МИНОБРНАУКИРОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Челябинский государственный университет»
(ФГБОУ ВО «ЧелГУ»)

Костанайский филиал

Карасева Э.М., Рак О.В.

# ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

учебное пособие

Костанай, 2019 г

**УДК 004.4 (075)**
**ББК 32.973.202я73**
**К 21**

***Авторы:***
**Карасева Эльмира Миндыхатовна** – кандидат педагогических наук
**Рак Олеся Валерьевна** – магистр прикладной математики и информатики

***Рецензенты:***
**Нурмагамбетов Рашид Габитович** – кандидат юридических наук
**Шумейко Татьяна Степановна** – кандидат педагогических наук

**Карасева, Э.М., Рак, О.В.**

**К 21** Основы информационной безопасности: Учебное пособие /Э.М.Карасева, О.В. Рак.– Костанайский филиал «ЧелГУ», Костанай, 2019.–90 с.

**ISBN 978-601-7586-07-2**

Учебное пособие «Основы информационной безопасности» рекомендовано ученым советом Костанайского филиала ФГБОУ ВО «ЧелГУ» для использования в качестве учебного пособия для студентов направлений подготовки 40.03.01 Юриспруденция, 38.03.01 Экономика.

УДК 004.4 (075)
ББК 32.973.202я73

ISBN 978-601-7586-07-2

## СОДЕРЖАНИЕ

# 1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 1.1 Определение и эволюция термина «информационная безопасность»

Издавна считалось, кто владеет информацией - тот владеет ситуацией. Поэтому еще на заре человеческого общества возникает разведывательная деятельность. Поэтому появляются государственные и коммерческие (состав фарфора, шелка) секреты, а в период войн - военные (расположение войск, орудия). Стремление сохранить втайне от других то, что дает преимущество и власть, видимо является главной мотивацией людей в исторической перспективе. Многие собственники в целях защиты своих интересов засекречивают информацию и тщательно ее охраняют или патентуют. Засекречивание информации приводит к постоянному совершенствованию средств и методов добывания охраняемой информации; и к совершенствованию средств и методов защиты информации.

В мировой практике сначала применялись термины "промышленная тайна", "торговая тайна", "тайна кредитных отношений", т.е. название тайны увязывалось с конкретной сферой деятельности. Российский юрист В. Розенберг сделал попытку объединить эти названия в одном - "промысловая тайна" и даже выпустил в 1910 г. одноименную книгу. Однако этот термин не прижился. И в Российской империи и за рубежом окончательно утвердился термин "коммерческая тайна", объединяющий тайну любой деятельности, имеющей целью извлечение прибыли.

Со второй половины XIX в. появляются и различные определения понятия коммерческой тайны, в первую очередь, в сфере уголовного и гражданского законодательства. Например, немецкое законодательство определяло коммерческую тайну как тайну технических процессов изготовления продукции и тайну операций по ее сбыту или, как выражались более высоким языком, тайну производства благ и тайну их распределения.

В России по Уголовному уложению 1903 г. под коммерческой тайной понимались особые употребляемые или предполагаемые к употреблению приемы производства, а в другой редакции - индивидуальные особенности процессов производства и торговли. Тайна процессов производства классифицировалась тайной имущественной, а торговли - тайной деловой.

В России в ноябре 1917 г. коммерческая тайна была отменена. Во время НЭПа она неофициально "возродилась", но в дальнейшем использовалась лишь внешнеторговыми предприятиями СССР при контактах с другими странами, однако отечественной законодательной основы под этим не было. Прекратилась и научная деятельность в этой области.

Во второй половине 80-х гг. предпринимательская деятельность потребовала разработки связанных с ней нормативных документов, в том числе касающихся коммерческой тайны. В первую очередь нужно было сформулировать определение коммерческой тайны. Такое определение было сделано в Законе "О предприятиях в СССР". В нем сказано: "Под коммерческой тайной предприятия понимаются не являющиеся государственными секретами сведения, свя-

занные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам".

Коммерческая тайна в современной трактовке - информация, данные, сведения, объекты, разглашение, передача или утечка которых третьими лицами могут нанести ущерб интересам или безопасности обладателя.

Стандарт ISO/IEC 17799 определяет информационную безопасность как обеспечение конфиденциальности, целостности и наличия информации.

Безопасность - это не только защита от преступных посягательств, но и обеспечение сохранности (особенно электронных) документов и информации, а также меры по защите важнейших документов и обеспечению непрерывности и/или восстановлению деятельности в случае катастроф.

Под информационной безопасностью следует понимать защиту субъектов информационных отношений. Основные ее составляющие - конфиденциальность, целостность, доступность.

В Доктрине информационной безопасности РФ термин "информационная безопасность" обозначает состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Конфиденциальность - защита от несанкционированного доступа. Следующее определение конфиденциальности дает ФЗ "Об информации, информационных технологиях и о защите информации" ст.2.п.7: конфиденциальность - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Под безопасностью информационных ресурсов (информации) понимается защищенность информации во времени и пространстве от любых объективных и субъективных угроз (опасностей), возникающих в обычных условиях функционирования фирмы в условиях экстремальных ситуаций: стихийных бедствии, других неуправляемых событий, пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу несанкционированного доступа к документам, делам, базам данных.

Конфиденциальность - правила и условия сохранности передачи данных и информации. Различают конфиденциальность внешнюю - как условие неразглашения информации во внешнюю среду, и внутреннюю - среди персонала.

Безопасность ценной документируемой информации (документов) определяется степенью ее защищенности от последствий экстремальных ситуаций, в том числе стихийных бедствий, а также пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу (опасность) несанкционированного доступа к документам с использованием организационных и технических каналов, в результате чего могут произойти хищение и неправомерное использование злоумышленником информации в своих целях, ее модификация, подмена, фальсификация, уничтожение.

Секретность - правила и условие доступа и допуска к объектам информации.

Таким образом, словосочетание "информационная безопасность" не сводится исключительно к защите от несанкционированного доступа к информации.

Это принципиально широкое понятие. Субъект информационных отношении может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе.

Несмотря на то, что конфиденциальность является синонимом секретности, этот термин широко используется исключительно для обозначения информационных ресурсов ограниченного доступа, не отнесенных к государственной тайне.

Конфиденциальность отражает ограничение, которое накладывает собственник информации па доступ к ней других лиц, т.е. собственник устанавливает правовой режим этой информации в соответствии с законом.

## 1.2 Цели, задачи, направления исследования и практической реализации информационной безопасности

В беседах со специалистами по защите информации зачастую обнаруживается, что взгляды и терминология в этой относительно новой области различаются иногда почти до противоположных. При прямом вопросе об определении информационной безопасности можно услышать такие разноуровневые термины, как "защита данных", "контроль использования", "борьба с хакерами" и т.д.

Между тем существуют сложившиеся определения самой информационной безопасности и примыкающего к ней круга понятий. Иногда они различаются у различных специалистов (или школ). Случается, в определениях просто используют синонимы, иногда — меняются местами даже целые группы понятий. Поэтому первоначально необходимо четко определиться, о чем же будет идти речь в данной статье. Хотя оба автора получали образование в области информационной безопасности совершенно независимо друг от друга, тем не менее их определения и понятия практически совпадают, поэтому было решено использовать именно данный подход. Для всей области знаний, охватываемой данной книгой, будет использоваться термин "информационная безопасность". Иногда, особенно в классификации зарубежных агентств по найму на работу, "информационная безопасность" рассматривается как один из подразделов общей безопасности, наряду с такими понятиями как "компьютерная безопасность", "сетевая безопасность", "безопасность телекоммуникаций", "безопасность данных".

На наш взгляд, понятие "информационная безопасность" более широкое, так как охватывает всё, что взаимодействует с информацией, и все вышеперечисленные понятия — это подразделы или отдельные направления информационной безопасности.

Информационная безопасность — это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы:

• конфиденциальность — возможность ознакомится с информацией (именно с данными или сведениями, несущими смысловую нагрузку, а не с последовательностью бит их представляющих) имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями;

• целостность — возможность внести изменение в информацию (опять речь идет о смысловом выражении) должны иметь только те лица, кто на это уполномочен;

• доступность — возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени.

Иногда можно встретить определения перечисленных факторов в варианте от противного, например разглашение или раскрытие, модификация (изменение или искажение) и уничтожение или блокирование. Главное, чтобы не был искажен смысл, заложенный в указанных определениях.

Это не полный список факторов, выделены именно эти три понятия, поскольку они обычно встречаются практически во всех определениях информационной безопасности и не вызывают споров. На наш взгляд, необходимо включить дополнительные факторы и понять различие между ними, а именно:

• учет, т. е. все значимые действия лица, выполняемые им в рамках, контролируемых системой безопасности (даже если они не выходят за рамки определенных для этого лица правил), должны быть зафиксированы и проанализированы;

• неотрекаемость или апеллируемость (характерно для организаций, в которых функционирует обмен электронными документами с юридической, финансовой или другой значимостью), т. е. лицо, направившее информацию другому лицу, не может отречься от факта направления информации, а лицо, получившее информацию, не может отречься от факта ее получения.

Отличие между двумя этими факторами, возможно, видимое не сразу, заключается в следующем. Учет обычно ведется средствами электронных регистрационных журналов, которые используются в основном только уполномоченными службами, и его основное отличие — в регулярности анализа этих журналов. Апеллируемость обеспечивается средствами криптографии (электронно-цифровой подписью), и ее характерная черта — возможность использования в качестве доказательного материала во внешних инстанциях, например в суде, при наличии соответствующего законодательства.

*Механизмы информационной безопасности*

Перечисленные объективные факторы или цели информационной безопасности обеспечиваются применением следующих механизмов или принципов:

• политика — набор формальных (официально утвержденных либо традиционно сложившихся) правил, которые регламентируют функционирование механизма информационной безопасности;

• идентификация — определение (распознавание) каждого участника процесса информационного взаимодействия перед тем как к нему будут применены какие бы то ни было понятия информационной безопасности;

• аутентификация — обеспечение уверенности в том, что участник процесса обмена информацией идентифицирован верно, т. е. действительно является тем, чей идентификатор он предъявил;

• контроль доступа — создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа;

• авторизация — формирование профиля прав для конкретного участника процесса информационного обмена (аутентифицированного или анонимного) из набора правил контроля доступа;

• аудит и мониторинг — регулярное отслеживание событий, происходящих в процессе обмена информацией, с регистрацией и анализом предопределенных значимых или подозрительных событий. Понятия "аудит" и "мониторинг" при этом несколько различаются, так как первое предполагает анализ событий постфактум, а второе приближено к режиму реального времени;

• реагирование на инциденты — совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационной безопасности;

• управление конфигурацией — создание и поддержание функционирования среды информационного обмена в работоспособном состоянии и в соответствии с требованиями информационной безопасности;

• управление пользователями — обеспечение условий работы пользователей в среде информационного обмена в соответствии с требованиями информационной безопасности.

В данном случае под пользователями понимаются все, кто использует данную информационную среду, в том числе и администраторы;

управление рисками — обеспечение соответствия возможных потерь от нарушения информационной безопасности мощности защитных средств (то есть затратам на их построение);

обеспечение устойчивости — поддержание среды информационного обмена в минимально допустимом работоспособном состоянии и соответствии требованиям информационной безопасности в условиях деструктивных внешних или внутренних воздействий.

Таким образом, перечислено то, за счет чего достигаются определенные выше цели информационной безопасности (в некоторых источниках описанные принципы, например, аутентификация, переносятся в цели). На наш взгляд, аутентификация сама по себе не может быть целью информационной безопасности. Она является лишь методом определения участника информационного обмена, чтобы далее определить, какая, например, политика в отношении конфиденциальности или доступности должна быть применена к данному участнику.

### *Инструментарий информационной безопасности*

Теперь рассмотрим, какие существуют средства или инструменты, которыми реализованы описанные принципы или механизмы. Естественно, что привести полный список здесь просто невозможно — он в значительной степени зависит от конкретной ситуации, в свете которой рассматривается тот или иной аспект информационной безопасности. Кроме того, возможно, кто-либо захо-

чет переместить некоторые пункты из списка механизмов в список средств или наоборот. Наши рассуждения имеют следующий базис. Например, персонал занимается аудитом, который обеспечивает учет. Значит, персонал — это средство, аудит — механизм, а учет — цель. Или пароли, обеспечивающие аутентификацию, сохраняются в шифрованном виде, аутентификация предшествует, например, разрешению на модификацию. Значит, криптография — средство защиты паролей, пароли используются для механизма аутентификации, аутентификация предшествует обеспечению целостности.

Перечислим основные средства (инструменты) информационной безопасности:

- персонал — люди, которые будут обеспечивать претворение в жизнь информационной безопасности во всех аспектах, то есть разрабатывать, внедрять, поддерживать, контролировать и исполнять;
- нормативное обеспечение — документы, которые создают правовое пространство для функционирования информационной безопасности;
- модели безопасности — схемы обеспечения информационной безопасности, заложенные в данную конкретную информационную систему или среду;
- криптография — методы и средства преобразования информации в вид, затрудняющий или делающий невозможным несанкционированные операции с нею (чтение и/или модификацию), вместе с методами и средствами создания, хранения и распространения ключей — специальных информационных объектов, реализующих эти санкции;
- антивирусное обеспечение — средство для обнаружения и уничтожения зловредного кода (вирусов, троянских программ и т. п.);
- межсетевые экраны — устройства контроля доступа из одной информационной сети в другую;
- сканеры безопасности — устройства проверки качества функционирования модели безопасности для данной конкретной информационной системы;
- системы обнаружения атак — устройства мониторинга активности в информационной среде, иногда с возможностью принятия самостоятельного участия в указанной активной деятельности;
- резервное копирование — сохранение избыточных копий информационных ресурсов на случай их возможной утраты или повреждения;
- дублирование (резервирование) — создание альтернативных устройств, необходимых для функционирования информационной среды, предназначенных для случаев выхода из строя основных устройств;
- аварийный план — набор мероприятий, предназначенных для претворения в жизнь, в случае если события происходят или произошли не так, как было предопределено правилами информационной безопасности;
- обучение пользователей — подготовка активных участников информационной среды для работы в условиях соответствия требованиям информационной безопасности.

Возможно, некоторые понятия слишком укрупнены (криптография), некоторые, наоборот, детализированы (сканеры). Основной целью этого списка ставилось показать типовой набор, характерный для предприятия, которое развивает у себя службу информационной безопасности.

*Основные направления информационной безопасности*

Теперь осталось рассмотреть основные направления информационной безопасности, которые иногда различают между собой. Собственно, на наш взгляд их всего два — физическая и компьютерная безопасность. Однако, учитывая имеющиеся различия в определениях, можно охарактеризовать их следующим образом.

• *Физическая безопасность* — обеспечение сохранности самого оборудования, предназначенного для функционирования информационной среды, контроль доступа людей к этому оборудованию. Дополнительно сюда может быть включено понятие защиты самих пользователей информационной среды от физического воздействия злоумышленников, а также защиты информации невиртуального характера (твердых копий — распечаток, служебных телефонных справочников, домашних адресов сотрудников, испорченных внешних носителей и т. п.).

• *Компьютерная безопасность (сетевая безопасность, телекоммуникационная безопасность, безопасность данных)* — обеспечение защиты информации в ее виртуальном виде. Возможно выделять этапы нахождения информации в среде, и по этим принципам разделять, например, компьютерную (на месте создания, сохранения или обработки информации) и сетевую (при пересылке) безопасность, но это, в принципе, нарушает комплексную картину безопасности. Единственное, с чем логично было бы согласиться, — это термин безопасность данных, или скорее, безопасность данных в рамках данного приложения. Дело в том, что в конкретном программном комплексе модель безопасности может быть реализована таким образом, что это потребует отдельного специалиста (или даже службы) по ее поддержанию. В этом случае, возможно разделить понятия безопасность данных (конкретного приложения) и безопасность сети (всей остальной информационной среды).

## 1.3 Обзор компьютерных преступлений

**Компьютерные преступления -** это предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть. Компьютерные преступления условно можно подразделить на две большие категории:

- преступления, связанные с вмешательством в работу компьютеров;
- преступления, использующие компьютеры как необходимые технические средства.

Перечислим основные виды преступлений, связанных с вмешательством в работу компьютеров.

**Несанкционированный доступ к информации, хранящейся в компьютере.** Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, мо-

дификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакер, «компьютерный пират» - лицо, совершающее систематические несанкционированные доступы в компьютерные системы и сети с целью развлечения, мошенничества или нанесения ущерба (в том числе и путем путем распространения компьютерных вирусов). С одной стороны «хакер», это человек, который прекрасно знает компьютер и пишет хорошие программы, а с другой - незаконно проникающий в компьютерные системы с целью получения информации.

Английский глагол «to hack» применительно к компьютерам может означать две вещи - взломать систему или починить ее. В основе этих действий лежит общая основа: понимание того, как устроен компьютер, и программы, которые на нем работают.

Таким образом, слово «хакер» совмещает в себе по крайней мере два значения: одно - окрашенное негативно («взломщик»), другое - нейтральное или даже хвалебное («ас», «мастер»). Другими словами, хакеров можно разделить на «плохих» и «хороших».

«Хорошие хакеры» двигают технический прогресс и используют свои знания и умения на благо человечества. Ими разработано большое число новых технических и программных систем.

Им, как водится, противостоят «плохие» - они читают чужие письма, воруют чужие программы и всеми доступными способами вредят прогрессивному человечеству.

«Плохих хакеров» можно условно разделить на четыре группы. Первая, состоящая в основном из молодежи, - люди, взламывающие компьютерные системы просто ради собственного удовольствия. Они не наносят вреда, а такое занятие весьма полезно для них самих - со временем из них получаются превосходные компьютерные специалисты.

Вторая группа - пираты. Они взламывают защиту компьютеров для похищения новых программ и другой информации.

Третья группа - хакеры, использующие свои познания действительно во вред всем и каждому. Они уничтожают компьютерные системы, в которые им удалось прорваться, читают чужие письма, а потом издеваются над их авторами. Когда читаешь в телеконференциях их рассказы о взломах, складывается впечатление, что это люди с ущемленным чувством собственного достоинства.

Есть и еще одна группа - хакеры, которые охотятся за секретной информацией по чьим-либо заказам.

*История жизни одного хакера*

Одним из известнейших хакеров прошлого столетия считается гражданин США Кевин Митник (Kevin Mitnick). Будучи 17-летним подростком, он взломал компьютерную систему тихоокеанского отделения компании Белл (Pacific Bell) через обычный телефонный автомат на платной автостоянке. Тогда он изменил несколько телефонных счетов, проник в частные ПК и выкрал данные стоимостью в $200 000 из компьютерной системы одной компании в Сан-Франциско. Митника приговорили к шестимесячному заключению, но вскоре выпустили, а

из полицейских компьютерных архивов вся информация об этом преступлении таинственным образом исчезла.

Через год Митние снова привлекает общественное внимание: используя ПК и модем он проникает в компьютер командного пункта воздушной обороны Северной Америки. Помимо этого, Митник стал контролировать офисы трех телефонных компаний в Нью-Йорке и все телефонные центры в Калифорнии, что позволило ему подслушивать телефонные переговоры и перепрограммировать номера некоторых телефонов так, что они стали требовать повышенной оплаты при любых разговорах. Не стоит даже говорить о серьезности подобных правонарушений, однако это, как говорится, были только "цветочки".

В 1988 году Митника обвинили в двух новых преступлениях против компании DEC (Digital Equipment Corporation): нанесение ущерба в 4 млн. долларов и кража программного обеспечения стоимостью еще в 1 млн. долларов. В том же году Митник проник в сеть одной из двух крупнейших телефонных компаний США - MCI - через университетские компьютеры в Лос-Анджелесе и Англии. Это позволило ему прослушивать секретную информацию и читать почту различных должностных лиц о защите компьютеров и телефонных аппаратов в этих компаниях, за что в начале 1989 года Митника снова приговорили к году тюремного заключения.

После освобождения Митник провел полгода в реабилитационном центре в Лос-Анджелесе, где на протяжении всего этого периода его ни на шаг не подпускали к компьютеру и модему, и в середине 1990 года он был выпущен на свободу.

Тем не менее, федеральные органы следили за ним до ноября 1992 года, пока Митник не скрылся из виду. В 1993 году калифорнийский отдел регистрации автомашин (аналог российского ГИБДД) обвинил Митника в подслушивании звонков агентов ФБР и использовании незаконно приобретенных секретных кодов для получения доступа к базе данных по водительским правам, выданным в Калифорнии. Кроме того, Митник подозревается еще в ряде незаконных проникновений в компьютерные и телефонные сети.

Митнику предъявлено два обвинения: первое - незаконное использование телефонного устройства, наказуемое 15 годами заключения и штрафом в $250,000, и второе - компьютерное мошенничество, наказание за которое предусматривает до 20 лет заключения и штраф в $250.000.

В настоящее время хакер находится в тюрьме. Его доступ к телефону ограничен: он может звонить только своему адвокату и некоторым родственникам, причем только под надзором служащих полиции - судебные исполнители опасаются возможности того, что Митник получит незаконный доступ к какой-либо секретной информации прямо из тюремной камеры.

**Ввод в программное обеспечение “логических бомб”**, которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

“Временная бомба” - разновидность “логической бомбы”, которая срабатывает по достижении определенного момента времени.

Способ “троянский конь” состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся

владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. С помощью “троянского коня” преступники, например, отчисляют на свой счет определенную сумму с каждой операции.

Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен, тысяч, а иногда и миллионов команд. Поэтому “троянский конь” из нескольких десятков команд вряд ли может быть обнаружен, если, конечно, нет подозрений относительно этого. Но и в последнем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Есть еще одна разновидность “троянского коня”. Ее особенность состоит в том, что в безобидно выглядящий кусок программы вставляются не команды, собственно, выполняющие “грязную” работу, а команды, формирующие эти команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти “троянского коня”, необходимо искать не его самого, а команды, его формирующие. Развивая эту идею, можно представить себе команды, которые создают команды и т.д. (сколь угодно большое число раз), создающие “троянского коня”.

*Дело Левина*

17 августа 1995 г. в Лондонском суде Bow Street Magistrates началось слушание уголовного дела, согласно которому россиянин Владимир Левин обвинялся в ограблении американского банка Citibank на 2,8 миллиона долларов. Из них 400 тыс. исчезло бесследно.

Хакер взломал банковскую сеть Citibank'a, находясь в маленьком офисе АОЗТ "Сатурн" в Петербурге, которое занималось торгово-посредническими операциями. В июле 1994 года он вместе со своим напарником - одним из совладельцев фирмы "Сатурн" - впервые проник в компьютерный центр Citibank'a и перевел из него деньги в калифорнийское отделение Bank of Amerika на счета своих друзей.

Похищенные деньги перемещались в банки Финляндии, Израиля, Германии, Голландии, Швейцарии и России. Часть сумм обнаружили в Сан-Франциско и в одном из голландских банков на счетах эмигрантов из России. Вскоре одновременно в нескольких городах были арестованы граждане, пытавшиеся обналичить счета В. Левина.

Технология оказалась несложной: хакер подключился к компьютеру одного из американских банкиров и запустил в него «троянского коня», который открыл доступ к файлам системы управления наличных счетов. Взломщик несколько месяцев «сидел» на линии, просматривая чужие файлы и следя за движением миллиардов долларов.

Сразу после инцидента служба безопасности Citibank'a совместно с правоохранительными органами начала работу по выявлению нарушителя. Однако в течение полугода американские спецслужбы (в том числе ФБР) не могли его достать - арестовать Левина было возможно только за пределами России. Специалисты американских спецслужб дурачили Левина, позволяя ему перекидывать несуществующие деньги со счетов Citibank'a (на жаргоне хакеров такая операция называется "dummy" - пустышка).

До сих пор держится в секрете, как лосанджелесские банкиры обнаружили компьютер, с которого была предпринята попытка проникновения в сеть

Citibank'a. Достоверно известно только то, что помощь в розыске Левина оказал хакер из Сан-Франциско, который около полутора лет тому назад был арестован по обвинению во взломе компьютерной банковской системы того же самого Citibank'a.

Приговор: 4 года лишения свободы плюс крупный штраф.

**Разработка и распространение компьютерных вирусов.**

**Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.**

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти не достижима.

**Подделка компьютерной информации.**

По-видимому, этот вид компьютерной преступности является одним из наиболее свежих. Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосовании, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

**Хищение компьютерной информации.**

Если “обычные” хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путем краж и обмена краденым. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться.

Рассмотрим теперь вторую категорию преступлений, в которых компьютер является “средством” достижения цели.

1. Разработка сложных математических моделей, входными данными в которых являются возможные условия проведения преступления, а выходными данными - рекомендации по выбору оптимального варианта действий преступника.

2. Преступления с общим названием - “воздушный змей”.

В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз ("воздушный змей" поднимается все выше и выше) до тех пор, пока на счете не оказывается приличная сумма (фактически она постоянно "перескакивает" с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются, а владелец счета исчезает. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое количество банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

**Вопросы по пройденному материалу:**

1. Дайте определение терминам «информационная безопасность», «коммерческая тайна».
2. Назовите факторы, которые должна обеспечивать система защиты.
3. Приведите примеры компьютерных преступлений.

# 2. АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ

## 2.1 Риски угроз информационным ресурсам. Понятие угрозы (опасности) информации, виды угроз

Организация обеспечения безопасности информации должна носить комплексный характер и основываться на глубоком анализе возможных негативных последствий. При этом важно не упустить какие-либо существенные аспекты. Анализ негативных последствий предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению и, как следствие, определение актуальных угроз безопасности информации.

В ходе такого анализа необходимо убедиться, что все возможные источники угроз идентифицированы, идентифицированы и сопоставлены с источниками угроз все возможные факторы (уязвимости), присущие объекту защиты, всем идентифицированным источникам и факторам сопоставлены угрозы безопасности информации.

Исходя их данного принципа, моделирование и классификацию источников угроз и их проявлений, целесообразно проводить на основе анализа взаимодействия логической цепочки: **источник угрозы - фактор (уязвимость) - угроза (действие) - последствия (атака).**

Под этими терминами будем понимать:

**Источник угрозы** - это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

**Угроза (действие)** [Threat]- это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.

**Фактор (уязвимость)** [Vulnerability]- это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.

**Последствия (атака)** - это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).

Как видно из определения, атака - это всегда пара "источник - фактор", реализующая угрозу и приводящая к ущербу. При этом, анализ последствий предполагает проведение анализа возможного ущерба и выбора методов парирования угроз безопасности информации

Угроз безопасности информации не так уж и много. Угроза, как следует из определения, это опасность причинения ущерба, то есть в этом определении проявляется жесткая связь технических проблем с юридической категорией, каковой является "ущерб".

*Ущерб как категория классификации угроз*

Проявления возможного ущерба могут быть различны:

- моральный и материальный ущерб деловой репутации организации;
- моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;
- материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;
- материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;
- материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;
- моральный и материальный ущерб от дезорганизации деятельности организации;
- материальный и моральный ущерб от нарушения международных отношений.

Ущерб может быть причинен каким-либо субъектом и в этом случае имеется на лицо правонарушение, а также явиться следствием независящим от субъекта проявлений (например, стихийных случаев или иных воздействий, таких как проявления техногенных свойств цивилизации). В первом случае налицо вина субъекта, которая определяет причиненный вред как состав преступления, совершенное по злому умыслу (умышленно, то есть деяние совершенное с прямым или косвенным умыслом) или по неосторожности (деяние, совершенное по легкомыслию, небрежности, в результате невиновного причинения вреда) и причиненный ущерб должен квалифицироваться как состав преступления, оговоренный уголовным правом.

Во втором случае ущерб носит вероятностный характер и должен быть сопоставлен, как минимум с тем риском, который оговаривается гражданским, административным или арбитражным правом, как предмет рассмотрения.

В теории права под ущербом понимается невыгодные для собственника имущественные последствия, возникшие в результате правонарушения. Ущерб выражается в уменьшении имущества, либо в недополучении дохода, который был бы получен при отсутствии правонарушения (упущенная выгода).

При рассмотрении в качестве субъекта, причинившего ущерб какую-либо личность, категория "ущерб" справедлива только в том случае, когда можно доказать, что он причинен, то есть деяния личности необходимо квалифицировать в терминах правовых актов, как состав преступления. Поэтому, при классификации угроз безопасности информации в этом случае целесообразно учитывать требования действующего уголовного права, определяющего состав преступления.

Вот некоторые примеры составов преступления, определяемых Уголовным Кодексом Российской Федерации.

**Хищение** - совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества.

**Копирование компьютерной информации** - повторение и устойчивое запечатление информации на машинном или ином носителе

**Уничтожение** - внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводятся в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота.

**Уничтожение компьютерной информации** - стирание ее в памяти ЭВМ.

**Повреждение** - изменение свойств имущества при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования.

**Модификация компьютерной информации** - внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных.

**Блокирование компьютерной информации** - искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

**Несанкционированное уничтожение, блокирование модификация, копирование информации** - любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией.

**Обман (отрицание подлинности, навязывание ложной информации)** - умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений.

Однако, говорить о злом умысле личности в уничтожении информации в результате стихийных бедствий не приходится, как и тот факт, что вряд ли стихия сможет воспользоваться конфиденциальной информацией для извлечения собственной выгоды. Хотя и в том и в другом случае собственнику информации причинен ущерб. Здесь правомочно применение категории "причинение вреда имуществу". При этом, речь пойдет не об уголовной ответственности за уничтожение или повреждение чужого имущества, а о случаях подпадающих под гражданское право в части возмещения причиненного ущерба (риск случайной гибели имущества - то есть риск возможного нанесения убытков в связи с гибелью или порчей имущества по причинам, не зависящим от субъектов). По общему правилу в этом случае убытки в связи с гибелью или порчей имущества несет собственник, однако, гражданское право предусматривает и другие варианты компенсации причиненного ущерба.

При рассмотрении в качестве субъекта, причинившего ущерб какое-либо природное или техногенное явление, под ущербом можно понимать невыгодные для собственника имущественные последствия, вызванные этими явлениями и которые могут быть компенсированы за счет средств третьей стороны (страхование рисков наступления события) или за счет собственных средств собственника информации.

Например, страхование представляет собой отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов. Объектами страхования могут быть не противоречащие законодательству Российской Федерации имущественные ин-

тересы связанные с возмещением страхователем причиненного им вреда личности или имуществу физического лица, а также вреда, причиненного юридическому лицу.

*Классификация угроз информационной безопасности*

Обобщая изложенное, можно утверждать, что угрозами безопасности информации являются:

- хищение (копирование) информации;
- уничтожение информации;
- модификация (искажение) информации;
- нарушение доступности (блокирование) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

*Классификация возможных угроз информационной безопасности по ряду базовых признаков:*

*1. По природе возникновения.*

• Естественные угрозы – угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.

• Искусственные угрозы – угрозы информационной безопасности АС, вызванные деятельностью человека.

*2. По степени преднамеренности проявления.*

• Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала. Например: проявление ошибок программно-аппаратных средств; неумышленная порча носителей информации; ввод ошибочных данных; неумышленное повреждение каналов связи и т.д.

• Угрозы преднамеренного действия.

*3. По непосредственному источнику угроз.*

• Угрозы, непосредственным источником которых является природная среда (магнитные бури, радиоактивное излучение).

• Угрозы, непосредственным источником которых является человек (разглашение, передача информации).

• Угрозы, непосредственным источником которых являются программно-аппаратные средства. Например: запуск программ, способных при некомпетентном использовании вызвать потерю работоспособности системы (зависание или зацикливание) или необратимые изменения в системе (форматирование носителей информации, удаление данных).

*4. По положению источника угроз.*

• Угрозы, источник которых расположен вне контролируемой зоны территории, на которой находится АС. Например: перехват побочных электромагнитных, акустических и других излучений и линий связи.

• Угрозы, источник которых расположен в пределах контролируемой зоны территории, на которой находится АС. Например: отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем

(электропитания, охлаждения, вентиляции, линий связи); применение подслушивающих устройств.

- Угрозы, источник которых расположен в системе. Например: проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации.

*5. По степени зависимости от активности АС.*

- Угрозы, которые могут проявляться независимо от активности АС. Например: вскрытие шрифтов криптозащиты, хищение носителей информации.
- Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных. Например: угрозы выполнения и распространения программных вирусов.

*6. По степени воздействия на АС.*

- Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС. Например: копирование данных.
- Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС. Например: внедрение вирусов.

*7. По текущему месту расположения информации, хранимой и обрабатываемой в АС.*

- Угроза доступа к информации на внешних запоминающих устройствах. Например: копирование информации с жесткого диска.
- Угрозы доступа к информации в оперативной памяти. Например: чтение остаточной информации из оперативной памяти; чтение информации из областей оперативной памяти, используемых операционной системой; угроза доступа к системной области оперативной памяти.
- Угроза доступа к информации, циркулирующей в линиях связи. Например: подключение к линиям связи с последующим вводом ложных сообщений или модификацией передаваемых сообщений.

## 2.2 Классификация методов и средств защиты информации

К настоящему времени разработан значительный по номенклатуре арсенал различных средств защиты информации, с помощью которых может быть обеспечен требуемый уровень защищенности информации. Множество и разнообразие возможных средств защиты определяются прежде всего способами воздействия на дестабилизирующие факторы или порождающие их причины, причем воздействия в направлении, способствующем повышению значений показателей защищенности или (по крайней мере) сохранению прежних (ранее достигнутых) их значений. Эти способы могут быть классифицированы так, как показано на рис. 1.


Рис.1. Классификация способов и средств защиты информации.

Существо выделенных на рисунке 1 способов защиты может быть охарактеризовано так.

1. *Препятствие* заключается в создании на пути возникновения или распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры. Типичными примерами препятствий являются блокировки, не позволяющие техническому устройству или программе выйти за опасные границы; создание физических препятствий на пути злоумышленников и т.п.

2. *Управление* есть определение на каждом шаге функционирования системы таких управляющих воздействий на элементы системы, следствием которых будет решение (или способствование решению) одной или нескольких задач защиты информации.

3. *Маскировка* (защищаемой информации) предполагает такие ее преобразования, вследствие которых она становится недоступной для злоумышленников или доступ к ней существенно затрудняется.

4. *Регламентация* как способ защиты информации заключается в разработке и реализации комплексов мероприятий, создающих такие условия обработки информации, при которых существенно затрудняется проявление и воздействие дестабилизирующих факторов.

5. *Принуждение* есть такой способ защиты, при котором пользователи и персонал вынуждены соблюдать правила и условия обработки под угрозой материальной, административной или уголовной ответственности.

6. *Побуждение* есть способ защиты информации, при котором пользователи и персонал внутренне (т.е. материальными, моральными, этическими, психологическими и другими мотивами) побуждаются к соблюдению всех правил обработки информации.

Перечисленные способы обеспечения защиты информации реализуются применением многих средств, причем различают формальные и неформальные средства. К *формальным* относятся такие средства, которые выполняют свои функции по защите информации формально, т.е. преимущественно без участия человека. К *неформальным* относятся средства, основу содержания которых составляет целенаправленная деятельность людей. Формальные средства делятся на технические (физические и аппаратные) и программные, неформальные — на организационные, законодательные и морально-этические.

Выделенные на рисунке 1 классы средств могут быть определены следующим образом.

*Физические средства* — механические, электрические, электромеханические, электронные, электронно-механические и т.п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

*Аппаратные средства* — различные электронные и электронно-механические и т.п. устройства, схемно- встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации.

*Программные средства* — специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации.

*Организационные средства* — организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации.

*Законодательные средства* — нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности.

*Морально-этические средства* — сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

**Вопросы по пройденному материалу:**

1. Дайте определение терминам «угроза», «ущерб».
2. Назовите классификацию угроз информационной безопасности.
3. Охарактеризуйте способы и средства защиты информации.

# 3. ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

## 3.1 Требования к законодательству в области информационной безопасности

Анализ зарубежного опыта формирования законодательной базы в области информационной безопасности показывает, что разработка проблемы правового обеспечения защиты информации идет по трем направлениям:

*Защита прав личности на частную жизнь*

Этот аспект не является новым для мирового сообщества. Основные принципы установления пределов вмешательства в частную жизнь со стороны государства и других субъектов определены основополагающими нормами: Декларацией прав человека, Конвенцией ООН и Конвенцией Совета Европы по правам человека.

Развитие информатики в странах Запада и связанный с этим рост угрозы нарушения прав личности (бесконтрольное распространение и доступ к персональной информации) потребовали разработки специальных актов, учитывающих фактор информационной безопасности.

К концу 70-х годов были сформулированы три основных принципа обеспечения информационной безопасности, нашедшие впоследствии отражение в национальном законодательстве по информатике:

- установление пределов вмешательства в частную жизнь с использованием компьютерных систем;
- введение административных механизмов защиты граждан от такого вмешательства;
- защита интеллектуальной собственности личности.

К этому направлению можно отнести резолюцию Европарламента «О защите прав личности в связи с прогрессом информатики» (1979 г.) и конвенцию ЕС «О защите лиц при автоматизированной обработке данных персонального характера» (1980 г.).

*Защита государственных интересов*

Проблема решается с помощью достаточно разработанных национальных законодательств, определяющих национальные приоритеты в этой области. Интеграция стран - членов ЕС потребовала координации усилий в данной области, в результате чего общие принципы засекречивания информации были отражены в Конвенции ЕС «По защите секретности». Механизм защиты предусматривает следующие аспекты:

- установление приоритетов защиты;
- определение исполнительских механизмов и нормативное обеспечение механизмов защиты.

*Защита предпринимательской и финансовой деятельности*

Это направление деятельности осуществляется путем создания законодательного механизма, обеспечивающего защиту коммерческой тайны и создающего условия для осуществления «добросовестной» конкуренции.

При создании в нашей стране правовой основы информационной безопасности необходимо учитывать:

- состояние и состав международных норм в области информатизации;
- состояние отечественного законодательства в этой и смежных областях;
- формирование системы законодательства с охватом всех ее уровней, обеспечением преемственности и совместимости норм в законах разного уровня – конституционных, общих, специальных;
- последовательный выход на развитие ведомственных и местных нормативных актов с опорой на законодательную основу;
- создание механизмов, обеспечивающих организацию, применение, действенность законодательной базы информатизации.

Направления создания правовой базы в области информационной безопасности должны затрагивать все уровни законодательства России:

- конституционное законодательство;
- основные общие законы;
- законы по организации государственной системы управления;
- специальные законы.

Например, конституционно должны быть закреплены и оформлены права граждан, организаций, государства на информацию и последовательно обеспечены во всех основных законах – о собственности, правах граждан, гражданстве, предпринимательстве и т.д.

Вопросы информационного обеспечения обязательно должны присутствовать в законах о разделении компетенции и правовом статусе различных государственных систем, органов и организаций государственного устройства по вертикали и горизонтали.

Специальные законы в области информатизации должны быть ориентированы на создание условий в организации и упорядочении самой информации, управление государственными информационными ресурсами, обеспечение процесса включения современных технологий во все направления информатизации, создание системы защиты информации, установление гарантий и т.д.

Кроме федерального законодательства вопросы информационной безопасности должны быть учтены в законодательстве республик в составе Российской Федерации.

Важное место в правовом обеспечении информатизации должны занимать подзаконные нормативные акты, отражающие процессы защиты информации.

Завершить эту иерархическую структуру системы законодательства должно правоохранительное законодательство, включающее нормы об ответственности за правонарушения при работе с информацией.

На уровне административного государственного регулирования в порядке исполнения указанных законов соответствующими органами государственного управления должны быть разработаны государственные стандарты, устанавливающие нормы защищенности информации, а также требования и правила организационного и технического характера. В них должны учитываться характеристики уязвимости информации, определена совокупность комплексных мер

защиты, необходимых для безопасной обработки информации в зависимости от уровня ее ценности или общественной опасности нарушений в работе информационных систем.

Анализ рассмотренной структуры законодательной базы информационной безопасности позволяет сделать вывод о том, что в настоящее время осуществляется переход от принципа «интегральной защиты» информации к принципу «дифференциальной защиты», обеспечивающему равносильную защиту различных видов защищаемых сведений. При этом следует отметить, что задача создания стройной законодательной системы, одновременно удовлетворяющей всем изложенным требованиям комплексной защиты информации, оказывается весьма сложной и на сегодняшний день не имеет адекватных решений.

### 3.2 Конституция и законодательные акты РФ о защите информации

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Самое важное (и, вероятно, самое трудное) на законодательном уровне — создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом развития современного общества, в частности, информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это может привести к снижению информационной безопасности.

Законодательство в сфере информационной безопасности в Российской Федерации начало развиваться только в начале девяностых годов прошлого столетия. Ряд законодательных актов довольно долго действовал в старых редакциях, часть документов утратили свою самостоятельность и были включены в Гражданский кодекс РФ. В рамках данной темы дается возможность проследить судьбу некоторых актуальных документов.

Одним из основных законов Российской Федерации является **Конституция**, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 — право на знание достоверной информации о состоянии окружающей среды.

Статья 23 Конституции гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных пере-

говоров, почтовых, телеграфных и иных сообщений, статья 29 — право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к *средствам защиты информации.*

В **Уголовном кодексе Российской Федерации** Глава 28 носит название «Преступления в сфере компьютерной информации», которая содержит три статьи:

- Статья 272. Неправомерный доступ к компьютерной информации;
- Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Статья 272 УК РФ описывает ситуации неправомерного доступа к охраняемой законом компьютерной информации лицом или группами лиц, повлекшие за собой уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Здесь описаны штрафные и уголовные меры за содеянное.

Статья 273 УК РФ знакомит с мерами пресечения действий в отношении создания программ для ЭВМ или внесения изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети и т. д.

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

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи интересны руководящие документы, выпущенные Федеральной службой по техническому и экспортному контролю Российской Федерации, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно можно выделить документ по межсетевым экранам, вводящий в официальную сферу один из самых современных классов защитных средств.

В информационном обществе нормативно-правовая база должна быть согласована с международной практикой. Особое внимание следует обратить на то, что желательно привести российские стандарты и сертификационные нормативы в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности. Есть целый ряд оснований для того, чтобы это сделать. Одно из них — необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских компаний. Второе (более существенное) — доминирование аппаратно-программных продуктов зарубежного производства.

На законодательном уровне должен быть решен вопрос об отношении к таким изделиям. Здесь необходимо выделить два аспекта: независимость в об-

ласти информационных технологий и информационную безопасность. Использование зарубежных продуктов в некоторых критически важных системах (в первую очередь, военных) может представлять угрозу национальной безопасности (в том числе информационной безопасности), поскольку нельзя исключить вероятности встраивания закладных элементов. В то же время, в подавляющем большинстве случаев потенциальные угрозы информационной безопасности носят исключительно внутренний характер. В таких условиях незаконность использования зарубежных разработок (ввиду сложностей с их сертификацией) при отсутствии отечественных аналогов затрудняет (или вообще делает невозможной) защиту информации без серьезных на то оснований.

Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно сложна, однако, как показывает опыт европейских стран, решить ее можно. Сложившаяся в Европе система сертификации по требованиям информационной безопасности позволила оценить операционные системы, системы управления базами данных и другие разработки американских компаний. Вхождение России в эту систему и участие российских специалистов в сертификационных испытаниях в состоянии снять имеющееся противоречие между независимостью в области информационных технологий и информационной безопасностью без какого-либо ущерба для национальной безопасности.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

- разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
- обеспечение баланса созидательных и ограничительных (в первую очередь преследующих цель наказать виновных) законов;
- интеграция в мировое правовое пространство;
- учет современного состояния информационных технологий.

Предлагаем ознакомиться с некоторыми важными нормативно-правовыми документами в области информационных технологий и информационной безопасности более подробно.

**Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992 г. 3523-1). Закон «Об авторском праве и смежных правах» (от 09.07.1993 г. 5351-1 с последующим изменением и дополнением). Четвертая часть Гражданского кодекса РФ (от 18.12.2006 г. 230-ФЗ). Федеральный закон «О введении в действие части четвертой Гражданского кодекса РФ» (от 18.12.2006 г. 231-ФЗ)**

Два важных документа — Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992 г. 3523—1) и Закон «Об авторском праве и смежных правах» (от 09.07.1993 г. 5351—1) были введены в действие с целью регулирования правовых норм в отношении авторского права и охране программ для ЭВМ. Законы работали самостоятельно

до 1 января 2008 года, в связи с введением в действие ФЗ «О введении в действие части четвертой гражданского кодекса РФ» (от 18.12.2006 г. 231-ФЗ).

Четвертая часть гражданского кодекса РФ (от 18.12.2006 г. 230-ФЗ), в текстах которого прописаны нормы правовой охраны программ для ЭВМ и баз данных, затрагивает права на результаты интеллектуальной деятельности и средства индивидуализации (к которым и относятся программы для ЭВМ и базы данных); авторское право; права, смежные с авторскими; патентное право и т. д. Отсюда можно узнать, как используется авторское право, как оно действует, какие есть ограничения в использовании авторских прав, как составляются договора и документы по авторскому праву и охране программ для ЭВМ, какие санкции могут применяться относительно неправомерного использования авторского права и т. д.

**Закон «О государственной тайне» (от 21.07.1993 г. 5485-1 с последующим изменением и дополнением)**

Рассмотрим подробнее закон «О государственной тайне» (от 21.07. 1993г. 5485-1 с последующим изменением и дополнением). Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе «О государственной тайне» (с изменениями и дополнениями от 6 октября 1997 года). В нем ***гостайна*** определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Согласно данному Закону, ***средства защиты информации*** — это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации «О Безопасности» и включает в себя настоящий закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

**Федеральный закон «О связи» (от 07.07.2003 г. 126-ФЗ с последующим изменением и дополнением)**

Данный Федеральный закон впервые был принят в редакции от 16.02.1995г. за номером 15-ФЗ. В настоящее время имеют дело с редакцией от 07.07.2003г. 126-ФЗ с последующим изменением и дополнением. Закон устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной дея-

тельности или пользующихся услугами связи. Целями настоящего Федерального закона являются:

• создание условий для оказания услуг связи на всей территории Российской Федерации;

- содействие внедрению перспективных технологий и стандартов;
- защита интересов пользователей услугами связи и осуществляющих деятельность в области связи хозяйствующих субъектов;
- обеспечение эффективной и добросовестной конкуренции на рынке услуг связи;
- создание условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи;
- обеспечение централизованного управления российским радиочастотным ресурсом, в том числе орбитально-частотным, и ресурсом нумерации;
- создание условий для обеспечения потребностей в связи для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

Статья 63 «Тайна связи» Главы 9 «Защита прав пользователей услугами связи» затрагивает проблему конфиденциальности передаваемой информации операторами связи.

**Федеральный закон «Об информации, информационных технологиях и защите информации» (от 27.07.2006 г. 149-ФЗ)**

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон «Об информации, информатизации и защите информации» от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В настоящее время его название видоизменено и звучит следующим образом — «Об информации, информационных технологиях и защите информации». Закон в обновленном виде действует с 27 июля 2006 г. за номером 149-ФЗ.

Настоящий Федеральный закон регулирует отношения, возникающие при:

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

• применении информационных технологий;

• обеспечении защиты информации.

В нем даются основные определения и намечаются направления развития законодательства в данной области.

Приведем основные определения согласно статье 2:

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

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

3)**информационная система** — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных тех-

нологий и технических средств;

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

5)**обладатель информации** — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6)**доступ к информации** — возможность получения информации и ее использования;

7)**конфиденциальность информации** — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8)**предоставление информации** — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9)**распространение информации** — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10)**электронное сообщение** — информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11)**документированная информация** — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию — или в установленных, законодательством Российской Федерации случаях ее материальный носитель;

12)**оператор информационной системы** — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации прописаны в статье 3. Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

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

2)установление ограничений доступа к информации только федеральными законами;

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

4)равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5)обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них ин-

формации;

6)достоверность информации и своевременность ее предоставления;

7)неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8)недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 16 носит название «Защита информации» и затрагивает следующие аспекты:

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

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

2)соблюдение конфиденциальности информации ограниченного доступа;

3)реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3.Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

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

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

2)своевременное обнаружение фактов несанкционированного доступа к информации;

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

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

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

6)постоянный контроль за обеспечением уровня защищенности информации.

5.Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполни-

тельной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6.Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

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

Исходя из того, что практические умения и навыки по указанным выше вопросам представляется целесообразным формировать в условиях, приближенных к жизненным, наиболее подходящим средством для этого являются ситуационные задачи, т. е. задачи, которые формулируются в виде описания жизненных ситуаций.

10 января 2002 года Президентом был подписан очень важный ***закон «Об электронной цифровой подписи» номер 1-ФЗ*** (принят Государственной Думой 13 декабря 2001 года), развивающий и конкретизирующий приведенные выше положения закона «Об информации...». Его роль поясняется в **статье 1**.

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

2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

**Закон вводит следующие основные понятия:**

**Электронный документ** - документ, в котором информация представлена в электронно-цифровой форме.

**Электронная цифровая подпись** - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

**Владелец сертификата ключа подписи** - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

**Средства электронной цифровой подписи** - аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

**Сертификат средств электронной цифровой подписи** - документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

**Закрытый ключ электронной цифровой подписи** - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

**Открытый ключ электронной цифровой подписи** - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

**Сертификат ключа подписи** - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

**Подтверждение подлинности электронной цифровой подписи в электронном документе** - положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности
электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

**Пользователь сертификата ключа подписи** - физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

**Информационная система общего пользования** - информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

**Корпоративная информационная система** - информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Пересказать такие определения своими словами невозможно... Обратим внимание на неоднозначное использование термина «сертификат», которое,

впрочем, не должно привести к путанице. Кроме того, данное здесь определение электронного документа слабее, чем в Законе «Об информации...», поскольку нет упоминания реквизитов.

Согласно Закону, электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

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

**Закон определяет сведения, которые должен содержать сертификат ключа подписи:**

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

**Вопросы по пройденному материалу:**

1. Какие требования предъявляются к законодательству в области информационной безопасности?
2. Какие виды наказаний предусмотрены Уголовным Кодексом РФ за преступления в области информационных технологий?
3. Какие отношения регулирует Федеральный закон «Об информации, информационных технологиях и защите информации»?

# 4. ОРГАНИЗАЦИОННЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 4.1 Понятие, цели и задачи системы защиты конфиденциальной информации

**Конфиденциальность** (от англ. *confidence* — доверие) — необходимость предотвращения утечки (разглашения) какой-либо информации.

С этимологической точки зрения, слово «конфиденциальный» происходит от латинского confidentia — доверие. В современном русском языке это слово означает «доверительный, не подлежащий огласке, секретный». Слово «секрет», заимствовано из французского secret означает — «тайна». В словаре В. Даля также названы аналогичные значения: «конфиденциальная» — «откровенная, по особой доверенности, неоглашаемая, задушевная»; «тайна» — «кто чего не знает, то для него тайна, все сокрытое, неизвестное, неведомое». Исходя из определений понятия конфиденциальная информация, тайна, секрет являются равнозначными.

С развитием информационных технологий проблема конфиденциальности и конфиденциальной информации приобретает большую значимость.

**Конфиденциальная информация** – это документы (приватная информация) в электронном или бумажном виде (рис.2), содержание которой доступно только определенной группе людей, а ее передача третьим лицам является грубым нарушением законодательства Российской Федерации.

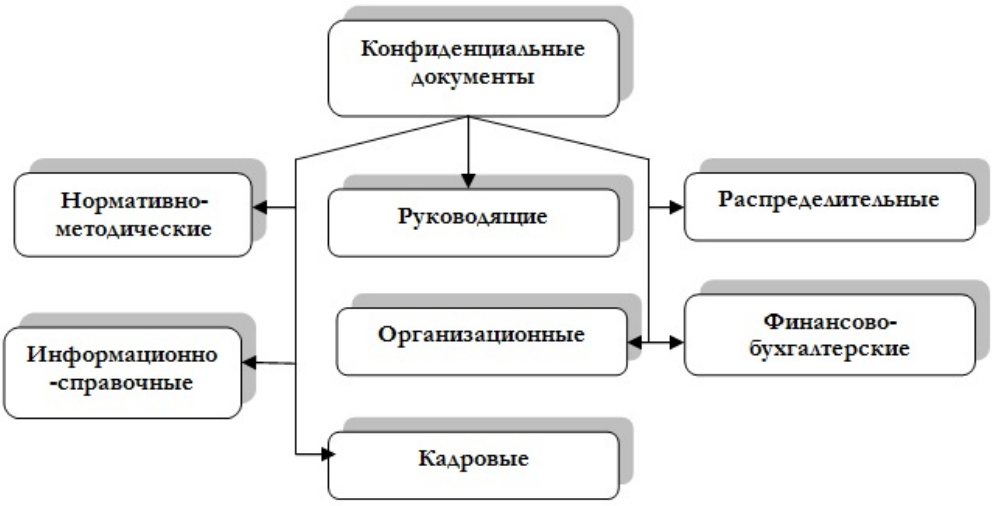


Рисунок 2. Виды конфиденциальных документов

*Конфиденциальная информация* – это коммерческая, военная, банковская, служебная или государственная тайна. Как правило, конфиденциальная информация может представлять собой особую категорию и относиться к коммерческой тайне.

**Виды конфиденциальной информации**

Сегодня можно выделить несколько основных категорий конфиденциальной информации, каждая из которых относится к своей категории (рис.3):


Рисунок 3. Категории конфиденциальной информации

*1. Научно-техническая.* Здесь идет речь о новых идеях, открытия, патентах, оригинальных ноу-хау, современных методиках организации в производственной сфере, рационализаторских предложениях по внедрению неизвестных ранее и более совершенных технологий, появлению новых типов продукции, уникальных методах анализа конкурентоспособности, кодах и паролях, открывающих доступ к конфиденциальной информации, а также уникальное программное обеспечение.

*2. Производственная.* К данной категории можно отнести новые технологии в производственной сфере, секретную конструкторскую информацию, схемы и чертежи, данные о материалах, планируемое время выхода товара на рынок, планы выпуска новой продукции, рецептура изготовления товаров, планы дальнейших вложений в новое производство и так далее.

*3. Финансовая.* К конфиденциальной информации финансового характера относится реальный размер прибыли компании, себестоимость производства (или продукции), банковские или торговые сделки, механизм формирования ценовой политики, уровень платежеспособности и так далее.

*4. Деловая.* Здесь речь идет о следующих данных – условиях заключения договоров с другими участниками рынка, внутренней организационной системы, планирования рекламной компании на ближайшее время, информации о конкурирующих компаниях и поставщиках, данные о работниках компании и переговорном процессе с деловыми партнерами, информации о коммерческой переписке и так далее.

**Организационная защита информации** - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией, и включает в себя организа-

цию режима охраны, организацию работы с сотрудниками, с документами, организацию использования технических средств и работу по анализу угроз информационной безопасности.

**Таким образом, защита информации — это деятельность собственника информации или уполномоченных им лиц по:**

- обеспечению своих прав на владение, распоряжение и управление защищаемой информацией;
- предотвращению утечки и утраты информации;
- сохранению полноты, достоверности, целостности защищаемой информации, ее массивов и программ обработки;
- сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

## 4.2 Направления, принципы организационной системы защиты информации; требования к системе защиты информации

Система защиты сведений, отнесенных к коммерческой тайне, и их носителей складывается из:

- органов защиты коммерческой тайны;
- средств и методов защиты коммерческой тайны;
- проводимых мероприятий.

Сложность обеспечения защиты информации требует создания специальной службы, осуществляющей реализацию всех защитных мероприятий и в первую очередь организационного плана. Структура, численность и состав службы безопасности компании определяются реальными потребностями (степенью влияния утраты конфиденциальной информации на показатели работы).

Безопасность предприятия и защита информации может быть реализована следующими тремя путями:

- абонементное обслуживание силами специальных организаций;
- создание собственной службы безопасности;
- комбинированный вариант.

В первом случае специализированное предприятие (организация), имеющее лицензию на соответствующие виды деятельности, на высоком профессиональном уровне проводит полный комплекс работ, связанный с организацией защиты и поддержание состояния защищенности на должном уровне. Поскольку для получения лицензии Гостехкомиссии при требуются квалифицированные кадры, дорогостоящие аппаратные, программные и технические средства контроля, методики проведения работ, то лицензия — своеобразная гарантия качества защиты. Однако этот способ имеет два крупных недостатка:

- услуги такого рода очень дороги;
- специалисты не могут постоянно находиться на объекте, следовательно при разовом «наезде» вполне вероятен пропуск факта вторжения.

Во втором случае в фирме создается своя служба безопасности, имеющая, например, следующую структуру (рис.4).

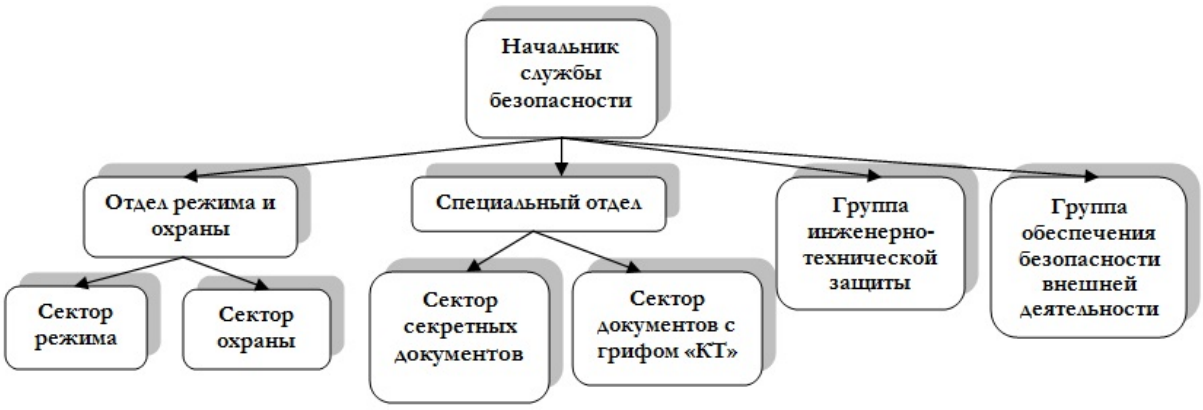


Рисунок 4. Примерная структура службы безопасности

Она возглавляется начальником, которому подчинены служба охраны, инспектор безопасности, консультант по безопасности и служба противопожарной охраны.

Основными задачами службы безопасности предприятия являются:

- обеспечение безопасности производственно-торговой деятельности, защита информации и сведений, являющихся коммерческой тайной;
- организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;
- организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;
- предотвращение необоснованного допуска и открытого доступа к сведениям и работам, составляющим коммерческую тайну;
- выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (авария, пожар и др.) ситуациях;
- обеспечение режима безопасности при проведении таких видов деятельности, как различные встречи, переговоры, совещания, заседания и другие мероприятия, связанные с деловым сотрудничеством на национальном и международном уровне;
- обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;
- обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
- оценка маркетинговых ситуаций при неправомерных действиях злоумышленников и конкурентов.

Для решения указанных задач служба безопасности предприятия должна выполнять следующие общие функции:

- организовывать и обеспечивать пропускной и внутриобъектовый (при наличии зон ограниченного доступа) режим в зданиях и помещениях, устанавливать порядок несения службы охраны, контролировать соблюдение требований режима сотрудниками, смежниками, партнерами и посетителями;

- руководить работами по правовому и организационному регулированию отношений по защите коммерческой тайны;
- участвовать в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты коммерческой тайны, в частности Устава, Коллективного договора. Правил внутреннего трудового распорядка, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;
- разрабатывать и осуществлять совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ, организовывать и контролировать выполнение требований «Инструкции по защите коммерческой тайны»;
- изучать все стороны производственной, коммерческой, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, вести учет и анализ нарушений режима безопасности, накапливать и анализировать данные о злоумышленных устремлениях конкурентов и других организаций получить доступ к информации о деятельности предприятия или его клиентов, партнеров, смежников;
- организовывать и проводить служебные расследования по фактам разглашения сведений, утрат документов и других нарушений режима безопасности предприятия;
- разрабатывать, вести, обновлять и пополнять «Перечень сведений, составляющих коммерческую тайну» и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;
- обеспечивать строгое выполнение требований нормативных документов по защите коммерческой тайны;
- осуществлять руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговоренных в договорах и условиях по защите коммерческой тайны;
- организовывать и регулярно проводить учебу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был достигнут глубоко обоснованный подход;
- вести учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;
- вести учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;
- поддерживать контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).

При наличии подобной службы безопасности процесс организации защиты информации, проходит по следующим этапам.

**Первый этап** (анализ объекта защиты) состоит в определении, что нужно защищать.

Анализ проводится по следующим направлениям:

- какая информация в первую очередь нуждается в защите;
- наиболее важные элементы (критические) защищаемой информации;
- определяется срок жизни критической информации (время, необходимое конкуренту для реализации добытой информации);
- определяются ключевые элементы информации (индикаторы), отражающие характер охраняемых сведений;
- классифицируются индикаторы по функциональным зонам предприятия (производственно-технологические процессы, система материально-технического обеспечения производства, подразделения, управления и т. д.).

**Второй этап** сводится к выявлению угроз:

- определяется — кого может заинтересовать защищаемая информация;
- оцениваются методы, используемые конкурентами для получения этой информации;
- оцениваются вероятные каналы утечки информации;
- разрабатывается система мероприятий по пресечению действий конкурента.

**Третий** — анализируется эффективность принятых и постоянно действующих подсистем обеспечения безопасности (физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т. д.).

**Четвертый** — определение необходимых мер защиты. На основании проведенных на первых трех этапах аналитических исследований определяются необходимые дополнительные меры и средства по обеспечению безопасности предприятия.

**Пятый** — рассматриваются руководителями фирмы (организации) представленные предложения по всем необходимым мерам безопасности и расчет их стоимости и эффективности.

**Шестой** — реализация дополнительных мер безопасности с учетом установленных приоритетов.

**Седьмой** — осуществление контроля и доведение до персонала фирмы реализуемых мер безопасности.

**План мероприятий по защите коммерческих секретов предприятия**

1. Определение целей плана по защите коммерческой тайны. Ими могут быть:

– предотвращение кражи коммерческих секретов;

– предотвращение разглашения коммерческих секретов сотрудниками или их утечки через технические каналы.

2. Анализ сведений, составляющих коммерческую тайну, для чего надо:

– определить, какие сведения на предприятии (технологические и деловые) являются коммерческой тайной;

– установить места их накопления и хранения;

– оценить возможности по перекрытию каналов утечки;

– проанализировать соотношение затрат на защиту и возможных потерь при утере информации, если использованы различные технологии, обеспечивающие защиту коммерческой тайны;

– назначить сотрудников, персонально ответственных за каждый участок системы обеспечения безопасности.

3. Обеспечить реализацию деятельности системы по следующим направлениям:

– контроль сооружений и оборудования предприятия (обеспечение безопасности производственных и конторских помещений, охрана фото- и иного копировального оборудования, контроль посещений предприятия и т. п.);

– работа с персоналом предприятия, в том числе проведение бесед при приеме на работу; инструктаж вновь потупивших на работу по правилам и процедурам, принятым для защиты коммерческой тайны на предприятии; обучение сотрудников правилам сохранения коммерческих секретов; стимулирование соблюдения конфиденциальности; беседы с увольняющимися;

– организация работы с конфиденциальными документами (установление порядка и правил ведения делопроизводства, контроль за конфиденциальными документами, контроль за публикациями, контроль и учет технических носителей конфиденциальных сведений, рассекречивание и уничтожение конфиденциальных документов, охрана чужих секретов); работа с конфиденциальной информацией, циркулирующей в технических средствах и системах, которые обеспечивают трудовую деятельность (создание системы предотвращения утечки информации через технические каналы);

– работа с конфиденциальной информацией, накопленной в компьютерных системах (создание системы защиты электронной информации от несанкционированного доступа к ней; обеспечение контроля за использованием ЭВМ); работа с конфиденциальной информацией, циркулирующей в технических средствах и системах, которые обеспечивают трудовую деятельность (создание системы предотвращения утечки информации через технические каналы);

– работа с конфиденциальной информацией, накопленной в компьютерных системах (создание системы защиты электронной информации от несанкционированного доступа к ней; обеспечение контроля за использованием ЭВМ);

После составления определяются те мероприятия плана, которые выполняются специализированной организацией (наличие квалифицированных специалистов в конкретной области, техническая и методическая оснащенность) и те из них, которые осуществляются силами и средствами собственной службы безопасности (знание оперативной обстановки, динамичность...). При такой работе достигаются оптимальные результаты с точки зрения финансовых затрат и качества защиты.

**Вопросы по пройденному материалу:**

1. Перечислите виды конфиденциальной информации.
2. Какова структура службы безопасности предприятия?
3. Охарактеризуйте этапы процесса организации защиты информации.

# 5. ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

## 5.1 Основные понятия

**Вредоносная программа (Malware)** – это любое программное обеспечение, созданное для получения несанкционированного доступа к компьютеру и его данным, с целью хищения информации или нанесению вреда. Термин "Вредоносная программа" можно считать общим для всех типов компьютерных вирусов, червей, троянских программ и т.д.

**Компьютерный вирус** — вид вредоносного программного обеспечения, способного внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Основная цель вируса — его распространение. Кроме того, часто его сопутствующей функцией является нарушение работы программно-аппаратных комплексов — удаление файлов и даже удаление операционной системы, приведение в негодность структур размещения данных, блокирование работы пользователей и т.п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют ресурсы системы.

**Пример.** CIH - вирус, который в ходе заражения записывает свои копии во все запускаемые пользователем программные файлы (PE EXE). Внедрение может происходить как одним куском, так и путем деления вредоносного кода на блоки и записи их в разных частях заражаемого файла. При этом инфицированная программа может дальше выполнять свои основные функции и вирус в ней никак себя не обнаруживает. Однако в определенный момент времени происходит уничтожение всей информации на жестком диске. Поскольку самая известная версия CIH срабатывала 26 апреля, то он получил второе имя - «Чернобыль».

## 5.2 Способы распространения вредоносных программ

В настоящее время имеется четыре основных способа передачи вредоносного ПО.

**1. Мобильные носители.** К мобильным носителям можно отнести все виды энергонезависимых запоминающих устройств. То есть таких устройств, которые позволяют достаточно долго хранить информацию и при этом не требуют дополнительного питания от компьютера. Это дискеты, компакт диски, flash-накопители, перфокарты и перфоленты.

Мобильные носители - достаточно распространенный способ для размножения компьютерных вирусов. Однако по скорости распространения этот путь существенно уступает компьютерным сетям.

**2. Локальная вычислительная сеть (ЛВС)** - это компьютерная сеть, покрывающая относительно небольшую территорию (дом, школу, институт, микрорайон).

Вредоносные программы в полной мере используют преимущества ЛВС - фактически, почти все современные вирусы имеют встроенные процедуры инфицирования по локальным сетям и как следствие высокие темпы распространения. Инфицирование обычно происходит в такой последовательности. Зараженный компьютер с заданным интервалом инициирует соединение поочередно со всеми другими компьютерами сети и проверяет наличие на них открытых для общего доступа файлов. Если такие есть, происходит инфицирование.

***3. Глобальная вычислительная сеть*** *(ГВС) - это компьютерная сеть, покрывающая большие территории* - города, страны, континенты. Самая большая и самая известная на сегодняшний день глобальная вычислительная сеть - это всемирная сеть Интернет. *Наличие сети такого масштаба делает возможным всемирные эпидемии компьютерных вирусов.*

**Пример.** 30 апреля 2004 года были обнаружены первые экземпляры вируса Sasser - в течение дня им было атаковано около 4 тысяч компьютеров, что вызвало серьезные сбои в работе таких компаний как Postbank, Delta Air Lines, Goldman Sachs. Впоследствии было поражено более 8 млн. компьютеров, а убытки от Sasser были оценены в 979 млн. долларов США.

***4. Электронная почта*** *- это способ передачи информации в компьютерных сетях, основанный на пересылке пакетов данных, называемых электронными письмами.*

*На сегодняшний день электронная почта выступает основным путем распространения вирусов.* Это происходит потому, что время доставки письма очень мало (обычно исчисляется минутами) и практически все пользователи Интернет имеют как минимум один почтовый ящик. При этом для того, чтобы доставить пользователю на компьютер зараженный файл, не нужно его принуждать куда-либо обратиться и скопировать к себе вирус. Достаточно лишь прислать на его электронный адрес инфицированное письмо и заставить адресата его открыть. Часто для инфицирования даже не требуется запускать вложение - существуют методы, позволяющие заражать даже при обычном прочтении письма.

**Пример 1.** Horillka распространяется через Интернет в виде файлов, прикрепленных к зараженным письмам с такими параметрами: заголовок - «Внимание!», текст: «Выпущено новое vbs обновление для поиска вирусов в памяти ОС Windows! Оно помогает бороться с вирусами, рассылающимися по почте. Антивирусный модуль написан на скрипт-языке, что помогает перехватывать vb и js вирусы, прежде чем они начнут деструктивную деятельность. Достаточно открыть файл и программа по устранению вирусов проведет поиск вредоносных программ в памяти компьютера». Во вложении находится файл с именем «WinSys32dll.vbs», после его запуска происходит заражение компьютера. Как результат, 11 декабря каждого года на экран выдается сообщение «COOOOOOOOL» и после следующей перезагрузки уничтожаются все данные на жестком диске С.

**Пример 2.** LoveLetter в мае 2000 года в течение всего нескольких часов заразил миллионы компьютеров по всему миру. Такому успеху способствовала удачно выбранная тема, интригующий текст и имя вложенного файла - «ILOVEYOU», «kindly check the attached LOVELETTER coming from me» и

«LOVE-LETTER-FOR-YOU.TXT.vbs. После заражения происходила кража конфиденциальной информации и искажение содержимого некоторых файлов на жестком диске.

## 5.3 Классификация вредоносных программ

Все вредоносные программы в соответствии со способами распространения и вредоносной нагрузкой можно разделить на четыре основных типа:

- *компьютерные вирусы,*
- *черви,*
- *трояны*
- *другие программы.*

Рассмотрим основные особенности указанных типов подробнее.

### Вирусы

Основная черта компьютерного вируса - это способность к саморазмножению.

Условно жизненный цикл любого компьютерного вируса можно разделить на пять стадий: проникновение на чужой компьютер, активация, поиск объектов для заражения, подготовка копий, внедрение копий.

Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения - фактически, все каналы, по которым можно скопировать файл. Однако в отличие от червей, вирусы не используют сетевые ресурсы - заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал. Например, скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.

После проникновения следует активация вируса. Это может происходить несколькими путями.

В соответствии с выбранным методом активации вирусы делятся на следующие виды:

- **Загрузочные вирусы** заражают загрузочные сектора жестких дисков и мобильных носителей.

**Примеры.** Вредоносная программа Virus.Boot.Snow.a записывает свой код в MBR жесткого диска или в загрузочные сектора дискет. При этом оригинальные загрузочные сектора шифруются вирусом. После получения управления вирус остается в памяти компьютера (резидентность) и перехватывает прерывания INT 10h, 1Ch и 13h. Иногда вирус проявляет себя визуальным эффектом - на экране компьютера начинает падать снег.

Другой загрузочный вирус Virus.Boot.DiskFiller также заражает MBR винчестера или загрузочные сектора дискет, остается в памяти и перехватывает прерывания - INT 13h, 1Ch и 21h. При этом, заражая дискеты, вирус форматирует дополнительную дорожку с номером 40 или 80 (в зависимости от объема дискеты он может иметь 40 либо 80 дорожек с номерами 0-39 или 0-79 соответственно). Именно на эту нестандартную дорожку вне поля обычной видимости вирус записывает свой код, добавляя в загрузочный сектор лишь небольшой фрагмент - головную часть вируса.

**Файловые вирусы** - заражают файлы. Отдельно по типу среды обитания в этой группе также выделяют следующие типы.

*Классические файловые вирусы* - они различными способами внедряются в исполняемые файлы (внедряют свой вредоносный код или полностью их перезаписывают), создают файлы-двойники, свои копии в различных каталогах жесткого диска или используют особенности организации файловой системы.

**Пример.** Самый известный файловый вирус всех времен и народов — Virus.Win9x.CIH, известный также как «Чернобыль». Имея небольшой размер - около 1 кб - вирус заражает PE-файлы (Portable Executable) накомпьютерах под управлением операционных систем Windows 95/98 таким образом, что размер зараженных файлов не меняется. Для достижения этого эффекта вирус ищет в файлах «пустые» участки, возникающие из-за выравнивания начала каждой секции файла под кратные значения байт. После получения управления вирус перехватывает IFS API, отслеживая вызовы функции обращения к файлам и заражая исполняемые файлы. 26 апреля срабатывает деструктивная функция вируса, которая заключается в стирании Flash BIOS и начальных секторов жестких дисков. Результатом является неспособность компьютера загружаться вообще (в случае успешной попытки стереть Flash BIOS) либо потеря данных на всех жестких дисках компьютера.

***Макровирусы**, которые написаны на внутреннем языке, так называемых макросах какого-либо приложения.* Подавляющее большинство макровирусов используют макросы текстового редактора Microsoft Word.

**Пример.** Одними из наиболее разрушительных макровирусов являются представители семейства Macro.Word97.Thus. Эти вирусы содержат три процедуры Document_Open, Document_Close и Document_New, которыми подменяет стандартные макросы, выполняющиеся при открытии, закрытии и создании документа, тем самым обеспечивая заражение других документов. 13 декабря срабатывает деструктивная функция вируса - он удаляет все файлы на диске C:, включая каталоги и подкаталоги.

***Скрипт-вирусы**, написанные в виде скриптов для определенной командной оболочки* - например, bat-файлы для DOS или VBS и JS - скрипты для Windows Scripting Host (WSH).

**Пример.** Virus.VBS.Sling написан на языке VBScript (Visual Basic Script). При запуске он ищет файлы с расширениями .VBS или .VBE и заражает их. При наступлении 16-го июня или июля вирус при запуске удаляет все файлы с расширениями .VBS и .VBE, включая самого себя.

Дополнительным отличием вирусов от других вредоносных программ служит их жесткая привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Это означает, что вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например Unix. Точно также макровирус для Microsoft Word 2003 скорее всего не будет работать в приложении Microsoft Excel 97.

При подготовке своих вирусных копий для маскировки от антивирусов могут применяться такие технологии как:

• **Шифрование** — вирус состоит из двух функциональных кусков: собственно вирус и шифратор. Каждая копия вируса состоит из шифратора, случайного ключа и собственно вируса, зашифрованного этим ключом.

**Метаморфизм** — создание различных копий вируса путем замены блоков команд на эквивалентные, перестановки местами кусков кода, вставки между значащими кусками кода «мусорных» команд, которые практически ничего не делают.

Сочетание этих двух технологий приводит к появлению следующих типов вирусов классифицируемых по технологии защиты от обнаружения:

**Шифрованный вирус** — вирус, использующий простое шифрование со случайным ключом и неизменный шифратор. Такие вирусы легко обнаруживаются по сигнатуре шифратора.

**Метаморфный вирус** — вирус, применяющий метаморфизм ко всему своему телу для создания новых копий.

**Полиморфный вирус** — вирус, использующий метаморфный шифратор для шифрования основного тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм.

**Пример.** Одним из наиболее сложных и относительно поздних полиморфных вирусов является Virus.Win32.Etap. При заражении файла вирус перестраивает и шифрует собственный код, записывает его в одну из секций заражаемого файла, после чего ищет в коде файла вызов функции ExitProcess и заменяет его на вызов вирусного кода. Таким образом, вирус получает управление не перед выполнением исходного кода зараженного файла, а после него.

Основные цели любого компьютерного вируса - это распространение на другие ресурсы компьютера и выполнение специальных действий при определенных событиях или действиях пользователя (например, 26 числа каждого четного месяца или при перезагрузке компьютера). Специальные действия нередко оказываются вредоносными.

## Черви

В отличие от вирусов черви - это вполне самостоятельные программы. Главной их особенностью также является способность к саморазмножению, однако при этом они способны к самостоятельному распространению с использованием сетевых каналов. Для подчеркивания этого свойства иногда используют термин «сетевой червь».

**Червь (сетевой червь)** - это вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом.

Жизненный цикл червей состоит из таких стадий: проникновение в систему, активация, поиск объектов для заражения, подготовка копий, распространение копий.

В зависимости от способа проникновения в систему черви делятся на типы:

• сетевые черви используют для распространения локальные сети и Интернет;

• почтовые черви - распространяются с помощью почтовых программ;

• IM-черви используют системы мгновенного обмена сообщениями; - IRC-черви распространяются по каналам IRC;

• P2P-черви - при помощи пиринговых файлообменных сетей.

## Троянские программы

Трояны или программы класса троянский конь, в отличие от вирусов и червей, не обязаны уметь размножаться.

**Троян (троянский конь)** - программа, основной целью которой является вредоносное воздействие по отношению к компьютерной системе путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы, с целью проникновения в нее. Однако в большинстве случаев они проникают на компьютеры вместе с вирусом либо червем - то есть такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу. Нередко пользователи сами загружают троянские программы из Интернет.

Жизненный цикл троянов состоит всего из трех стадий: проникновение в систему, активация, выполнение вредоносных действий.

Для проникновения на компьютер, трояну необходима активация и здесь он похож на червя - либо требует активных действий от пользователя или же через уязвимости в программном обеспечении самостоятельно заражает систему.

Поскольку главная цель написания троянов - это производство несанкционированных действий, они классифицируются по типу вредоносной нагрузки.

• Клавиатурные шпионы, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору.

• Похитители паролей предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат.

**Пример.** Trojan-PSW.Win32.LdPinch.kw собирает сведения о системе, а также логины и пароли для различных сервисов и прикладных программ - мессенджеров, почтовых клиентов, программ дозвона. Часто эти данные оказываются слабо защищены, что позволяет трояну их получить и отправить злоумышленнику по электронной почте.

• Утилиты скрытого удаленного управления - это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Перечень действий, которые позволяет выполнять тот или иной троян, определяется его функциональностью, заложенной автором. Обычно это возможность скрыто загружать, отсылать, запускать или уничто-

жать файлы. Такие трояны могут быть использованы как для получения конфиденциальной информации, так и для запуска вирусов, уничтожения данных.

- Люки (backdoor) — трояны предоставляющие злоумышленнику ограниченный контроль над компьютером пользователя. От утилит удаленного управления отличаются более простым устройством и, как следствие, небольшим количеством доступных действий.
- Анонимные SMTP-сервера и прокси-сервера - разновидность троянов, которые на зараженном компьютере организовывают несанкционированную отправку электронной почты, что часто используется для рассылки спама.

**Пример.** Трояны из семейства Trojan-Proxy.Win32.Mitglieder распространяются с различными версиями червей Bagle. Троян запускается червем, открывает на компьютере порт и отправляет автору вируса информацию об IP-адресе зараженного компьютера. После этого компьютер может использоваться для рассылки спама.

- Утилиты дозвона - в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернет.
- Модификаторы настроек браузера меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т. п.
- Логические бомбы характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов.

Отдельно отметим, что существуют программы из класса троянов, которые наносят вред другим, удаленным компьютерам и сетям, при этом не нарушая работоспособности инфицированного компьютера. Яркие представители этой группы - организаторы DDoS-атак.

### Другие вредоносные программы

Среди множества других вредоносных программ, для которых нельзя привести общий критерий, можно выделить следующие небольшие группы.

Условно опасные программы, то есть такие, о которых нельзя однозначно сказать, что они вредоносны. Такие программы обычно становятся опасными только при определенных условиях или действиях пользователя.

***К условно опасным программам относятся:***

- **Riskware** - вполне легальные программы, которые сами по себе не опасны, но обладают функционалом, позволяющим злоумышленнику использовать их с вредоносными целями. К riskware относятся обычные утилиты удаленного управления, которыми часто пользуются администраторы больших сетей, клиенты IRC, программы для загрузки файлов из Интернет, утилиты восстановления забытых паролей и другие.

• **Рекламные утилиты** (adware) - условно-бесплатные программы, которые в качестве платы за свое использование демонстрируют пользователю рекламу, чаще всего в виде графических баннеров.

После официальной оплаты и регистрации обычно показ рекламы заканчивается и программы начинают работать в обычном режиме. Проблема adware кроется в механизмах, которые используются для загрузки рекламы на компьютер. Кроме того, что для этих целей часто используются программы сторонних и не всегда проверенных производителей, даже после регистрации такие модули могут автоматически не удаляться и продолжать свою работу в скрытом режиме.

• **Pornware** - к этому классу относятся утилиты, так или иначе связанные с показом пользователям информации порнографического характера. На сегодняшний день это программы, которые самостоятельно дозваниваются до порнографических телефонных служб, загружают из Интернет порнографические материалы или утилиты, предлагающие услуги по поиску и показу такой информации. Отметим, что к вредоносным программам относятся только те утилиты класса pornware, которые устанавливаются на компьютер пользователя не санкционированно - через уязвимость в операционной системы или браузера или при помощи троянов. Обычно это делается с целью насильственного показа рекламы платных порнографических сайтов или служб.

• **Хакерские утилиты** - К этому виду программ относятся программы скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов), автоматизации создания сетевых червей, компьютерных вирусов и троянских программ (конструкторы вирусов), наборы программ, которые используют хакеры для скрытного взятия под контроль взломанной системы (RootKit) и другие подобные утилиты. То есть такие специфические программы, которые обычно используют только хакеры.

• **Злые шутки** - программы, которые намеренно вводят пользователя заблуждение путем показа уведомлений о, например, форматировании диска или обнаружении вирусов, хотя на самом деле ничего не происходит.

Текст таких сообщений целиком и полностью отражает фантазию автора.

**Вопросы по пройденному материалу:**

1. Объясните термины «вредоносная программа» и «компьютерный вирус».
2. Охарактеризуйте способы распространения вредоносных программ.
3. Чем отличаются «черви» от «троянов»?

# 6. ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 6.1 Физические средства защиты

**Физические средства защиты** - это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников (рис.5).


Рисунок 5. Виды физических средств защиты

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа, выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Эти средства применяются для решения следующих задач:

- охрана территории предприятия и наблюдение за ней;
- охрана зданий, внутренних помещений и контроль за ними;
- охрана оборудования, продукции, финансов и информации;
- осуществление контролируемого доступа в здания и помещение.

Все физические средства защиты объектов можно разделить на три категории:

1. средства предупреждения,
2. средства обнаружения
3. системы ликвидации угроз.

Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов - это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов и др.). Средства пожаротушения относятся к системам ликвидации угроз.

В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

- охранные и охранно-пожарные системы;
- охранное телевидение;
- охранное освещение;
- средства физической защиты.

К средствам физической защиты относятся:

- ограждение и физическая изоляция,
- запирающие устройства,
- системы контроля доступа.

К системам контроля доступа относятся:

- системы, использующие различные карты и карточки, на которых помещается кодированная или открытая информация о владельце,
- системы опознавания по отпечаткам пальцев,
- системы опознавания по голосу,
- системы опознавания по почерку,
- система опознавания по геометрии рук.

Все устройства идентификации могут работать как отдельно, так и в комплексе.

## 6.2 Виды, назначение, задачи и организационные формы охраны объектов, функции персонала охраны. Контрольно-пропускные пункты. Системы контроля доступа.

Электронные системы охраны весьма разнообразны и в целом достаточно эффективны. Однако большинство из них имеют общий недостаток: они не могут обеспечить раннее детектирование вторжения на территорию объекта. Такие системы, как правило, ориентированы на обнаружение нарушителя, который уже проник на охраняемую территорию или в здание. Это касается, в частности, систем видеонаблюдения; они зачастую с помощью устройства видеозаписи могут лишь подтвердить факт вторжения после того, как он уже произошел.

Квалифицированный нарушитель всегда рассчитывает на определенное временное “окно”, которое проходит от момента проникновения на объект до момента срабатывания сигнализации. Минимизация этого интервала времени является коренным фактором, определяющим эффективность любой охранной системы, и в этом смысле привлекательность периметральной охранной сигнализации неоспорима.

Периметральная граница объекта является наилучшим местом для раннего детектирования вторжения, т.к. нарушитель взаимодействует в первую очередь с физическим периметром и создает возмущения, которые можно зарегистрировать специальными датчиками. Если периметр представляет собой ограждение в виде металлической решетки, то ее приходится перерезать или преодолевать сверху; если это стена или барьер, то через них нужно перелезть; если это стена или крыша здания, то их нужно разрушить; если это открытая территория, то ее нужно пересечь.

Все эти действия вызывают физический контакт нарушителя с периметром, который предоставляет идеальную возможность для электронного обнару-

жения, т.к. он создает определенный уровень вибраций, содержащих специфический звуковой "образ" вторжения. При определенных условиях нарушитель может избегнуть физического контакта с периметром. В этом случае можно использовать "объемные" датчики вторжения, обычно играющие роль вторичной линии защиты.

Датчик любой периметральной системы реагирует на появление нарушителя в зоне охраны или определенные действия нарушителя. Сигналы датчика анализируются электронным блоком (анализатором или процессором), который, в свою очередь, генерирует сигнал тревоги при превышении заданного порогового уровня активности в охраняемой зоне.

**Общие требования к периметральным системам.**

Любая периметральная система охраны должна отвечать определенному набору критериев, некоторые из которых перечислены ниже:

- Возможность раннего обнаружения нарушителя — еще до его проникновения на объект
- Точное следование контурам периметра, отсутствие "мертвых" зон
- По возможности скрытая установка датчиков системы
- Независимость параметров системы от сезона (зима, лето) и погодных условий (дождь, ветер, град и т.д.)
- Невосприимчивость к внешним факторам "нетревожного" характера — индустриальные помехи, шум проходящего рядом транспорта, мелкие животные и птицы
- Устойчивость к электромагнитным помехам — грозовые разряды, источники мощных электромагнитных излучений и т.п.

Очевидно, что периметральная охранная система должна обладать максимально высокой чувствительностью, чтобы обнаружить даже опытного нарушителя. В то же время эта система должна обеспечивать по возможности низкую вероятность ложных срабатываний. Причины ложных тревог могут быть различными. Система может, например, среагировать при появлении в зоне охраны птиц или мелких животных. Сигнал тревоги может появиться при сильном ветре, граде или дожде. Кроме того, ложная тревога может возникнуть из-за "технологических" причин: неграмотный монтаж датчиков на ограде, неправильная настройка электронных блоков или просто неудовлетворительное инженерное состояние самой ограды, которая может, например, вибрировать при сильном ветре.

Сегодня рынок периметральных систем, как отечественных, так и импортных, весьма широк. Тем не менее, выбрать наиболее эффективную систему, отвечающую специфическим требованиям объекта, иногда бывает непросто. При выборе и проектировании системы нужно учитывать множество факторов — тип ограды, топографию и рельеф местности, возможность выделения полосы отчуждения, наличие растительности, соседство железных дорог, эстакад и автомагистралей, наличие линий электропередач.

Весьма важным фактором является квалификация и опыт организации, которая проектирует и монтирует периметральную систему охраны. Опыт показывает, что зачастую эффективность системы определяется не столько ее ис-

ходными техническими параметрами, сколько правильностью выбора и грамотностью ее монтажа.

Для оценки эффективности периметральных систем чаще всего используют специальные испытательные полигоны. Охранные системы там монтируют на стандартных оградах и оценивают их по специальным методикам, имитируя различные действия нарушителя — разрушение ограды, перелезание, подкоп и др.

### 6.3 Технические средства идентификации

В настоящее время всё наряду с указанными выше средствами защиты информации в системах и сетях шире применяются биометрические системы безопасности. По данным аналитической компании Frost&Sullivan, общий объем продаж биометрического оборудования в Америке в 2000 году не превысил 86,8 млн. долларов, вырос в 2001 году до 160,3 млн. долларов и превысил в 2012 году 9 миллиардов долларов. В настоящее время рынок таких устройств перевалил за десятки миллиардов долларов в год.

Биометрические технологии идентификации имеют ряд преимуществ перед традиционными средствами. Под биометрией понимают методы автоматической идентификации человека и подтверждения личности, основанные на физиологических или поведенческих характеристиках.

В качестве уникального биологического кода человека в биометрии используются параметры двух групп (рис.6).

*Поведенческие*, основанные на специфике действий человека, - это тембр голоса, подпись, индивидуальная походка, клавиатурный почерк. Главный недостаток поведенческих характеристик – временна́я неустойчивость, т.е. возможность значительного изменения со временем. Это в значительной степени ограничивает применение поведенческих характеристик как средств ограничения доступа. Однако на протяжении относительного короткого временного интервала они применимы как идентифицирующие личность средства.

Физиологические, использующие анатомическую уникальность каждого человека, - радужная оболочка глаза, сетчатка глаза, отпечатки пальцев, отпечаток ладони, геометрия кисти руки, геометрия лица, термограмма лица, структура кожи (эпителия) на пальцах на основе ультразвукового цифрового сканирования, форма ушной раковины, трехмерное изображение лица, структура кровеносных сосудов руки, структура ДНК, анализ индивидуальных запахов.

Наиболее часто применяются три основных биометрических метода — это распознавание человека по отпечаткам пальцев, по радужной оболочке глаза и по изображению лица. По информации консалтинговой компании International Biometric Group из Нью-Йорка, наиболее распространенной технологией стало сканирование отпечатков пальцев.

Отмечается, что из 127 млн. долларов, вырученных от продажи биометрических устройств, 44% приходится на дактилоскопические сканеры. Системы распознавания черт лица занимают второе место по уровню спроса, который составляет 14%, далее следуют устройства распознавания по форме ладони (13%), по голосу (10%) и радужной оболочке глаза (8%). Устройства верификации подписи в этом списке составляют 2%.


Рисунок 6. Система биометрических параметров для идентификации личности

Преимущества биометрических систем безопасности очевидны. Уникальные человеческие качества хороши тем, что их трудно подделать, трудно оставить фальшивый отпечаток пальца при помощи своего собственного или сделать радужную оболочку своего глаза похожей на чью-то другую.

В отличие от бумажных идентификаторов (паспорт, водительское удостоверение или иное удостоверение личности), от пароля или персонального идентификационного номера (ПИН), биометрические характеристики невозможно забыть или потерять. Кроме того, в силу своей уникальности они используются для предотвращения воровства или мошенничества.

Методы распознавания по изображению лица могут работать с двухмерным или с трехмерным изображением (так называемые 2D- и 3D-фото). Стоит отметить, что идентификация человека по чертам лица — одно из самых динамично развивающихся направлений в биометрической индустрии. Привлекательность данного метода основана на том, что он наиболее близок к тому, как люди обычно идентифицируют друг друга. Распространение мультимедийных технологий, благодаря которому все чаще можно встретить видеокамеры, установленные на городских улицах и площадях, на вокзалах, в аэропортах и других местах скопления людей, определило развитие этого направления.

Распознавание лица предусматривает выполнение любой из следующих функций: аутентификация (установление подлинности "один в один") или идентификация (поиск соответствия "один из многих"). Система автоматически

оценивает качество изображения для опознания лица и, если необходимо, способна его улучшить. Она также создает изображение лица из сегментов данных, генерирует цифровой код или внутренний шаблон, уникальный для каждого индивидуума.

### 6.4 Идентификация и аутентификация. Парольная защита.

*Идентификацию* и *аутентификацию* можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. *Идентификация* и *аутентификация* - это первая линия обороны, "проходная" информационного пространства организации.

***Идентификация*** позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством ***аутентификации*** вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "*аутентификация*" иногда используют словосочетание "проверка подлинности".

Аутентификация бывает ***односторонней*** (обычно клиент доказывает свою подлинность серверу) и ***двусторонней*** (***взаимной***). Пример *односторонней аутентификации* - процедура входа пользователя в систему.

В сетевой среде, когда стороны *идентификации/аутентификации* территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

- что служит ***аутентификатором*** (то есть используется для подтверждения подлинности субъекта);
- как организован (и защищен) обмен данными *идентификации/аутентификации*.

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

- нечто, что он знает (пароль, личный *идентификационный* номер, криптографический ключ и т.п.);
- нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

В открытой сетевой среде между сторонами *идентификации/аутентификации* не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от ***перехвата***, ***изменения*** и/или ***воспроизведения*** данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от *воспроизведения*. Нужны более сложные протоколы *аутентификации*.

Надежная *идентификация* и затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все *аутентификационные* сущности

можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью *аутентификации*, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно *вводить аутентификационную информацию (ведь на его место мог сесть другой человек),* а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства *идентификации/аутентификации* должны поддерживать концепцию *единого входа в сеть*. *Единый вход в сеть* - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная *идентификация/аутентификация* становится слишком обременительной. К сожалению, пока нельзя сказать, что *единый вход в сеть* стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств *идентификации* и *аутентификации*.

Любопытно отметить, что сервис *идентификации/аутентификации* может стать объектом атак на доступность. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

**Парольная аутентификация**

Главное достоинство ***парольной аутентификации*** - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Известна классическая история про советского разведчика Рихарда Зорге, объект внимания которого через слово говорил "карамба"; разумеется, этим же словом открывался сверхсекретный сейф.

Пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Ввод пароля можно подсмотреть. Иногда для подглядывания используются даже оптические приборы.

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

Пароль можно угадать "методом грубой силы", используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен).

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");
- обучение пользователей;
- использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

## 6.5 Межсетевые экраны как средство защиты от несанкционированного доступа

**Межсетевой экран**, **сетевой экран** — это комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита сети или отдельных её узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Некоторые сетевые экраны также позволяют осуществлять трансляцию адресов — динамическую заменувнутрисетевых (серых) адресов или портов на внешние, используемые за пределами локальной сети, — что может обеспечивать дополнительную безопасность.

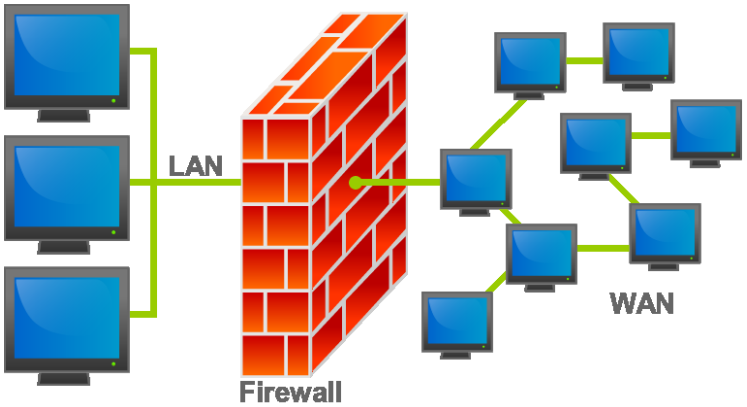


Рисунок 7. Принцип работы брандмауэра

**Брандмауэр** (нем. *Brandmauer*) — заимствованный из немецкого языка термин, являющийся аналогом английского *firewall* в его оригинальном значении (противопожарная перегородка — стена, которая разделяет смежные здания, предохраняя от распространения пожара). Интересно, что в области компьютерных технологий в немецком языке употребляется слово *Firewall*.

В настоящее время не существует единой и общепризнанной классификации межсетевых экранов. Выделим следующие классы межсетевых экранов:

1. Фильтрующие маршрутизаторы.
2. Шлюзы сеансового уровня.
3. Шлюзы уровня приложений.

Эти категории можно рассматривать как базовые компоненты реальных межсетевых экранов. Лишь немногие межсетевые экраны включают лишь одну из перечисленных категорий. Тем не менее эти компоненты отражают ключевые возможности, отличающие межсетевые экраны друг от друга.

*Фильтрующие маршрутизаторы*

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов.

Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы следующих полей заголовка пакета:

- IP-адрес отправителя;
- IP-адрес получателя;
- порт отправителя;
- порт получателя.

Некоторые маршрутизаторы проверяют, с какого сетевого интерфейса маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации.

Фильтрация может быть реализована различными способами для блокирования соединений с определенными компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех компьютеров и сетей, которые считаются враждебными или ненадежными.

Правила фильтрации пакетов формулируются сложно, к тому же обычно не существует средств для проверки их корректности, кроме медленного ручного тестирования. При этом в отсутствие фильтрующего маршрутизатора средств протоколирования (если правила фильтрации пакетов все-таки позволят опасным пакетам пройти через маршрутизатор) такие пакеты не смогут быть выявлены до обнаружения последствий проникновения. Даже если администратору сети удастся создать эффективные правила фильтрации, их возможности останутся ограниченными. Например, администратор задает правило, в соответствии с которым маршрутизатор будет отбраковывать все пакеты с неизвестным адресом отправителя. Однако в данном случае хакер для проникновения внутрь защищенной сети может осуществить атаку, которую называют подменой адреса. В таких условиях фильтрующий маршрутизатор не сумеет отличить подделный пакет от настоящего и пропустит его.

К положительным качествам фильтрующих маршрутизаторов можно отнести следующие:

- сравнительно невысокая стоимость;
- гибкость в определении правил фильтрации;
- небольшая задержка при прохождении пакетов.

Недостатки фильтрующих маршрутизаторов:

- внутренняя сеть видна (маршрутизируется) из сети Интернет;
- правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;
- при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;
- отсутствует аутентификация на пользовательском уровне.

*Шлюзы сеансового уровня*

Данный класс маршрутизаторов представляет собой транслятор TCP-соединения. Шлюз принимает запрос авторизованного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с местом назначения (внешним хостом). После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации. Как правило, пункт назначения задается заранее, в то время как источников может быть много. Используя различные порты, можно создавать разнообразные конфигурации соединений. Данный тип шлюза позволяет создать транслятор TCP-соединения для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису и сбор статистики по его использованию.

Шлюз следит за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым. Чтобы выявить допустимость запроса на сеанс связи, шлюз выполняет следующую процедуру. Когда авторизованный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли данный клиент базовым критериям фильтрации. Затем, действуя от имени клиента, шлюз устанавливает соединение с внешним хостом и следит за выполнением процедуры квитирования связи по протоколу TCP. Эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить).

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число, например 500, является запросом клиента на открытие сеанса. Внешний хост, получивший этот пакет, посылает в ответ другой, помеченный флагом ACK и содержащий число на единицу большее, чем в принятом пакете (в нашем случае 501), подтверждая тем самым прием пакета SYN от клиента.

Далее осуществляется обратная процедура: хост посылает клиенту пакет SYN с исходным числом, например 700, а клиент подтверждает его получение передачей пакета ACK, содержащего число 701. На этом процесс квитирования связи завершается.

Шлюз сеансового уровня признает завершенное соединение допустимым только в том случае, если при выполнении процедуры квитирования связи фла-

ги SYN и ACK, а также числа, содержащиеся в TCP-пакетах, оказываются логически связанными между собой.

После того как шлюз определил, что доверенный клиент и внешний хост являются авторизованными участниками сеанса TCP, и проверил его допустимость, он устанавливает соединение. Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, не проводя никакой фильтрации. Он поддерживает таблицу установленных соединений, пропуская данные, которые относятся к одному из сеансов связи, зафиксированных в данной таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает сеть, использовавшуюся в текущем сеансе.

Недостатком шлюзов сеансового уровня является отсутствие проверки содержимого передаваемых пакетов, что дает возможность нарушителю проникнуть через такой шлюз.

*Шлюзы уровня приложений*

С целью защиты ряда уязвимых мест, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, как Telnet и FTP. Подобное приложение называется proxy-службой, а хост, на котором работает proxy-служба, — шлюзом уровня приложений. Такой шлюз исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне.

Обнаружив сетевой сеанс, шлюз приложений останавливает его и вызывает уполномоченное приложение для оказания завершаемой услуги. Для достижения более высокого уровня безопасности и гибкости шлюзы уровня приложений и фильтрующие маршрутизаторы могут быть объединены в межсетевом экране.

Шлюзы прикладного уровня позволяют обеспечить надежную защиту, поскольку взаимодействие с внешним миром реализуется через небольшое число уполномоченных приложений, полностью контролирующих весь входящий и исходящий трафик. Следует отметить, что шлюзы уровня приложений требуют отдельного приложения для каждого сетевого сервиса.

По сравнению с работающими в обычном режиме, при котором прикладной трафик пропускается непосредственно к внутренним хостам, шлюзы прикладного уровня имеют ряд преимуществ:

- невидимость структуры защищаемой сети из глобальной сети Интернет. Имена внутренних систем можно не сообщать внешним системам через DNS, поскольку шлюз прикладного уровня может быть единственным хостом, имя которого будет известно внешним системам;
- надежная аутентификация и регистрация. Прикладной трафик может быть аутентифицирован, прежде чем он достигнет внутренних хостов, и зарегистрирован более эффективно, чем с помощью стандартной регистрации;
- приемлемое соотношение цены и эффективности. Дополнительные программные или аппаратные средства аутентификации или регистрации нужно устанавливать только на шлюзе прикладного уровня;
- простые правила фильтрации. Правила на фильтрующем маршрутизаторе оказываются менее сложными, чем на маршрутизаторе, который самостоя-

тельно фильтрует прикладной трафик и отправляет его большому числу внутренних систем. Маршрутизатор должен пропускать прикладной трафик, предназначенный только для шлюза прикладного уровня, и блокировать весь остальной;

• возможность организации большого числа проверок. Защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, что снижает вероятность взлома с использованием «дыр» в программном обеспечении.

Недостатками шлюзов уровня приложений являются:

• относительно низкая производительность по сравнению с фильтрующими маршрутизаторами. В частности, при использовании клиент-серверных протоколов, таких как Telnet, требуется двухшаговая процедура для входных и выходных соединений;

• более высокая стоимость по сравнению с фильтрующими маршрутизаторами.

Одним из важных элементов концепции межсетевых экранов является аутентификация (проверка подлинности пользователя), то есть пользователь получает право воспользоваться тем или иным сервисом только после того, как будет установлено, что он действительно тот, за кого себя выдает. При этом считается, что сервис для данного пользователя разрешен (процесс определения, какие сервисы разрешены конкретному пользователю, называется авторизацией).

При получении запроса на использование сервиса от имени какого-либо пользователя межсетевой экран проверяет, какой способ аутентификации определен для данного субъекта, и передает управление серверу аутентификации. После получения положительного ответа от сервера аутентификации межсетевой экран осуществляет запрашиваемое пользователем соединение. Как правило, большинство коммерческих межсетевых экранов поддерживает несколько различных схем аутентификации, предоставляя администратору сетевой безопасности возможность сделать выбор наиболее приемлемой в сложившихся условиях схемы.

**Вопросы по пройденному материалу:**

1. Какие устройства относятся к физическим средствам защиты?
2. Какие требования предъявляются к охранным система предприятия?
3. На чем основываются биометрические системы идентификации?

# 7. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

## 7.1 Криптология и основные этапы ее развития

Криптология (от др.-греч. κρυπτς— скрытый и λόγος— слово) — наука, занимающаяся методами шифрования и расшифровывания. Криптология состоит из двух частей — криптографии и криптоанализа. Криптография занимается разработкой методов шифрования данных, в то время как криптоанализ занимается оценкой сильных и слабых сторон методов шифрования, а также разработкой методов, позволяющих взламывать криптосистемы.

Слово «криптология» (англ. cryptology) встречается в английском языке с XVII века, и изначально означало «скрытность в речи»; в современном значении было введено американским учёным Уильямом Фридманом и популяризовано писателем Дэвидом Каном.

Можно выделить следующие три периода развития криптологии.

*Первый период* — эра донаучной криптологии, являвшейся ремеслом — уделом узкого круга искусных умельцев.

Началом *второго периода* можно считать 1949 год, когда появилась работа К. Шеннона «Теория связи в секретных системах», в которой проведено фундаментальное научное исследование шифров и важнейших вопросов их стойкости. Благодаря этому труду криптология оформилась как прикладная математическая дисциплина.

Начало *третьему периоду* было положено появлением в 1976 году работы У. Диффи, М. Хеллмана «Новые направления в криптографии», где показано, что секретная связь возможна без предварительной передачи секретного ключа.

*XX в. до н. э.* При раскопках в Месопотамии был найден один из самых древних шифротекстов. Он был написан клинописью на глиняной табличке и содержал рецепт глазури для покрытия гончарных изделий, что, по-видимому, было коммерческой тайной. Известны древнеегипетские религиозные тексты и медицинские рецепты.

*Середина IX в. до н. э.* Именно в это время, как сообщает Плутарх, использовалось шифрующее устройство — скиталь, которое реализовывало так называемый шифр перестановки. При шифровании слова писались на узкую ленту, намотанную на цилиндр, вдоль образующей этого цилиндра (скиталя). После этого лента разматывалась и на ней оставались переставленные буквы открытого текста. Неизвестным параметром-ключом в данном случае служил диаметр этого цилиндра. Известен и метод дешифрования такого шифротекста, предложенный Аристотелем, который наматывал ленту на конус, и то место, где появлялось читаемое слово или его часть, определяло неизвестный диаметр цилиндра.

*56 г. н. э.* Во время войны с галлами Ю. Цезарь использует другую разновидность шифра — шифр замены. Под алфавитом открытого текста писался тот же алфавит со сдвигом (у Цезаря на три позиции) по циклу. При шифровании буквы открытого текста у верхнего алфавита заменялись на буквы нижнего алфавита.

Другим более сложным шифром замены является греческий шифр — «квадрат Полибия». Алфавит записывается в виде квадратной таблицы. При шифровании буквы открытого текста заменялись на пару чисел — номера столбца и строки этой буквы в таблице. При произвольном расписывании алфавита по таблице и шифровании такой таблицей короткого сообщения этот шифр является стойким даже по современным понятиям. Идея была реализована в более сложных шифрах, применявшихся во время Первой мировой войны.

*Крах Римской империи в V в. н. э.* сопровождался закатом искусства и наук, в том числе и криптографии. Церковь в те времена преследовала тайнопись, которую она считала чернокнижием и колдовством. Сокрытие мыслей за шифрами не позволяло церкви контролировать эти мысли.

*Р. Бэкон (1214—1294)* — францисканский монах и философ — описал семь систем секретного письма. Большинство шифров в те времена применялись для закрытия научных записей.

*Вторая половина XVв.* Леон Баттиста Альберта, архитектор и математик, работал в Ватикане, автор книги о шифрах, где описал шифр замены на основе двух концентрических кругов, по периферии которых были нанесены на одном круге — алфавит открытого текста, а на другом — алфавит шифротекста. Важно, что шифроалфавит был непоследовательным и мог быть смещен на любое количество шагов. Именно Альберта впервые применил для дешифрования свойство неравномерности встречаемости различных букв в языке. Он впервые также предложил для повышения стойкости применять повторное шифрование с помощью разных шифросистем.

Известен факт, когда король Франции Франциск 1 в 1546 году издал указ, запрещающий подданным использование шифров. Хотя шифры того времени были исключительно простыми, они считались нераскрываемыми.

*Иоганн Тритемий (1462—1516)* — монах-бенедиктинец, живший в Германии. Написал один из первых учебников по криптографии. Предложил оригинальный шифр многозначной замены под названием «Ave Maria». Каждая буква открытого текста имела не одну замену, а несколько, по выбору шифровальщика. Причем буквы заменялись буквами или словами так, что получался некоторый псевдо-открытый текст, тем самым скрывался сам факт передачи секретного сообщения. Разновидность шифра многозначной замены применяется до сих пор, например в архиваторе ARJ.

*Джироламо Кардано (1506—1576)* — итальянский математик, механик, врач — изобрел систему шифрования, так называемую решетку Кардано, на основе которой, например, был создан один из наиболее стойких военно-морских шифров Великобритании во время Второй мировой войны. В куске картона с размеченной решеткой определенным образом прорезались отверстия, нумерованные в произвольном порядке. Чтобы получить шифротекст, нужно положить этот кусок картона на бумагу и начинать вписывать в отверстия буквы в выбранном порядке. После снятия картона промежутки бессмысленного набора букв дописывались до псевдосмысловых фраз, так можно было скрыть факт передачи секретного сообщения. Скрытие легко достигается, если эти промежутки большие

и если слова языка имеют небольшую длину, как, например, в английском языке. «Решетка Кардано» — это пример шифра перестановки.

*XVI в.* Шифры замены получили развитие в работах итальянца Джованни Батиста Порты (математик) и француза Блеза де Вижинера (дипломат).

*XVII в. Кардинал Ришелье* (министр при короле Франции Людовике XIII) создал первую в мире шифрслужбу.

*Лорд Френсис Бэкон (1562—1626)* был первым, кто обозначил буквы 5-значным двоичным кодом: A = 00001, B = 00010, ... и т. д. Правда, Бэкон никак не обрабатывал этот код, поэтому такое закрытие было совсем нестойким. Просто интересно, что через три века этот принцип был положен в основу электрической и электронной связи. Тут уместно вспомнить коды Морзе, Бодо, международный телеграфный код № 2 (МККТТ-2), код ASCII, также представляющие собой простую замену.

В XVII же веке были изобретены так называемые словарные шифры. При шифровании буквы открытого текста обозначались двумя числами — номером строки и номером буквы в строке на определенной странице какой-нибудь выбранной распространенной книги. Эта система является довольно стойкой, но неудобной. К тому же книга может попасть в руки противника.

*К. Гаусс (1777—1855)* — великий математик тоже не обошел своим вниманием криптологию. Он создал шифр, который ошибочно считал нераскрываемым. При его создании использовался интересный прием — рандомизация (random — случайный) открытого текста. Открытый текст можно преобразовать в другой-текст, содержащий символы большего алфавита, путем замены часто встречающихся букв случайными символами из соответствующих определенных им групп. В получающемся тексте все символы большого алфавита встречаются с примерно одинаковой частотой. Зашифрованный таким образом текст противостоит методам раскрытия на основе анализа частот появления отдельных символов. После расшифрования законный получатель легко снимает рандомизацию. Такие шифры называют «шифрами с многократной подстановкой» или «равночастотными шифрами».

## 7.2 Криптографические методы защиты информации

Криптографические методы защиты информации – это мощное оружие в борьбе за информационную безопасность.

Криптография (от древне-греч. κρυπτος – скрытый и γραφω – пишу) – наука о методах обеспечения конфиденциальности и аутентичности информации.

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

- защиту конфиденциальности;
- защиту целостности.

Проблемы защиты конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы (рис.8):

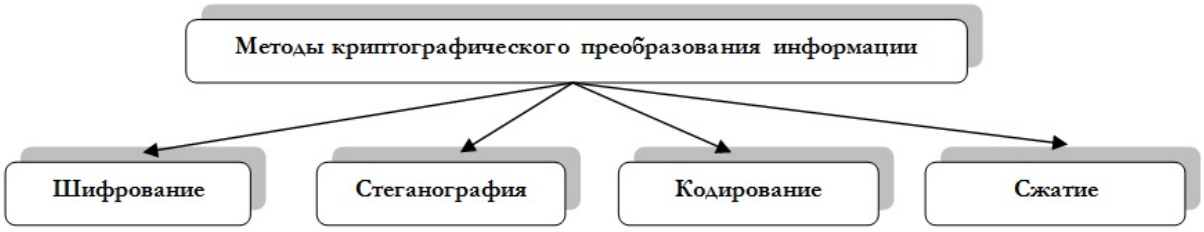


Рисунок 8. Классификация методов криптографического преобразования информации

Процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов.

Для шифрования информации используются **алгоритм преобразования** и **ключ**. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служит информация, подлежащая зашифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор преобразования на определенных шагах алгоритма и величины операндов, используемых при реализации алгоритма шифрования. Операнд – это константа, переменная, функция, выражение и другой объект языка программирования, над которым производятся операции.

В отличие от других методов криптографического преобразования информации, методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В основе всех методов стеганографии лежит маскирование закрытой информации среди открытых файлов, т.е. скрываются секретные данные, при этом создаются реалистичные данные, которые невозможно отличить от настоящих. Обработка мультимедийных файлов в информационных системах открыла практически неограниченные возможности перед стеганографией.

Графическая и звуковая информация представляются в числовом виде. Так, в графических объектах наименьший элемент изображения может кодироваться одним байтом. В младшие разряды определенных байтов изображения в соответствии с алгоритмом криптографического преобразования помещаются биты скрытого файла. Если правильно подобрать алгоритм преобразования и изображение, на фоне которого помещается скрытый файл, то человеческому глазу практически невозможно отличить полученное изображение от исходного. С

помощью средств стеганографии могут маскироваться текст, изображение, речь, цифровая подпись, зашифрованное сообщение.

Скрытый файл также может быть зашифрован. Если кто-то случайно обнаружит скрытый файл, то зашифрованная информация будет воспринята как сбой в работе системы. Комплексное использование стеганографии и шифрования многократно повышает сложность решения задачи обнаружения и раскрытия конфиденциальной информации.

Содержанием процесса кодирование информации является замена исходного смысла сообщения (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, знаков. При кодировании и обратном преобразовании используются специальные таблицы или словари. В информационных сетях кодирование исходного сообщения (или сигнала) программно-аппаратными средствами применяется для повышения достоверности передаваемой информации.

Часто кодирование и шифрование ошибочно принимают за одно и тоже, забыв о том, что для восстановления закодированного сообщения, достаточно знать правило замены, в то время как для расшифровки сообщения помимо знания правил шифрования, требуется ключ к шифру.

Сжатие информации может быть отнесено к методам криптографического преобразования информации с определенными оговорками. Целью сжатия является сокращение объема информации. В то же время сжатая информация не может быть прочитана или использована без обратного преобразования. Учитывая доступность средств сжатия и обратного преобразования, эти методы нельзя рассматривать как надежные средства криптографического преобразования информации. Даже если держать в секрете алгоритмы, то они могут быть сравнительно легко раскрыты статистическими методами обработки. Поэтому сжатые файлы конфиденциальной информации подвергаются последующему шифрованию. Для сокращения времени передачи данных целесообразно совмещать процесс сжатия и шифрования информации.

Основным видом криптографического преобразования информации в компьютерных сетях является шифрование. Под шифрованием понимается процесс преобразования открытой информации в зашифрованную информацию (шифртекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название зашифрование, а процесс преобразования закрытой информации в открытую – расшифрование.

За многовековую историю использования шифрования информации человечеством изобретено множество методов шифрования или шифров. Методом шифрования (шифром) называется совокупность обратимых преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования. Большинство методов шифрования не выдержали проверку временем, а некоторые используются и до сих пор. Появление компьютеров и компьютерных сетей инициировало процесс разработки новых шифров, учитывающих возможности использования компьютерной техники как для зашифрования/расшифрования информации, так и для атак на шифр. Атака на шифр (криптоанализ, криптоатака) – это процесс расшифрования закрытой

информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

Современные методы шифрования должны отвечать следующим требованиям:

- стойкость шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;
- криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;
- шифртекст не должен существенно превосходить по объему исходную информацию;
- ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;
- время шифрования не должно быть большим;
- стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифртексту, при условии, что ему неизвестен ключ.

Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь скрытых слабых мест, которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации – перебор комбинаций ключа и выполнение алгоритма расшифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.

Работа простой криптосистемы проиллюстрирована на рисунке 9.

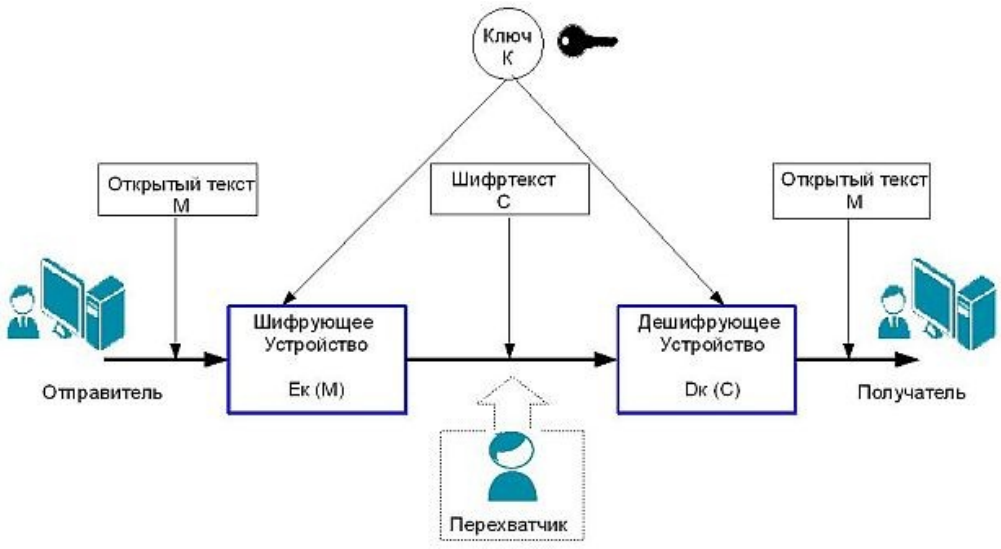


Рисунок 9. Простая криптосистема

## 7.3. Симметричное шифрование

Свою историю алгоритмы симметричного шифрования ведут с древности: именно этим способом сокрытия информации пользовался римский император Гай Юлий Цезарь в I веке до н. э., а изобретенный им алгоритм известен как "криптосистема Цезаря".

В настоящее время наиболее известен алгоритм симметричного шифрования DES (Data Encryption Standard), разработанный в 1977 г. До недавнего времени он был "стандартом США", поскольку правительство этой страны рекомендовало применять его для реализации различных систем шифрования данных. Несмотря на то, что изначально DES планировалось использовать не более 10-15 лет, попытки его замены начались только в 1997 г.

Мы не будем рассматривать DES подробно (почти во всех книгах из списка дополнительных материалов есть его подробнейшее описание), а обратимся к более современным алгоритмам шифрования. Стоит только отметить, что основная причина изменения стандарта шифрования - его относительно слабая криптостойкость, причина которой в том, что длина ключа DES составляет всего 56 значащих бит. Известно, что любой криптостойкий алгоритм можно взломать, перебрав все возможные варианты ключей шифрования (так называемый метод грубой силы - brute force attack). Легко подсчитать, что кластер из 1 млн процессоров, каждый из которых вычисляет 1 млн ключей в секунду, проверит 256 вариантов ключей DES почти за 20 ч. А поскольку по нынешним меркам такие вычислительные мощности вполне реальны, ясно, что 56-бит ключ слишком короток и алгоритм DES необходимо заменить на более "сильный".

Сегодня все шире используются два современных криптостойких алгоритма шифрования: отечественный стандарт ГОСТ 28147-89 и новый криптостандарт США - AES (Advanced Encryption Standard).

### Стандарт ГОСТ 28147-89

Алгоритм, определяемый ГОСТ 28147-89 (рис. 10), имеет длину ключа шифрования 256 бит. Он шифрует информацию блоками по 64 бит (такие алгоритмы называются блочными), которые затем разбиваются на два субблока по 32 бит (N1 и N2). Субблок N1 обрабатывается определенным образом, после чего его значение складывается со значением субблока N2 (сложение выполняется по модулю 2, т. е. применяется логическая операция XOR - "исключающее или"), а затем субблоки меняются местами. Данное преобразование выполняется определенное число раз ("раундов"): 16 или 32 в зависимости от режима работы алгоритма. В каждом раунде выполняются две операции.

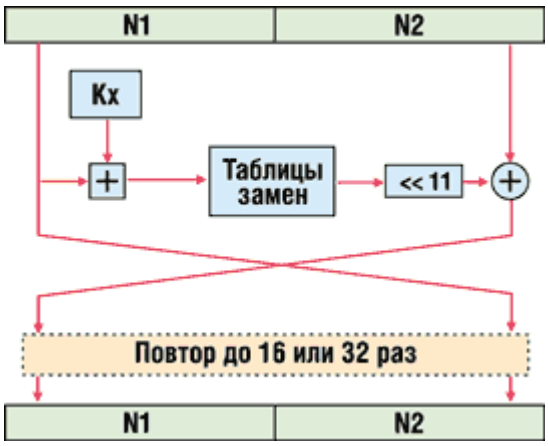


Рисунок 10. Схема алгоритма ГОСТ 28147-89.

Первая - наложение ключа. Содержимое субблока N1 складывается по модулю 2[32] с 32-бит частью ключа Kx. Полный ключ шифрования представляется в виде конкатенации 32-бит подключей: K0, K1, K2, K3, K4, K5, K6, K7. В процессе шифрования используется один из этих подключей - в зависимости от номера раунда и режима работы алгоритма.

Вторая операция - табличная замена. После наложения ключа субблок N1 разбивается на 8 частей по 4 бит, значение каждой из которых заменяется в соответствии с таблицей замены для данной части субблока. Затем выполняется побитовый циклический сдвиг субблока влево на 11 бит.

**Табличные замены** (Substitution box - S-box) часто используются в современных алгоритмах шифрования, поэтому стоит пояснить, как организуется подобная операция. В таблицу записываются выходные значения блоков. Блок данных определенной размерности (в нашем случае - 4-бит) имеет свое числовое представление, которое определяет номер выходного значения. Например, если S-box имеет вид 4, 11, 2, 14, 15, 0, 8, 13, 3, 12, 9, 7, 5, 10, 6, 1 и на вход пришел 4-бит блок "0100" (значение 4), то, согласно таблице, выходное значение будет равно 15, т. е. "1111" (0 а 4, 1 а 11, 2 а 2 ...).

Алгоритм, определяемый ГОСТ 28147-89, предусматривает четыре режима работы: простой замены, гаммирования, гаммирования с обратной связью и генерации имитовставок. В них используется одно и то же описанное выше шифрующее преобразование, но, поскольку назначение режимов различно, осуществляется это преобразование в каждом из них по-разному.

## Стандарт AES

В отличие от алгоритма ГОСТ 28147-89, который долгое время оставался секретным, американский стандарт шифрования AES (новый стандарт шифрования данных Advanced Encryption Standard), призванный заменить DES, выбирался на открытом конкурсе, где все заинтересованные организации и частные лица могли изучать и комментировать алгоритмы-претенденты.

Конкурс на замену DES был объявлен в 1997 г. Национальным институтом стандартов и технологий США (NIST - National Institute of Standards and Technology). На конкурс было представлено 15 алгоритмов-претендентов, разработанных как известными в области криптографии организациями (RSA Security, Counterpane и т. д.), так и частными лицами. Итоги конкурса были под-

ведены в октябре 2000 г.: победителем был объявлен алгоритм Rijndael, разработанный двумя криптографами из Бельгии, Винсентом Риджменом (Vincent Rijmen) и Джоан Даймен (Joan Daemen).

Алгоритм Rijndael не похож на большинство известных алгоритмов симметричного шифрования, структура которых носит название "сеть Фейстеля" и аналогична российскому ГОСТ 28147-89. Особенность сети Фейстеля состоит в том, что входное значение разбивается на два и более субблоков, часть из которых в каждом раунде обрабатывается по определенному закону, после чего накладывается на необрабатываемые субблоки.

В отличие от отечественного стандарта шифрования, алгоритм Rijndael представляет блок данных в виде двухмерного байтового массива размером 4X4, 4X6 или 4X8 (допускается использование нескольких фиксированных размеров шифруемого блока информации). Все операции выполняются с отдельными байтами массива, а также с независимыми столбцами и строками.

Алгоритм Rijndael выполняет четыре преобразования: BS (ByteSub) - табличная замена каждого байта массива (рис. 11); SR (ShiftRow) - сдвиг строк массива (рис. 12). При этой операции первая строка остается без изменений, а остальные циклически побайтно сдвигаются влево на фиксированное число байт, зависящее от размера массива. Например, для массива размером 4X4 строки 2, 3 и 4 сдвигаются соответственно на 1, 2 и 3 байта. Далее идет MC (MixColumn) - операция над независимыми столбцами массива (рис. 13), когда каждый столбец по определенному правилу умножается на фиксированную матрицу c(x). И, наконец, AK (AddRoundKey) - добавление ключа. Каждый бит массива складывается по модулю 2 с соответствующим битом ключа раунда, который, в свою очередь, определенным образом вычисляется из ключа шифрования (рис. 14).


Рисунок 11. Операция BS.


Рисунок 12. Операция SR.

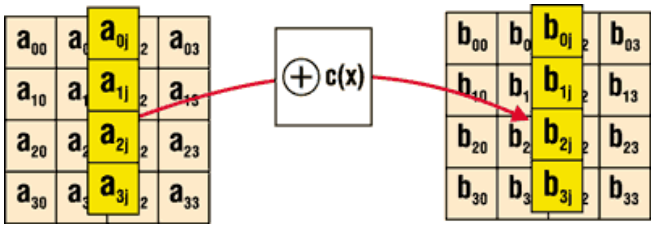


Рисунок 13. Операция MC.

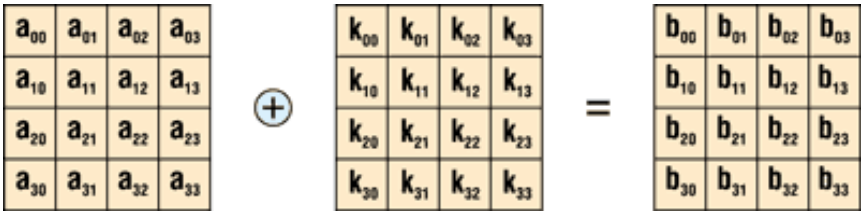

Рисунок 14. Операция AK.

В каждом раунде (с некоторыми исключениями) над шифруемыми данными поочередно выполняются перечисленные преобразования (рис. 15). Исключения касаются первого и последнего раундов: перед первым раундом дополнительно выполняется операция AK, а в последнем раунде отсутствует MC. В результате последовательность операций при зашифровании выглядит так:
AK, {BS, SR, MC, AK} (повторяется R-1 раз), BS, SR, AK.

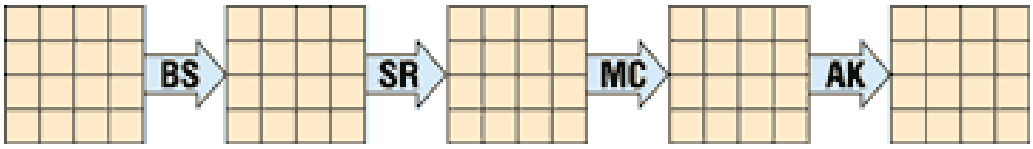


Рисунок 15. Раунд алгоритма Rijndael.

Количество раундов шифрования (R) в алгоритме Rijndael переменное (10, 12 или 14 раундов) и зависит от размеров блока и ключа шифрования (для ключа также предусмотрено несколько фиксированных размеров).

Расшифрование выполняется с помощью следующих обратных операций. Выполняется обращение таблицы и табличная замена на инверсной таблице (относительно применяемой при зашифровании). Обратная операция к SR - это циклический сдвиг строк вправо, а не влево. Обратная операция для MC - умножение по тем же правилам на другую матрицу d(x), удовлетворяющую условию: c(x) * d(x) = 1. Добавление ключа AK является обратным самому себе, поскольку в нем используется только операция XOR. Эти обратные операции применяются при расшифровании в последовательности, обратной той, что использовалась при зашифровании.

Rijndael стал новым стандартом шифрования данных благодаря целому ряду преимуществ перед другими алгоритмами. Прежде всего он обеспечивает высокую скорость шифрования на всех платформах: как при программной, так и при аппаратной реализации. Его отличают несравнимо лучшие возможности распараллеливания вычислений по сравнению с другими алгоритмами, представленными на конкурс. Кроме того, требования к ресурсам для его работы ми-

нимальны, что важно при его использовании в устройствах, обладающих ограниченными вычислительными возможностями.

Недостатком же алгоритма можно считать лишь свойственную ему нетрадиционную схему. Дело в том, что свойства алгоритмов, основанных на сети Фейстеля, хорошо исследованы, а Rijndael, в отличие от них, может содержать скрытые уязвимости, которые могут обнаружиться только по прошествии какого-то времени с момента начала его широкого распространения.

## 7.4 Асимметричное шифрование

**Криптосистема RSA**

RSA – криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись (аутентификация – установление подлинности). Криптосистема RSA разработана в 1977 году и названа в честь ее разработчиков Ronald Rivest, Adi Shamir и Leonard Adleman.

Алгоритм RSA работает следующим образом: берутся два достаточно больших простых числа p и q и вычисляется их произведение n = p*q; n называется модулем.

Затем выбирается число e, удовлетворяющее условию 1< e < (p - 1)*(q - 1) и не имеющее общих делителей кроме 1 (взаимно простое) с числом (p - 1)*(q - 1).

Затем вычисляется число d таким образом, что (e*d - 1) делится на (p - 1)*(q – 1).

- e – открытый (public) показатель
- d – частный (private) показатель.
- (n; e) – открытый (public) ключ
- (n; d). – частный (private) ключ.

Делители (факторы) p и q можно либо уничтожить либо сохранить вместе с частным (private) ключом.

Если бы существовали эффективные методы разложения на сомножители (факторинга), то, разложив n на сомножители (факторы) p и q, можно было бы получить частный (private) ключ d. Таким образом надежность криптосистемы RSA основана на трудноразрешимой – практически неразрешимой – задаче разложения n на сомножители (то есть на невозможности факторинга n) так как в настоящее время эффективного способа поиска сомножителей не существует.

Ниже описывается использование системы RSA для шифрования информации и создания цифровых подписей (практическое применение немного отличается).

*Шифрование*

Предположим, Алиса хочет послать Бобу сообщение M. Алиса создает зашифрованный текст C, возводя сообщение M в степень e и умножая на модуль n: $C = M^e \pmod n$, где e и n – открытый (public) ключ Боба. Затем Алиса посылает C (зашифрованный текст) Бобу. Чтобы расшифровать полученный текст, Боб возводит полученный зашифрованный текст C в степень d и умножает на модуль n: $M = c^d \pmod n$; зависимость между e и d гарантирует, что Боб вычислит M верно. Так как только Боб знает d, то только он имеет возможность расшифровать полученное сообщение.

*Цифровая подпись*

Предположим, Алиса хочет послать Бобу сообщение M , причем таким образом, чтобы Боб был уверен, что сообщение не было взломано и что автором сообщения действительно является Алиса. Алиса создает цифровую подпись S возводя M в степень d и умножая на модуль n: $S = M^d \pmod n$, где d и n – частный ключ Алисы. Она посылает M и S Бобу.

Чтобы проверить подпись, Боб возводит S в степень e и умножает на модуль n: $M = S^e \pmod n$, где e и n – открытый (public) ключ Алисы.

Таким образом шифрование и установление подлинности автора сообщения осуществляется без передачи секретных (private) ключей: оба корреспондента используют только открытый (public) ключ своего корреспондента или собственный частный (private) ключ. Послать зашифрованное сообщение и проверить подписанное сообщение может любой, но расшифровать или подписать сообщение может только владелец соответствующего частного (private) ключа.

*Криптоанализ шифртекста, полученного с помощью шифра RSA.*

Существует несколько способов взлома шифра RSA:

1. Попытка найти закрытый ключ, соответствующий необходимому открытому ключу. Это позволит нападающему читать все сообщения, зашифрованные открытым ключом и подделывать подписи. Для выполнения такой задачи необходимо найти сомножители p и q, что является сложной задачей, если ключи выбраны в соответствии с требованиями.

2. Поиск метода вычисления корня степени e из mod n. Т.к. $C = M^e \pmod n$, то корнем степени e из (mod n) является сообщение M. Вычислив корень, можно вскрыть зашифрованные сообщения и подделывать подписи, даже не зная закрытый ключ. Но в настоящее время неизвестны методы, которые позволяют взломать RSA таким образом, если ключ имеет большой размер.

3. Атака по предполагаемому открытому тексту. Нападающий, имея зашифрованный текст, предполагает, что сообщение содержит какой-то определенный текст, например, «Дальнейшие инструкции завтра», затем шифрует предполагаемый текст открытым ключом получателя и сравнивает полученный текст с имеющимся зашифрованным текстом. Такую атаку можно предотвратить, добавив в конец сообщения несколько случайных битов.

4. Если кто-то посылает одно и то же сообщение M трем корреспондентам, каждый из которых использует общий показатель $e = 3$, нападающий может перехватить эти сообщения и расшифровать сообщение M. Такую атаку можно предотвратить, вводя в сообщение перед каждым шифрованием несколько случайных бит.

5. Также существуют несколько атак по зашифрованному тексту (или атаки отдельных сообщений с целью подделки подписи), при которых нападающий создает некоторый зашифрованный текст и получает соответствующий открытый текст, например, заставляя обманным путем зарегистрированного пользователя расшифровать поддельное сообщение.

Кроме вышеперечисленного нужно соблюдать все необходимые требования безопасности, чтобы секретные ключи оставались в секрете, т.к. злоумышленник может попробовать завладеть ими, если система должным образом не защищена.

Поиск закрытого ключа, соответствующего необходимому открытому ключу. Закрытый ключ является произведением простых чисел p и q, поэтому нам необходимо найти эти сомножители. Для этого можно воспользоваться методом факторизации Ферма.

Метод основан на поиске таких целых чисел x и y, которые удовлетворяют соотношению $x^2-y^2=n$, что ведёт к разложению n=(x-y)(x+y). Рассмотрим алгоритм поиска простых сомножителей по методу факторизации Ферма:

$x^2-y^2=n$ равносильно $x^2-n= y^2$

Найдем $x = \sqrt{n}$ – наименьшее число, при котором разность $x^2$-n неотрицательна. Для этого для каждого значения k∈N, начиная с k=1, будем вычислять $(\sqrt{n}+k)^2 - n$ до тех пор, пока значение этого выражения не будет являться точным квадратом. Таким образом, находим k, а затем вычисляем $x = \sqrt{n}+k$ и $y = \sqrt{x^2-n}$. Полученные x и y являются искомыми простыми сомножителями.

Для обеспечения высокой надежности алгоритма RSA необходимо, чтобы используемые ключи соответствовали ряду требований:

-размеры ключей должны быть очень большими (рекомендовано 1024 бит, для особо важной информации — 2048 бит);

- числа p и q должны иметь приблизительно одинаковую длину, поскольку в этом случае найти сомножители (факторы) сложнее, чем в случае, когда длина чисел значительно различается;

-если разность p— q достаточно мала, то их очень легко найти, следовательно, их значения не должны быть близки друг к другу.

Так как компьютер, который был использован для шифрования, имеет невысокие возможности, были выбраны небольшие ключи, поэтому вскрыть текст возможно (число 17053 легко раскладывается на множители).

Итак, алгоритм RSA является достаточно криптостойким шифром. Трудоемкость криптоанализа обеспечивается сложностью нахождения простых сомножителей закрытого ключа. В зависимости от защищаемых данных определяется длина ключа для обеспечения необходимой криптостойкости.

В настоящее время криптографическая система RSA получила широкое распространение. Она была первой системой, пригодной и для шифрования, и для цифровой подписи. Сейчас она используется в большом числе криптографических приложений, также ее используют в сочетании с симметричными криптосистемами.

Наука не стоит на месте. Вычислительные машины становятся еще мощнее, с их помощью можно решать все более и более сложные задачи. Поэтому и криптография должна постоянно совершенствовать свои методы, чтобы суметь противодействовать злоумышленникам.

**Вопросы по пройденному материалу:**

1. Назовите методы криптографического преобразования информации.
2. Дайте характеристику симметричным методам шифрования.
3. Дайте характеристику асимметричным методам шифрования.

## ГЛОССАРИЙ

**AES** (Advanced Encryption Standard) — Симметричный криптографический алгоритм.

**ARL** (Authority Revocation List) — Список аннулированных удостоверяющих центров, то есть тех удостоверяющих центров, сертификаты которых недействительны.

**ASN.1** (Abstract Syntax Notation One) — Абстрактная синтаксическая нотация, которая была предложена комитетом разработчиков стандартов взаимодействия открытых систем для использования с протоколами X.500. ASN. 1 описывает синтаксис различных структур данных, предоставляя четко определенные примитивные объекты и средства описания комбинаций примитивных объектов.

**CMP** (certificate management protocol) — Протокол управления сертификатами, обеспечивает связь с совместимыми приложениями.

**DES** (Digital Encryption Standard) — Симметричный алгоритм шифрования, разработанный специалистами компании IBM и Управления национальной безопасности США.

**DH** (Diffie-Hellman) — Алгоритм Диффи-Хэллмана, используется для согласования ключей (обмена ключами). Две стороны могут сформировать один и тот же секрет, а затем использовать его для построения сеансового ключа, используемого в симметричном алгоритме.

**DNS** (Domain Name System) — Система доменных имен.

**DSA** (Digital Signature Algorithm) — Алгоритм цифровой подписи, разработанный Дэвидом Кравицем. Официальный алгоритм цифровой подписи правительственных учреждений США.

**ECDH** (Elliptic Curve Diffie-Hellman) — Алгоритм эллиптических кривых Диффи-Хэллмана, используется для решения проблемы распределения ключей.

**ECDSA** (Elliptic Curve Digital Signature Algorithm) — Алгоритм цифровой подписи, использующий эллиптические кривые.

**ETSI** (European Telecommunications Standards Institute) — Европейский институт стандартов связи.

**HMAC** (Hash Message Authentication Checksum) — Код аутентификации сообщения на основе вычисления хеш-кода.

**HTTP** (HyperText Transfer Protocol) — Протокол обмена гипертекстовыми документами между HTTP-сервером и браузером клиента.

**IETF** (Inernet Engineering Task Force) — Группа инженерной поддержки Интернет — интернациональное сообщество разработчиков, производителей и исследователей, занимающихся обеспечением функционирования и эволюции Интернет.

**IP** (Internet Protocol) — Протокол передачи данных сетевого уровня группы протоколов TCP/IP, базовый протокол передачи данных в Интернет.

**IPSec** — Набор стандартов, описывающих архитектуру безопасности Интернет-протоколов (IP), регламентирующие контроль целостности на уровне IP-пакетов, аутентификацию источника данных и защиту от воспроизведения

ранее посланных IP-пакетов, обеспечение конфиденциальности: шифрование содержимого IP-пакетов, а также частичную защиту от анализа трафика путем применения туннельного режима.

**IP-спуфинг** — Преднамеренная подмена (имитация) системы с использованием ее сетевого IP-адреса.

**ITU** (International Telecommunication Union) — Международный союз по телекоммуникациям — международная организация, занимающаяся координацией функционирования телекоммуникационных сетей и сервисов, а также публикацией стандартов и рекомендаций в сфере телекоммуникационных технологий.

**MD2** — Алгоритм вычисления дайджеста сообщения (хеш-кода), разработанный Роном Ривестом. Выдает 128-битный (16-байтный) дайджест сообщения произвольной длины.

**MD4** — Алгоритм вычисления дайджеста сообщения (хеш-кода), разработанный Роном Ривестом. Выдает 128-битный (16-байтный) дайджест сообщения произвольной длины.

**MD5** — Алгоритм вычисления дайджеста сообщения (хеш-кода), разработанный Роном Ривестом для усовершенствования алгоритма MD4.

**Object Identifier (OID)** — Идентификатор объекта — указатель, характеризующий объект, в т.ч. политику применения сертификатов, используется в сертификате формата X.509 версии 3.

**OCSP** (Online Certificate Status Protocol) — Онлайновый протокол статуса сертификата, применяется для проверки действительности сертификатов в режиме реального времени.

**PGP** (Pretty Good Privacy) — Система для обеспечения конфиденциальности файлов и сообщений электронной почты в глобальных вычислительных и коммуникационных средах. Pretty Good Privacy (конфиденциальность без проблем), была разработана американским программистом Филом Циммерманном.

**PKCS** (Public Key Cryptography Standards) — Стандарты криптографии с открытым ключом — промышленные стандарты, разработанные в 1991 году компанией RSA Laboratories совместно с представителями компьютерных компаний.

**PKIX** — Комитет группы инженерной поддержки Интернет (IETF), занимающийся совершенствованием сертификатов X.509 и соответствующих сервисов.

**RSA** (Rivest-Shamir-Adleman) — Асимметричный алгоритм шифрования, получил название по инициалам его авторов: Рона Ривеста, Ади Шамира и Лена Эдльмана. Данные, зашифрованные с помощью открытого ключа, могут быть расшифрованы только с помощью закрытого ключа. Используется для решения проблемы распределения ключей и для вычисления цифровой подписи (дайджест сообщения (хеш-код) шифруется с помощью закрытого ключа).

**SET** (Secure Electronic Transaction) — Протокол защиты платежей по кредитным картам в Интернет.

**SHA-1** — Алгоритм государственного стандарта США на вычисление дайджеста сообщения (хеш-кода) для цифровой подписи.

**SHTTP** (Secure HyperText Transfer Protocol) — Расширенный вариант протокола HTTP, который обеспечивает шифрование данных, передаваемых между web-сайтом и web-браузером, а также аутентификацию сервера и клиента.

**SSL** (Secure Sockets Layer) — Протокол, обеспечивающий защиту транзакций в Интернет за счет поддержки шифрования и аутентификации.

**TLS** (Transport Layer Security) — Протокол, обеспечивающий защиту транзакций в Интернет за счет поддержки шифрования и аутентификации, является развитием SSL.

**Triple-DES** — Симметричный криптографический алгоритм, который выполняет алгоритм DES три раза.

**Абонент информационной сети общего пользования** (абонент Сети) — юридическое (учреждение, предприятие, организация) или физическое лицо, в том числе являющееся сотрудником организации, осуществляющее взаимодействие с Сетью.

**Абонентский пункт** (АП) — автоматизированная система, подключаемая к Сети с помощью коммуникационного оборудования и предназначенная для работы абонента Сети. АП могут быть выполнены как автономные персональные электронно-вычислительные машины (ПЭВМ) с модемом и не иметь физических каналов связи с другими средствами вычислительной техники (СВТ) организации, а также в виде одной или нескольких объединенных локальных вычислительных сетей (ЛВС) с рабочими станциями и серверами, соединенными с Сетями через коммуникационное оборудование (модемы, мосты, шлюзы, маршрутизаторы-роутеры, мультиплексоры, коммуникационные серверы и т.п.).

**Автоматизированная система** (АС) — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Авторизованный субъект доступа** — субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

**Авторство информации** — Однозначное соответствие между содержанием и/или формой информации и субъектом (объектом), сформировавшим эту информацию. Для пользователя авторство полученной им из системы или по каналу связи информации означает однозначное установление источника, сформировавшего эту информацию (ее автора).

**Администратор АС** — лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

**Администратор защиты (безопасности) информации** — лицо, ответственное за защиту АС от несанкционированного доступа к информации.

**Аннулирование сертификата** — Признание сертификата недействительным в период его действия в случаях компрометации секретного ключа или изменения атрибутов сертификата с момента его выпуска (например, при изменении имени пользователя).

**Аутентификация** — Проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. Аутентификация осуществляется на основании того или иного секретного элемента (аутентификатора), которым располагают как субъект, так и информационная система.

**Аутентификация информации** — Установление подлинности информации исключительно на основе внутренней структуры самой информации независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и при этом не была заменена или искажена.

**Аутсорсинг** — Выполнение отдельных задач проекта компании сторонними организациями, специализирующимися в этой области.

**Безопасность информации** — состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

**Безопасность информационной технологии** — защищенность технологического процесса переработки информации.

**Биометрическая аутентификация** — Аутентификация, опирающаяся на уникальные биологические показатели человека. К основным биометрическим идентификаторам относятся отпечатки пальцев, рукописные подписи, образцы голоса, результаты сканирования сетчатки и радужной оболочки глаза, формы ладони или черт лица.

**Браузер** — Программа, обеспечивающая доступ к текстовым и графическим страницам World Wide Web.

**Верификация (проверка) цифровой подписи документа** — Проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ подписавшего пользователя. Если рассматриваемое соотношение оказывается выполненным, то подпись признается действительной, а сам документ — подлинным, в противном случае документ считается измененным, а подпись под ним — недействительной.

**Взаимная (перекрестная) сертификация** — Двусторонний процесс сертификации двух доверенных удостоверяющих центров.

**Владелец информации** — Субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

**Владелец сертификата ключа подписи** — физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

**Вспомогательные технические средства и системы** (ВТСС) — технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях. К ВТСС относятся: телефонные средства и системы; средства и системы передачи данных, системы радиосвязи; средства и системы охранной и пожарной сигнализации; средства и системы оповещения и сигнализации; контрольно-

измерительная аппаратура; средства и системы кондиционирования; средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.п.); средства электронной оргтехники; иные технические средства и системы.

**Выпуск сертификата** — Генерация сертификата и уведомление владельца, зафиксированного в нем, о подробном содержании этого сертификата.

**Депонирование ключей** — Предоставление копий секретных ключей третьей стороне и разрешение пользоваться ими при определенных обстоятельствах, в качестве третьей стороны чаще всего выступают правительственные учреждения и правоохранительные органы. Депонирование ключей может быть возложено на независимое подразделение внутри организации, развертывающей PKI, или на внешнее агентство.

**Доверяющая сторона** — Лицо, которое получает сертификат и полагается на него при совершении сделок или обмене сообщениями.

**Доказательство доставки данных** — Атрибут сервиса неотказуемости. Гарантирует, что сторона, принимающая информацию, не сможет отрицать того, что получила сообщение.

**Доказательство происхождения данных** — Атрибут сервиса неотказуемости. Гарантирует, что сторона, отправляющая информацию, не сможет отрицать того, что сообщение отправлено ей.

**Документ** — Документированная информация, снабженная определенными реквизитами.

**Документированная информация** — Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

**Домен безопасности** — Группа (компания, рабочая группа или коллектив), сертификаты которой выпущены одним и тем же удостоверяющим центром.

**Домен доверия** — Множество субъектов, сертификаты которых выпущены одним и тем же удостоверяющим центром. Пользователи, чьи сертификаты подписаны данным удостоверяющим центром, могут полагаться на идентичность (действительность, подлинность) другого пользователя, который владеет сер¬тификатом, выпущенным тем же удостоверяющим центром.

**Дополнения сертификата** — Необязательные атрибуты сертификата, позволяющие включать в сертификат информацию, которая отсутствует в основном содержании сертификата.

**Доступ к информации (доступ)** — ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

**Доступ к ресурсу** — получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным ресурсом.

**Доступность информации** — состояние информации, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

**Заверение (нотаризация)** — Регистрация данных у доверенного третьего лица для повышения уверенности в правильности таких характеристик, как содержание, источник данных, время доставки.

**Закладочное устройство** — элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Закрытая система PKI** — Характеризуется наличием договоров, определяющих права и обязанности всех участников системы в отношении аутентификации сообщений или транзакций.

**Закрытый ключ электронной цифровой подписи** — уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

**Защита информации от несанкционированного доступа (защита от НСД) или воздействия** — деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию).

**Защищаемые помещения (ЗП)** — помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

**Идентификация** — Процесс сопоставления введенной им своей характеристики с некоторым хранимым системой идентификатором. В дальнейшем идентификатор субъекта используется для предоставления субъекту определенного уровня прав и полномочий.

**Иерархия доверия** — Система проверки цифровых сертификатов. Каждый сертификат связан с сертификатом ключа подписи того субъекта, который снабдил его цифровой подписью. Так, сертификат абонента связан с сертификатом УЦ низшего уровня, который, в свою очередь, связан с сертификатом УЦ более высокого уровня и так далее до УЦ высшего уровня. Следуя по цепочке доверия до известной доверенной стороны, можно убедиться в действительности сертификата.

**Информативный сигнал** — Электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах или обсуждаемая в ЗП.

**Информационная система общего пользования** — информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

**Информационные сети общего пользования (Сети)** — вычислительные (информационно-телекоммуникационные) сети открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

**Инфраструктура открытых ключей (ИОК)** — Технологическая инфраструктура и сервисы, гарантирующие безопасность информационных и коммуникационных систем, использующих алгоритм с открытыми ключами.

**Компрометация ключей** — Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

**Контролируемая зона (КЗ)** — пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств. Границей КЗ могут являться: периметр охраняемой территории организации; ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории. В отдельных случаях, на период обработки техническими средствами конфиденциальной информации, границы КЗ временно могут расширяться. При этом должны приниматься организационные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

**Контроль доступа (управление доступом)** — Процесс ограничения доступа к ресурсам системы только разрешенным субъектам или объектам.

**Конфиденциальная информация** — информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

**Конфиденциальность информации** — состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

**Корневой удостоверяющий центр** — Удостоверяющий центр, находящийся на вершине иерархии в инфраструктуре открытых ключей, выпускает самоподписанный сертификат и сертификаты для подчиненных удостоверяющих центров.

**Корпоративная информационная система** — информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

**Криптографическая защита** — Защита данных при помощи криптографического преобразования данных.

**Криптографические операции**: безопасное хеширование; выработка и верификация контрольных сумм (имитовставки); зашифрование и (или) расшифрование данных; зашифрование и (или) расшифрование криптографических ключей, выработка и верификация электронной цифровой подписи.

**Криптографический ключ** — Последовательность символов, которая контролирует криптографические операции (зашифрование, расшифрование, вычисление хэш-функции, вычисление или проверку цифровой подписи).

**Криптографический модуль** — Комплекс программных, программно-аппаратных и аппаратных средств, используемый с целью гарантирования безопасности при генерации, хранении и применении криптографического ключа.

**Криптографическое преобразование** — Преобразование данных при помощи шифрования и (или) выработки имитовставки.

**Криптосистема с открытыми ключами** — Система построенная на основе асимметричного криптографического алгоритма, использующего два ключа (открытый ключ и секретный ключ), соответствующих друг другу. Если информация зашифровается одним ключом (открытым), система может расшифровать ее при помощи другого ключа (секретного). Аналогично, если информация подписывается одним ключом (секретным), абонент может использовать другой ключ (открытый) для аутентификации лица, поставившего подпись. Атрибуты этих двух ключей не позволяют вычислить секретный ключ, даже если известен открытый ключ.

**Локальная вычислительная сеть (ЛВС)** — совокупность основных технических средств и систем, осуществляющих обмен информацией между собой и с другими информационными системами, в том числе с ЛВС, через определенные точки входа/выхода информации, которые являются границей ЛВС.

**Межсетевой экран (МЭ)** — локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и (или) выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя, таким образом, разграничение доступа субъектов из одной АС к объектам другой АС.

**Модель доверия** — Модель, задающая порядок сертификации одних удостоверяющих центров другими.

**Мостовой удостоверяющий центр** — Удостоверяющий центр, предназначенный для установления связей между разнородными инфраструктурами открытых ключей.

**Набор положений PKI** — Совокупность положений практики и/или политики PKI, охватывающих круг стандартных тем для формулирования политики применения сертификатов или регламента.

**Нарушитель** — лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства (чисто агентурные методы получения сведений, технические средства перехвата без модификации компонентов системы, штатные средства и недостатки систем защиты, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ и т.п.).

**Некорректный электронный документ** — Электронный документ, не прошедший процедуры расшифрования данных, проверки электронной цифровой подписи информации, контроля формата документов, а также документ, имеющий искажения в тексте сообщения (наличие символов, букв или цифр в расшифрованном (открытом) тексте документа, не позволяющих понять его смысл).

**Неотказуемость получения** — Невозможность для получателя отрицать прием информации, поскольку свидетельство получения (например, цифровая подпись) доказывает связь между атрибутами получателя и информацией.

**Несанкционированное действие** — действие субъекта в нарушение установленных в системе правил обработки информации.

**Несанкционированный доступ (НСД)** — доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых СВТ или АС.

**Основные технические средства и системы (ОТСС)** — технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации. В контексте настоящего документа к ним относятся АС различного уровня и назначения на базе СВТ, средства и системы связи и передачи данных, включая коммуникационное оборудование, используемые для обработки и передачи конфиденциальной информации.

**Открытая система PKI** — Характеризуется отсутствием формальных договоров, регулирующих отношения субъектов системы.

**Открытый ключ** — Криптографический ключ, который связан с секретным с помощью особого математического соотношения. Открытый ключ известен всем другим пользователям системы и предназначен для проверки электронной цифровой подписи и расшифрования, позволяет определить автора подписи и достоверность электронного документа, но не позволяет вычислить секретный ключ.

**Открытый ключ электронной цифровой подписи** — уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

**Пара ключей (ключевая пара)** — Открытый ключ, используемый в криптосистеме с открытыми ключами, и соответствующий ему секретный (закрытый) ключ.

**Подписчик (владелец) сертификата** — Лицо, которое заключает с удостоверяющим центром договор об обслуживании и становится владельцем сертификатов, выпущенных УЦ.

**Подтверждение подлинности электронной цифровой подписи в электронном документе** — положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

**Политика (Правила) применения сертификатов** — Установленный набор правил, характеризующих возможность применения сертификата определенным сообществом и/или для класса приложений с определенными требованиями безопасности. Политика применения сертификатов позволяет доверя-

ющей стороне оценить надежность использования сертификата для определенного приложения.

**Пользователь сертификата ключа подписи** — физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

**Правила разграничения доступа** — совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

**Приостановление сертификата** — Временное аннулирование сертификата в период его действия с последующим его возобновлением или отзывом.

**Провайдер Сети** — уполномоченная организация, выполняющая функции поставщика услуг Сети для абонентов Сети.

**Профиль сертификата** — Набор характеристик, которые задают тип данного сертификата.

**Путь доверия** — Связывает доверяющую сторону с одной или многими третьими доверенными сторонами и позволяет конфиденциально проверять законность используемого доверяющей стороной сертификата.

**Разграничение доступа к ресурсам АС** — это такой порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

**Разностный список аннулированных сертификатов** — Список, фиксирующий изменения списка аннулированных сертификатов, произошедшие с момента выпуска последнего.

**Расшифрование данных** — Процесс преобразования зашифрованных данных в открытые при помощи шифра.

**Регистрационный центр (РЦ)** — Лицо (физическое или юридическое), которое с санкции удостоверяющего центра выполняет функции аутентификации в процессе выпуска или аннулирования сертификата. Регистрационный центр не выпускает сертификаты и не ведет списки аннулированных сертификатов.

**Регламент УЦ** — Документ, который устанавливает и детализирует процедуры сертификации и управления ключами в соответствии с политикой удостоверяющего центра.

**Риск** — фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери — прямые или косвенные).

**Секретный (закрытый) ключ** — Ключ асимметричной ключевой пары, который доступен только одному пользователю системы и хранится им в тайне. В системе цифровой подписи определяет криптопреобразование подписи, в асимметричной системе шифрования определяет криптопреобразование расшифрования.

**Сервер восстановления ключей** — Сервер инфраструктуры открытых ключей, который поддерживает создание резервных копий и восстановление ключей шифрования конечных субъектов.

**Сервер каталогов** — Сервер инфраструктуры открытых ключей, который хранит информацию о сертификатах и атрибутах субъектов сертификатов открытых ключей.

**Сервер сертификатов (центр сертификации)** — Сервер инфраструктуры открытых ключей, на который возлагаются функции выпуска и управления сертификатами, защищенного хранения секретного ключа удостоверяющего центра, поддержки жизненного цикла сертификатов и ключей, восстановления данных, ведения контрольного журнала и регистрации всех операций удостоверяющего центра.

**Сервисы безопасности** — Совокупность механизмов, процедур и других средств управления для снижения рисков, связанных с угрозой утраты или раскрытия данных.

**Сервис неотказуемости** — Сервис предотвращения отказа от участия в обмене информацией, гарантирующего, что стороны, отправляющие и принимающие электронные сообщения или документы, не смогут отрицать свое участие в информационном обмене в целом или на отдельных его этапах.

**Сертификат ключа подписи** — документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи. Содержит информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, о выпустившем удостоверяющем центре и т.д.

**Сертификат сервера** — Цифровой сертификат, выпущенный удостоверяющим центром для web-сервера. Предназначен для аутентификации web-сервера при выполнении транзакций, основанных на протоколах TLS/SSL.

**Сертификат средств электронной цифровой подписи** — документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

**Сертификация (открытых ключей)** — Процесс выпуска сертификатов и их последующего обслуживания для физических и юридических лиц, оборудования и т.д.

**Система асимметричного шифрования** — Система, основанная на асимметричных методах, когда преобразование с открытым ключом используется для шифрования, а соответствующее преобразование с закрытым ключом — для расшифрования.

**Система защиты АС (информации)** — совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения безопасности АС (циркулирующей в АС информации).

**Служебная информация СЗИ НСД** — информационная база АС, необходимая для функционирования СЗИ НСД (уровень полномочий эксплуатационного персонала АС, матрица доступа, ключи, пароли и т.д.).

**Согласование ключа** — Процесс установления общего ключа для взаимодействия между пользователями, при котором ни один из пользователей не может предопределять значение этого ключа.

**Специальный защитный знак (СЗЗ)** — сертифицированное и зарегистрированное в установленном порядке изделие, предназначенное для контроля несанкционированного доступа к объектам защиты, определяя подлинность и целостность СЗЗ, путем сравнения самого знака или композиции «СЗЗ — подложка» по критериям соответствия характерным признакам визуальными, инструментальными и другими методами.

**Список аннулированных (отозванных) сертификатов (CAC/COC)** — Список недействительных сертификатов, генерируется удостоверяющим центром.

**Средства электронной цифровой подписи** — аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

**Техническая защита конфиденциальной информации (ТЗКИ)** — защита информации некриптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения или блокирования.

**Технический канал утечки информации** — совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Токен** — Устройство хранения криптографических ключей, аппаратный ключ. Транспортировка ключа — Защищенный процесс передачи ключа от одного пользователя к другому.

**Угроза безопасности информации** — потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию.

**Удостоверяющий центр (УЦ)** — Доверенное лицо (физическое или юридическое), которое выпускает, публикует, аннулирует сертификаты, приостанавливает их действие.

**Управление ключами** — Создание (генерация) ключей, их хранение, распространение, удаление (уничтожение), учет и применение в соответствии с политикой безопасности.

**Услуги Сети** — комплекс функциональных возможностей, предоставляемых абонентам сети с помощью прикладных протоколов (протоколы электронной почты, FTP — File Transfer Protocol — прием/передача файлов, HTTP —

Hyper Text Transfer Protocol — доступ к Web-серверам, IRC — Internet Relay Chat -диалог в реальном времени, Telnet терминальный доступ в сети, WAIS — Wide Area Information Servers — система хранения и поиска документов в сети и т.д.).

**Уязвимость информации** — подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности, или неправомерному ее тиражированию.

**Хеш-код (дайджест)** — Строка битов фиксированной длины, полученная из строки битов произвольной длины при помощи математической операции над данными, является выходом хэш-функции.

**Хеш-функция (функция хеширования)** — Функция, которая переводит строку битов произвольной длины в строку битов фиксированной длины. По данному значению хеш-функции вычислительно невозможно найти аргумент, а по данному аргументу хеш-функции вычислительно невозможно найти другой аргумент, дающий такое же значение функции.

**Целостность информации** — состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

**Цифровая подпись (ЭЦП)** — Результат криптографического преобразования, при котором дайджест (хеш-код) подписываемого сообщения шифруется секретным (закрытым) ключом. Цифровая подпись может быть проверена путем сопоставления значения, расшифрованного при помощи открытого ключа, и дайджеста (хеш-кода) исходного сообщения. Цифровая подпись может быть выработана только лицом, имеющим секретный ключ — результат ее использования в электронном документообороте аналогичен собственноручной подписи на бумажном документе.

**Шифровальный ключ (симметричный)** — Параметр, используемый в симметричном криптографическом алгоритме, позволяющий отправителю и получателю использовать один и тот же криптографический ключ для зашифрования и расшифрования данных.

**Шифрование** — Шифрование информации — взаимнооднозначное математическое (криптографическое) преобразование, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации, представленной в некоторой цифровой кодировке, блок шифрованной информации, также представленной в цифровой кодировке.

**Шифротекст** — Зашифрованная информация.

**Электронная цифровая подпись (ЭЦП)** — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

**Электронный документ** — Задокументированная совокупность данных, представленных в электронно-цифровой форме и зафиксированных на матери-

альном носителе с реквизитами, позволяющими идентифицировать эту информацию и авторов документа. Идентификация электронного документа обеспечивается средствами защиты на основе алгоритмов шифрования, электронной цифровой подписи и защиты от несанкционированного доступа.

## СПИСОК ЛИТЕРАТУРЫ


1. Бабаш, А.В. Криптографические методы защиты информации. Т.1 : Уч.-метод.пос./Бабаш А. В., 2-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2019. - 413 с.
2. Баранова, Е.К. Основы информационной безопасности : учебник/ Е.К. Баранова, А.В. Бабаш. - М. : РИОР : ИНФРА-М, 2019. — 202 с.
3. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — Москва : Издательство МГТУ им. Н. Э. Баумана, 2016. — 250, [2] с. : ил.
4. Гаврилов, М.В. Информатика и информационные технологии [Текст]: учебник для прикладного бакалавриата/ М.В.Гаврилов, В.А.Климов. — 4-е изд., перераб. и доп. — М.: Издательство Юрайт, 2014. — 383 с.
5. Доктрина информационной безопасности Российской Федерации от 5 декабря 2016 г. №646 // http://www.consultant.ru
6. Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика №1(35) 2016 с. 86-94
7. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил.
8. Международный стандарт ISO/IEC 17799 - Информационные технологии – практические правила управления информационной безопасностью. Первое издание 2000-12-01. 87 с.
9. Мельников, В.П. Информационная безопасность [Текст]: учебное пособие/ В.П.Мельников, С.А.Клейменов, А.М.Петраков; под ред. С.А.Клейменова. — М.: Издательский центр "Академия", 2013. — 336 с.
10. Нестеров, С.А. Информационная безопасность: учебник и практикум для прикладного бакалавриата / С.А. Нестеров.- М.: Издательство Юрайт 2016.- 321 с.
11. Родичев, Ю. А. Информационная безопасность. Национальные стандарты Российской Федерации / Ю. А. Родичев — «Питер», 2018. – 256 с.
12. Трунова А. А. Исследование криптосистем с открытым ключом на основе анализа алгоритма RSA // Молодой ученый. — 2015. — №13. — С. 39-44. — URL https://moluch.ru/archive/93/20632/
13. Хлебников, А.А. Информационные технологии [Текст]: учебник/ А.А. Хлебников. - М.: КНОРУС, 2014. - 472 С. - (Бакалавриат).

Карасева Э.М., Рак О.В.

**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

учебное пособие

Формат 60x84 1/16
Бумага офисная.
Печать цифровая
5,625 усл. печ. л.
Тираж 100 экз.

Отпечатано: ТОО «New Line Media»
г. Костанай, пр. Аль-Фараби, 115, оф. 512
тел.: 8(7142) 53-11-47, 53-06-71
e-mail: geosprint@mail.ru