифрованный шифром перестановки, имея ключ.
Текст: «ПОРИКТФЧРАГИА СКЕЯИААЩЗТ»
Ключ:

1	2	3	4	5	6
5	3	4	1	6	2

Решение:
Составим **ключ-обратной подстановки**:

1	2	3	4	5	6
4	6	2	3	1	5

Разбьем текст в соответствии с длинной ключа и запишем в столбик

П	О	Р	И	К	Т
Ф	Ч	Р	А	Г	И
А		С	К	Е	Я
И	А	А	Щ	З	Т

Переставим столбцы в соответствии с этим ключом. Первый столбец станет четвертым, второй — шестым и т.д. После перестановки получим таблицу:

К	Р	И	П	Т	О
Г	Р	А	Ф	И	Ч
Е	С	К	А	Я	
З	А	Щ	И	Т	А

Затем выпишем строки по порядку и получим **расшифрованный текст:** «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА».

ГЛАВА 7. ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ЭФФЕКТИВНОСТИ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Очевидно, что ни один проект в современном мире не может быть принят к исполнению без экономического обоснования инвестиций в него. Сложность задач экономического анализа практически во всех областях деятельности обусловлена тем, что многие ключевые параметры экономических моделей невозможно оценить с высокой степенью достоверности, поскольку они носят вероятностный характер. Особенно это касается информационной безопасности, где формализации поддаются далеко не все параметры, вероятностный характер носят не только потенциальные угрозы и уязвимости системы, но и стоимость ущерба от реализации этих угроз, а оценка риска может производиться не на количественном, а на качественном уровне. Трудность оценки экономической эффективности систем обеспечения ИБ связана и с такими объективными причинами, как:

– быстрое развитие информационных технологий, методов и средств, используемых как для защиты, так и для атак;
– невозможность достоверно предугадать все возможные сценарии атак на информационные системы и модели поведения атакующих;
– невозможность дать достаточно точную оценку стоимости информационных ресурсов, а также оценить последствия различных нарушений в денежном выражении.

Оценка экономической эффективности системы обеспечения ИБ компании зависит от следующих основных факторов:

– потребность в том или ином мероприятии по обеспечению ИБ;
– планируемые инвестиции в информационную безопасность.

Взаимосвязь факторов обусловлена возрастающим характером функции, отражающей потребность в защите информации, и ограничивающим характером инвестиций в ИБ. Первая возрастает с развитием рынка и самой компании (увеличивается число сотрудников, контрагентов, конкурентов, возрастают риски, как внутренние, так и внешние). Инвестиции же в целях оценки экономической эффективности системы ИБ играют роль некоего ограничителя, поскольку финансовые ресурсы компании ограничены, и вкладывать их в информационную безопасность компания готова только до определенного уровня — такого, который позволит компании достигать своей первичной цели в основном виде деятельности.

Экономическое обоснование затрат на ИБ во многих методиках проводится с помощью использования совокупных показателей.

Наибольшее распространение в практике по обеспечению ИБ получили следующие показатели:

1) PP (Payback Period) — срок окупаемости;

2) TCO (Total Cost of Ownership) — совокупная стоимость владения;

3) ROI (Return on Investment) — отдача от инвестиций и ROSI — изменение ROI от инвестиций в информационную безопасность;

4) NPV (Net Present Value) — чистый дисконтированный доход.

Рассмотрим значения этих показателей более подробно.

Показатель Payback Period

Показатель Payback Period (срок окупаемости) характеризует период времени, необходимый, чтобы доходы, полученные в результате инвестиций, покрыли затраты на эти самые инвестиции. Иначе говоря, если деньги на проект заемные, то отдадим мы их через срок, который и называется Payback Period. Логично, что доход от инвестиций должен быть «чистым», поскольку вкладываем мы конечную и свою «чистую» сумму денег.

Формула расчета показателя выглядит следующим образом:

$$\mathrm{PP} = \min n, \text{ при котором } \sum_{i=1}^{n} \mathrm{CF}_i > \mathrm{IC},$$

где IC (Invest Capital) — инвестиционный капитал, первоначальные затраты инвестора в объект вложения;

CF (Cash Flow) — денежный поток, который создается объектом инвестиций, при этом здесь подразумевается чистый денежный поток (приход минус расход по проекту);

i — период времени, по которому учитывается денежный поток CF_i;

n — количество периодов времени.

Формула расчета периода окупаемости может иметь и следующий вид:

$$\mathrm{PP} = \frac{\mathrm{IC}}{\mathrm{CF}}.$$

Здесь затраты на инвестиции представляют собой все издержки инвестора при вложении в инвестиционный проект. Денежный поток необходимо учитывать за определенные периоды времени (день, неделя, месяц, год). В результате период окупаемости инвестиций будет иметь аналогичную шкалу измерения.

Следует отметить, что показатель окупаемости оценивает риски невозврата инвестиций. То есть чем больше период окупаемости, тем больше риски (например, если окупаемость приближается к времени

жизни системы, то риски считаются очень большими). Однако данный показатель не универсален. В целом, он не показывает инвестиционную привлекательность проекта с точки зрения дальнейшего дохода (после истечения срока окупаемости). Если окупаемость равна одному году, это не означает, что проект через два года и более будет приносить доход на том же уровне.

Вместе с тем в реальных условиях достаточно сложно прогнозировать будущие устойчивые денежные поступления, поэтому период окупаемости может существенно измениться. Для того чтобы снизить возможные отклонения от плана окупаемости, следует обеспечить надежность источников поступления денежного потока инвестиционного проекта. К тому же показатель не учитывает влияние инфляции на изменение стоимости денег во времени. Срок окупаемости инвестиций может быть использован как критерий отсева на первом этапе оценки и отбора «тяжелых» инвестиционных проектов.

Показатель TCO

Показатель TCO определяется как сумма прямых и косвенных затрат, которые несет владелец системы на протяжении всего жизненного цикла ее эксплуатации. TCO считается для ограниченного периода времени, поскольку для каждой ИТ-системы существует определенный срок функционирования.

Формула расчета показателя TCO в общем виде выглядит следующим образом:

$$\mathrm{TCO} = \mathrm{DE} + \mathrm{IDC},$$

где DE (Direct Expenses) — прямые расходы;

IDC (Indirect Costs) — косвенные расходы.

На примере внедрения IT-системы суммарная величина TCO включает в себя затраты на:

- проектирование информационной системы (DE);
- приобретение аппаратных и программных средств (DE);
- разработку программного обеспечения и его документирование, а также на исправление ошибок и доработку в течение периода эксплуатации (IDC);
- текущее администрирование информационных систем (IDC);
- техническую поддержку и сервисное обслуживание (IDC);
- расходные материалы (IDC);
- телекоммуникационные услуги (IDC);
- затраты на обучение (IDC);
- издержки, связанные с потерей времени пользователями в случае сбоев в работе информационных систем (IDC).

Также в расчет затрат на повышение уровня ИБ необходимо включать расходы на реорганизацию бизнес-процессов и информационную работу с персоналом. Кроме того, при анализе расходов необходимо учитывать, что в большинстве случаев внедрение средств защиты информации предполагает появление дополнительных обязанностей у персонала компании и необходимости осуществления дополнительных операций при работе с информационными системами. Значение TCO в каждом конкретном случае необходимо определять индивидуально с учетом особенностей проекта, который предстоит реализовать: основной востребованной функциональности, существующей инфраструктуры, количества пользователей и других факторов.

Показатель TCO позволяет руководителям служб безопасности обосновывать бюджет на информационную безопасность. Кроме того, поскольку оценка экономической эффективности системы защиты информации становится «измеримой», возможно оперативно решать задачи контроля и коррекции показателей экономической эффективности деятельности службы безопасности.

Немаловажный аспект состоит в том, что при оценке стоимости внедрения какого-либо решения большое внимание уделяется стоимости его приобретения (капитальные затраты), а то, сколько денег позволяет сэкономить его эксплуатация, как правило, остается в тени. Экономия происходит не только за счет снижения прямых затрат (применения новых технологий и алгоритмов, повышающих производительность и позволяющих получить больше требуемых результатов в единицу времени), но и за счет снижения косвенных издержек (например: электроэнергия, аренда, техническое сопровождение, обучение персонала). Очевидно, функциональность продукта сильно влияет на второй тип затрат (косвенные затраты), поэтому такого рода затраты обязательно учитываются при расчете TCO.

Одним из преимуществ показателя TCO является то, что он позволяет сделать выводы о целесообразности реализации проекта в области ИБ на основании оценки одних лишь только затрат.

Другим преимуществом этого показателя является то, что модель расчета TCO предполагает оценку не только первоначальных затрат на создание системы защиты информации, но и затрат, которые могут иметь место на различных этапах всего жизненного цикла системы. Но, несмотря на это, показатель TCO является статичным и не учитывает изменения ситуации во времени.

Особенность применения этого показателя состоит в сравнении полученной оценки для конкретной компании с рекомендуемой или оцениваемой экспертно оптимальной величиной TCO для данного типа компаний. Если полученная совокупная стоимость владения системы безопасности значительно превышает рекомендованное значение и приближается к предельному, то необходимо принять меры по снижению TCO.

Показатели ROI и ROSI

ROI — это процентное отношение прибыли (или экономического эффекта) от внедрения проекта к инвестициям, необходимым для реализации этого проекта. В общем случае под инвестициями подразумевается показатель TCO.

Формула расчета показателя ROI выглядит следующим образом:

$$\mathrm{ROI} = \frac{\text{Доходы} - \text{Расходы}}{\text{Инвестиции}},$$

где Доходы — фактические доходы компании за отчетный период (год);
Расходы — фактические расходы компании за отчетный период (год);
Инвестиции — инвестиции, необходимые для реализации проекта.

Таким образом, ROI — это интегральный показатель, позволяющий оценить, насколько эффективно работают вложенные в компанию деньги, т.е. сколько денег «производит» за год каждый рубль, вложенный в компанию по данному проекту.

Показатель ROI может быть скорректирован на ставку дисконтирования. Функция дисконтирования используется при анализе инвестиционных вложений для учета влияния фактора времени и приведения разновременных затрат к единому моменту. Ставка дисконтирования в этом случае позволяет учесть изменение стоимости денег с течением времени.

Совместно с показателем ROI рассмотрим показатель ROSI (Return on Security Investment — оценка эффективности инвестиций в безопасность). Формула его расчета:

$$\mathrm{ROSI} = \frac{\Delta\text{Доходы} - \Delta\text{Расходы}}{\Delta\text{Инвестиции}},$$

где ROSI — показатель изменения ROI за счет инвестиций в ИБ;
ΔДоходы — изменение в доходах, обусловленное инвестициями ИБ;
ΔРасходы — изменение в расходах, обусловленное инвестициями ИБ;
ΔИнвестиции — инвестиции, сделанные в ИБ.

Смысл совместного расчета показателей ROI и ROSI сводится к сопоставлению этих показателей для понимания того, влияет ли реализация проекта на деятельность компании, и если да, то каким образом.

В зависимости от эффективности проекта организации системы ИБ и от отношения размера инвестиций в него к общим инвестициям в компанию изменяется общая эффективность компании.

Так, ROI может:
– увеличиться (ROSI > ROI);
– уменьшиться (ROSI < ROI);
– остаться прежним (ROSI = ROI).

Подсчитав ROSI, его значение необходимо сравнить со следующими «пороговыми величинами»:
– ROSI < 0, т.е. эффективность проекта отрицательна и это, конечно, худший вариант, но он не так редок, как может показаться;
– ROI > ROSI > 0, т.е. внедрение проекта приведет к уменьшению общего ROI в компании;
– ROSI > ROI, т.е. внедрение проекта приведет к увеличению общего ROI в компании.

Однако, применяя показатель ROI для расчета эффективности вложений в информационную безопасность, следует понимать, что прямого влияния на рост доходов система информационной безопасности не имеет. Поэтому, как правило, не стоит ожидать увеличения выручки компании после инвестиций в сферу информационной защищенности.

Показатель NPV

Чистый дисконтированный доход (чистая текущая стоимость, чистый приведенный доход, текущая стоимость) — показатель, отражающий изменение денежных потоков и разность между дисконтированными денежными доходами и расходами.

Из определения очевидно, что при расчете данного показателя учитываются динамичные факторы изменения денежного потока (например, инфляция). Влияние таких факторов расчетным способом нейтрализуется, и в итоге получается стоимость, приведенная к определенному периоду времени. Общая формула расчета показателя выглядит следующим образом:

$$\mathrm{NPV} = \sum_{t=0}^{n} \frac{\mathrm{CF}_t}{(1+r)^t},$$

где CF_t — денежный поток в период времени t;
r — ставка дисконтирования;
t — период времени, по которому учитывается CF_t;
n — количество периодов времени.

Отметим, что под периодом $t = 0$ здесь подразумевается «начальная точка», когда были осуществлены инвестиции. При таком подходе стоимость всех дальнейших денежных потоков приводится к их стоимости в период $t = 0$.

Расчет денежного потока сводится к суммированию положительных денежных потоков (потенциальных доходов) и вычитанию из них возникающих отрицательных потоков (расходов).

Критерии оценки показателя NPV следующие:
– NPV < 0 — результатом реализации инвестиционного проекта будут убытки;
– NPV = 0 — инвестиционный проект обеспечит уровень безубыточности, когда все доходы равны расходам;
– NPV > 0 — инвестиционный проект принесет прибыль.

Следует отметить, что при расчете показателя NPV будущие денежные потоки мы можем скорректировать на риски, умножив тот или иной вид дохода и расхода на соответствующий коэффициент. Также здесь может быть учтена количественная оценка риска.

Одним из немногих способов, который может помочь компании определить экономический эффект от осуществления мероприятий в сфере защиты информации, является финансовая оценка того ущерба, который может быть нанесен информационным ресурсам компании, и который может быть предотвращен в результате реализации предлагаемых мероприятий. Таким образом, предполагаемый предотвращенный ущерб и будет составлять полученный экономический эффект или дополнительный денежный поток. При таком подходе большинство расчетов могут быть только оценочными и носить приблизительный характер. Это связано с тем, что активность злоумышленников, являющихся источниками угроз ИБ, практически непредсказуема: невозможно достоверно предсказать стратегии нападения, квалификацию нападающих, их конкретные намерения и ресурсы, которые будут задействованы для совершения тех или иных действий, а также намерения в отношении украденной информации. Соответственно, для осуществления всех необходимых расчетов необходимо сделать множество допущений и экспертных оценок в контексте деятельности данного конкретного предприятия, а также по возможности изучить статистическую информацию, касающуюся атак на информационные ресурсы, аналогичные защищаемым. При таком подходе, экономическая оценка эффективности мер по защите информации предполагает: оценку существующих угроз для информационных активов, которых коснется реализация защитных мер; оценку вероятности реализации каждой из выявленных угроз; экономическую оценку последствий реализации угроз.

Рассмотренные методики оценки экономической эффективности защиты информации и ключевые показатели, положенные в основу применения этих методик, представлены в табл. 7.1.

Таблица 7.1

Методики оценки экономической эффективности системы обеспечения информационной безопасности

Наименование показателя	Формула расчета
Срок окупаемости, PP	$PP = \min n$, при котором $\sum_{i=1}^{n} CF_i > IC$; $PP = \frac{IC}{CF}$, где IC (Invest Capital) — инвестиционный капитал, первоначальные затраты инвестора в объект вложения; CF (Cash Flow) — денежный поток, который создается объектом инвестиций, при этом здесь подразумевается чистый денежный поток (приход минус расход по проекту); i — период времени, по которому учитывается денежный поток CF_i; n — количество периодов времени.
Совокупная стоимость владения, TCO	$TCO = DE + IDC$, где DE (Direct Expenses) — прямые расходы; IDC (Indirect Costs) — косвенные расходы.
Отдача от инвестиций, ROI, ROSI	$ROI = \frac{\text{Доходы} - \text{Расходы}}{\text{Инвестиции}}$; $ROSI = \frac{\Delta\text{Доходы} - \Delta\text{Расходы}}{\Delta\text{Инвестиции}}$, где ΔДоходы — изменение в доходах, обусловленное инвестициями в ИБ; ΔРасходы — изменение в расходах, обусловленное инвестициями в ИБ; ΔИнвестиции — инвестиции, сделанные в ИБ.
Чистый дисконтированный доход, NPV	$NPV = \sum_{t=0}^{n} \frac{CF_t}{(1+r)^t}$, где CF_t — денежный поток в период времени t; r — ставка дисконтирования; t — период времени, по которому учитывается CF_t; n — количество периодов времени.

ВАРИАНТЫ ИТОГОВЫХ ТЕСТОВЫХ ЗАДАНИЙ

Вариант № 1

1. Информационная безопасность характеризует защищенность:
   1) пользователя информационной системы;
   2) информации и поддерживающей ее инфраструктуры;
   3) источника информации;
   4) носителя информации.
2. Что из перечисленного является составляющей информационной безопасности?
   1) нарушение целостности информации;
   2) проверка прав доступа к информации;
   3) доступность информации;
   4) выявление нарушителей.
3. Конфиденциальность информации гарантирует:
   1) доступность информации кругу лиц, для кого она предназначена;
   2) защищенность информации от потери;
   3) защищенность информации от фальсификации;
   4) доступность информации только автору.
4. Сколько существует уровней формирования режима информационной безопасности?
   1) три;
   2) четыре;
   3) два;
   4) пять.
5. Какой из перечисленных уровней не относится к уровням формирования режима информационной безопасности?
   1) законодательно-правовой;
   2) информационный;
   3) административный (организационный);
   4) программно-технический.
   5) все перечисленные.
6. Средства защиты информации какого из уровней формирования режима информационной безопасности связаны непосредственно с защищаемой информацией?
   1) законодательно-правового;
   2) информационного;
   3) административного (организационного);
   4) программно-технического.

7. Основополагающим документом по информационной безопасности в России является:

1) Конституция РФ;
2) Уголовный кодекс;
3) Закон о средствах массовой информации;
4) Доктрина информационной безопасности.

8. Сколько категорий государственных информационных ресурсов определяет ФЗ «Об информации, информационных технологиях и защите информации»?

1) три;
2) четыре;
3) два;
4) пять.

9. Неправомерный доступ к компьютерной информации наказывается штрафом:

1) от пяти до двадцати минимальных размеров оплаты труда;
2) от двухсот до пятисот минимальных размеров оплаты труда;
3) от ста пятидесяти до двухсот минимальных размеров оплаты труда;
4) до трехсот минимальных размеров оплаты труда.

10. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается ограничением свободы на срок:

1) до года;
2) до двух лет;
3) до пяти лет;
4) до трех месяцев.

11. Подберите слово к данному определению:

_____ — это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.
1) компьютерная безопасность;
2) информационная безопасность;
3) защита информации;
4) защита государственной тайны.

12. Что из перечисленного является задачей информационной безопасности?

1) устранение неисправностей аппаратных средств;
2) устранение последствий стихийных бедствий;
3) защита технических и программных средств информатизации от ошибочных действий персонала;
4) восстановление линий связи.

13. Выберите правильную иерархию пространства требований в «Общих критериях»:

1) класс – семейство – компонент – элемент;
2) элемент – класс – семейство – компонент;
3) компонент – семейство – класс – элемент;
4) семейство – компонент – класс – элемент;

14. Что не относится к механизмам безопасности в соответствии с X.800?

1) шифрование;
2) электронная цифровая подпись;
3) механизм управления доступом;
4) механизм подотчетности.

15. Сколько классов СВТ по уровню защищенности от НСД к информации определено в руководящем документе «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?

1) три;
2) семь;
3) пять;
4) четыре.

16. Подберите слово к данному определению:

_____ — комплекс предупредительных мер по обеспечению информационной безопасности организации.
1) информационная политика;
2) политика безопасности;
3) информационная безопасность;
4) защита информации.

17. Что не рассматривается в политике безопасности?

1) требуемый уровень защиты данных;
2) роли субъектов информационных отношений;
3) анализ рисков;
4) защищенность механизмов безопасности.

18. Подберите слово к данному определению:

_____ — это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.
1) троянская программа;
2) компьютерный вирус;
3) программный вирус;
4) вирус.

19. Основная особенность компьютерных вирусов заключается:

1) в возможности их самопроизвольного внедрения в различные объекты операционной системы;
2) в возможности нарушения информационной безопасности;
3) в возможности заражения окружающих;
4) в их постоянном существовании.

20. По особенностям алгоритма работы вирусы бывают:

1) резидентные и стелс-вирусы;
2) полиморфик-генераторы и загрузочные вирусы;
3) макровирусы и логические бомбы;
4) утилиты скрытого администрирования;

21. «Маски» вирусов используются:

1) для поиска известных вирусов;
2) для создания известных вирусов;
3) для уничтожения известных вирусов;
4) для размножения вирусов.

22. Подберите слово к данному определению:

_____ — это достаточно труднообнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода.

1) полиморфик-вирусы;
2) стелс-вирусы;
3) макровирусы;
4) конструкторы вирусов.

23. Угроза перехвата данных может привести к нарушению:

1) доступности данных;
2) доступности и целостности данных;
3) целостности данных;
4) конфиденциальности данных.

24. Идентификация и аутентификации применяются:

1) для повышения физической защиты информационной системы;
2) для ограничения доступа случайных и незаконных субъектов к информационной системе;
3) для защиты от компьютерных вирусов;
4) для обеспечения целостности данных.

25. Подберите слово к данному определению

_____ — присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

1) аутентификация;
2) идентификация;

3) аутентичность;
4) конфиденциальность.

26. Подберите слово к данному определению

_____ — проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

1) аутентификация;
2) идентификация;
3) целостность;
4) конфиденциальность.

27. Что из перечисленного не является идентификатором при аутентификации?

1) пароль;
2) особенности поведения пользователя;
3) персональный идентификатор;
4) секретный ключ.

28. Постоянные пароли относятся к

1) статической аутентификации;
2) временной аутентификации;
3) устойчивой аутентификации;
4) постоянной аутентификации.

29. Подберите слово к данному определению:

_____ — представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом.

1) закрытый ключ шифрования;
2) электронная цифровая подпись;
3) вирусная маска;
4) открытый ключ шифрования.

30. К какому из перечисленных методов управления доступом относится определение?

_____ — основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах и официального разрешения субъекта к информации соответствующего уровня конфиденциальности.

1) мандатное управление доступом;
2) принудительное управление доступом;
3) дискретное управление доступом;
4) статистическое управление доступом.

Вариант № 2

1. Что из перечисленного является составляющей информационной безопасности?

1) целостность информации;
2) несанкционированный доступ к информации;
3) санкционированный доступ к информации;
4) антивирусная защита.

2. Доступность информации гарантирует:

1) неизменность информации в любое время;
2) получение требуемой информации за определенное время;
3) получение требуемой информации за неопределенное время;
4) защищенность информации от возможных угроз.

3. На каком из уровней формирования режима информационной безопасности разрабатывается политика безопасности?

1) информационный;
2) административный (организационный);
3) законодательно-правовой;
4) программно-технический.

4. Программно-технический уровень формирования режима информационной безопасности включает:

1) три подуровня;
2) два подуровня;
3) шесть подуровней.

5. Неправомерный доступ к компьютерной информации наказывается лишением свободы:

1) до пяти лет;
2) до трех лет;
3) до года;
4) до двух лет.

6. Создание, использование и распространение вредоносных программ для ЭВМ наказывается:

1) лишением свободы до года;
2) штрафом до двадцати минимальных размеров оплаты труда;
3) лишением свободы до трех лет и штрафом от двухсот до пятисот минимальных размеров оплаты труда;
4) исправительными работами до пяти лет;

7. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается:

1) штрафом до ста минимальных размеров оплаты труда;
2) ограничением свободы;
3) лишением свободы;
4) штрафом до пятисот минимальных размеров оплаты труда.

8. Наиболее общую, «предметную» группировку требований в «Общих критериях» определяет:

1) класс требований;
2) элемент требований;
3) компонент требований;
4) семейство требований.

9. Какой документ определяет сервисы безопасности для вычислительных сетей?

1) «Оранжевая» книга;
2) Рекомендации X.800;
3) Рекомендации X.200;
4) Рекомендации X.450.

10. Сколько классов автоматизированных систем, подлежащих защите от несанкционированного доступа к информации определено в руководящем документе «АС. Защита от НСД к информации. Классификация АС и требования по защите информации»?

1) девять;
2) семь;
3) пять;
4) двенадцать.

11. Что не является содержанием административного уровня формирования режима информационной безопасности?

1) разработка политики безопасности;
2) проведение анализа угроз и расчета рисков;
3) выбор механизмов обеспечения информационной безопасности.
4) внедрение механизмов безопасности.

12. Подберите слово к данному определению:

_____ — это потенциальная возможность нарушения режима информационной безопасности.
1) несанкционированный доступ к информации;
2) просмотр конфиденциальной информации;
3) угроза информационной безопасности;
4) фальсификация информации.

13. Что не является причиной случайных воздействий на информационную систему?

1) отказы и сбои аппаратуры;
2) ошибки персонала;
3) помехи в линиях связи из-за воздействий внешней среды;
4) подбор пароля.

14. Что является самым эффективным при борьбе с непреднамеренными случайными ошибками?

1) определение степени ответственности за ошибки;
2) резервирование аппаратуры;
3) максимальная автоматизация и строгий контроль;
4) контроль действий пользователя.

15. Какая организация в РФ разрабатывает стандарты и руководящие документы, направленные на обеспечение информационной безопасности?

1) ФСТЭК;
2) Гостехнадзор;
3) Государственная Дума;
4) Гостехконтроль.

16. Что из перечисленного не относится к вредоносным программам?

1) логическая бомба;
2) «троянский конь»;
3) макровирус;
4) конструкторы вирусов;

17. Какой из вирусов при инфицировании компьютера оставляет в оперативной памяти свою часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них?

1) нерезидентный вирус;
2) файловый вирус;
3) резидентный вирус;
4) загрузочный вирус.

18. Что из перечисленного не относится к вредоносным программам?

1) файловый вирус;
2) логическая бомба;
3) «троянский конь»;
4) конструкторы вирусов;

19. Главной функцией полиморфик-генератора является:

1) поиск новых вирусов;
2) удаление антивирусной программы;
3) шифрование тела вируса;
4) размножение вируса.

20. Подберите слово к данному определению

_____ — потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи.

1) перехват данных;
2) удаленная угроза;
3) угроза информационной безопасности;
4) программный вирус.

21. Для повышения защищенности вычислительных сетей при установлении виртуального соединения наиболее надежно:

1) повысить уровень физической защиты линий связи;
2) использовать криптоалгоритмы с открытым ключом;
3) выбрать оптимальный канал передачи данных;
4) использовать межсетевой экран.

22. Что из перечисленного не является идентификатором при аутентификации?

1) пароль;
2) секретный ключ;
3) персональный идентификатор;
4) отпечатки пальцев.

23. Что из перечисленного не относится к категориям аутентификации?

1) статическая аутентификация;
2) временная аутентификация;
3) устойчивая аутентификация;
4) постоянная аутентификация.

24. Что из перечисленного не входит в криптосистему?

1) алгоритм шифрования;
2) набор ключей, используемых для шифрования;
3) полиморфик-генератор;
4) система управления ключами.

25. Что не является задачей криптосистемы?

1) обеспечение конфиденциальности;
2) регистрация и аудит нарушений;
3) обеспечение целостности данных;
4) аутентификация данных и их источников.

26. При асимметричных криптосистемах для шифрования и расшифрования используются:

1) два взаимосвязанных ключа;
2) один открытый ключ;
3) один закрытый ключ;
4) два открытых ключа.

27. Для контроля целостности передаваемых по сетям данных используется:

1) аутентификация данных;
2) электронная цифровая подпись;
3) аудит событий;
4) межсетевое экранирование.

28. Какой вид разграничения доступа определен в документах ФСТЭК?

1) принудительное управление доступом;
2) дискретное управление доступом;
3) произвольное управление доступом;
4) статистическое управление доступом.

29. Подберите слово к данному определению:

_____ — это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день).

1) аудит;
2) аутентификация;
3) регистрация;
4) идентификация.

30. Какой механизм безопасности является наиболее сильным психологическим средством?

1) VPN;
2) аутентификация;
3) идентификация;
4) регистрация и аудит.

Вариант № 3

1. Целостность информации гарантирует:

1) существование информации в исходном виде;
2) принадлежность информации автору;
3) доступ информации определенному кругу пользователей;
4) защищенность информации от несанкционированного доступа.

2. Какой из уровней формирования режима информационной безопасности включает комплекс мероприятий, реализующих практические механизмы защиты информации?

1) законодательно-правовой;
2) информационный;
3) административный (организационный);
4) программно-технический.

3. Какой из уровней формирования режима информационной безопасности включает физический подуровень?

1) административный (организационный);
2) законодательно-правовой;
3) информационный;
4) программно-технический.

4. Создание, использование и распространение вредоносных программ для ЭВМ, повлекшее тяжкие последствия, наказывается лишением свободы:

1) до пяти лет;
2) до шести лет;
3) до семи лет;
4) до четырех лет.

5. Минимальный набор требований в «Общих критериях» определяет:

1) класс требований;
2) элемент требований;
3) компонент требований;
4) семейство требований.

6. Сколько классов защищенности межсетевых экранов определено в руководящем документе «СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации»?

1) три;
2) семь;
3) пять;
4) шесть.

7. Что не является содержанием административного уровня формирования режима информационной безопасности?

1) разработка политики безопасности;
2) настройка механизмов безопасности;
3) проведение анализа угроз и расчета рисков;
4) выбор механизмов обеспечения информационной безопасности.

8. Аутентичность связана:

1) с проверкой прав доступа;
2) с доказательством авторства документа;
3) с изменением авторства документа;
4) с контролем целостности данных.

9. Что из перечисленного является компьютерным вирусом?

1) полиморфик-генератор;
2) утилита скрытого администрирования;
3) макровирус;
4) логическая бомба.

10. Какой вирус заражает файлы-документы и электронные таблицы офисных приложений?

1) файловый вирус;
2) сетевой вирус;
3) макровирус;
4) загрузочный вирус.

11. Самошифрование и полиморфичность используются для:

1) саморазмножения вируса;
2) максимального усложнения процедуры обнаружения вируса;
3) расшифровки тел вируса;
4) для скрытия действий антивирусной программы.

12. Одним из наиболее эффективных способов борьбы с вирусами является:

1) использование антивирусного программного обеспечения;
2) профилактика компьютерных вирусов;
3) ограничение доступа пользователей к ЭВМ;
4) шифрование данных.

13. Какой вид антивирусных программ перехватывает вирусоопасные ситуации и сообщающает об этом пользователю?

1) иммунизатор;
2) блокировщик;
3) сканер;
4) CRC-сканер.

14. Какой вид антивирусных программ основан на подсчете контрольных сумм для присутствующих на диске файлов/системных секторов?

1) иммунизатор;
2) блокировщик;
3) сканер;
4) CRC-сканер.

15. Что из перечисленного не является причиной успешной реализации удаленных угроз в вычислительных сетях?

1) отсутствие выделенного канала связи между объектами вычислительной сети;
2) взаимодействие объектов без установления виртуального канала;
3) отсутствие в распределенных вычислительных сетях криптозащиты сообщений;
4) взаимодействие объектов с установлением виртуального канала.

16. Что из перечисленного не является идентификатором при идентификации?

1) голос;
2) рисунок радужной оболочки глаза;
3) персональный идентификатор;
4) отпечатки пальцев.

17. Какая категория аутентификации использует динамические данные аутентификации, меняющиеся с каждым сеансом работы?

1) статическая аутентификация;
2) временная аутентификация;
3) устойчивая аутентификация;
4) постоянная аутентификация.

18. Какая категория аутентификации защищает данные от несанкционированной модификации?

1) постоянная аутентификация;
2) временная аутентификация;
3) статическая аутентификация;
4) устойчивая аутентификация.

19. Что не является задачей криптосистемы?

1) обеспечение конфиденциальности;
2) обеспечение целостности данных;
3) аутентификация данных и их источников;
4) межсетевое экранирование.

20. В симметричных криптосистемах для шифрования и расшифрования используются?

1) два ключа разной длины;
2) два разных по значению ключа;
3) один и тот же ключ;
4) два открытых ключа.

21. Что из перечисленного не является функцией управления криптографическими ключами?

1) генерация;
2) хранение;
3) распределение;
4) изучение.

22. Что из перечисленного не относится к разграничению доступа пользователей?

1) матрицы установления полномочий;
2) парольное разграничение доступа;
3) разграничение криптографических ключей;
4) разграничение доступа по спискам.

23. Какой вид разграничения доступа определен в документах ФСТЭК?

1) эвристическое управление доступом;
2) мандатное управление доступом;
3) принудительное управление доступом;
4) статистическое управление доступом.

24. К какому из перечисленных методов управления доступом относится определение?

_____ — представляет собой разграничение доступа между поименованными субъектами и поименованными объектами.

1) мандатное управление доступом;
2) дискретное управление доступом;
3) принудительное управление доступом;
4) статистическое управление доступом.

25. Какой из механизмов безопасности основан на подотчетности системы обеспечения безопасности?

1) аудит;
2) аутентификация;
3) регистрация;
4) шифрование.

26. Подберите слово к данному определению:

_____ — это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

1) матрица полномочий;
2) регистрационный журнал;
3) справочник безопасности;
4) журнал учета времени работы на ЭВМ.

27. Что из перечисленного относится к аудиту безопасности?

1) сбор информации о событиях;
2) хранение информации о событиях;
3) защита содержимого журнала регистрации;
4) анализ содержимого журнала регистрации.

28. Идентификация и аутентификации применяются:

1) для регистрации событий безопасности;
2) для выявления попыток несанкционированного доступа;
3) для обеспечения целостности данных;
4) для ограничения доступа случайных и незаконных субъектов информационной системы к ее объектам.

29. Подберите слово к данному определению:

_____ — программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее и обеспечивает защиту информационной системы посредством фильтрации информации.

1) межсетевой экран;
2) криптоалгоритм;
3) сервер удаленного доступа;
4) криптосистема.

30. Виртуальные частные сети включают следующие сервисы безопасности:

1) экранирование и аудит;
2) шифрование и туннелирование;
3) регистрацию и контроль доступа;
4) шифрование и электронную подпись.

Ответы на итоговые тестовые задания

№ вопроса	Номер правильного ответа		
	Вариант № 1	Вариант № 2	Вариант № 3
1	2	1	1
2	3	2	3
3	1	2	4
4	1	1	3
5	2	4	3
6	4	3	3
7	4	2	2
8	4	1	2
9	2	2	3
10	2	1	3
11	2	4	2
12	3	3	1
13	1	4	2
14	4	3	4
15	2	1	4
16	2	3	3
17	4	3	3
18	3	1	1
19	1	3	4
20	1	2	3
21	1	2	4
22	1	4	3
23	4	2	2
24	2	3	2
25	2	2	3
26	1	1	2
27	2	2	4
28	1	2	4
29	2	1	1
30	1	4	2

СЛОВАРЬ ТЕРМИНОВ

Антивирусная программа — программа, предназначенная для поиска, обнаружения, классификации и удаления вредоносных программ.

Аудит —это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день).

Аутентификация (установление подлинности) — проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

Вредоносная программа — программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

Доступность — гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Идентификация — присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Информационная безопасность, ИБ (information security) — защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность.

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

Инцидент ИБ — это возникновение одного или нескольких нежелательных или непредвиденных событий ИБ, в результате которых велика вероятность компрометации бизнес-процессов и угрозы ИБ для организации.

Криптоанализ — раздел, посвященный исследованию возможности чтения сообщений без знания ключей. Он связан непосредственно со взломом шифров. Специалисты, занимающиеся криптоанализом и исследованием шифров называются криптоаналитиками.

Компьютерный вирус — вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы.

Конфиденциальность — гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Криптографическая система с открытым ключом (асимметричная криптосистема) — система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передается по открытому (то есть незащищенному) каналу и используется для проверки ЭП и/или для шифрования сообщения.

Криптография (др.греч. κρυπτός — скрытый + γράφω — пишу) — наука о создании безопасных методов связи, о создании стойких (устойчивых к взлому) шифров. Она занимается поиском математических методов преобразования информации.

Облачное хранилище данных (cloud storage) — модель онлайн-хранилища, в котором данные хранятся на многочисленных распределенных в сети серверах, предоставляемых в пользование клиентам, как правило, третьей стороной.

Политика безопасности — комплекс предупредительных мер по обеспечению информационной безопасности организации.

Регистрация основана на подотчетности системы обеспечения безопасности, фиксирующий все события, касающиеся безопасности.

Риск информационной безопасности (information security risk) — возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Симметричные криптосистемы, также симметричное шифрование, симметричные шифры (symmetric-key algorithm) — способ шифрования, в котором для зашифрования и расшифрования применяется один и тот же криптографический секретный ключ.

Событие ИБ — идентифицированный случай состояния системы или сети, который указывает на возможное нарушение политики информационной безопасности или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности.

Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Удаленная угроза — потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемое программно по каналам связи.

Уязвимость информационной системы — свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Целостность — гарантия того, что информация сейчас существует в ее исходном виде, т.е. при ее хранении или передаче не было произведено несанкционированных изменений.

Шифр — совокупность обратимых преобразований множества открытых текстов (исходного сообщения) на множество зашифрованных текстов, проводимых с целью их защиты. Конкретный вид преобразования определяется с помощью ключа шифрования.

Электронная подпись — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Энтропия (от греч. ἐντροπία — превращение, обращение) представляет собой меру неопределенности и в теории информации характеризует способность источника отдавать информацию.

СПИСОК ЛИТЕРАТУРЫ

1. Бабаш А.В., Шанкин Г.П. Криптография / Под ред. В.П. Шерстюка, Э.А. Применко. — М.: СОЛОН-Р, 2002.

2. Бабаш А.В., Баранова Е.К. Криптографические методы защиты информации. — М.: КНОРУС, 2016.

3. Бабаш А.В., Баранова Е.К. Актуальные вопросы защиты информации: монография. — М.: РИОР: ИНФРА-М, 2017.

4. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учеб. пособие. — 4-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2018.

5. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. Практикум: учеб. пособие. — 2-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2016.

6. Баранова Е.К., Бабаш А.В. Криптографические методы защиты информации. Лабораторный практикум: учеб. пособие (+ CD-ROM). — М.: КНОРУС, 2015.

7. Баранова Е.К. Основы информатики и защиты информации. — М.: РИОР: ИНФРА-М, 2013.

8. Башлы П.Н. Информационная безопасность: учебник. — Ростов-н/Д.: Фолиант, 2005.

9. Башлы П.Н., Бабаш А.В., Баранова Е.К. Информационная безопасность. — М.: Изд. центр ЕАОИ, 2010.

10. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учебное пособие для вузов. — М.: Горячая линия — Телеком, 2006.

11. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности: учебник. — М.: Академия, 2018.

12. Вельшенбах М. Криптография на Си и С + + в действии (+ CD-ROM). — М.: Триумф, 2004.

13. Галатенко В.А. Основы информационной безопасности. — М.: Интернет-университет информационных технологий — ИНТУИТ.РУ, 2003.

14. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учеб. пособие. — СПб.: СПбГУ ИТМО, 2009.

15. Горбенко А.О. Основы информационной безопасности : учебное пособие для студентов по направлению «Информационная безопасность» — СПб : Интермедия, 2016.

16. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии. — М.: Академия, 2009.

17. Зегжда Д. П., Ивашко А.М. Основы безопасности информационных систем. СПб.: Горячая Линия — Телеком, 2010.

18. Касперский Е. Компьютерное зловредство. — СПб.: Питер, 2009.

19. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. — М.: Постмаркет, 2001.

20. Куприянов А.И., Сахаров А.В. Основы защиты информации. — М.: Академия, 2006.

21. Нестеров С.А. Основы информационной безопасности: учеб. пособие. — М.: Лань, 2016.

22. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2002.

23. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности: учеб. пособие. — СПб.: Питер, 2017.

24. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 2001.

25. Саломаа А. Криптография с открытым ключом. — М.: Мир, 1996.

26. Семененко В.А. Информационная безопасность: учеб. пособие. 2-е изд. — М.: МГИУ, 2006.

27. Смарт Н. Криптография. — М.: Техносфера, 2006.

28. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. — М.: Академия, 2006.

29. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. — М.: Форум, 2009.

30. Хохлов Г.И. Основы теории информации: учеб.пособие для студ. высш. учеб. заведений. — М.: Академия, 2008.

31. Шеннон К. Математическая теория связи // К. Шеннон. Работы по теории информации и кибернетике: пер.с англ.; под ред. Р.Л. Добрушина и О.Б.Лупанова. — М.: ИЛ, 1963.

32. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке «Си». — М.: Триумф, 2002.