

Информация и информационная безопасность

- **Информация** (лат. informatio — разъяснение, изложение), первоначально — сведения, передаваемые людьми устным, письменным или другим способом с помощью условных сигналов, технических средств и т.д.
- **Информация** - сведения о лицах, предметах, фактах, событиях, явлениях и процессах.
- **Информация** может существовать в виде бумажного документа, физических полей и сигналов, биологических полей. В дальнейшем будем рассматривать информацию в документированной форме и в форме физических полей.
- **Угроза информационной безопасности объекта** - возможные воздействия на него, приводящие к ущербу.
- **Уязвимость** - некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы.
- **Атака** - действие злоумышленника, заключающееся в поиске и использовании той или иной уязвимости.
- **Защита информации** — комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.
- **Информационная безопасность** — это одна из характеристик информационной системы, т.е. информационная система на определенный момент времени обладает определенным состоянием (уровнем) защищенности, а защита информации — это процесс, который должен выполняться непрерывно на всем протяжении жизненного цикла информационной системы.
- **Информационная угроза** — потенциальная возможность неправомерного или случайного воздействия на объект

защиты, приводящая к потере, искажению или разглашению информации.

- **Политика информационной безопасности (ПИБ)** организации или учреждения – совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.
- **Объект** – пассивный компонент системы, хранящий, перерабатывающий, передающий или принимающий информацию; примеры объектов: страницы, файлы, папки, директории, компьютерные программы, устройства (мониторы, диски, принтеры и т. д.).
- **Субъект** – активный компонент системы, который может инициировать поток информации; примеры субъектов: пользователь, процесс либо устройство.

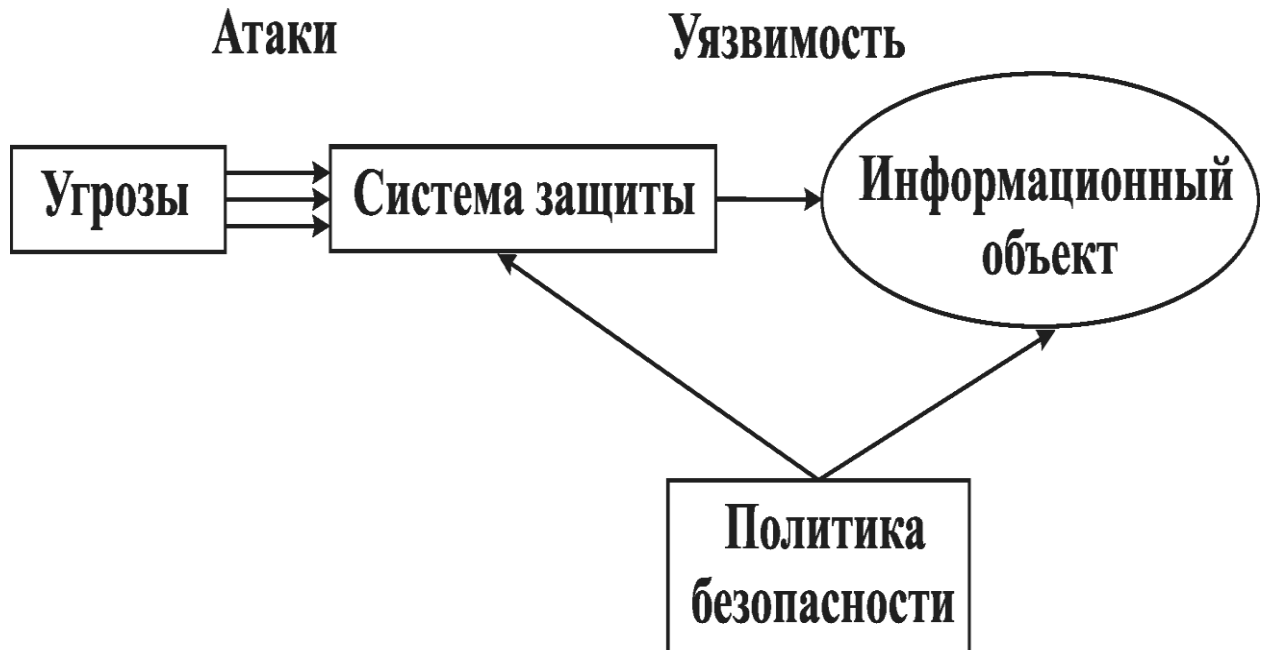
Цель защиты информационного объекта - противодействие угрозам безопасности

- **Защищенный информационный объект** — это объект со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.
- **Комплексная защита информационного объекта (ИО)** — совокупность методов и средств (правовых, организационных, физических, технических, программных).
- **Вывод: Политика безопасности** — совокупность норм, правил, рекомендаций, регламентирующих работу средств защиты ИО от заданного множества угроз безопасности.
- Понятие информационной безопасности в узком смысле этого слова подразумевает: надежность работы компьютера; сохранность ценных данных; защиту информации от внесения

в нее изменений неуполномоченными лицами; сохранение тайны переписки в электронной связи.

Содержание
основы защиты информации

предмета



Этапы развития информационной безопасности:

- I этап — до 1816 года — характеризуется использованием естественно возникавших средств информационных коммуникаций.
- II этап — начиная с 1816 года — связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи.
- III этап — начиная с 1935 года — связан с появлением радиолокационных и гидроакустических средств.
- IV этап — начиная с 1946 года — связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров).
- V этап — начиная с 1965 года — обусловлен созданием и развитием локальных информационно-коммуникационных сетей.

- VI этап — начиная с 1973 года — связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьезнее. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.
- VII этап — начиная с 1985 года — связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить что очередной этап развития информационной безопасности, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

Основные задачи системы ИБ

- своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба его интересам;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия;

- эффективное пресечение посягательств на ресурсы и угрозы персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение целей организации.

Составляющие

ИБ:

Доступность информации

- – свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними. Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность информации

- – свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к

корректному выполнению сложных действий (транзакций⁴)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений. Целостность оказывается важнейшим аспектом информационной безопасности в тех случаях, когда информация служит «руководством к действию». Рецептúra лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным.

Конфиденциальность информации

- – свойство информации быть известной и доступной только правомочным субъектам системы (пользователям, программам, процессам). К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.
- Информационная безопасность не сводится исключительно к защите от НСД к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от НСД, но и от поломки системы, вызвавшей перерыв в работе.
- **Информационный объект** - это среда, в которой информация создается, передается, обрабатывается или хранится.

- **Безопасность информационного объекта** понимается его защищенность от случайного или преднамеренного вмешательства в нормальный процесс его функционирования.

Природа воздействия на информационный объект может быть двух видов:

- — непреднамеренной (стихийные бедствия, отказы оборудования, ошибки персонала и т.д.);
- — преднамеренной (действия злоумышленников).

Все воздействия могут привести к последствиям (ущербу) трех видов: нарушению конфиденциальности, целостности, доступности.

- **Нарушение конфиденциальности** — нарушение свойства информации быть известной только определенным субъектам.
- **Нарушение целостности** — несанкционированное изменение, искажение, уничтожение информации.
- **Нарушение доступности (отказ в обслуживании)** — нарушаются доступ к информации, работоспособность объекта, доступ в который получил злоумышленник.
- В отличие от разрешенного (санкционированного) доступа к информации в результате преднамеренных действий злоумышленник получает несанкционированный доступ. Суть несанкционированного доступа состоит в получении нарушителем доступа к объекту в нарушение установленных правил.

Классификация угроз

- Под **угрозой информационной безопасности объекта** будем понимать возможные воздействия на него, приводящие к ущербу.
- **По виду:**
 - — физической и логической целостности (уничтожение или искажение информации);

- — конфиденциальности (несанкционированное получение);
- — доступности (работоспособности);
- — права собственности;

■ **По происхождению:**

- — случайные (отказы, сбои, ошибки, стихийные явления);
- — преднамеренные (злоумышленные действия людей);

По источникам:

- — люди (персонал, посторонние);
- — технические устройства;
- — модели, алгоритмы, программы;
- — внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

■ **Информационные угрозы могут быть обусловлены:**

- естественными факторами (пожар, наводнение, и др.);
- человеческими факторами.
- Последние (человеческий фактор), в свою очередь, подразделяются на:
 - угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации;
 - угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с несанкционированным доступом к ресурсам АИС.
- Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.
- **Пассивные угрозы**, как правило, направлены на несанкционированное использование информационных

ресурсов, не оказывая при этом влияния на их функционирование (прослушивание).

- **Активные угрозы** имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.
- Умышленные угрозы также подразделяются на внутренние, возникающие внутри управляемой организации, и внешние.
- Под **внутренними угрозами** понимаются — угрозы безопасности информации инсайдером (исполнителем) которых является внутренний по отношению к ресурсам организации субъект (инсайдер).
- Под **внешними угрозами** понимаются — угрозы безопасности информации инициатором (исполнителем) которых является внешний по отношению к ресурсам организации субъект (удаленный хакер, злоумышленник).
- **Внутренние угрозы**
 - Утечки информации
 - Неавторизованный доступ
- **Внешние угрозы**
 - Вредоносные программы (вирусы, троянцы, черви и т.д.)
 - Атаки хакеров
 - DDos-атаки
 - Таргетированные атаки
 - Спам
 - Фишинг
 - Промышленные угрозы (stuxnet, flame, duqu)

- Шпионское программное обеспечение (spyware, adware)
- botnets (ботнеты или зомби-сети)
- **Случайные угрозы** обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибками персонала. Методы оценки воздействия этих угроз рассматриваются в других дисциплинах (теории надежности, программировании, инженерной психологии и т. д.).
- **Преднамеренные угрозы** связаны с действиями людей (работники спецслужб, самого объекта, хакеры). Огромное количество разнообразных информационных объектов делает бессмысленным перечисление всех возможных угроз для информационной безопасности, поэтому в дальнейшем при изучении того или иного раздела мы будем рассматривать основные угрозы для конкретных объектов.
- Например, для **несанкционированного доступа к информации** вычислительной системы злоумышленник может воспользоваться:
 - — штатными каналами доступа, если нет никаких мер защиты;
 - — через терминалы пользователей;
 - — через терминал администратора системы;
 - — через удаленные терминалы,
 - или нештатными каналами доступа:
 - — побочное электромагнитное излучение информации с аппаратуры системы;
 - — побочные наводки информации по сети электропитания и заземления;
 - — побочные наводки информации на вспомогательных коммуникациях;
 - — подключение к внешним каналам связи.

Категории и носители информации

- В соответствии с законом «О государственных секретах» к охраняемым сведениям могут быть отнесены сведения, несанкционированное распространение которых создает или может нанести ущерб национальной безопасности, обороноспособности и жизненно важным интересам Республики Беларусь. Государственные секреты являются собственностью Республики Беларусь. Установление и снятие ограничений на распространение сведений, составляющих государственные секреты, производится в определенном настоящим Законом порядке.
- Государственные секреты Республики Беларусь подразделяются на две категории: государственная тайна и служебная тайна.
- **Государственная тайна** – государственные секреты, разглашение или утрата которых может повлечь тяжкие последствия для национальной безопасности, обороноспособности, экономических и политических интересов Республики Беларусь, а также создать реальную угрозу безопасности правам и свободам граждан.
- **Служебная тайна** – государственные секреты, разглашение или утрата которых может нанести ущерб национальной безопасности, обороноспособности, политическим и экономическим интересам Республики Беларусь, а также правам и свободам граждан. Сведения, составляющие служебную тайну, как правило, имеют характер отдельных данных, входящих в состав сведений, являющихся государственной тайной, и не раскрывают ее в целом.
- **Конфиденциальная информация** – документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности.

- **Информация, запрещенная к распространению**, определена в многочисленных нормативных документах. В частности: Конституция Республики Беларусь, Уголовный Кодекс Республики Беларусь

Средства защиты информации

- **I. Формальные средства защиты** – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.
- **II. Неформальные средства защиты** – регламентируют деятельность человека.

Формальные средства защиты

- **Физические средства** - механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно от информационных систем, создавая различного рода препятствия на пути дестабилизирующих факторов (замок на двери, жалюзи, забор, экраны).
- **Аппаратные средства** - механические, электрические, электромеханические, электронные, электронно-механические, оптические, лазерные, радиолокационные и тому подобные устройства, встраиваемые в информационных системах или сопрягаемые с ней специально для решения задач защиты информации.
- **Программные средства** - пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной аппаратуры, однако они ведут к снижению производительности информационных систем, требуют выделения под их нужды определенного объема ресурсов и т.п.

- К **специфическим средствам защиты информации** относятся криптографические методы. В информационных системах криптографические средства защиты информации могут использоваться как для защиты обрабатываемой информации в компонентах системы, так и для защиты информации, передаваемой по каналам связи. Само преобразование информации может осуществляться аппаратными или программными средствами, с помощью механических устройств, вручную и т.д.

Неформальные средства защиты

- **Законодательные средства** – законы и другие нормативно-правовые акты, с помощью которых регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Распространяются на всех субъектов информационных отношений.
- **Организационные средства** - организационно-технические и организационно-правовые мероприятия, осуществляемые в течение всего жизненного цикла защищаемой информационной системы (строительство помещений, проектирование информационных систем, монтаж и наладка оборудования, испытания и эксплуатация информационных систем). Другими словами – это средства уровня организации, регламентирующие перечень лиц, оборудования, материалов и т.д., имеющих отношение к информационным системам, а также режимов их работы и использования. К организационным мерам также относят сертификацию информационных систем или их элементов, аттестацию объектов и субъектов на выполнение требований обеспечения безопасности и т.д.
- **Морально-этические средства** - сложившиеся в обществе или в данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите

информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе, ведет к потере престижа и авторитета.

Способы передачи конфиденциальной информации на расстоянии.

- Способов передачи конфиденциальной информации на расстоянии существует множество, среди которых можно выделить **три** основных направления.
- 1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.
- 2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.
- 3. Использовать общедоступный канал связи, но передавать по нему нужную информацию в таком преобразованном виде, чтобы восстановить ее мог только адресат.

Классификация методов защиты информации

- — законодательные (правовые);
- — организационные;
- — технические;
- — комплексные.
- Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

- Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации. К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.
- Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты. Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т.е. комплексно.

РАДУЖНАЯ СЕРИЯ

- **Радужная серия** (Радужные книги) — серия стандартов информационной безопасности, разработанная и опубликованная в США в период с 1980 по 1990 гг. Изначально книги были опубликованы Министерством обороны США, а затем в Центре национальной компьютерной безопасности США.
- Эти стандарты описывают процесс оценки доверенных систем. Многие из этих стандартов стали основой для Общих критериев оценки защищённости информационных технологий. Книги получили свои названия по цвету обложек. Например, книга Критерии определения безопасности компьютерных систем получила название Оранжевая книга.

NIST Радужная серия				
Документ	Название	Дата	Цвет	
5200.28-STD	Критерии определения безопасности компьютерных систем	15 августа 1983	Оранжевая книга	
CSC-STD-002-85	Руководящие принципы использования паролей	12 апреля 1985	Зелёная книга	
CSC-STIS-003-85	Руководство по применению критериев определения безопасности компьютерных систем в конкретных условиях	25 июня 1985	Светло-жёлтая книга	
CSC-STIS-004-85	Техническое обоснование CSC-STD-003-85: Требования компьютерной безопасности	25 июня 1985	Жёлтая книга	
NCSC-TG-001	Руководство к пониманию аудита в доверенных системах	1 июня 1988	Жёлто-коричневая книга	
NCSC-TG-002	Оценка безопасности программных продуктов	22 июня 1990	Ярко-голубая книга	
NCSC-TG-003	Дискреционный контроль доступа в доверенных системах	30 сентября 1987	Ярко-оранжевая книга	
NCSC-TG-004	Глоссарий терминов компьютерной безопасности	21 октября 1988	Тёмно-зелёная книга	
NCSC-TG-005	Безопасная сетевая интерпретация	31 июля 1987	Красная книга	
NCSC-TG-006	Управление конфигурациями в доверенных системах	28 марта 1988	Янтарная книга	
NCSC-TG-007	Руководство к проектной документации в доверенных системах	6 октября 1988	Бордовая книга	
NCSC-TG-008	Механизмы распределения аппаратного и программного обеспечения автоматизированных систем	15 декабря 1988	Тёмно-лиловая книга	
NCSC-TG-009	Интерпретация подсистем компьютерной защиты TCSEC	16 сентября 1988	Тёмно-голубая книга	
NCSC-TG-010	Руководство к пониманию безопасности моделирования в доверенных системах	октябрь 1992	Аква книга	
NCSC-TG-011	Безопасная сетевая интерпретация среды (TNI)	1 августа 1990	Красная книга	

NCSC-TG-018	Объект повторного использования в доверенных системах	июль 1992	Светло-голубая книга	
NCSC-TG-019	Руководство по выбору системы защиты информации	2 мая 1992	Синяя книга	
NCSC-TG-020	Безопасность UNIX рабочей группы (TRUSIX) Обоснование выбора Списка контроля доступа для системы UNIX	7 июля 1989	Серебристая книга	
NCSC-TG-021	Надёжные системы управления базами данных TCSEC (TDI)	апрель 1991	Пурпурная книга	
NCSC-TG-022	Восстановление в доверенных системах	30 декабря 1991	Жёлтая книга	
NCSC-TG-023	Тестирование безопасности и тестовой документации в доверенных системах	июль 1993	Ярко-оранжевая книга	
NCSC-TG-024 Vol. 1/4	Закупка доверенных систем: Введение в закупки, требования компьютерной безопасности	декабрь 1992	Пурпурная книга	
NCSC-TG-024 Vol. 2/4	Закупка доверенных систем: язык для спецификации запроса предложений	30 июня 1993	Пурпурная книга	
NCSC-TG-024 Vol. 3/4	Закупка доверенных систем: компьютерная безопасность, требования к данным	28 февраля 1994	Пурпурная книга	
NCSC-TG-024 Vol. 4/4	Закупка доверенных систем: Как оценить предложение?	Publication TBA	Пурпурная книга	
NCSC-TG-025	Руководство к пониманию данных остаточной намагниченности в автоматизированных информационных системах	сентябрь 1991	Тёмно-зелёная книга	
NCSC-TG-026	Руководство пользователя доверенных систем	сентябрь 1991	Персиковая книга	
NCSC-TG-027	Сотрудник службы безопасности в Автоматизированных информационных системах	май 1992	Бирюзовая книга	
NCSC-TG-028	Оценка защиты доступа	25 мая 1992	Фиолетовая книга	
NCSC-TG-029	Сертификация и аккредитация	январь 1994	Синяя книга	
NCSC-TG-030	Анализ доверенных систем	ноябрь 1993	Светло-розовая книга	

Роль стандартов информационной безопасности

- С развитием информационных технологий появилась необходимость стандартизации требований в области защиты информации.
- Главная задача стандартов информационной безопасности — создать основу для взаимодействия между производителями, потребителями и специалистами по сертификации.

Оранжевая книга

- «Критерии безопасности компьютерных систем» (Trusted Computer System Evaluation Criteria), получившие неформальное название Оранжевая книга, были разработаны Министерством обороны США в 1983 году с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем, и выработки соответствующей методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах военного назначения.
- Предложенные в этом документе концепции защиты и набор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности

Классификация требований и критериев Оранжевой книги

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

1. Политика безопасности

<p>Политика безопасности</p>	<p>Система должна поддерживать точную политику безопасности. Возможность осуществления доступа к объектам должна определяться на основе политики и набора правил управления доступом. Для реализации политики должна использоваться политика нормативного управления доступом, позволяющая эффективно реагировать на запросы доступа к категоризированной информации, помеченной грифом секретности: «секретно».</p>
<p>Метки</p>	<p>С объектами должны быть ассоциированы метки, используемые в качестве атрибутов контроля доступа при реализации нормативного управления доступом, обеспечивать возможность присваивать метки или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объектам информации, доступ к этому объекту.</p>
<p>Регистрация и учет</p>	<p>Для определения степени ответственности за действия в системе все происходящие события должны регистрироваться с значением с точки зрения безопасности, регистрироваться в защищенном протоколе. Система должна осуществлять анализ общего потока событий, из него только те события, которые оказывают влияние на безопасность для сокращения объема потока событий, эффективность его анализа. Протокол событий должен надежно защищен от несанкционированной модификации и уничтожения.</p>

2. Корректность

<p>Контроль корректности функционирования средств защиты</p>	<p>Средства защиты должны содержать аппаратные и/или программные механизмы, обеспечивающие работоспособность. Это означает, что все средства защиты, обеспечивающие политику безопасности, атрибутами и метками безопасности, аутентификацию, регистрацию и т.д. должны находиться под контролем средств защиты. Средства защиты должны обеспечивать корректность их функционирования. Средства защиты, обеспечивающие контроль корректности состояния, должны находиться под контролем средств защиты.</p>
<p>Непрерывность защиты</p>	<p>Все средства защиты (в т. ч. и требования) должны быть защищены от несанкционированного вмешательства, отключения, причем эта защита должна быть постоянной и непрерывной в течение всего функционирования системы защиты. Данное требование должно выполняться на весь жизненный цикл компьютерной системы. Данное требование является одним из аспектов формального доказательства безопасности системы.</p>

Классы безопасности компьютерных систем

- Оранжевая книга предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от **минимальной (группа D)** до **формально доказанной (группа A)**. Каждая группа включает один или несколько классов. Группы D и A содержат по одному классу (классы D и A соответственно), группа C — классы C1, C2, а группа B — B1, B2, B3, характеризующиеся различными наборами требований

безопасности. Уровень безопасности возрастает при движении от группы D к группе А, а внутри группы — с возрастанием номера класса.

Группа D. Минимальная защита.

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

Группа C. Дискреционная защита

Класс C1. Дискреционная защита	Системы этого класса удовлетворяют требованиям обеспечения разделения пользователей. Они включают средства контроля и управления, позволяющие задавать ограничения на доступ пользователей, что дает им возможность хранить приватную информацию от других пользователей. Система рассчитана на многопользовательское использование. Осуществляется совместная обработка информации на уровне секретности
Класс C2. Управление доступом	Системы этого класса осуществляют управление доступом, чем отличаются от систем класса C1 применением средств индивидуального контроля действий пользователей, регистрацией действий и выделением ресурсов.

Группа B. Мандатная защита

Класс В1. Защита с применением меток безопасности

Системы класса В1 должны соответствовать требованиям, предъявляемым к классу В1, и, кроме того, должны поддерживать модель безопасности, маркированную нормативное управление доступом. Информация о системе должна быть маркирована. Обнаруженные недостатки должны быть устранены.

**Класс В2.
Структурированная защита**

Для соответствия классу В2 ТСО должны поддерживать формально описанную документированную модель безопасности, предусматривающую произвольное управление доступом, которое должно быть сравнено с системами класса В1. Кроме того, должен быть осуществлен аудит каналов утечки информации. Должны быть выделены элементы, критичные для безопасности. Интерфейс ТСВ должен быть определен, а ее архитектура должна быть разработана с учетом возможности проведения испытаний. По сравнению с классом В1 усилены средства аутентификации. Безопасность осуществляется с помощью систем. Должны быть предусмотрены средства управления конфигурацией.

Класс ВЗ. Домены безопасности

Для соответствия этому классу необходимо поддерживать монитор взаимных действий, который контролирует все типы доступов, который невозможно обойти. Политика безопасности должна быть структурирована с целью обеспечения безопасности подсистем, не отвечающих за безопасность, и достаточно компактна для тестирования и анализа. В ходе реализации ТСВ необходимо использовать средства, направленные на минимизацию сложности. Средства аудита должны включать механизмы оповещения администраторов о возникновении событий, имеющих отношение к безопасности системы. Требования к становлению работоспособности

Группа А. Верифицированная защита

**Класс А1.
Формальная
верификация**

Системы класса А1 функционально эквивалентны классу ВЗ, и к ним не предъявляется дополнительных функциональных требований. В отличие от ВЗ, в ходе разработки должны применяться формальные верификации, что позволяет с высокой вероятностью получить корректную реализацию функциональных требований. Доказательства адекватности реализации функциональных требований на ранней стадии разработки с построением формальной политики безопасности и спецификацией методов обеспечения методов верификации. Средства должны содержать более мощные средства верификации с конфигурацией и защищенную процессором

- Согласно «Оранжевой книге» безопасная компьютерная система — это система, поддерживающая управление доступом к обрабатываемой в ней информации таким образом, что только соответствующие авторизованные пользователи или

процессы, действующие от их имени, получают возможность читать, писать, создавать и удалять информацию.

- «Критерии безопасности компьютерных систем» Министерства обороны США представляют собой первую попытку создать единый стандарт безопасности, рассчитанный на разработчиков, потребителей и специалистов по сертификации компьютерных систем. В свое время этот документ явился настоящим прорывом в области безопасности информационных технологий и послужил отправной точкой для многочисленных исследований и разработок.
- Оранжевая книга послужила основой для разработчиков всех остальных стандартов информационной безопасности и до сих пор используется в США в качестве руководящего документа при сертификации компьютерных систем обработки информации.

Европейские критерии безопасности информационных технологий (ITSEC)

- Данные критерии были опубликованы в июне 1991 года от имени четырех стран: Франции, Германии, Нидерландов и Великобритании.
- Европейские критерии рассматривают следующие задачи средств информационной безопасности:
- защита информации от несанкционированного доступа с целью обеспечения конфиденциальности;
- обеспечение целостности информации посредством защиты от ее несанкционированной модификации или уничтожения;
- обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.
- Европейские критерии безопасности информационных технологий, появившиеся вслед за Оранжевой книгой, оказали существенное влияние на стандарты безопасности и методику сертификации.



Главное достижение этого документа — введение понятия

адекватности средств защиты и определение отдельной шкалы для критериев адекватности. Как уже упоминалось, Европейские критерии придают адекватность средств защиты даже большее значение, чем их функциональности. Этот подход используется во многих появившихся позднее стандартах информационной безопасности.

Федеральные критерии безопасности информационных технологий США

- Федеральные критерии безопасности информационных технологий (Federal Criteria for Information Technology Security) разрабатывались как одна из составляющих Американского федерального стандарта по обработке информации (Federal Information Processing Standard), призванного заменить Оранжевую книгу. Разработчиками стандарта выступили Национальный институт стандартов и технологий США (National Institute of Standards and Technology) и Агентство национальной безопасности США (National Security Agency). (1992)
- Основными объектами применения требований безопасности Федеральных критериев являются
- продукты информационных технологий (Information Technology Products);
- системы обработки информации (Information Technology Systems).
- Федеральные критерии безопасности информационных технологий — первый стандарт информационной безопасности, в котором определяются три независимые группы требований: функциональные требования к средствам защиты, требования к технологии разработки и к процессу квалификационного анализа. Авторами этого стандарта впервые предложена концепция Профиля защиты — документа, содержащего описание всех требований безопасности как к самому ИТ-продукту, так и к процессу его проектирования, разработки, тестирования и квалификационного анализа.

- Разработчики Федеральных критериев отказались от используемого в Оранжевой книге подхода к оценки уровня безопасности ИТ-продукта на основании обобщенной универсальной шкалы классов безопасности. Вместо этого предлагается независимое ранжирование требований каждой группы, т. е. вместо единой шкалы используется множество частных шкал-критериев, характеризующих обеспечиваемый уровень безопасности. Данный подход позволяет разработчикам и пользователям ИТ-продукта выбрать наиболее приемлемое решение и точно определить необходимый и достаточный набор требований для каждого конкретного ИТ-продукта и среды его эксплуатации.
- Стандарт рассматривает устранение недостатков существующих средств безопасности как одну из задач защиты наряду с противодействием угрозам безопасности и реализацией модели безопасности.
- Данный стандарт ознаменовал появление нового поколения руководящих документов в области информационной безопасности, а его основные положения послужили базой для разработки Канадских критериев безопасности компьютерных систем и Единых критериев безопасности информационных технологий.

Единые критерии безопасности информационных технологий

- Единые критерии безопасности информационных технологий (Common Criteria for Information Technology Security Evaluation, далее — Единые критерии) являются результатом совместных усилий авторов Европейских критериев безопасности информационных технологий, Федеральных критериев безопасности информационных технологий и Канадских критериев безопасности компьютерных систем, направленных на объединение основных положений этих документов и создание Единого международного стандарта безопасности информационных технологий. Работа над этим самым масштабным в истории стандарте информационной

безопасности проектом началась в июне 1993 года с целью преодоления концептуальных и технических различий между указанными документами, их согласования и создания единого международного стандарта. Версия 2.1 этого стандарта утверждена Международной организацией по стандартизации (ISO) в 1999 г. в качестве Международного стандарта информационной безопасности ISO/IEC 15408.

- Требования Единых критериев охватывают практически все аспекты безопасности ИТ-продуктов и технологии их создания, а также содержат все исходные материалы, необходимые потребителям и разработчикам для формирования Профилей и Проектов защиты.
- Кроме того, требования Единых критериев являются практически всеобъемлющей энциклопедией информационной безопасности, поэтому их можно использовать в качестве справочника по безопасности информационных технологий.
- Данный стандарт ознаменовал собой новый уровень стандартизации информационных технологий, подняв его на межгосударственный уровень. За этим проглядывается реальная перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что предоставит возможности для интеграции национальных информационных систем.

Группа международных стандартов 270000

- Основное назначение международных стандартов — это создание на межгосударственном уровне единой основы для разработки новых и совершенствования действующих систем качества. Сотрудничество в области стандартизации направлено на приведение в соответствие национальной системы стандартизации с международной. Международные стандарты не имеют статуса обязательных для всех стран-участниц. Любая страна мира вправе применять или не применять их. Решение вопроса о применении

международного стандарта связано в основном со степенью участия страны в международном разделении труда.

- Международные стандарты принимаются Международной организацией по стандартизации — ИСО (International Organization for Standardization, ISO).

Группа стандартов, связанная с информационной безопасностью (ISO/IEC 27000)

- ГОСТ Р ИСО/МЭК 27000-2012- «СМИБ. Общий обзор и терминология».
- ГОСТ Р ИСО/МЭК 27001-2006- «СМИБ. Требования» ГОСТ Р ИСО/МЭК 27002-2012- «СМИБ. Свод норм и правил менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК 27003-2012-«СМИБ. Руководство по реализации системы менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК 27004-2011- «СМИБ. Измерения».
- ГОСТ Р ИСО/МЭК 27005-2010 - «СМИБ. Менеджмент риска информационной безопасности».
- ГОСТ Р ИСО/МЭК 27006-2008- «СМИБ. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК 27007-2014 - «СМИБ. Руководства по аудиту систем менеджмента информационной безопасности».
- И т.д.

Правовое обеспечение информационной безопасности в Республике Беларусь

- Международные договора в области информационной безопасности. К ним можно отнести: Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. (для Беларуси вступило в силу 04.06.2015 г.), постановление Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств от 18 ноября 2005 г. № 26-7 «О гармонизации законодательства государств –

участников СНГ в области информатизации и связи»,
Соглашение между Правительством Республики Беларусь и
Правительством Республики Казахстан о сотрудничестве в
области защиты информации, Соглашение между
Правительством Республики Беларусь и Правительством
Российской Федерации о сотрудничестве в области защиты
информации и т.д.

- Конституция Республики Беларусь от 15 марта 1994 г. (с
изменениями и дополнениями, принятыми на
республиканских референдумах 24.11.1996 и 17.10.2004), в
соответствии со статьей 34 которой, гражданам Республики
Беларусь гарантируется право на получение, хранение и
распространение полной, достоверной и своевременной
информации о деятельности государственных органов,
общественных объединений, о политической, экономической,
культурной и международной жизни, состоянии окружающей
среды; и указывается, что пользование информацией может
быть ограничено законодательством в целях защиты чести,
достоинства, личной и семейной жизни граждан и полного
осуществления ими своих прав.

Кодифицированные нормативные правовые акты:

- Гражданский кодекс Республики Беларусь (далее — ГК)
содержит нормы, касающиеся служебной и
коммерческой тайны, закрепляет такие форма
отношений, как информационные услуги, электронную
подпись признает как средство, подтверждающее
подлинность сторон в сделках, предусматривает
ответственность за незаконное использование
информации (статья 140, часть 2 статьи 161, статья 1011 и
др.).
- Кодекс Республики Беларусь об административных
правонарушениях (далее — КоАП), в котором
определяются административно-правовые санкции за
правонарушения в информационной сфере. К таким
правонарушениям относятся: отказ в предоставлении

гражданину информации, посредственно затрагивающей его права, свободы и законные интересы (статья 9.6), несанкционированный доступ к компьютерной информации (статья 22.6), нарушение правил защиты информации (статья 22.7) и др.

- Уголовный кодекс Республики Беларусь (далее — УК) закрепляет ответственность за преступления против информационной безопасности (глава 31), а также иные составы преступлений в информационной сфере (хищение путем использования компьютерной техники (статья 212), умышленное разглашение государственной тайны (статья 373), разглашение государственной тайны по неосторожности (статья 374), умышленное разглашение служебной тайны (статья 375) и др.
- Трудовой кодекс Республики Беларусь (далее — ТК), в соответствии с которым для работников устанавливается обязанность хранить государственную и служебную тайну, не разглашать коммерческую тайну нанимателя, коммерческую тайну третьих лиц, к которой наниматель получил доступ (п.10 части 1 статьи 53).
- Налоговый кодекс Республики Беларусь (общая часть) (далее — НК) включает нормы, определяющие порядок защиты различных видов конфиденциальной информации.

Законы, среди которых следует отметить:

- Закон Республики Беларусь 21.06.2008 № 418-З «О регистре населения» (далее – Закон «О регистре населения»);
- Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (далее – Закон «Об информации»);
- Закон Республики Беларусь от 13 июля 2006 г. № 144-З «О переписи населения» (далее – Закон «О переписи населения»);

- Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи».

Указы Президента Республики Беларусь и постановления Совета Министров Республики Беларусь.

- Среди данных правовых актов можно выделить основные блоки нормативных правовых актов:
 - о защите информации;
 - о доступе граждан к информации; о компетенции органов государственной власти в сфере защиты информации;
 - о международном сотрудничестве в данной сфере, включая государства-члены Содружества Независимых Государств.
- К таким законодательным актам можно отнести: указы Президента Республики Беларусь от 9 ноября 2010 г. № 575 **«Об утверждении Концепции национальной безопасности Республики Беларусь»**, от 01 февраля 2010 г. № 60 **«О мерах по совершенствованию использования национального сегмента сети Интернет»**, от 8 ноября 2011 г. № 515 **«О некоторых вопросах развития информационного общества в Республике Беларусь»**, от 25 октября 2011 г. № 486 **«О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»**, от 16 апреля 2013 г. № 196 **«О некоторых мерах по совершенствованию защиты информации»**; постановления Совета Министров Республики Беларусь от 29 апреля 2010 г. № 645 **«О некоторых вопросах интернет-сайтов государственных органов и организаций и признании утратившим силу постановления Совета Министров Республики Беларусь от 11 февраля 2006 г. № 192»**, от 15 мая 2013 г. № 375 **«Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность»** (ТР 2013/027/BY).
Приказы и Постановления

- Приказы и постановления Оперативно-аналитического центра при Президенте Республики Беларусь (далее — ОАЦ), среди которых особое внимание заслуживают: Постановление ОАЦ и Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 г. № 6/8 **«Об утверждении положения о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет»**, приказ ОАЦ от 2 августа 2010 г. № 60 **«Об утверждении Положения о порядке определения поставщиков интернет-услуг, уполномоченных оказывать интернет-услуги государственным органам и организациям, использующим в своей деятельности сведения, составляющие государственные секреты»**, приказ ОАЦ от 16 ноября 2010 г. № 82 **«Об утверждении Инструкции о порядке согласования выполнения работ и (или) оказания услуг в государственных организациях при осуществлении деятельности по технической и (или) криптографической защите информации»**, Приказ ОАЦ от 17 декабря 2010 г. № 92 **«Об утверждении перечня поставщиков интернет-услуг, уполномоченных оказывать интернет-услуги государственным органам и организациям, использующим в своей деятельности сведения, составляющие государственные секреты»** и др.

Государственные программы, утвержденных с целью формирования современных подходов к проектированию и созданию защищенных компьютерных систем, новых технологий и средств технической защиты информации

- Государственную программу развития цифровой экономики и информационного общества на 2016-2020 годы, утвержденную постановлением Совета Министров Республики Беларусь от 23 марта 2016 г. № 235;
- Государственную научно-техническую программу **«Развитие методов и средств системы комплексной защиты информации и специальных технических**

средств (ГНТП «Защита информации – 3»), 2016 – 2020 годы, утвержденную приказом Государственного комитета по науке и технологиям Республики Беларусь от 30 мая 2016 г. № 93. Основными целями последней программы являются:

- совершенствование нормативно-методической базы в области защиты информации;
 - разработка и совершенствование высокопроизводительных средств защиты информации, средств оценки степени защищенности информационных систем, специальных технических средств;
 - создание научно-технических условий для эффективного обеспечения безопасности информации на критически важных объектах информатизации и повышения степени защищенности объектов информатизации, систем связи и передачи данных;
 - обеспечение импортозамещения средств защиты информации и специальных технических средств.
- В Республике Беларусь существует необходимость принятия Концепции информационной безопасности, которая бы комплексно урегулировала данную сферу отношений и отразила государственную политику в сфере обеспечения информационной безопасности, меры защиты информации, виды и источники угроз в сфере информационной безопасности, первоочередные мероприятия по обеспечению информационной безопасности. Концепция информационной безопасности Республики Беларусь должна развивать и дополнять Конституцию Республики Беларусь и Концепцию национальной безопасности Республики Беларусь

Политика безопасности

- **Политика безопасности** - набор законов, правил и норм поведения, определяющих, как организация обрабатывает,

защищает и распространяет информацию. **Политика безопасности должна включать в себя анализ возможных угроз и выбор мер противодействия.**

- **Гарантированность** - мера доверия, которая может быть оказана архитектуре и реализации системы.
Гарантированность может проистекать как из тестирования, так и из проверки общего замысла и исполнения системы в целом и ее компонентов.
- **Механизм подотчетности (протоколирования).** Надежная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом.
- **Периметр безопасности** - граница надежной вычислительной базы. То, что внутри периметра, считается надежным, а то, что вне - нет.
Основные элементы политики безопасности
- Согласно "Оранжевой книге", политика безопасности должна включать в себя по крайней мере следующие элементы:
 - произвольное управление доступом;
 - безопасность повторного использования объектов;
 - метки безопасности;
 - принудительное управление доступом.

Произвольное управление доступом

- **это метод ограничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит.** Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению давать другим субъектам или отбирать у них права доступа к объекту.
- Текущее состояние прав доступа при произвольном управлении описывается матрицей, в строках которой перечислены субъекты, а в столбцах - объекты. В клетках, расположенных на пересечении строк и столбцов, записываются способы доступа, допустимые для субъекта по

отношению к объекту - например, чтение, запись, выполнение, возможность передачи прав другим субъектам и т.п.

Безопасность повторного использования объектов

- важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и носителей в целом.
- Поскольку информация о субъектах также представляет собой объект, необходимо позаботиться о безопасности "повторного использования субъектов". Когда пользователь покидает организацию, следует не только лишить его возможности входа в систему, но и запретить доступ ко всем объектам. В противном случае, новый сотрудник может получить ранее использовавшийся идентификатор а с ним и все права своего предшественника.

Метки безопасности

- для реализации принудительного управления доступом с субъектами и объектами. Метка субъекта описывает его благонадежность, метка объекта - степень закрытости содержащейся в нем информации.
- **Согласно "Оранжевой книге", метки безопасности состоят из двух частей - уровня секретности и списка категорий.** Уровни секретности, поддерживаемые системой, образуют упорядоченное множество, которое может выглядеть, например, так:
 - совершенно секретно,
 - секретно,
 - конфиденциально,
 - несекретно.

- Категории образуют неупорядоченный набор. Их назначение - описать предметную область, к которой относятся данные. Механизм категорий позволяет разделить информацию по отсекам, что способствует лучшей защищенности, при этом, **субъект не может получить доступ к "чужим" категориям, даже если его уровень благонадежности - "совершенно секретно"**.
- Главная проблема, которую необходимо решать в связи с метками, это обеспечение их целостности:
 - не должно быть непомеченных субъектов и объектов;
 - при любых операциях с данными метки должны оставаться правильными.
- Например, печатный документ должен открываться заголовком, содержащим текстовое и/или графическое представление метки безопасности.
- Разделение устройств на многоуровневые и одноуровневые. На многоуровневых устройствах может храниться информация разного уровня секретности. Зная уровень устройства, система может решить, допустимо ли записывать на него информацию с определенной меткой.

Принудительное управление доступом

- Основано на сопоставлении меток безопасности субъекта и объекта.
- Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.
- Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен.
- Принудительное управление доступом реализовано во многих вариантах операционных систем и СУБД,

отличающихся повышенными мерами безопасности.

Впрочем, в реальной жизни произвольное и принудительное управление доступом сочетается в рамках одной системы, что позволяет использовать сильные стороны обоих подходов.

Подотчетность

- Цель подотчетности - в каждый момент времени знать, кто работает в системе и что он делает.
- Средства подотчетности делятся на три категории:
- Идентификация и аутентификация.
- Предоставление надежного пути.
- Анализ регистрационной информации.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

- Каждый пользователь, прежде чем получить право совершать какие-либо действия в системе, должен идентифицировать себя. В свою очередь, система должна проверить подлинность личности пользователя, то есть что он является именно тем, за кого себя выдает.
- **Идентификация и аутентификация - первый и важнейший программно-технический рубеж информационной безопасности. Если не составляет проблемы получить доступ к системе под любым именем, то другие механизмы безопасности, например, управление доступом, очевидно, теряют смысл.**

ПРЕДОСТАВЛЕНИЕ НАДЕЖНОГО ПУТИ

- Надежный путь связывает пользователя непосредственно с надежной вычислительной базой, минуя другие, потенциально опасные компоненты системы. Цель предоставления надежного пути - дать пользователю возможность убедиться в подлинности обслуживающей его системы.
- Относительно несложно реализовать надежный путь, если используется неинтеллектуальный терминал - достаточно иметь зарезервированную управляющую последовательность.

Если же пользователь общается с интеллектуальным терминалом, персональным компьютером или рабочей станцией, задача обеспечения надежного пути становится чрезвычайно сложной, если вообще разрешимой.

АНАЛИЗ РЕГИСТРАЦИОННОЙ ИНФОРМАЦИИ

- Аудит имеет дело с действиями, так или иначе затрагивающими безопасность системы. К числу таких событий, например, относятся:
- Вход в систему (успешный или нет).
- Выход из системы.
- Обращение к удаленной системе.
- Операции с файлами (открыть, закрыть, переименовать, удалить).
- Смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).
- Протоколирование помогает следить за пользователями и реконструировать прошедшие события. Слежка важна в первую очередь как профилактическое средство. **Можно надеяться, что многие воздержатся от нарушений безопасности, зная, что их действия фиксируются.**

Гарантированность

- Гарантированность - это мера уверенности, с которой можно утверждать, что для проведения в жизнь сформулированной политики безопасности выбран подходящий набор средств, и что каждое из этих средств правильно исполняет отведенную ему роль.
- В "Оранжевой книге" рассматривается два вида гарантированности - операционная и технологическая.

Операционная гарантированность

- Операционная гарантированность включает в себя проверку следующих элементов:
- Архитектура системы.
- Целостность системы.
- Анализ тайных каналов передачи информации.

- Надежное администрирование.
- Надежное восстановление после сбоев.
- Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно проводят в жизнь избранную политику безопасности.
- Среди архитектурных решений, предусматриваемых "Оранжевой книгой", упомянем следующие:
- Деление аппаратных и системных функций по уровням привилегированности и контроль обмена информацией между уровнями;
- Защита различных процессов от взаимного влияния;
- Наличие средств управления доступом;
- Структурированность системы, явное выделение надежной вычислительной базы, обеспечение компактности этой базы.
- Следование принципу минимизации привилегий - каждому компоненту дается ровно столько привилегий, сколько необходимо для выполнения им своих функций.
- Сегментация (в частности, сегментация адресного пространства процессов) как средство повышения надежности компонентов.
- **Целостность системы** в данном контексте означает, что аппаратные и программные компоненты надежной вычислительной базы работают должным образом и что имеется аппаратное и программное обеспечение для периодической проверки целостности.
- **Надежное администрирование** в трактовке "Оранжевой книги" означает всего лишь, что **должны быть логически выделены три роли - системного администратора, системного оператора и администратора безопасности.**
- **Надежное восстановление после сбоев** - вещь необходимая, однако ее реализация может быть сопряжена с серьезными техническими трудностями. Прежде всего, должна быть сохранена целостность информации и, в частности, целостность меток безопасности. В принципе возможна ситуация, когда сбой приходится на момент записи нового

файла с совершенно секретной информацией. Если файл окажется с неправильной меткой, информация может быть скомпрометирована.

- Надежное восстановление включает в себя два вида деятельности - подготовку к сбою (отказу) и собственно восстановление. Подготовка к сбою - это и регулярное выполнение резервного копирования, и выработка планов действий в экстренных случаях, и поддержание запаса резервных компонентов. Восстановление связано с перезагрузкой системы и выполнением ремонтных и/или административных процедур.

Технологическая гарантированность

- Технологическая гарантированность охватывает весь жизненный цикл системы, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы обезопаситься от утечки информации и нелегальных "закладок".
- **Первое, на что обычно обращают внимание, это тестирование.** Тесты должны показать, что защитные механизмы функционируют в соответствии со своим описанием и что не существует очевидных способов обхода или разрушения защиты. Должна быть уверенность, что надежную вычислительную базу нельзя привести в состояние, когда она перестанет обслуживать пользовательские запросы.

Документация

- Документация - необходимое условие гарантированной надежности системы и, одновременно, - инструмент проведения политики безопасности. Без документации люди не будут знать, какой политике следовать и что для этого нужно делать.
- Согласно "Оранжевой книге", в комплект документации надежной системы должны входить следующие тома:
- Руководство пользователя по средствам безопасности.

- Руководство администратора по средствам безопасности.
- Тестовая документация.
- Описание архитектуры.
- На практике требуется еще по крайней мере одна книга - письменное изложение политики безопасности данной организации.

Работы по обеспечению режима ИБ

- – определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания;
- – оценка рисков;
- – выбор контрмер, обеспечивающих режим ИБ;
- – управление рисками;
- – аудит системы управления ИБ;
- – выработка политики безопасности.
- Этап 1. Выбор национальных и международных руководящих документов и стандартов в области ИБ и формулирование на их базе основных требований и положений политики ИБ компании, включая:
 - – управление доступом к средствам вычислительной техники (СВТ), программам и данным, а также антивирусную защиту;
 - – вопросы резервного копирования;
 - – проведение ремонтных и восстановительных работ;
 - – информирование об инцидентах в области ИБ и пр.
- Этап 2. Выработка подходов к управлению информационными рисками и принятие решения о выборе уровня защищенности КИС. Уровень защищенности в соответствии с зарубежными стандартами может быть минимальным (базовым) либо повышенным. Этим уровням защищенности соответствует минимальный (базовый) или полный вариант анализа информационных рисков.
- Этап 3. Структуризация контрмер по [защите информации](#) по следующим основным уровням: административному, процедурному, программно-техническому.

- Этап 4. Установление порядка сертификации и аккредитации КИС на соответствие стандартам в сфере ИБ. Назначение периодичности проведения совещаний по тематике ИБ на уровне руководства, в том числе периодического пересмотра положений политики ИБ, а также порядка обучения всех категорий пользователей информационной системы в области ИБ. Известно, что выработка политики безопасности организации – наименее формализованный этап. Однако в последнее время именно здесь сосредоточены усилия многих специалистов по защите информации.
- Этап 5. Определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания. На этом этапе определяются границы системы, для которой должен быть обеспечен режим ИБ. Соответственно, система управления ИБ строится именно в этих границах.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

В основе криптографических методов защиты информации лежат математические алгоритмы преобразования (шифрования) данных с целью их защиты от прочтения незаконными пользователями. Различают математические дисциплины: криптографию и криптоанализ.

Криптоанализ – наука о методах и способах вскрытия шифров и кодов, анализа надежности криптоалгоритмов.

Криптография – наука (искусство) о защите информации от прочтения ее посторонними, о методах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей.

В криптографии широко используются следующие преобразования и термины.

- *Перестановка* – нарушение нормального порядка следования единиц информации, например, букв (СЕКРЕТ – ЕТКРСЕ).
- *Замена на основе шифралфавита* – перечень эквивалентов, используемых для преобразования открытого текста в шифрованный. Иногда шифралфавит предусматривает несколько замен одного знака. Например, С {16, 21, 35, 72}, т.

е. С заменяется одним из чисел. Этот выбор называется гомофоном. Время от времени в шифралфавит включают символ, который ничего не значит (символ-пустышка).

- *Код* – огромный шифр замены. С одной стороны – тысячи слов, фраз, букв и слогов открытого текста, с другой – заменяющие их кодовые слова или кодовые обозначения.
- *Шифр* – код, основной единицей которого является знак, несколько знаков или битовый блок.
- *Криптограмма* – окончательно обработанное и отосланное сообщение.
- *Расшифровка* (раскодирование) – преобразование шифротекста (кодотекста), при наличии ключа и системы шифрования.
- Для построения абсолютно стойкого шифра необходимо уметь получать совершенно случайный ключ.
- Иначе можно выявить некоторую закономерность в зашифрованных сообщениях.
- Стойкость шифра – это сложность задачи его вскрытия.
- Сложность задачи – минимальная сложность алгоритмов ее решения.

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Симметричные системы шифрования, в отличие от асимметричных, используют один и тот же ключ как на этапе зашифрования данных, так и на этапе их расшифрования.

Все эти алгоритмы в той или иной мере строгости обладают следующими основными свойствами:

- *рассеивание* (распространение влияния);
 - *перемешивание* (исключение статистической взаимосвязи).
- ### СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ
- Простая перестановка
 - Простая перестановка без ключа — один из самых простых методов шифрования. Сообщение записывается в таблицу по столбцам. После того, как открытый текст записан колонками, для образования шифровки он считывается по строкам. Для

использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы.

Простая перестановка

например, зашифруем фразу «ХОЧУ_ЗАЧЁТ_ПО_ОЗИ», разместим текст в "таблице" - по три строки.

Шифр будет иметь такой вид: ХУАТОЗО_Ч_ _ИЧЗЁПО_

Х	У	А	Т	О	З
О	–	Ч	–	–	И
Ч	З	Ё	П	О	–

Одиночная перестановка по ключу

Более практический метод шифрования, называемый одиночной перестановкой по ключу очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Одиночная перестановка по ключу

Шифровать будем ту же фразу, которую шифровали без ключа
Ключом у нас будет слово ЗАЩИТА

З	А	Щ	И	Т	А
З	1	6	4	5	2
Х	У	А	Т	О	З
О	–	Ч	–	–	И
Ч	З	Ё	П	О	–

Одиночная перестановка по ключу

Шифровать будем ту же фразу, которую шифровали без ключа
Ключом у нас будет слово ЗАЩИТА

1	2	3	4	5	6
У	З	Х	Т	О	А
–	И	О	–	–	Ч
З	–	Ч	П	О	Ё

Шифр будет иметь такой вид: УЗХТОФ_ИЩ_ _ЧЗ_ЧПОЁ
СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Двойная перестановка по ключу

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов были другие, чем в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным.

Перестановка «Магический квадрат Дюрера»

Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации.

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

Перестановка «Магический квадрат Дюрера»

Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв.

Перестановка «Магический квадрат Дюрера»

Например, требуется зашифровать фразу:

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

«**РЕАЛЬНОСТЬ_БЫТИЯ**». Буквы этой фразы вписываются последовательно в квадрат согласно записанным в них

числам: позиция буквы в предложении соответствует порядковому числу.

9 Т	16 Я	2 Е	7 О
6 Н	3 А	13 Ы	12 Б
15 И	10 Ъ	8 С	1 Р
4 Л	5 Ь	11 _	14 Т

ТЯЕОНАЫБИЬСРЛЬ_Т

Стандарты шифрования:

Достоинства

- скорость на 3 порядка выше
- простота реализации (за счёт более простых операций)
- меньшая требуемая длина ключа для сопоставимой стойкости
- изученность (за счёт большего возраста)

Недостатки

- сложность управления ключами в большой сети. Означает квадратичное возрастание числа пар ключей, которые надо генерировать, передавать, хранить и уничтожать в сети. Для сети в 10 абонентов требуется 45 ключей, для 100 уже 4950, для 1000 — 499500 и т. д.
- сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи ключей каждому абоненту, так как нужен секретный канал для передачи каждого ключа обеим сторонам.

Классические симметрические системы

Шифрование с использованием системы Цезаря:

- один из простых и наиболее широко известных методов шифрования.
- Это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

- Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$$y = (x + k) \mod n$$

$$x = (y - k + n) \mod n,$$

Шифрование с использованием системы Цезаря:

- Шифрование с использованием ключа $k = 3$. Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее. :
- Исходный алфавит:
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
- Шифрованный:
ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ
- Оригинальный текст:
ХОЧУ ЗАЧЁТ ПО ОЗИ.
- Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:
ШСЪЦ ЛГЪИХ ТС СКЛ.
- Шифрование с использованием системы Трисемуса:
- Представляет собой усовершенствованный шифр Цезаря, то есть шифр подстановки.
- По алгоритму шифрования, каждый символ сообщения смещается на символ, отстающий от данного на некоторый шаг.
- Здесь шаг смещения делается переменным, то есть зависящим от каких-либо дополнительных факторов. Например, можно задать закон смещения в виде линейной

функции (уравнения зашифрования) позиции шифруемой буквы.

- Сама функция должна гарантировать целочисленное значение. Прямая функция шифрования должна иметь обратную функцию шифрования, тоже целочисленную.

Введем такое понятие:

- *Уравнением зашифрования* называется соотношение, описывающее процесс образования зашифрованных данных из открытых данных в результате преобразований, заданных алгоритмом криптографического преобразования.

Шифрование с использованием системы Трисемуса:

- *Уравнение зашифрования для шифра Тритемеуса имеет следующий вид:*

$$L=(m+k)\bmod N$$

- *Некоторые варианты вычисления шага смещения k :*

$$k=A * p+B,$$

$$k=A * p^2+B * p+C,$$

где p — позиция буквы в сообщении; A, B, C — ключи.

Шифрование с использованием системы Трисемуса:

1. *Определяем порядковый номер шифруемой буквы в тексте.*
2. *Определяем код буквы в алфавите.*
3. *Вычисляем смещение k .*
4. *Находим код зашифрованной буквы, пользуясь нашим уравнением зашифрования. $L=(m+k)\bmod N$*
Расшифрование $m=(L-k)\bmod N$
5. *По коду L восстанавливаем очередную букву криптограммы.*
6. *Повторяем пункты 1..5 до окончания текста шифрограммы.*

Шифрование с использованием системы Трисемуса:

Для $k=2p^2+5p+3$ и алфавита:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я		.	.
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

Оригинальный текст:

Съешь же ещё этих мягких французских булок, да выпей чаю.

Шифрованный текст:

ФБЩШЛГД Ч.ЪСЧДП ЕО,ЧЁЬЙЛЮЩЛ РЬА

РЙХАКЕЛ,РЮШЮЭ,НТЦВ,ПЁФЦВ

Зашифруем сообщение **«САМАЯ ЛУЧШАЯ РАБОТА»**

В качестве ключа возьмем слово «Правитель»

п	р	а	в	и	т	е	л
ь	б	г	д	ж	з	й	к
м	н	о	с	у	ф	х	ц
ч	ш	щ	ъ	ы	э	ю	я

Получим зашифрованное сообщение **«ЪГЧГЛ КЫПРГЛ
БГНЩЗГ»**

Шифрование с использованием системы Плейфера:

- Представляет собой ручную симметричную технику шифрования, в которой впервые использована замена биграмм.
 - Шифр предусматривает шифрование пар символов (биграмм) вместо одиночных символов, как в шифре подстановки
 - Шифр Плейфера использует матрицу 5x5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4x8), содержащую ключевое слово или фразу.
 - Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила.
 - Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку.
3. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Ъ», зашифровываем новую пару символов и продолжаем.

4. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.
5. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.
6. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Разобьем слово «Россия» на биграммы

РО СЪ СИ ЯЪ

Используем ключ «АВИАЦИЯ», тогда матрица примет вид:

а	в	и	ц	я	б	г	д
е	ж	з	й	к	л	м	н
о	п	р	с	т	у	ф	х
ч	ш	щ	ъ	ы	ь	э	ю

Зашифруем биграммы сообщения по приведенным выше правилам:

а	в	и	ц	я	б	г	д
е	ж	з	й	к	л	м	н
о	п	р	с	т	у	ф	х
ч	ш	щ	ъ	ы	ь	э	ю

1. Биграмма АЮ формирует прямоугольник, заменяем её на ДЧ.
2. Биграмма ЖШ расположена в одном столбце, заменяем её на ПВ.

3. Биграмма ЗН расположена в одной строке, заменяем её на ЙЕ.

Зашифруем сообщение

«СКАЖИ КА ДЯДЯ ВЕДЬ НЕ ДАРОМ»

Разбиваем на биграммы

СК АЖ ИК АД ЯД ЯВ ЕД ЫН ЕД АР ОМ

Получаем зашифрованный текст:

«ТЙ ВЕ ЯЗ ВА БА БИ НА ЮЛ НА ИО ФЕ»

Шифрование с использованием системы Виженера:

- Представляет собой метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.
- Этот метод является простой формой многоалфавитной замены.
- В шифре Цезаря каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, А стало бы D, В стало бы Е и так далее.
- Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига.
- Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера.
- Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций.

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

- Например, предположим, что исходный текст имеет вид:
ПОЛУЧИТЬ ЗАЧЁТ
- Человек, посылающий сообщение, записывает ключевое слово («РАБОТА») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:
РАБОТАРАБОТАР

Таблица Виженера для русского алфавита

	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
0	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
1	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а
2	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б
3	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
4	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г
5	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д
6	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е
7	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж
8	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з
9	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и
10	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й
11	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
12	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л
13	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м
14	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
15	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
16	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
17	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
18	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
19	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
20	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
21	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
22	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
23	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
24	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
25	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
26	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
27	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
28	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы
29	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь
30	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
31	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю

Классические симметрические системы

Шифрование с использованием системы Виженера:

Первый символ исходного текста П зашифрован последовательностью Р, которая является первым символом ключа. Первый символ Я шифрованного текста находится на пересечении строки Р и столбца П в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста О получается на пересечении строки А и столбца О. Остальная часть исходного текста шифруется подобным способом.

Исходный текст:

ПОЛУЧИТЬ ЗАЧЁТ

Ключ:

РАБОТА

Зашифрованный текст:

ЯОМБЙИВЬ ИОЙЕВ

Если буквы А—Z соответствуют числам 0—25, то шифрование Виженера можно записать в виде формулы:

$$C_i = (P_i + K_i) \bmod 26$$

Расшифровка:

$$P_i = (C_i - K_i + 26) \bmod 26$$

Классические симметрические системы

Шифр «двойной квадрат» Уитстона:

Шифр "двойной квадрат" использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра.

Шифр «двойной квадрат» Уитстона:

Пусть имеются две таблицы. В качестве ключей будем использовать два слова «Работа» и «Халява».

р	а	б	о	т	в	г	д		х	а	л	я	в	б	г	д
е	ж	з	и	й	к	л	м		е	ж	з	и	й	к	м	н
н	п	с	у	ф	х	ц	ч		о	п	р	с	т	у	ф	ц
ш	щ	ъ	ы	ь	э	ю	я		ч	ш	щ	ъ	ы	ь	э	ю

Перед шифрованием исходное сообщение разбивают на биграммы.

Каждая биграмма шифруется отдельно.

Первую букву биграммы находят в левой таблице, а вторую букву - в правой таблице.

Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах.

Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

Предположим, что шифруется биграмма исходного текста РЮ. Получаем зашифрованную биграмму шифртекста ДШ.

Шифр «двойной квадрат» Уитстона:

► Сообщение

ПОЛУЧИТЬ ЗАЧЁТЪ

► Шифртекст

НП КЦ СМ ЖБ ОМ ЯЬ

Ассиметричные криптосистемы

Ассиметричные системы

В 1970-х годах появилась новая система шифрования, называемая шифрованием на ассиметричном (открытом) ключе. Она называется ассиметричной, потому что не требует использования идентичных ключей отправителем и получателем шифрованного сообщения. Она является системой с открытым ключом, так как один из ключей не содержится в секрете.

Система шифрования при которой **открытый ключ** передаётся по открытому каналу и используется для шифрования сообщения.

Шифрование на открытом ключе использует два различных ключа, составляющих пару, но не идентичных. В шифровании с симметричным ключом каждый ключ является уникальным. Пара ключей открытый/секретный работает сообща: один ключ предназначен для шифрования данных, а другой – для расшифровки, и наоборот. Секретный ключ должен содержаться в секретности в целях безопасности, а открытый ключ может передаваться по небезопасному соединению без угрозы для системы. Следовательно, система шифрования на открытом ключе решает одну из главных проблем старых систем шифрования, заключающуюся в безопасном способе передачи ключа шифрования другой стороне.

Как правило, открытые ключи используются только для зашифровки данных. Расшифровать их сможет только тот пользователь, чей компьютер содержит соответствующий секретный ключ. Эта система построена на математических принципах, используемых в шифрах с открытыми ключами и обеспечивающих существование одного и только одного уникального секретного ключа, соответствующего уникальному открытому ключу. Следовательно, если выполняется шифрование данных пользователя на общем

ключе, можете быть уверены, что только пользователь, владеющий второй, секретной, половиной ключа, сможет их расшифровать.

Основана на идее **односторонней функции**, то есть таких функций $f(x)$, что по известному x довольно просто найти значение $f(x)$, тогда как определение x из $f(x)$ невозможно за разумный срок.

Лазейка — это некий секрет, который помогает расшифровать.

Пусть пользователь **«Алиса»** придумала пароль **«гладиолус»**. Функция от пары данных **«Алиса_гладиолус»** будет давать результат **«ромашка»**.

$$f(\text{Алиса_гладиолус}) = \text{"ромашка"}$$

Логин пароль для входа в систему:

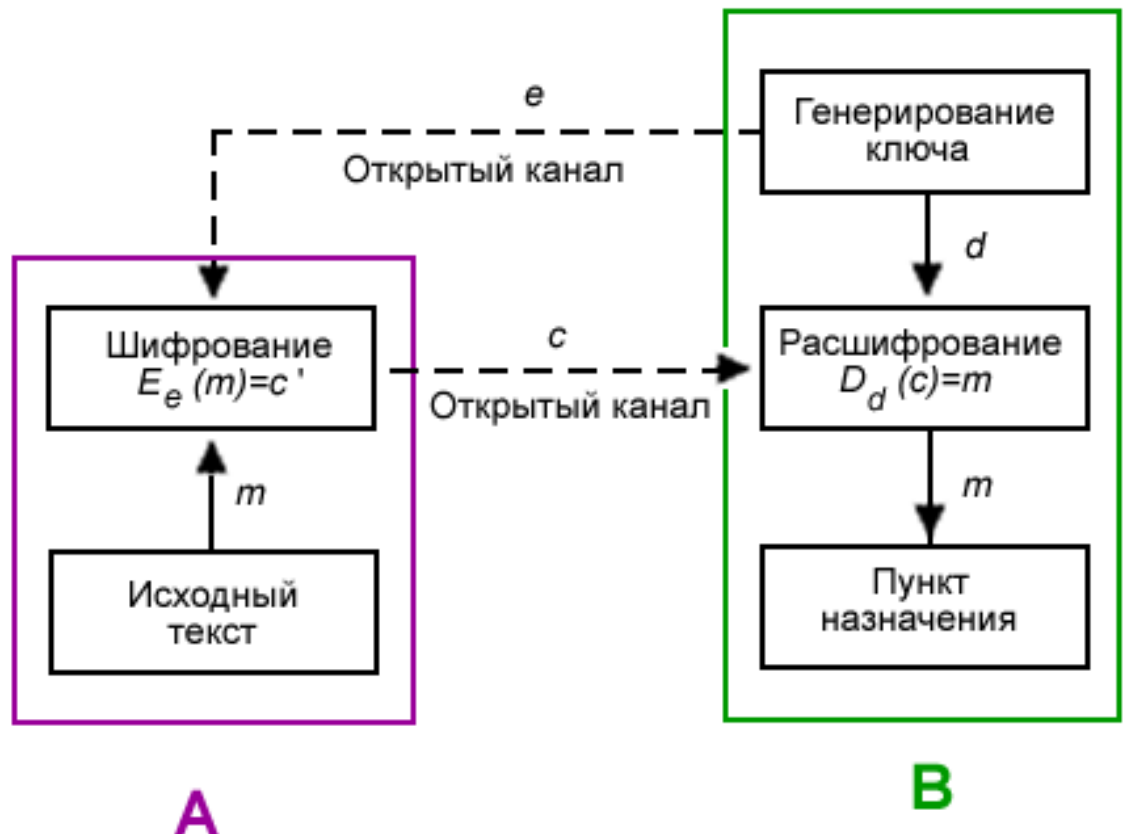
Имя:	АЛИСА
Пароль:	ГЛАДИОЛУС

Файл паролей примет следующий вид:

Имя	$f(\text{имя_пароль})$
АЛИСА	РОМАШКА
БОБ	НАРЦИСС

Логин пароль для входа в систему:

- Пусть e и d — ключи шифрования и расшифрования соответственно.
- E_e — функция шифрования
- D_d — функция расшифрования



1. Боб выбирает пару (e,d) и шлёт ключ шифрования e (открытый ключ) Алисе по открытому каналу, а ключ расшифрования d (закрытый ключ) защищён и секретен (он не должен передаваться по открытому каналу).
2. Чтобы послать сообщение m Бобу, Алиса применяет функцию шифрования, определённую открытым ключом e : $E_e(m)=c$, c — полученный шифротекст.
3. Боб расшифровывает шифротекст c , применяя обратное преобразование D_d , однозначно определённое значением d .

Алгоритм шифрования:

RSA - аббревиатура от фамилий Rivest, Shamir и Adleman

1. Генерация ключей:

Выбрать два простых различных числа	$p = 3557,$ $q = 2579$
Вычислить модуль(произведение)	$n = p * q = 3557 * 2579 = 9173503$
Вычислить функцию Эйлера	$\varphi(n) = (p - 1)(q - 1) = 9167368$
Выбрать открытую экспоненту	$e = 3$
Вычислить секретную экспоненту	$d = e^{-1} \bmod \varphi(n)$ $d = 6111579$
Опубликовать открытый ключ	$\{e, n\} = \{3, 9173503\}$
Сохранить закрытый ключ	$\{d, n\} = \{6111579, 9173503\}$

2. Шифрование:

Открытый ключ	$\{e, n\} = \{3, 9173503\}$
Выбрать текст для зашифровки	$m = 111111$
Вычислить <u>шифротекст</u>	$c = E(m) = m^e \bmod n =$ $= 111111^3 \bmod 9173503 = 4051753$

3. Расшифрование:

Закрытый ключ	$\{d, n\} = \{6111579, 9173503\}$
<u>Шифротекст</u>	$c = 4051753$
Вычислить исходное сообщение	$m = D(c) = c^d \bmod n =$ $= 4051753^{6111579} \bmod 9173503$ $= 111111$

Ассиметричные системы.

Применение

Алгоритмы криптосистемы с открытым ключом можно использовать:

- как самостоятельное средство для защиты передаваемой и хранимой информации,
- как средство распределения ключей,
- как средство аутентификации пользователей.

Недостатки в сравнении с симметричными системами:

- В алгоритм сложнее внести изменения.

- Хотя сообщения надежно шифруются, но получатель и отправитель самим фактом пересылки шифрованного сообщения «засвечиваются».
- Более длинные ключи.

Ниже приведена таблица, сопоставляющая длину ключа симметричного алгоритма с длиной ключа RSA с аналогичной криптостойкостью:

Длина симметричного ключа, бит	Длина ключа RSA, бит
56	384
64	512
80	768
112	1792
128	2304

- Шифрование-расшифрование с использованием пары ключей проходит на два-три порядка медленнее, чем шифрование-расшифрование того же текста симметричным алгоритмом.
- Требуются существенно бóльшие вычислительные ресурсы, поэтому на практике асимметричные криптосистемы используются в сочетании с другими алгоритмами

Электронная цифровая подпись

- Если обратиться к федеральному закону, то можно найти следующее её определение:
- «Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию»
- Электронная подпись предназначена для идентификации лица, подписавшего электронный документ, и является полноценной заменой собственноручной подписи

Словарь терминов:

- *Открытый текст* – данные, подлежащие шифрованию или полученные в результате расшифрования;
- *Шифртекст* – данные, полученные в результате применения шифра к открытому тексту;
- *Шифр* – совокупность обратимых преобразований, зависящая от некоторого параметра (ключа);
- *Ключ* – параметр шифра, определяющий выбор одного преобразования из совокупности;
- *Факторизация* – процесс разложения числа на простые множители;
- *НОД* – наибольший общий делитель;
- Числа a и b называются *взаимно простыми*, если НОД этих чисел равен 1;
- *Функция Эйлера $\varphi(n)$* – функция, равная количеству натуральных чисел, меньших n и взаимно простых с ним.

Использование электронной подписи позволяет осуществить:

- Контроль целостности передаваемого документа.
- Защиту от изменений (подделки) документа.
- Невозможность отказа от авторства.
- Доказательное подтверждение авторства документа.



Наиболее известные схемы создания электронной цифровой подписи:

- DSA;
- RSA;
- Эль-Гамаль (ElGamal);
- Рабина;
- Шнорра;
- Диффи-Лампорта.

Электронная подпись на основе алгоритма RSA

- Схема использования алгоритма *RSA* при большом модуле N практически не позволяет злоумышленнику получить закрытый *ключ* и прочитать зашифрованное сообщение. Однако она дает возможность злоумышленнику подменить сообщение от абонента *A* к абоненту *Б*, так как *абонент A* шифрует свое сообщение открытым ключом, полученным от *Б* по открытому каналу связи. А раз *открытый ключ* передается по открытому каналу, любой может получить его и использовать для подмены сообщения. Избежать этого можно, используя более сложные протоколы, например, следующий.
- Пусть, как и раньше, *пользователь A* хочет передать пользователю *Б* сообщение, состоящее из нескольких блоков m_i . Перед началом сеанса связи абоненты генерируют открытые и закрытые ключи, обозначаемые, как указано в следующей таблице:

	Открытый ключ	Закрытый ключ
Пользователь А	N_A, d_A	e_A
Пользователь Б	N_B, d_B	e_B

В результате каждый *пользователь* имеет свои собственные открытый (состоящий из двух частей) и закрытый ключи. Затем пользователи обмениваются открытыми ключами. Это подготовительный этап протокола.

Основная часть протокола состоит из следующих шагов.

1. Сначала пользователь А вычисляет числа $c_i = m_i^{e_A} \bmod N_A$, то есть шифрует сообщение своим закрытым ключом. В результате этих действий пользователь А подписывает сообщение.
2. Затем пользователь А вычисляет числа $g_i = c_i^{d_B} \bmod N_B$, то есть шифрует то, что получилось на шаге 1 открытым ключом пользователя Б. На этом этапе сообщение шифруется, чтобы никто посторонний не мог его прочитать.
3. Последовательность чисел g_i передается к пользователю Б.
4. Пользователь Б получает g_i и вначале вычисляет последовательно числа $c_i = g_i^{e_B} \bmod N_B$, используя свой закрытый ключ. При этом сообщение расшифровывается.
5. Затем Б определяет числа $m_i = c_i^{d_A} \bmod N_A$, используя открытый ключ пользователя А. За счет выполнения этого этапа производится проверка подписи пользователя А.

В результате *абонент* Б получает исходное сообщение и убеждается в том, что его отправил именно *абонент* А. Данная схема позволяет защититься от нескольких видов возможных нарушений, а именно:

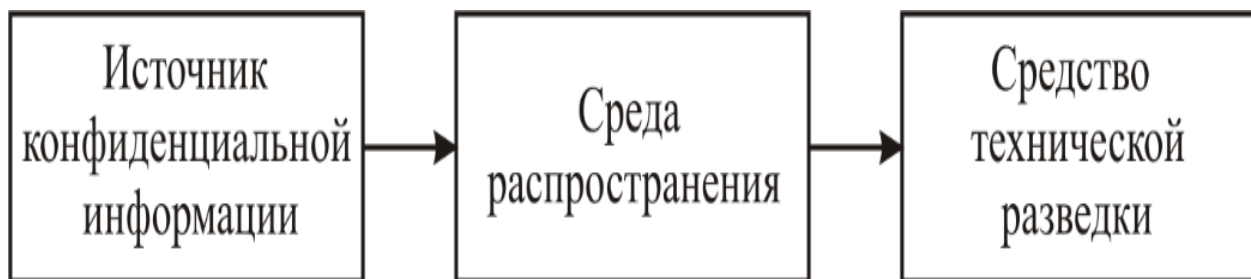
- пользователь А не может отказаться от своего сообщения, если он признает, что секретный ключ известен только ему;
- нарушитель без знания секретного ключа не может ни сформировать, ни сделать осмысленное изменение сообщения, передаваемого по линии связи.

- Данная схема позволяет избежать многих конфликтных ситуаций. Иногда нет необходимости зашифровывать передаваемое сообщение, но нужно его скрепить электронной подписью. В этом случае из приведенного выше протокола исключаются шаги 2 и 4, то есть текст шифруется закрытым ключом отправителя, и полученная последовательность присоединяется к документу. Получатель с помощью открытого ключа отправителя расшифровывает прикрепленную подпись, которая, по сути, является зашифрованным повторением основного сообщения. Если расшифрованная подпись совпадает с основным текстом, значит, подпись верна.
- Существуют и другие варианты применения алгоритма *RSA* для формирования ЭЦП. Например, можно шифровать (то есть подписывать) открытым ключом не само сообщение, а хеш-код от него.
- Возможность применения алгоритма *RSA* для получения электронной подписи связана с тем, что секретный и открытый ключи в этой системе равноправны. Каждый из ключей, d или e , могут использоваться как для шифрования, так и для расшифрования. Это свойство выполняется не во всех криптосистемах с открытым ключом.

- *Алгоритм RSA* можно использовать также и для обмена ключами.
- **Отметим некоторые недостатки алгоритма цифровой подписи RSA:**
 1. При вычислении ключей для системы цифровой подписи RSA необходимо проверять ряд дополнительных условий. Невыполнение любого из этих условий делает возможным фальсификацию цифровой подписи со стороны того, кто обнаружит такое невыполнение.
 2. Для обеспечения криптостойкости цифровой подписи RSA по отношению к попыткам фальсификации, например, на уровне алгоритма шифрования DES, необходимо использовать при вычислениях ключей очень большие целые числа, (около 10^{154}), что требует относительно больших вычислительных затрат, превышающих на 20-30% вычислительные затраты других алгоритмов цифровой подписи при сохранении того же уровня криптостойкости.
 3. Цифровая подпись RSA уязвима к так называемой мультипликативной атаке. Иначе говоря, *алгоритм цифровой подписи RSA* позволяет злоумышленнику без знания секретного ключа сформировать подписи под теми документами, у которых результат хэширования можно вычислить как произведение результатов хэширования уже подписанных документов. Хотя следует заметить, что вероятность реализации такой атаки весьма незначительна. Для работы смарт-карт с цифровыми подписями RSA рекомендуется использование ключей с длиной модуля 1024 бит.

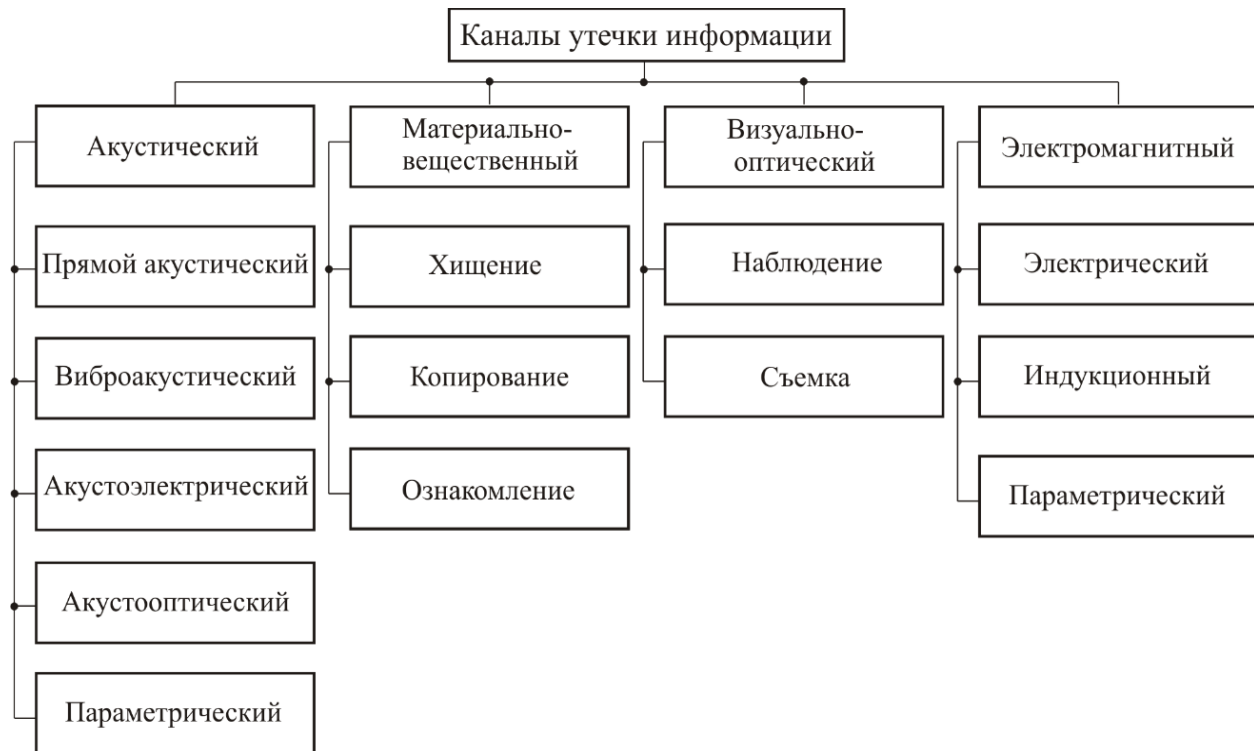
Технические каналы утечки информации

- **Технический канал утечки информации** – совокупность источника конфиденциальной информации, среды распространения и средства технической разведки для перехвата информации.



- Источники конфиденциальной информации:
 - – человек;
 - – электронная аппаратура;
 - – документы (содержание);
 - – здания и сооружения (внешний вид).
- Среда распространения конфиденциальной информации:
 - – воздушная;
 - – твердые вещества (строительные конструкции);
 - – электрические цепи.
- Средства технической разведки:
 - – визуально-оптические (оптические увеличительные приборы);
 - – оптоэлектронные (телевизионные, приборы ночного видения, тепловизоры и т. д.);
 - – акустические (закладные устройства, направленные микрофоны, электронные стетоскопы и т. д.);
 - – радиоперехвата (перехвата сообщений радио-, сотовой связи и т. д.);
 - – фотографические;
 - – электронные (для перехвата сигналов в проводных коммуникациях).
- По физическим принципам возникновения каналы утечки информации можно разделить на следующие группы:

- – акустический;
- – материально-вещественный;
- – визуально-оптический;
- – электромагнитный.

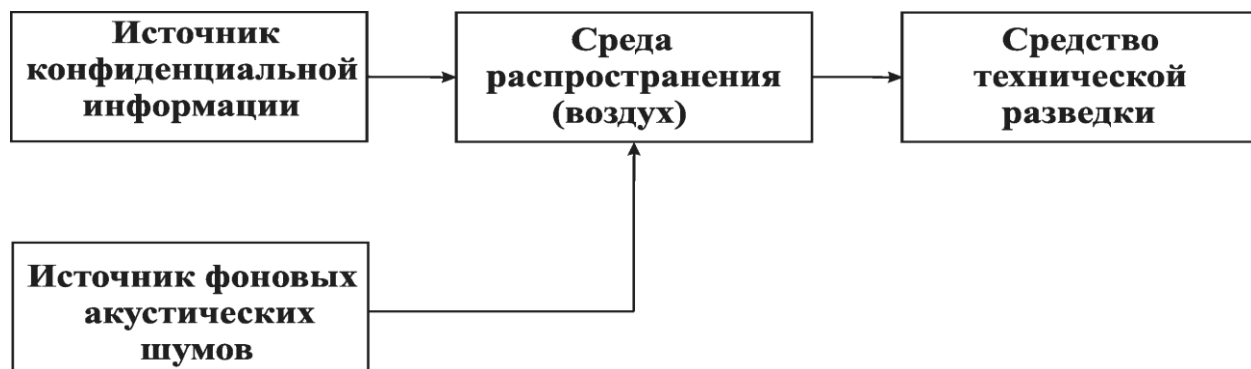


Акустические каналы утечки информации

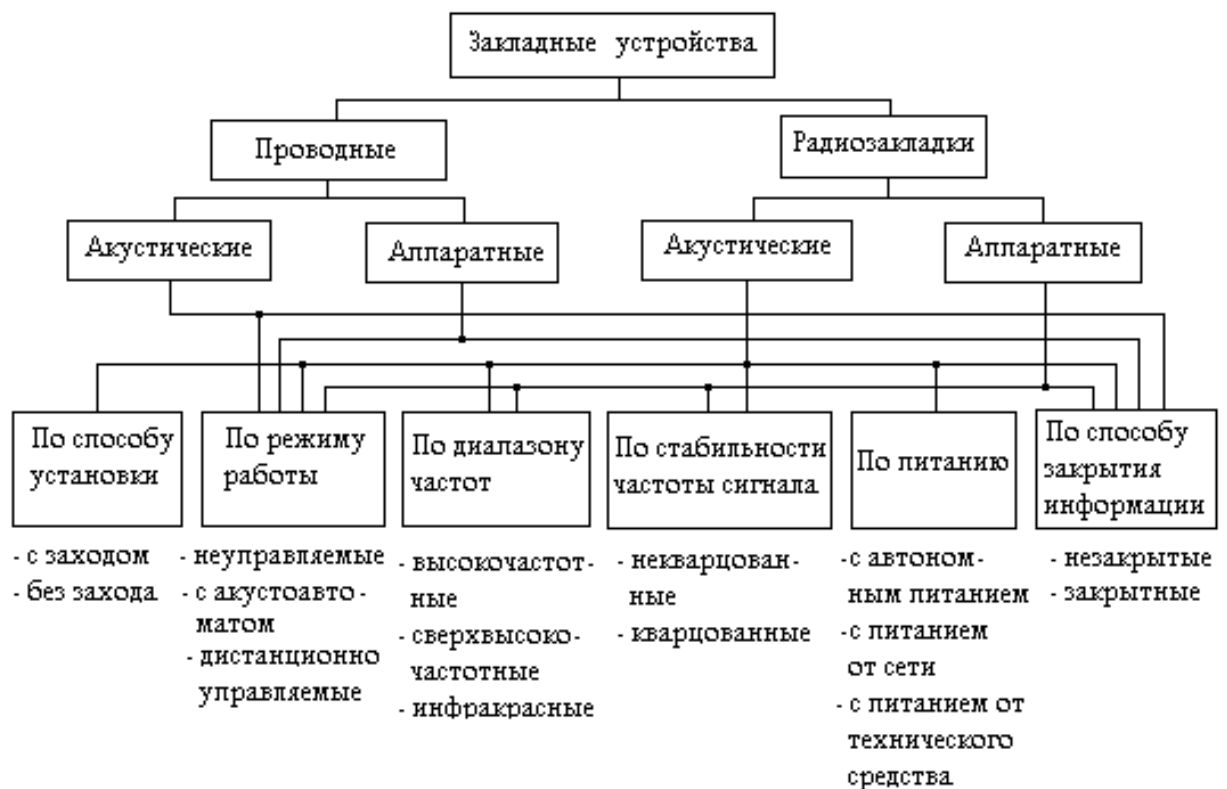
- В случае, когда источником информации является голосовой аппарат человека, информация называется **речевой**.
- Области спектра звука, в которых сосредоточивается основная мощность акустического сигнала, называются **формантами**. Большинство звуков речи имеют одну или две форманты.
- Психологическая (с учетом чувствительности уха на разных частотах) интенсивность акустических сигналов изменяется в широких пределах (0...130 дБ). Для человека как основного источника соотношение между уровнем громкости и его качественной оценкой характеризуется следующими данными: очень тихая речь (шепот) – 5...10 дБ, тихая речь – 30...40 дБ, речь умеренной громкости 50...60 дБ, громкая речь – 60...70 дБ, крик – 70...80 дБ и более. Для сравнения: звук

сирены «скорой помощи» – 100 дБ, а шум реактивного двигателя на расстоянии 5 м – 120 дБ.

- Голосовой аппарат человека является первичным источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения.



- Перехват информации средствами технической разведки в данном случае может реализовываться за счет применения закладных устройств, устанавливаемых внутри помещения или при помощи направленных микрофонов, путем перехвата акустических сигналов через открытые окна, двери. В данном случае акустическая волна без существенного ослабления попадает в средство технической разведки. Таким образом, образуется **прямой** акустический канал утечки информации.
- **Закладное устройство (ЗУ)** – автономное устройство для перехвата речевой информации, конструктивно объединяющее микрофон и передатчик



► Перехваченная ЗУ речевая информация может передаваться по радиоканалу, сети электропитания, оптическому каналу, телефонной линии, посторонним проводникам, инженерным коммуникациям в ультразвуковом диапазоне частот. Прием информации, передаваемой закладными устройствами, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн.

► **Направленный микрофон** – электронное устройство, обладающее высокими чувствительностью и помехоустойчивостью за счет его узкой диаграммы направленности

Виброакустические каналы утечки информации

► Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Таким образом, в своем первоначальном состоянии речевой сигнал в помещении

присутствует в виде акустических и вибрационных колебаний. В данном случае строительные конструкции выполняют преобразование акустических колебаний в вибрационные и возникает виброакустический (вибрационный) канал утечки информации.

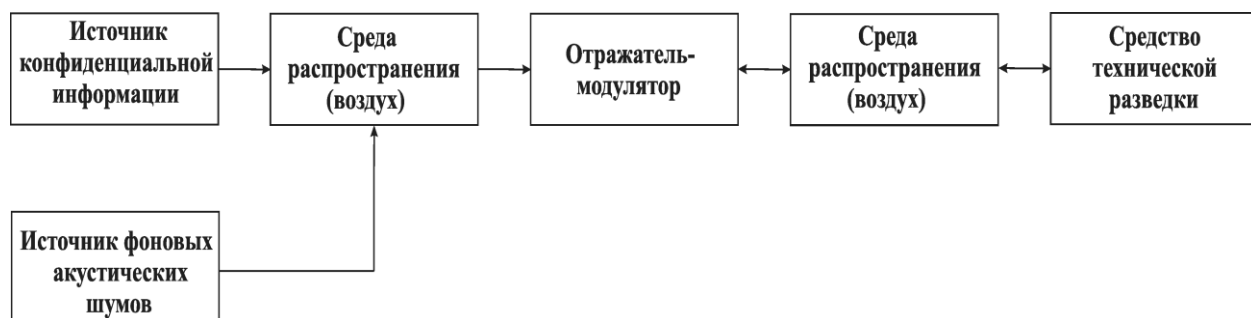


- Перехват информации в виброакустических каналах обеспечивается электронными стетоскопами, выполняющими преобразование механических колебаний строительных конструкций (пол, потолок, стены) в электрические. В качестве преобразователей, подключаемых к электронному стетоскопу, используются акселерометры.
- По виброакустическому каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют радиостетоскопами. Возможно использование закладных устройств с передачей информации по инженерным коммуникациям (ультразвуковые колебания).
- Вспомогательные технические средства и системы (ВТСС), кроме указанных элементов, могут содержать непосредственно акустоэлектрические преобразователи. К таким ВТСС относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Эффект акустоэлектрического преобразования в специальной литературе называют «микрофонным эффектом».
- Электромеханический вызывной звонок телефонного аппарата – типичный представитель индуктивного

акустоэлектрического преобразователя, микрофонный эффект которого проявляется при положенной микрофонной трубке



- Структурная схема акустоэлектрического канала утечки информации



- Структурная схема акустооптического канала утечки информации
- Для перехвата речевой информации по данному каналу используются сложные лазерные системы, которые часто называют «лазерными микрофонами». Работают они, как правило, в ближнем инфракрасном диапазоне длин волн.
- На рисунке приведен простейший вариант подобной системы: луч лазера падает на стекло окна под некоторым углом (например 45 градусов). На границе стекло–воздух происходит модуляция луча речевыми колебаниями. Отражённый луч принимается фотодетектором, расположенным с другой стороны окна под углом, равным углу падения луча лазера. Такая система требует тщательной юстировки.
- Второй способ, использующий сплиттер (делитель пучка), несколько сложнее, но он позволяет совместить лазер и детектор. Отпадает необходимость в тщательной юстировке

системы. Применение сплиттера позволяет свести падающий и отражённый луч в одну точку.

Материально-вещественный канал утечки информации

- Утечка информации по материально-вещественному каналу обусловлена хищением, копированием и ознакомлением с информацией, представленной на бумажном, электронном или каком-либо другом носителе.

Электромагнитные каналы утечки информации

- Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве побочные электромагнитные излучения (ПЭМИ), которые в той или иной степени связаны с обрабатываемой информацией (электромагнитный канал).
- Физические явления, лежащие в основе появления этих излучений, имеют различный характер, но тем не менее они могут рассматриваться как непреднамеренная передача конфиденциальной информации по некоторой "побочной системе связи", образованной источником излучения, средой и средством перехвата информации.
- Регистрация средством технической разведки ПЭМИ источника информации (персональный компьютер и др.) распространяющихся через воздушную среду обуславливает возникновение индукционного канала утечки информации.
- Структурная схема индукционного канала утечки информации

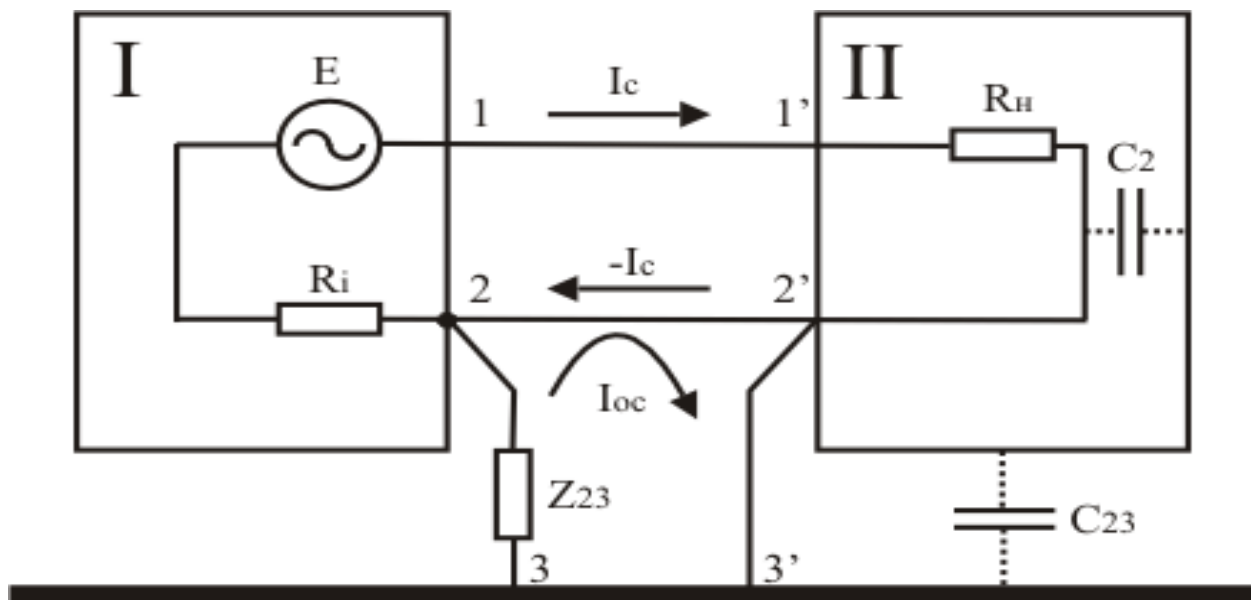


- Структурная схема электрического канала утечки информации



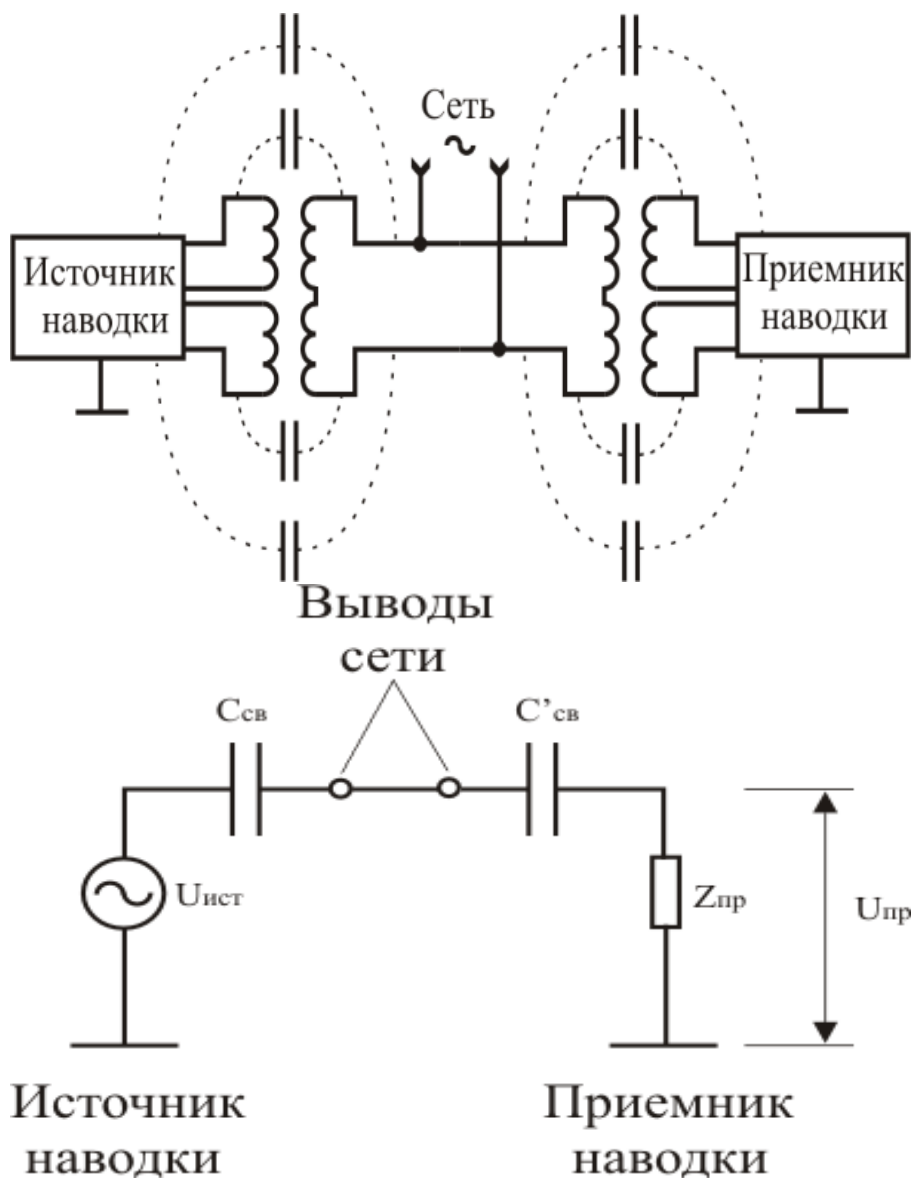
Утечка информации по цепям заземления

- **Заземлением** называется преднамеренное соединение объекта с заземляющим устройством, осуществляемое путем создания системы проводящих поверхностей и электрических соединений, предназначенных для выполнения различных функций.
- Одной из причин попадания опасного (информационного) сигнала в систему заземления является наличие ПЭМИ – носителя информационного сигнала в местах расположения элементов системы. Это ПЭМИ будет наводить в расположенной поблизости системе заземления ток опасного сигнала.
- Проникновение опасного сигнала в цепи заземления может быть связано с образованием так называемых контуров заземления.
- Образование контуров заземления между двумя устройствами



Утечка информации по цепям электропитания

- Как правило, провода общей сети питания распределяются по различным помещениям, где расположены технические системы, и соединены с различными устройствами. Вследствие этого образуется нежелательная связь между отдельными техническими средствами. Кроме того, провода сети питания являются линейными антеннами, способными излучать или воспринимать электромагнитные поля.
- На практике значительная часть нежелательных наводок между удаленными друг от друга устройствами происходит с участием сети питания. При этом возможны различные ситуации. В случае асимметричной наводки, когда провода сети питания прокладываются вместе и имеют одинаковые емкости относительно источников и приемников наводки, в них наводятся напряжения, одинаковые по величине и по фазе относительно земли и корпуса приборов.

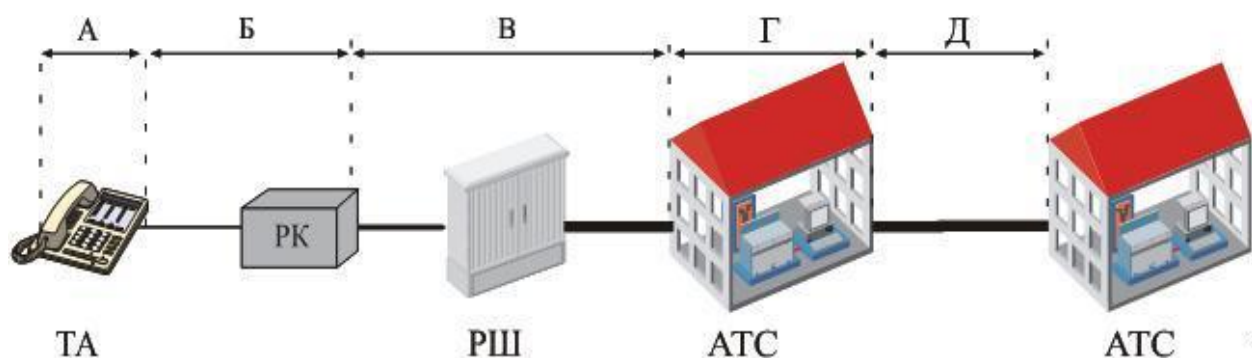


- Действительная (а) и эквивалентная (б) схемы нежелательной асимметричной связи двух устройств

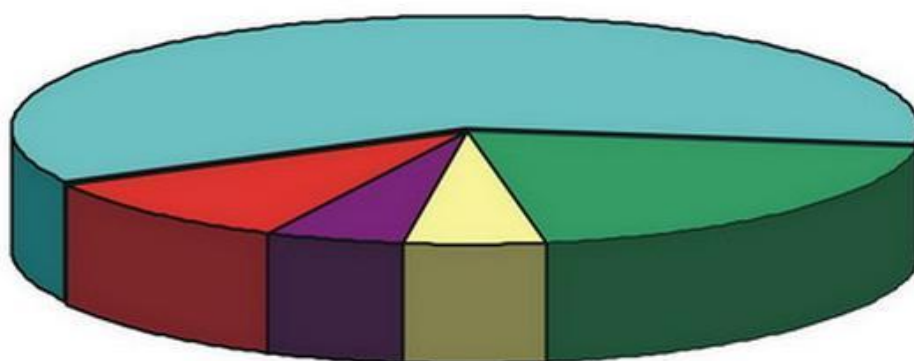
Перехват информации в телефонных каналах связи

- Телефонную систему связи можно представить в виде нескольких условных зон. К зоне «А» относится телефонный аппарат (ТА) абонента. Сигнал с аппарата по телефонному проводу попадает в распределительную коробку (РК) (зона «Б») и оттуда в магистральный кабель (зона «В»). После коммутации на автоматической телефонной станции (АТС) (зона «Г») сигнал распространяется по многоканальным кабелям (зона «Д») до следующей автоматической телефонной станции (АТС). В каждой зоне имеются свои

особенности по перехвату информации, но принципы, на которых построена техника несанкционированного подключения, практически не отличается.



- Наиболее опасными зонами, с точки зрения вероятности применения подслушивающих устройств, считаются зоны «А», «Б» и «В»



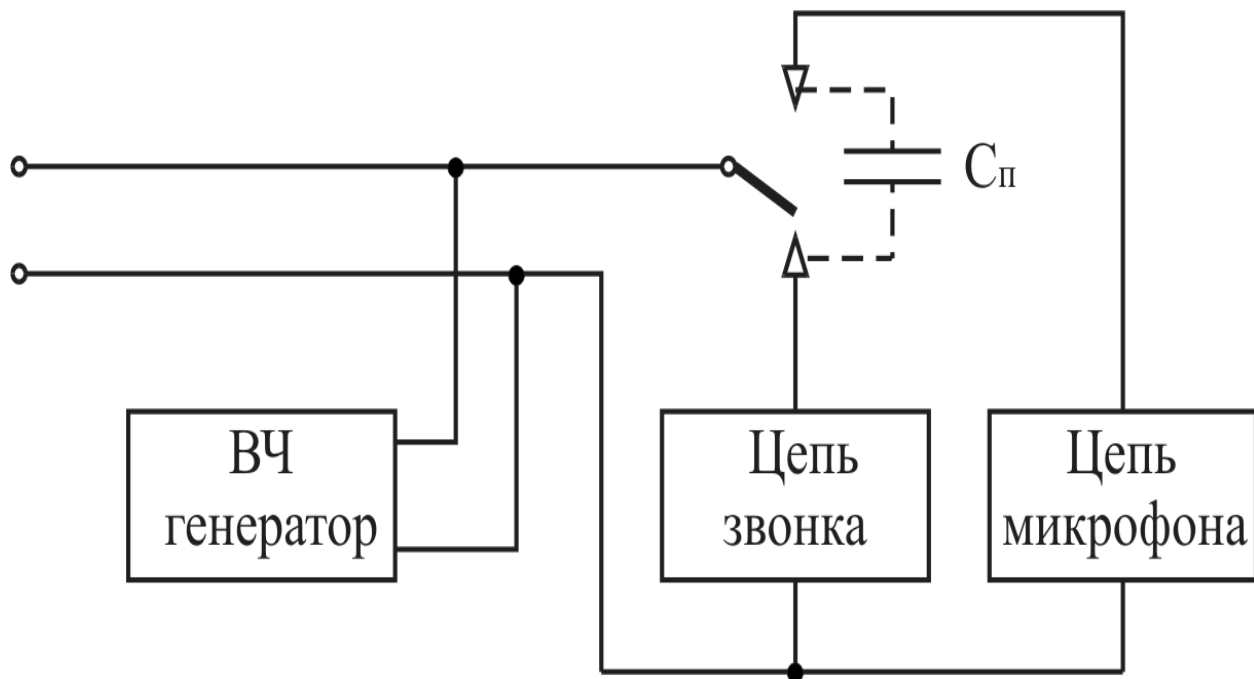
- Непосредственное подключение к линии – это самый простой и распространенный способ подслушивания телефонных разговоров. Для негосударственных организаций, занимающихся промышленным шпионажем, реально

доступным местом подключения для перехвата информации являются зоны «А», «Б», «В». Подключение может быть:

- – контактным;
- – бесконтактным.

Высокочастотное навязывание

- **Высокочастотное навязывание** - это воздействие на технические средства высокочастотных сигналов.
- В настоящее время используются два способа высокочастотного навязывания:
 - 1. Посредством контактного введения высокочастотного сигнала в электрические цепи, имеющие функциональные или паразитные связи с техническим средством.
 - 2. Путем излучения высокочастотного электромагнитного поля. Возможность утечки информации при использовании высокочастотного навязывания связана с наличием в цепях технических средств нелинейных или параметрических элементов. Навязываемые высокочастотные колебания воздействуют на эти элементы одновременно с низкочастотными сигналами, возникающими при работе этих средств и содержащими конфиденциальные сведения.
- Принцип реализации высокочастотного навязывания в телефонном аппарате



- Излучение высокочастотных колебаний, промодулированных опасным сигналом, в свободное пространство осуществляется с помощью случайной антенны – телефонного провода. Промодулированный высокочастотный сигнал распространяется также в телефонной абонентской линии за пределы контролируемой территории. Следовательно, прием высокочастотных колебаний можно осуществлять либо путем подключения приемного устройства к телефонной линии, либо по полю.

Пассивные и активные методы защиты информации от утечки по техническим каналам

- **Пассивные методы защиты информации** – предназначены для предотвращения или существенного затруднения перехвата информации по техническим каналам за счет снижения соотношения сигнал/шум на входе средства технической разведки путем уменьшения уровня сигнала.
- К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры и т. д. Цель пассивного

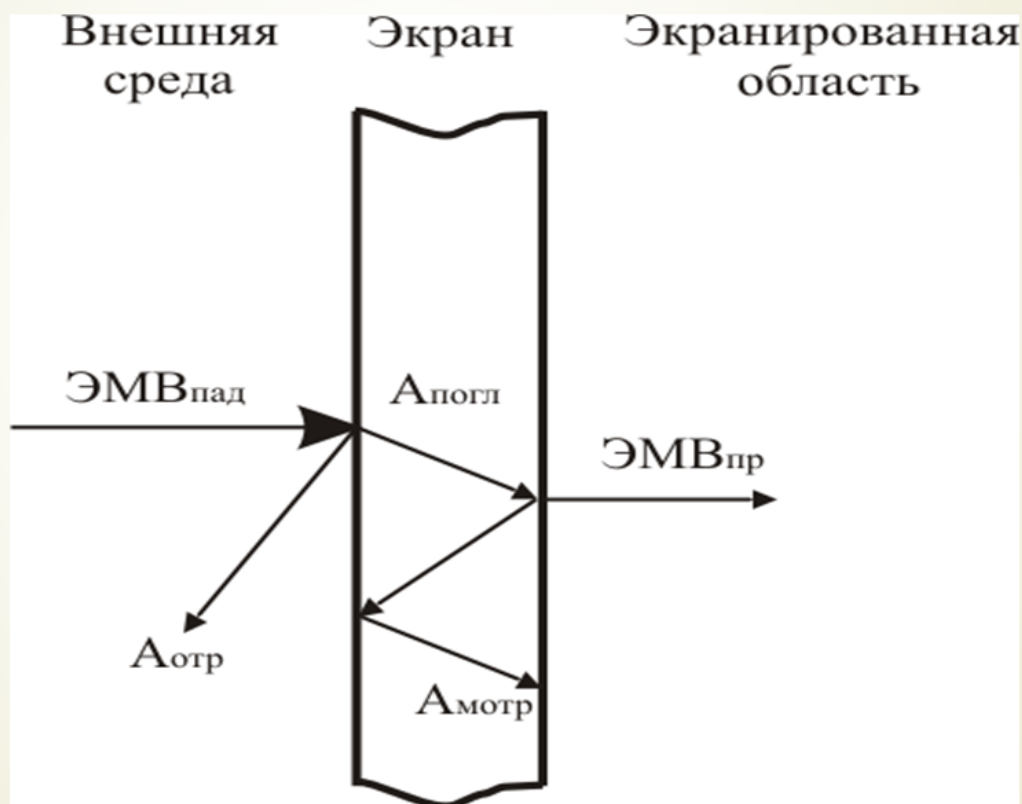
способа – максимально ослабить сигнал от источника информативного сигнала, например, за счет отделки стен звукопоглощающими материалами или экранирования технических средств.

Пассивные методы защиты информации направлены на:

- ослабление побочных электромагнитных излучений (информационных сигналов) ТСПИ на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- • ослабление наводок побочных электромагнитных излучений (информационных сигналов) ТСПИ в посторонних проводниках и соединительных линиях ВТСС, выходящих за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;
- +• исключение (ослабление) просачивания информационных сигналов ТСПИ в цепи электропитания, выходящие за пределы контролируемой зоны, до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов.

Экранирование электромагнитного поля

Экранирование электромагнитного поля металлическим экраном



■ Экранирование электромагнитных полей

На границе раздела двух сред (воздух–металл и металл–воздух) волна претерпевает отражение и преломление, а в толще экрана происходит частичное поглощение энергии электромагнитного поля.

Общая эффективность экранирования определяется суммой потерь за счет затухания энергии в толще материала $A_{\text{погл}}$, отражения энергии от границ раздела внешняя среда–металл и металл–экранируемая область $A_{\text{отр}}$ и многократных внутренних отражений в стенках экрана $A_{\text{мотр}}$:

$$A = A_{\text{погл}} + A_{\text{отр}} + A_{\text{мотр}}$$

- Защита информации от утечки по электромагнитному каналу может быть обеспечена за счет снижения уровней побочных электромагнитных излучений средств обработки информации при размещении их в экранированных помещениях, а также экранировании непосредственно таких средств.

Конструкции экранов электромагнитного излучения

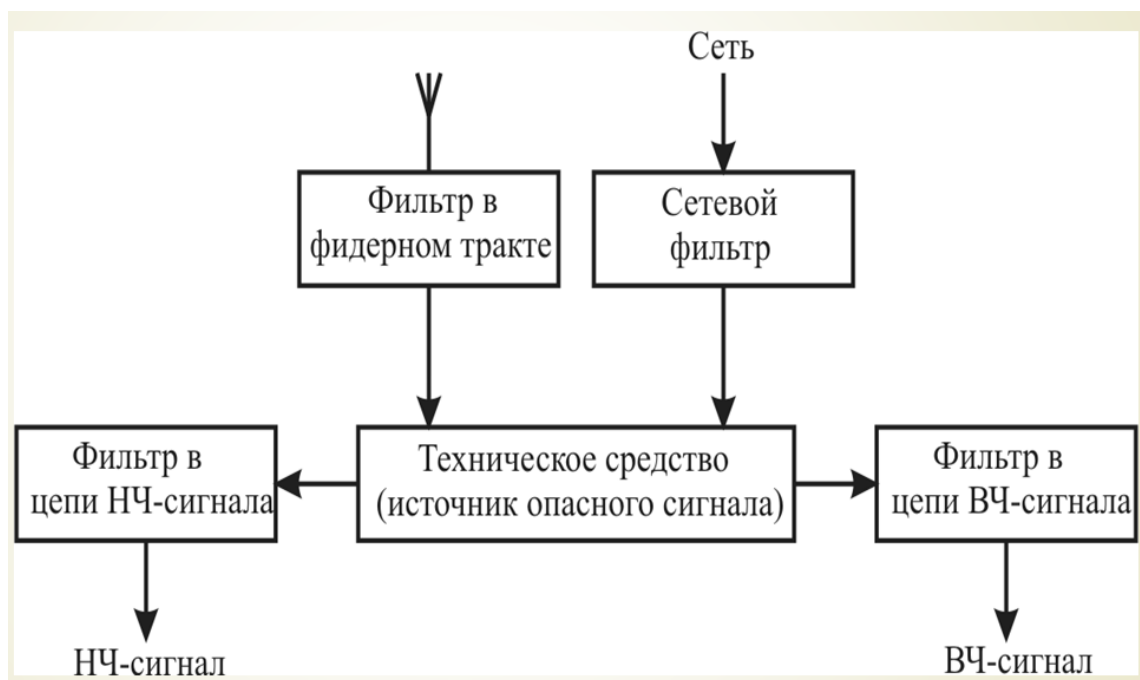
- Защита информации от утечки по электромагнитному каналу может быть обеспечена за счет снижения уровней ПЭМИ средств обработки информации при размещении их в экранированных помещениях, а также экранировании непосредственно таких средств.
- Для изготовления экранов ЭМИ применяются различные материалы, объединяемые в единую конструкцию.
- Выбор материала экрана проводится исходя из обеспечения требуемой эффективности экранирования в заданном диапазоне частот при определенных ограничениях. Эти ограничения связаны с массогабаритными характеристиками экрана, его влиянием на экранируемый объект, с механической прочностью и устойчивостью экрана против коррозии, с технологичностью его конструкции и т. д.



Фильтрация

- В системах и средствах информатизации и связи фильтрация может осуществляться в:

- – высокочастотных тактах передающих и приемных устройств для подавления нежелательных излучений – носителей опасных сигналов – и исключения возможности их нежелательного приема;
- – различных сигнальных цепях технических средств для устранения нежелательных связей между устройствами и исключения прохождения сигналов, отличающихся по спектральному составу от полезных сигналов;
- – цепях электропитания, управления, контроля, коммутации технических средств для исключения прохождения опасных сигналов по этим цепям;
- – проводных и кабельных соединительных линиях для защиты от наводок;
- – цепях пожарной и охранной сигнализации для исключения прохождения опасных сигналов и воздействия навязываемых высокочастотных колебаний.



Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:

- – величины рабочих напряжения и тока фильтра должны соответствовать величинам напряжения и тока цепи, в которой фильтр установлен;
- – эффективность ослабления нежелательных сигналов должна быть не меньше заданной в защищаемом диапазоне частот;
- – ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным, не влияющим на качество функционирования системы;
- – габариты и масса фильтров должны быть, по возможности, минимальными;
- – фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление, удары, вибрация и т. д.);
- – конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования:

- – затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть незначительным (например 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 10^{10} Гц);
- – сетевые фильтры должны эффективно работать при больших проходящих токах, высоких напряжениях и высоких уровнях мощности рабочих и подавляемых электромагнитных колебаний;

- – ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

Заземление технических средств

- Основные требования, предъявляемые к системе заземления, заключаются в следующем:
 - – система заземления должна включать общий заземлитель, заземляющий кабель, шины и провода, соединяющие заземлитель с объектом;
 - – сопротивления заземляющих проводников, а также земляных шин должны быть незначительными;
 - – каждый заземляемый элемент должен быть присоединен к заземлителю или к заземляющей магистрали при помощи отдельного ответвления.
 - Последовательное включение в заземляющий проводник нескольких заземляемых элементов запрещается;
- – в системе заземления должны, по возможности, отсутствовать замкнутые контуры, образованные соединениями или нежелательными связями между сигнальными цепями и корпусами устройств, между корпусами устройств и землей;
- – следует избегать использования общих проводников в системах экранирующих заземлений, защитных заземлений и сигнальных цепей;

- – качество электрических соединений в системе заземления должно обеспечивать минимальное сопротивление контакта, надежность и механическую прочность контакта в условиях климатических воздействий и механических нагрузок;
- – контактные соединения должны исключать возможность образования оксидных пленок на контактирующих поверхностях и связанных с этими пленками нелинейных явлений;
- – контактные соединения должны исключать возможность образования гальванических пар для предотвращения коррозии в цепях заземления;
- – запрещается использовать в качестве заземляющего устройства нулевые фазы электросетей, металлоконструкции зданий, трубы систем отопления, водоснабжения, канализации и т. д.

Звукоизоляция помещений

- Защита речевой информации от утечки по акустическим каналам может быть реализована за счет создания защищенных методом звукоизоляции помещений.
- Выделение акустического сигнала на фоне естественных шумов происходит при определенных соотношениях сигнал/шум. Производя звукоизоляцию, добиваются его снижения до предела, затрудняющего (исключающего) возможность выделения речевых сигналов, проникающих за пределы контролируемой зоны по акустическому или виброакустическому (ограждающие конструкции, трубопроводы) каналам.

- При выборе ограждающих конструкций выделенных помещений в процессе проектирования необходимо руководствоваться следующими правилами:
- – в качестве перекрытий рекомендуется использовать акустически неоднородные конструкции;
- – в качестве полов целесообразно использовать конструкции на упругом основании или конструкции, установленные на виброизоляторы;
- – потолки целесообразно выполнять подвесными, звукопоглощающими со звукоизолирующим слоем;
- – в качестве стен и перегородок предпочтительно использование многослойных акустически неоднородных конструкций с упругими прокладками (резина, пробка, ДВП, МВП и т. п.).

Прохождение волн через препятствия осуществляется различными путями:

- – через поры, окна, щели, двери и т. д. (путем воздушного переноса);
- – через материал стен, по трубам тепло-, водо- и газоснабжения и т. д. за счет их продольных колебаний (путем материального переноса);
- – через материал стен и перегородок помещения за счет их поперечных колебаний (путем мембранного переноса).
- Звукоизоляция помещений обеспечивается за счет использования звукопоглощающих материалов – имеющих сквозную пористость и относительно высокий коэффициент звукопоглощения (более 0,2) и обладающих динамическим модулем упругости не более 150 кгс/см².

- По форме звукопоглощающие материалы разделяют на штучные (блоки, плиты), рулонные (маты, полосовые прокладки, холсты), рыхлые и сыпучие (вата минеральная, стеклянная, керамзит, шлак).
- По величине относительного сжатия (жесткости) звукопоглощающие и звукоизоляционные строительные материалы подразделяются на мягкие, полужесткие и твердые.

Активные методы ЗИ от утечки по техническим каналам

- **Активные методы ЗИ** – предназначены для предотвращения или существенного затруднения перехвата информации по техническим каналам за счет снижения соотношения сигнал/шум на входе средства технической разведки путем уменьшения уровня шума.
- **Активное техническое средство защиты** – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации. Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

Активные методы защиты информации направлены на:

- Создание маскирующих пространственных электромагнитных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ;
- Создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях ВТСС с

целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала ТСПИ.

Акустическая маскировка

Мероприятия акустической маскировки позволяют обеспечить:

- – неузнаваемость голоса диктора;
- – существенное снижение разборчивости речи диктора;
- – скрыть факт передачи речевой информации.

Электромагнитная маскировка

- Активные маскирующие помехи (шумовые).
- Реализуется с помощью систем активной защиты. Такие системы подразделяются на системы линейного и пространственного зашумления.

Обнаружение закладных устройств

- Для повышения скрытности работы мощность передатчика ЗУ делается небольшой, но достаточной для перехвата высокочувствительным приемником с небольшого расстояния (20...400 м).
- Микрофоны делают как встроенными, так и выносными. Они бывают двух типов: акустическими или вибрационными.

Наиболее информативными признаками проводной микрофонной системы являются:

- – тонкий провод неизвестного назначения, подключенный к малогабаритному микрофону (часто закамуфлированному и скрытно установленному) и выходящий в другое помещение;

- – наличие в линии (проводе) неизвестного назначения постоянного (в несколько вольт) напряжения и низкочастотного информационного сигнала.

Демаскирующие признаки автономных некамуфлированных акустических закладок:

- признаки внешнего вида – малогабаритный предмет неизвестного назначения;
- одно или несколько отверстий малого диаметра в корпусе;
- наличие автономных источников питания;
- наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором;
- наличие в устройстве проводников или других деталей, определяемых при просвечивании его рентгеновскими лучами.
- Некоторые камуфлированные ЗУ не отличаются от оригиналов даже при тщательном внешнем осмотре. Их можно обнаружить только при просвечивании предметов рентгеновскими лучами.

Методы поиска закладных устройств:

- специальное обследование выделенных помещений;
- поиск ЗУ с использованием технических средств;
- измерение параметров линий электропитания, телефонных линий связи и т. д.;
- проведение тестового «прозвона» всех телефонных аппаратов, установленных в проверяемом помещении, с

контролем (на слух) прохождения всех вызывных сигналов автоматических телефонных станций.

Технические средства обнаружения закладных устройств

- *Индикаторы электромагнитных излучений.*
- Порог устанавливается так, чтобы индикатор не реагировал на внешние излучения (фон). В результате подслушивающее устройство обнаруживается только в тех точках помещения, где уровень его поля превосходит фоновый на 15...20 дБ
- *Индикаторы-частотомеры.* Отличаются от индикаторов электромагнитных излучений встроенным счетчиком – частотомером, который измеряет частоту радиосигнала, превысившего установленный порог, и помогает оператору идентифицировать сигнал подслушивающего устройства.
- *Нелинейные локаторы.* Используются для физического обнаружения и определения местоположения скрытно размещенных электронных устройств, которые могут находиться в выключенном состоянии
- *Сканирующие радиоприемники.* Современные сканеры могут автоматически перестраиваться в диапазоне до нескольких ГГц и обнаруживать сигналы с различными видами модуляции
- *Тепловизоры.* Техническое средство, обеспечивающее преобразование электромагнитного излучения (теплого), излучаемого различными объектами в видимое изображение
- *Компьютерные комплексы контроля помещений и зданий (радиомониторинга).* Представляют собой аппаратно-программные системы на базе стандартных узлов компьютера и недорогого сканера, которые оснащаются дополнительной аппаратурой и программами

Идентификация – процедура распознавания субъекта по его идентификатору.

Аутентификация – процедура проверки подлинности субъекта, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует.

Авторизация – процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации.

Электронные ключи, Dongle

Аппаратное средство, предназначенное для защиты ПО и защиты от несанкционированного доступа к данным

Могут иметь различные форм-факторы, но чаще всего они подключаются к компьютеру через USB. Также встречаются с LPT-или PCMCIA-интерфейсами.

Карты с магнитной полосой. В данном типе карты информация заносится на магнитную полосу. Карты с магнитной полосой бывают трёх форматов: ID-1, ID-2, ID-3. Магнитная полоса содержит 3 дорожки, на которые в закодированном виде записывают номер карты, срок ее действия, фамилию держателя карты и тому подобные данные. Объем записанной информации около 100 байт.

Магнитная полоса может быть изготовлена для различных мощностей магнитного поля, и по этому параметру различают **высококоэрцитивную (HiCo)** и **низкокоэрцитивную (LoCo)**. Степень коэрцитивности влияет на устойчивость записанной информации к размагничиванию. **Пластиковые карты с магнитной полосой HiCo** более надежны и долговечны, так как информация на магнитных полосах HiCo менее подвержена размагничиванию внешними магнитными полями, чем на полосах LoCo.

Штрих-код — это наносимая в виде штрихов закодированная информация, считываемая при помощи специальных устройств. С помощью штрихового кода кодируют информацию о некоторых наиболее существенных параметрах объекта.

Был разработан в 1973 году.

26 июня 1974 года был просканирован первый товар — блок 10 фруктовых жевательных резинок компании Wrigley.

Первоначально 11 цифр кода были распределены следующим образом:

Префикс — 1 цифра.

Код производителя — 5 цифр.

Код товара — 5 цифр.

1. Суммируются все цифры на нечётных позициях (первая, третья, пятая, и т. д.) и результат умножается на три.
2. Суммируются все цифры на чётных позициях (вторая, четвёртая, шестая, и т. д.).
3. Числа, полученные на предыдущих двух шагах, складываются, и из полученного результата оставляется только последняя цифра.
4. Эту цифру вычитают из 10.
5. Конечный результат этих вычислений и есть контрольная цифра (десятке соответствует цифра 0).

QR-код (англ. quick response - быстрый отклик) — двумерный штрихкод, разработанный в 1994 году японской фирмой Denso-Wave. В нём кодируется информация, состоящая из символов (включая кириллицу, цифры и спецсимволы).

Максимальное количество символов, которые помещаются в один QR-код:

цифры — 7089;

цифры и буквы (латиница) — 4296;

двоичный код — 2953 байт (следовательно, около 2953 букв кириллицы в кодировке windows-1251 или около 1450 букв кириллицы в utf-8);

иероглифы — 1817.

Есть четыре уровня избыточности: 7, 15, 25 и 30 %. Благодаря исправлению ошибок, удаётся нанести на QR-код рисунок и всё равно оставить его читаемым.

► **Двухфакторная аутентификация** — это метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов, что обеспечивает более эффективную защиту аккаунта. *На практике это обычно выглядит так:*

► первый рубеж — это логин и пароль,

► второй — специальный код, приходящий по SMS или электронной почте.

► Реже второй «слой» защиты запрашивает специальный USB-ключ или биометрические данные пользователя. В общем, суть подхода очень проста: чтобы куда-то попасть, нужно дважды подтвердить тот факт, что вы — это вы, причем при помощи двух «ключей», одним из которых вы владеете, а другой держите в памяти.

► **Многофакторная аутентификация** – в процессе которой используются аутентификационные факторы нескольких типов.

Смфрт-карты

Аппаратный токен – это устройство, предназначенное специально для аутентификации.

Все смарт-карты можно разделить по способу обмена со считывающим устройством на:

- контактные смарт-карты с интерфейсом ISO 7816;
- контактные смарт-карты с USB-интерфейсом;
- бесконтактные (RFID) смарт-карты.

По функциональности карты можно разделить на:

- карты памяти;
 - интеллектуальные карты.
- **Смарт-карты** представляют собой пластиковые карты со встроенной микросхемой. В большинстве случаев смарт-карты содержат микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти. *Смарт-карты обладают возможностью проводить криптографические вычисления.*
 - **Назначение смарт-карт** — одно- и двухфакторная аутентификация пользователей, хранение ключевой информации и проведение криптографических операций в доверенной среде.
 - Все смарт-карты можно разделить **по способу обмена со считывающим устройством** на:
 - Контактные смарт-карты с интерфейсом ISO 7816.
 - *Контактные смарт-карты имеют зону соприкосновения, содержащую несколько*

небольших контактных лепестков. Когда карта вставляется в считыватель, чип соприкасается с электрическими коннекторами, и считыватель может считать и\или записать информацию с чипа.

► **Контактные смарт-карты с USB интерфейсом.**

► *Обычно представляют из себя микросхему обычной ISO 7816 карты совмещенную с USB-считывателем в одном миниатюрном корпусе. Это делает применение смарт-карт для компьютерной аутентификации гораздо удобнее.*

► **Бесконтактные (RFID) смарт-карты.**

► *Это смарт-карты, в которых карта общается со считывателем через технологию RFID (Radio Frequency IDentification). Требуется подносить карточки достаточно близко к считывателю, чтобы провести необходимые операции. Они часто применяются в областях, где необходимо провести операцию быстро, например, в общественном транспорте.*

Парольная аутенфикация

► В настоящее время парольная аутентификация является наиболее распространенной, прежде всего, благодаря своему единственному достоинству – простоте использования.

Однако парольная аутентификация имеет недостатки:

► Пароли пользователя можно подобрать из-за достаточно небрежного отношения большинства пользователей к формированию пароля. Часто встречаются случаи выбора пользователями легко предугадываемых паролей, например:

- пароль эквивалентен идентификатору (имени) пользователя (или имени пользователя, записанному в обратном порядке, или легко формируется из имени пользователя и т.д.);
- паролем является слово или фраза какого-либо языка; такие пароли могут быть подобраны за ограниченное время путем перебора всех слов согласно словарю;
- достаточно часто пользователи применяют короткие пароли, которые взламываются простым перебором всех возможных вариантов.
- Существуют свободно доступны различные утилиты подбора паролей, в том числе, специализированные для конкретных широкораспространенных программных средств.
- Пароль может быть получен путем применения насилия к его владельцу.
- Пароль может быть подсмотрен или перехвачен при вводе.
- Самая простая идея одноразовых паролей заключается в том, что пользователь получает **список паролей** P_1, P_2, \dots, P_n . Каждый из паролей действует только на один сеанс входа (P_1 — на первый, P_2 — на второй и т.д.). В этом случае знание уже использовавшегося пользователем пароля ничего не даст нарушителю, а при каждом входе легального пользователя возможна проверка на использование данного пароля кем-либо еще.
- Подобная схема имеет свои **трудности**:
 - организация защищенного хранения длинного списка паролей (либо его запоминание, что маловероятно);

- неясность с номером следующего пароля, если после ввода предыдущего пароля из списка вход пользователя в систему не был осуществлен из-за сбоя в работе КС.
- Указанные недостатки могут быть устранены, если список паролей **генерировать на основе некоторой необратимой функции**, например функции хеширования.
- **Хэширование** – ввод информации любой длины и размера в исходной строке и выдачу результата фиксированной длины, заданной алгоритмом функции хэширования.
- Примеры алгоритмов хеширования: md5, sha-1, CRC32, ГОСТ Р 34.11-2012
 - При сбое в процессе входа пользователя всегда осуществляется выбор следующего пароля из списка, а система последовательно применяет функцию F к введенному пользователем паролю, вплоть до совпадения с последним принятым от него паролем (и тогда пользователь допускается к работе в системе) или до превышения длины списка паролей (в этом случае попытка входа пользователя в КС отвергается). На базе этой идеи и работают все современные технологии аутентификации с помощью одноразовых паролей.

Метод запрос-ответ

- Принцип работы:
- Пользователь отправляет на сервер свой логин.
- Сервер генерирует некую случайную строку и посылает ее обратно.

- Пользователь с помощью своего ключа зашифровывает эти данные и возвращает их серверу.
- Сервер же в это время «находит» в своей памяти секретный ключ данного пользователя и кодирует с его помощью исходную строку.
- Сравнение обоих результатов шифрования. При их полном совпадении считается, что аутентификация прошла успешно.
- Этот метод реализации технологии одноразовых паролей называется **асинхронным**, поскольку процесс аутентификации не зависит от истории работы пользователя с сервером и других факторов.

Метод только ответ

- В этом случае алгоритм аутентификации несколько проще:
- Программное или аппаратное обеспечение пользователя генерирует исходные данные, которые будут зашифрованы и отправлены на сервер для сравнения. В процессе создания строки используется значение предыдущего запроса.
- Сервер тоже обладает этими сведениями; зная имя пользователя, он находит значение предыдущего его запроса и генерирует по тому же алгоритму точно такую же строку.
- Зашифровав ее с помощью секретного ключа пользователя (он также хранится на сервере), сервер получает значение, которое должно полностью совпадать с присланными пользователем данными.

Метод синхронизации по времени

- В нем в качестве исходной строки выступают текущие показания таймера специального устройства или компьютера, на котором работает человек. При этом обычно используется

не точное указание времени, а текущий интервал с установленными заранее границами (например, 30 с).

- Эти данные зашифровываются с помощью секретного ключа и в открытом виде отправляются на сервер вместе с именем пользователя.
- Сервер при получении запроса на аутентификацию выполняет те же действия: получает текущее время от своего таймера и зашифровывает его.
- После этого сервер сравнивает два значения: вычисленное и полученное от удаленного компьютера.

Метод синхронизации по событию

- Этот метод практически идентичен предыдущему.
- В качестве исходной строки в нем используется не время, а количество успешных процедур аутентификации, проведенных до текущей.
- Это значение подсчитывается обеими сторонами отдельно друг от друга.
- В настоящее время этот метод получил наиболее широкое распространение.
- В некоторых системах реализуются так называемые смешанные методы, где в качестве начального значения используется два типа информации или больше. Например, существуют системы, которые учитывают как счетчики аутентификаций, так и показания встроенных таймеров. Такой подход позволяет избежать недостатков отдельных методов.

- Наиболее известным программным *генератором одноразовых паролей* является система **S/KEY** компании Bellcore. Идея этой системы состоит в следующем. Пусть имеется **односторонняя функция** f (то есть функция, вычислить обратную которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и **серверу аутентификации**. Пусть, далее, имеется **секретный ключ** K , известный только пользователю.
- **Kerberos**— это программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

Биометрия

- **Биометрия** - это идентификация человека по уникальным биологическим признакам. Методы биометрической идентификации делятся на **две группы**:
- **1. Статические методы**
- Основываются на уникальной физиологической (статической) характеристике человека, данной ему от рождения и неотъемлемой от него.
- **2. Динамические методы**
- Основываются на поведенческой (динамической) характеристике человека, построены на особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия.

Статические методы

- **По отпечатку пальца.**

- По форме ладони.
- По расположению вен на лицевой стороне ладони.
- По сетчатке глаза.
- По радужной оболочке глаза.
- По форме лица.
- По термограмме лица.
- По ДНК.
- Другие методы.

Динамические методы

- По рукописному почерку.
- По клавиатурному почерку.
- По голосу.
- Другие методы.
- С целью более широкого применения биометрических технологий, производители биометрических систем разработали ряд унифицированных программных интерфейсов приложений: *BAPI*, *HA-API*, *SVAPI*, *BioAPI*.
- Из них наиболее универсальным является интерфейс *BioAPI*.

В интерфейсе *BioAPI* определены два уровня.

- Уровень '*H*' (*high*) является «верхним» уровнем, на котором выполняются основные биометрические функции, вызываемые приложением для идентификации (аутентификации) человека
- Уровень *SPI* (*Service Provider Interface*) определяет интерфейс к практически любой поддерживающие этот интерфейс

биометрической системе, устройства или программному обеспечению

Для верхнего уровня определены три основные абстрактные функции:

- *Enroll* (регистрация).
- *Verify* (верификация, распознавание один к одному).
- *Identify* (идентификация, распознавание один ко многим).

Для клиент-серверной обработки биометрических данных используют следующие базовые функции:

- *Process* (Обработка).
- *Match* (Сопоставление).
- *CreateTemplate* (Создание шаблона).
- *StreamingCallback* (Потоковый обратный вызов).

Полезные стороны биометрических технологий:

- запрос и получение качества биометрических данных при их фиксации и обработке;
- запрос и получение фактических вероятностных характеристик биометрической системы для конкретного пользователя;
- управление графическим интерфейсом пользователя (*GUI*) со стороны приложения;
- обнаружение источника биометрических данных;
- использование клиент-серверной технологии;
- адаптация шаблонов;
- работа с автономными биометрическими устройствами;

- ограничение размерности области поиска в базах данных при идентификации один ко многим.

Недостатки биометрических систем:

- Необходимо учитывать, что биометрия подвержена тем же угрозам, что и другие методы аутентификации.
- Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти.
- Во-вторых, биометрические методы не более надежны, чем база данных шаблонов.
- В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в "полевых" условиях, когда, например к устройству сканирования роговицы могут поднести муляж и т.п.
- В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

Управление доступом

- С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над **объектами** (информацией и другими компьютерными ресурсами).

- Логическое управление доступом – это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).
- При принятии решения о предоставлении доступа обычно анализируется следующая информация:
 - идентификатор субъекта (идентификатор пользователя, сетевой адрес компьютера и т.п.). Подобные идентификаторы являются основой **произвольного (или дискреционного) управления доступом**;
 - атрибуты субъекта (метка безопасности, группа пользователя и т.п.). Метки безопасности – основа **принудительного (мандатного) управления доступом**.
- Матрицу доступа, ввиду ее разреженности (большинство клеток – пустые), неразумно хранить в виде двумерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами.
- Списки доступа – исключительно гибкое средство. С их помощью легко выполнить требование о гранулярности прав с точностью до пользователя. Посредством списков несложно добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством произвольного управления доступом.
- Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное

управление доступом. Основное достоинство произвольного управления – гибкость. Где для каждой пары "субъект-объект" можно независимо задавать права доступа.

Недостатки произвольного управления доступом:

- 1. Рассредоточенность управления доступом ведет к тому, что доверенными должны быть многие пользователи, а не только системные операторы или администраторы. Из-за рассеянности или некомпетентности сотрудника, владеющего секретной информацией, эту информацию могут узнать и все остальные пользователи.
- 2. Права доступа существуют отдельно от данных. Ничто не мешает пользователю, имеющему доступ к секретной информации, записать ее в доступный всем файл или заменить полезную утилиту ее "троянским" аналогом.

Ролевое управление:

- Между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права
- **Пользователь** (человек, интеллектуальный автономный агент и т.п.);
- **Сеанс работы пользователя;**
- **Роль** (обычно определяется в соответствии с организационной структурой);
- **Объект** (сущность, доступ к которой разграничивается; например, файл ОС или таблица СУБД);
- **Операция** (зависит от объекта; для файлов ОС – чтение, запись, выполнение и т.п.; для таблиц СУБД – вставка,

удаление и т.п., для прикладных объектов операции могут быть более сложными);

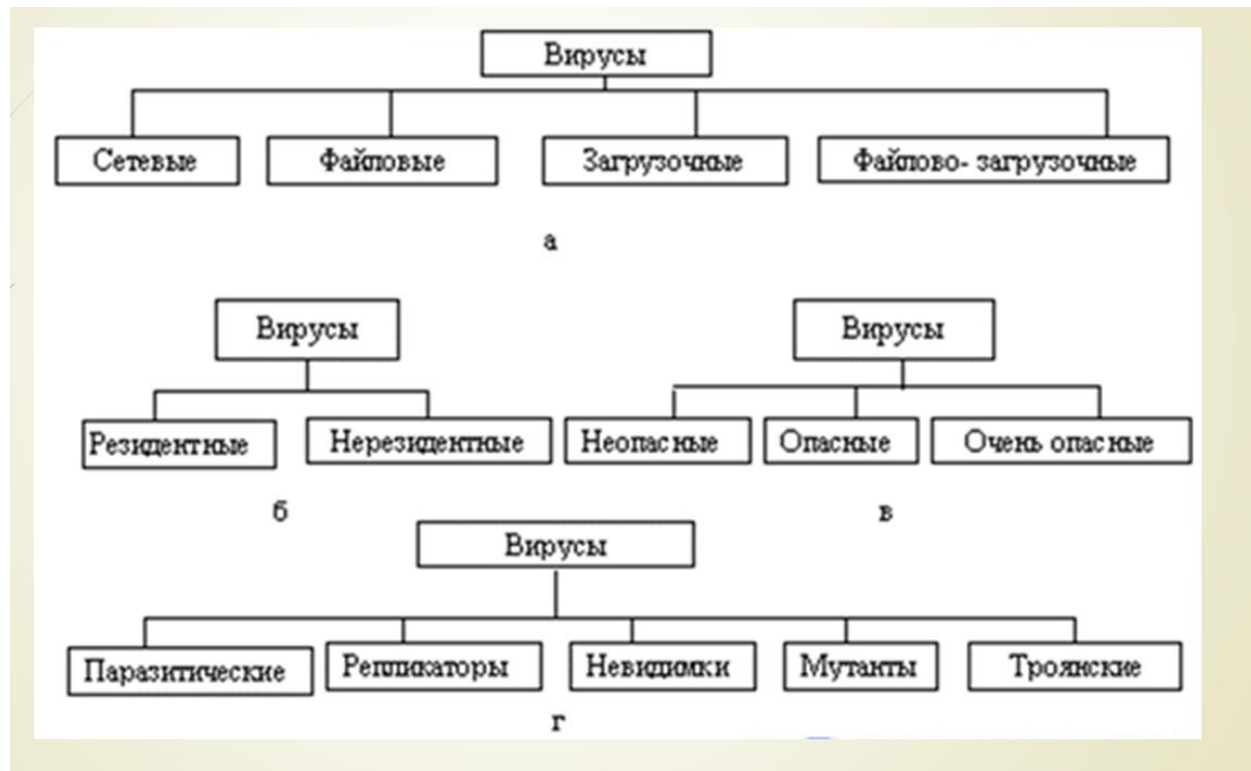
- **Право доступа** (разрешение выполнять определенные операции над определенными объектами).
- **Статическое разделение обязанностей** налагает ограничения на **приписывание пользователей ролям**. В простейшем случае членство в некоторой роли запрещает приписывание пользователя определенному множеству других ролей. В общем случае данное ограничение задается как пара "множество ролей – число" (где множество состоит, по крайней мере, из двух ролей, а число должно быть больше 1), так что никакой пользователь не может быть приписан указанному (или большему) числу ролей из заданного множества. Например, может существовать пять бухгалтерских ролей, но политика безопасности допускает членство не более чем в двух таких ролях (здесь число=3).
- **Динамическое разделение обязанностей** отличается от статического только тем, что рассматриваются роли, одновременно активные (быть может, в разных сеансах) для данного пользователя (а не те, которым пользователь статически приписан). Например, один пользователь может играть роль и кассира, и контролера, но не одновременно; чтобы стать контролером, он должен сначала закрыть кассу. Тем самым реализуется так называемое **временное ограничение доверия**, являющееся аспектом минимизации привилегий.

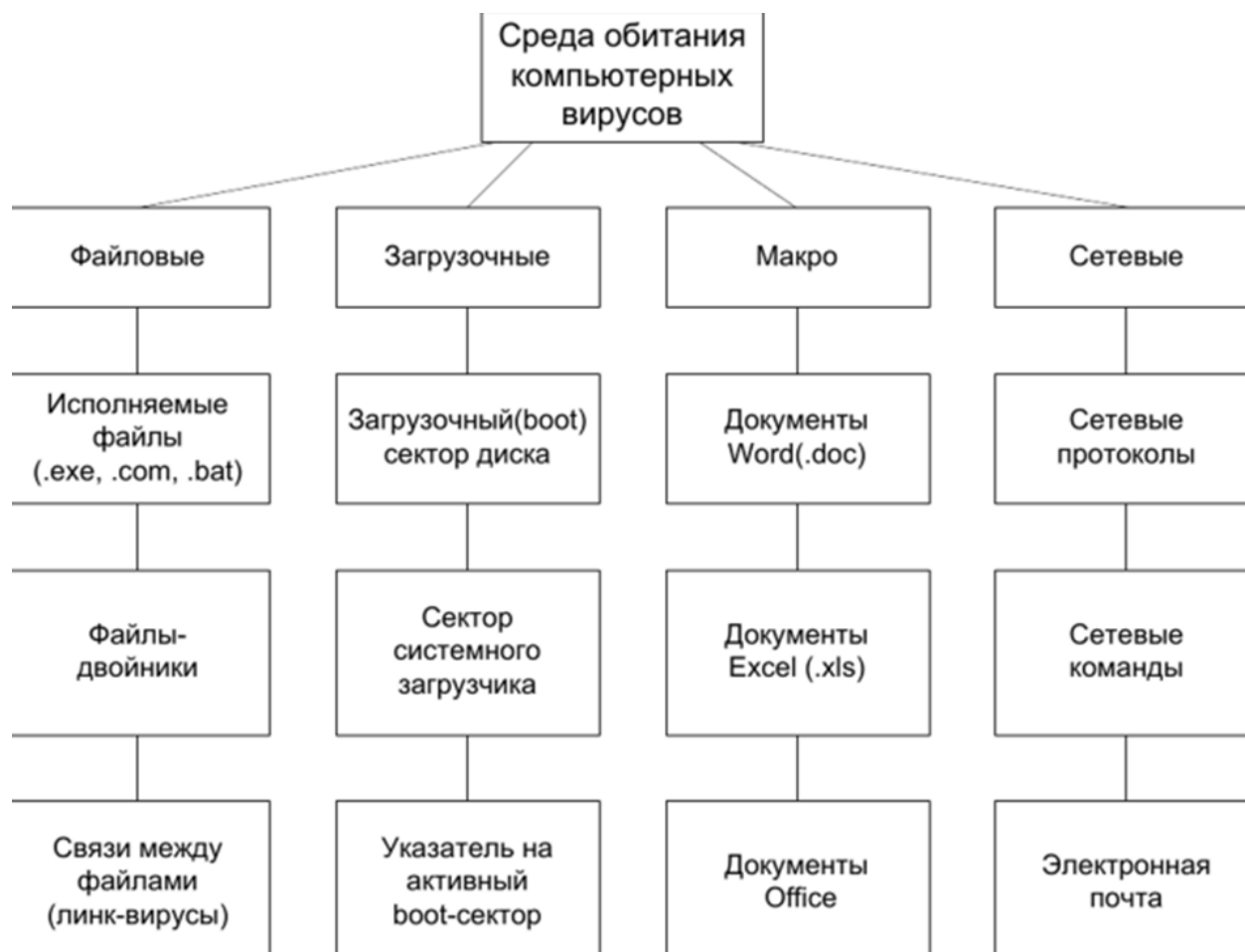
Компьютерные вирусы

- **Компьютерный вирус** – это специально написанная программа, способная самопроизвольно присоединяться к другим программам (заражать их), создавать свои копии и

внедрять их в файлы, системные области компьютера и другие объединенные с ним компьютеры в целях нарушения нормальной работы программ, порчи файлов и каталогов, а также создания разных помех при работе на компьютере.

Классификация компьютерных вирусов





Классификация вирусов по среде обитания:

- **Загрузочные вирусы** внедряются в загрузочный сектор диска или в сектор, который содержит программу загрузки системного диска.
- **Файловые вирусы** помещаются в основном в исполняемых файлах с расширением .COM и .EXE.
- **Системные вирусы** внедряются в системные модули и драйверы периферийных устройств, таблицы размещения файлов и таблицы разделов.
- **Сетевые вирусы** находятся в компьютерных сетях, а **файлово-загрузочные** – заражают загрузочные секторы дисков и файлы прикладных программ.

Классификация вирусов по пути заражения:

- *Резидентные вирусы* при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая после заражения перехватывает обращение ОС к другим объектам заражения, внедряется в них и выполняет свои разрушительные действия, которые могут привести к выключению или перезагрузке компьютера. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.
- *Нерезидентные вирусы* не заражают ОП компьютера и проявляют активность ограниченное время.
- *Логическая бомба* является программой, которая встраивается в большой программный комплекс. Она безвредна до наступления определенного события, после которого реализуется ее логический механизм.
- *Программы-мутанты*, самовоспроизводясь, создают копии, явно отличающиеся от оригинала.
- *Вирусы-невидимки*, или стелс-вирусы, перехватывают обращения ОС к пораженным файлам и секторам дисков и подставляют вместо себя незараженные объекты. Эти вирусы при обращении к файлам применяют достаточно оригинальные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы.
- *Макровирусы* используют возможности макроязыков, которые встроены в офисные программы обработки данных (текстовые редакторы, электронные таблицы).

По степени воздействия на ресурсы компьютерных систем и сетей, или по деструктивным возможностям, выделяют:

- *Безвредные вирусы* не оказывают патологического влияния на работу компьютера.
- *Неопасные вирусы* не разрушают файлы, однако уменьшают свободную дисковую память, выводят на экран графические или звуковые эффекты.
- *Опасные вирусы* часто вызывают значительные нарушения в работе компьютера.
- *Разрушительные вирусы* могут привести к стиранию информации, полному или частичному нарушению работы прикладных программ. Важно иметь в виду, что любой файл, способный к загрузке и выполнению кода программы, является потенциальным местом, где может помещаться вирус.
- ***Файловые вирусы*** либо внедряются в выполняемые файлы (наиболее распространенный тип вирусов) различными способами, либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы). *Файловые вирусы* внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управления и, следовательно, теряют способность к размножению. Обычно файловые вирусы размещаются в конце файла или в его начальной части, реже в середине файла.
- ***Загрузочные вирусы*** записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (MasterBoot Record). Загрузочные вирусы замещают код программы, получающей

управление при загрузке системы. В результате при перезагрузке управление передается вирусу. При этом оригинальный boot-сектор обычно переносится в какой-либо другой сектор диска. Иногда загрузочные вирусы называют бутовыми вирусами. Они заражают макропрограммы и файлы документов современных систем обработки информации, в частности файлы-документы и электронные таблицы популярных редакторов Microsoft Word, Microsoft Excel и др. Для размножения макровирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла в другие. Вирусы этого типа получают управление при открытии зараженного файла и инфицируют файлы, к которым впоследствии идет обращение из соответствующего офисного приложения.

- **Файлово - загрузочные вирусы** заражают как файлы, так и загрузочные сектора дисков.
- **Сетевые вирусы** используют для своего распространения протоколы или команды компьютерных сетей и электронной почты. Иногда сетевые вирусы называют программами типа «червь». Сетевые черви подразделяются на Internet-черви (распространяются по Internet), LAN-черви (распространяются по локальной сети), IRC-черви Internet Relay Chat (распространяются через чаты). Существуют также смешанные типы, которые совмещают в себе сразу несколько технологий. *Сетевые вирусы* распространяются по различным компьютерным сетям. Их первые реализации -- mIRC.Acoragil и mIRC. Simpsalarim -- относятся 1997 г. Названия эти вирусы получили по используемым кодовым словам. Стоило ввести слова Acoragil и Simpsalarim, как вирусы тут же отключали пользователей от канала.

Жизненный цикл вирусов

- *латентный период(стадия хранения)*, в течение которого вирусом никаких действий не предпринимается;
- *2. инкубационный период(первая стадия исполнения)*, в рамках которого вирус только размножается;
- *3. период проявления(вторая стадия исполнения)*, в течение которого наряду с размножением выполняется несанкционированные пользователем действия.
- **Стадия хранения** соответствует периоду, когда вирус просто хранится на диске совместно с объектом, в который он внедрен. На этой стадии вирус является наиболее уязвимым со стороны антивирусного ПО, так как он не активен и не может контролировать работу ОС с целью самозащиты.
- Некоторые вирусы на этой стадии используют механизмы защиты своего кода от обнаружения. Наиболее распространенным способом защиты является шифрование большей части тела вируса. Его использование совместно с механизмами мутации кода делает невозможным выделение сигнатур — устойчивых характеристических фрагментов кода вирусов.
- **Стадия исполнения** компьютерных вирусов, как правило, включает пять этапов:
 - 1) загрузка вируса в память;
 - 2) поиск жертвы;
 - 3) заражение найденной жертвы;
 - 4) выполнение деструктивных функций;
 - 5) передача управления программе-носителю вируса.
- Загрузка вируса в память осуществляется ОС одновременно с загрузкой исполняемого объекта, в который вирус внедрен. Например, если пользователь запустил на исполнение

программный файл, содержащий вирус, то, очевидно, вирусный код будет загружен в память как часть этого файла.

- *Полиморфные вирусы* (polymorphic) — это трудно обнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Полиморфизм встречается в вирусах всех типов — файловых, загрузочных и макровирусах.
- Дополнительные действия, которые выполняют полиморфные вирусы на этапе загрузки, состоят в расшифровывании основного тела вируса.
- *Стелс-вирусы* (Stealth) способны скрывать свое присутствие в системе и избегать обнаружения антивирусными программами. Эти вирусы могут перехватывать запросы ОС на чтение/запись зараженных файлов, при этом они либо временно лечат эти файлы, либо «подставляют» вместо себя незараженные участки информации, эмулируя «чистоту» зараженных файлов.
- К первому классу относятся вирусы, осуществляющие «активный» поиск с использованием функций ОС. Примером являются файловые вирусы, использующие механизм поиска исполняемых файлов в текущем каталоге.
- Второй класс составляют вирусы, реализующие «пассивный» механизм поиска, т.е. вирусы, расставляющие «ловушки» для программных файлов. Как правило, файловые вирусы устраивают такие ловушки путем перехвата функции Exec ОС, а макровирусы - с помощью перехвата команд типа Save as из меню File.

- В простейшем случае заражение представляет собой самокопирование кода вируса в выбранный в качестве жертвы объект. Классификация вирусов на этом этапе связана с анализом особенностей этого копирования и способов модификации заражаемых объектов.

Заражение файловыми вирусами:

- К первому классу относятся вирусы, которые не внедряют свой код непосредственно в программный файл, а изменяют имя файла и создают новый, содержащий тело вируса.
- Второй класс составляют вирусы, внедряющиеся непосредственно в файлы-жертвы. Они характеризуются местом внедрения.

- *Варианты внедрения вирусов в файлы:*

- *Внедрение в начало файла.*
- *Внедрение в конец файла.*
- *Внедрение в середину файла.*

- *Особенности заражения загрузочными вирусами* определяются особенностями объектов, в которые они внедряются, — загрузочными секторами жестких дисков и главной загрузочной записью (MBR) жестких дисков.

- Существуют различные способы решения этой задачи. Ниже приводится классификация, предложенная Е. Касперским:

- *Используются псевдосбойные секторы.*
- *Используются редко применяемые секторы в конце раздела.*
- *Используются зарезервированные области разделов.*

- *Короткие вирусы могут уместиться в один сектор загрузчика и полностью взять на себя функции MBR или загрузочного сектора.*
- Процесс заражения сводится к сохранению вирусного макроязыка в выбранном документе-жертве.
- По деструктивным возможностям вирусы можно разделить на следующие категории:
 - Безвредные.
 - Неопасные.
 - Опасные.
 - Очень опасные.

Передача управления программе-носителю вируса

- Разрушающие вирусы не заботятся о сохранении работоспособности инфицированных программ, поэтому для них этот этап функционирования отсутствует.
- Для неразрушающих вирусов этот этап связан с восстановлением в памяти программы в том виде, в котором она должна корректно исполняться, и передачей управления программе-носителю вируса.

Основные каналы распространения вирусов и других
вредоносных программ

- **Классические способы распространения**
- **Электронная почта**
- **Троянские Web-сайты**
- **Локальные сети**
- **Другие каналы распространения вредоносных программ**


Признаки появления вирусов:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файла и каталога или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.
- **Ложные антивирусы** (также известные как «scareware») – это программы, которые внешне похожи на приложения для обеспечения безопасности компьютера, но в действительности такой защиты почти или совсем не обеспечивают, генерируют ошибочные или заведомо ложные уведомления об угрозах или пытаются вовлечь пользователя в мошеннические операции.

Виды антивирусных программ:

- Программы-детекторы;

- Программы-доктора или фаги;
- Программы-ревизоры;
- Программы-фильтры;
- Программы-вакцины или иммунизаторы.

Бесплатные антивирусы		Итоговая оценка		Надежность		Потребление ресурсов		Скорость работы		Ложные срабатывания		Функциональность		Интерфейс	
	Avast! Free Antivirus	4,7	5	4	5	5	4	5	4	5					
	Kaspersky Free	4,5	5	3	5	5	4	5	4	5					
	AVG AntiVirus Free	4,5	5	5	5	5	3	5	4						
	Panda Cloud Antivirus	4,5	5	5	5	5	3	5	4						
	360 Total Security	4,3	5	5	4	4	5	3							
	Avira Free Antivirus	4,3	4	4	5	4	4	5							
	Zillya! Antivirus Free	4,2	4	5	5	4	3	4							
	Bitdefender Antivirus Free	4,2	5	5	4	5	3	3							
	Comodo Antivirus	4,0	4	4	4	4	3	5							
	Microsoft Security Essentials	3,8													

moiProgrammy.net
скачать программы для Windows

К объектам интеллектуальной собственности в Республике Беларусь относятся:

- 1) результаты интеллектуальной деятельности:
 - – объекты авторского права и смежных прав.
 - – объекты патентного права.
- 2) средства индивидуализации участников гражданского оборота, товаров, работ или услуг.
- 3) другие результаты интеллектуальной деятельности и средства индивидуализации участников гражданского оборота, товаров, работ или услуг в случаях, предусмотренных Гражданским кодексом РБ и иными законодательными актами.

Интеллектуальную собственность делят на две составляющие:

- 1) промышленную собственность; 2) авторское право
- К промышленной собственности относятся промышленные образцы, изобретения, полезные модели, товарные знаки, знаки обслуживания и фирменные наименования.
- Авторское право относится к произведениям искусства, литературным и музыкальным произведениям, творениям кинематографии, а также к научным произведениям.

Систему белорусского права интеллектуальной собственности (ИС) составляют следующие институты:

- а) авторское право;
- б) права, смежные с авторским;
- в) патентное право;
- г) право интеллектуальной собственности на товарный знак;
- д) право интеллектуальной собственности на фирменное наименование;
- е) право интеллектуальной собственности на топологии интегральных схем;
- ж) право интеллектуальной собственности на программы для ЭВМ и базы данных;
- з) право интеллектуальной собственности на селекционные достижения;
- и) правоотношения в сфере коммерческой и служебной тайны.

Система источников права интеллектуальной собственности

- 1) Конституция Республики Беларусь.
- 2) Гражданский кодекс Республики Беларусь.
- 3) Таможенный кодекс Республики Беларусь.
- 4) Уголовный кодекс Республики Беларусь.
- 5) Инвестиционный кодекс Республики Беларусь.
- 6) законы Республики Беларусь.
- 7) указы Президента Республики Беларусь;
- 8) постановления Правительства Республики Беларусь;
- 9) международные договоры и соглашения.

**Право промышленной собственности в Республике Беларусь
распространяется на:**

- 1) изобретения;
- 2) полезные модели;
- 3) промышленные образцы;
- 4) селекционные достижения;
- 5) технологии интегральных микросхем;
- 6) нераскрытую информацию, в том числе секреты производства (ноу-хау);
- 7) фирменные наименования;
- 8) товарные знаки (знаки обслуживания);
- 9) наименования мест происхождения товаров;
- 10) другие объекты ПС и средства индивидуализации участников гражданского оборота товаров, работ или услуг в случаях, предусмотренных законодательством

Авторское право

- Законодательство Республики Беларусь об авторском праве и смежных правах основывается на Конституции Республики Беларусь и состоит из Гражданского кодекса Республики Беларусь, Закона Республики Беларусь «Об авторском праве и смежных правах», нормативных правовых актов Президента и Правительства Республики Беларусь, других актов законодательства Республики Беларусь.

Основные положения авторского права:

- Авторское право распространяется на произведения науки, литературы и искусства, существующие в какой-либо объективной форме. Оно возникает в силу факта их создания. Для возникновения и осуществления авторского права не требуется соблюдения каких-либо формальностей.
- Субъектами авторского права являются авторы (соавторы), наследники и иные правопреемники.
- Первичными субъектами авторского права являются авторы произведений. Автор – физическое лицо, творческим трудом которого создано произведение. Если произведение создано совместным творческим трудом двух или более лиц, они признаются соавторами. При отсутствии доказательств иного автором произведения считается лицо, указанное в качестве автора на оригинале или экземпляре произведения (презумпция авторства).

По закону субъектами авторского права в части имущественных прав, кроме авторов произведений, могут быть:

- наследники авторов;
- наниматели авторов служебных произведений;

- юридические лица и физические лица, заключившие с авторами и их наследниками договоры на использование произведений науки, литературы и искусства;
- правопреемники юридических и физических лиц;
- организации, управляющие имущественными правами авторов на коллективной основе.

Классификация объектов авторского права:

- Авторское право распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой-либо объективной форме:
 - письменной (рукопись, машинопись, нотная запись и др.);
 - устной (публичное произнесение, публичное исполнение и др.);
 - звуко- или видеозаписи (механическая, магнитная, цифровая, оптическая и др.);
 - изображения (рисунок, эскиз, картина, карта, план, чертеж, кино-, теле-, видео-, фотокадр и др.);
 - объемно-пространственной (скульптура, модель, макет, сооружение и др.);
 - электронной, в том числе цифровой.

Объекты авторского права:

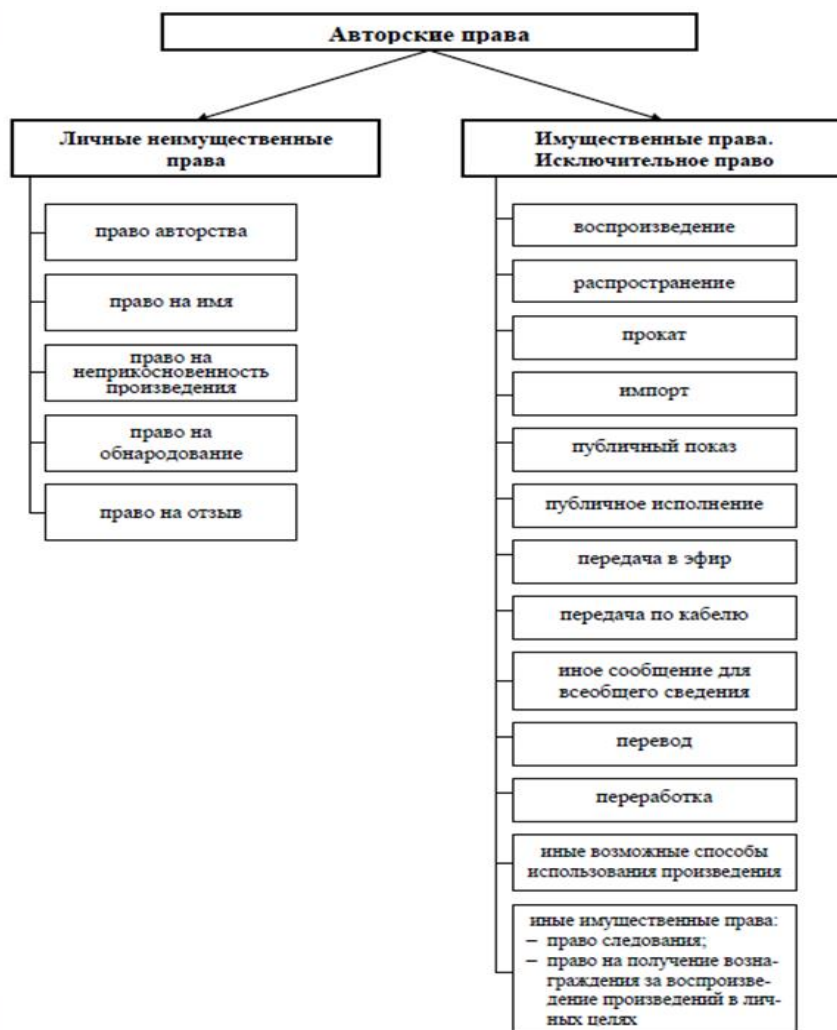
- литературные произведения;
- драматические и музыкально-драматические произведения, произведения хореографии и пантомимы и другие сценарные произведения;

- музыкальные произведения с текстом и без текста;
- аудиовизуальные произведения;
- произведения изобразительного искусства;
- произведения прикладного искусства и дизайна;
- произведения архитектуры, градостроительства и садово-паркового искусства;
- фотографические произведения, в том числе произведения, полученные способами, аналогичными фотографии;
- карты, планы, эскизы, иллюстрации и пластические произведения, относящиеся к географии, картографии и другим наукам;
- компьютерные программы;
- произведения науки;
- *производные произведения*;
- *составные произведения* – сборники.

Не являются
объектами авторского права:

- официальные документы (правовые акты, судебные постановления, иные документы административного и судебного характера, учредительные документы организаций), а также их официальные переводы;
- государственные символы и знаки (флаг, герб, гимн, государственные награды, денежные и иные знаки, почтовые марки);
- произведения народного творчества, авторы которых не известны.

- **Авторское право не распространяется** на собственно идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты, даже если они выражены, отображены, объяснены или воплощены в произведении.
- Смежные права являются производными от авторских прав. Они распространяются на:
 - исполнения;
 - фонограммы;
 - передачи организаций эфирного или кабельного вещания.



Личные неимущественные права:

- **право авторства;**

- **право на имя;**
- **право на неприкосновенность произведения;**
- **право на обнародование;**
- **право на отзыв.**

Использованием произведения признаются:

- воспроизведение произведения;
- распространение оригинала или экземпляров;
- прокат оригиналов или экземпляров произведения;
- импорт экземпляров произведения;
- публичный показ оригинала или экземпляров произведения;
- публичное исполнение произведения;
- передача произведения в эфир;
- передача произведения по кабелю;
- иное сообщение произведения для всеобщего сведения;
- перевод произведения на другой язык;
- переработка произведения для создания производного произведения;

иные возможные способы использования произведения.

Служебные произведения:

- К **служебным** относятся произведения науки, литературы, искусства (их части, имеющие самостоятельное значение), созданные автором по заданию нанимателя или в порядке выполнения обязанностей, обусловленных трудовым договором.

- Исключительное право на служебное произведение с момента его создания переходит к нанимателю, если иное не предусмотрено договором между ним и автором. В случаях, предусмотренных договором между нанимателем и автором, если исключительное право на служебное произведение принадлежит нанимателю, автор (наследники автора) имеет право на получение авторского вознаграждения за использование этого произведения.
- Автор или иной правообладатель для оповещения о принадлежащем им исключительном праве на произведение вправе по своему усмотрению использовать знак охраны авторского права, который помещается на каждом экземпляре произведения и обязательно состоит из трех элементов:
 - латинской буквы «С» в окружности;
 - имени (наименования) правообладателя;
 - года первого опубликования произведения.

Исполнителю в отношении его исполнения принадлежат личные неимущественные права:

- *право авторства в отношении исполнения;*
- *право на имя;*
- *право на неприкосновенность исполнения.*

Использованием исполнения признаются:

- запись исполнения;
- воспроизведение записи исполнения;
- распространение записи исполнения посредством продажи или иной передачи права собственности;

- прокат оригинала или экземпляров записи исполнения;
- публичное исполнение записи исполнения, а также публичное исполнение постановки режиссера-постановщика спектакля или ее записи;
- передача исполнения или его записи в эфир;
- передача исполнения или его записи по кабелю;
- иное сообщение исполнения для всеобщего сведения;
- иные возможные способы использования исполнения.

Сроки действия авторского права и смежных прав:

- Личные неимущественные права на произведения науки, литературы и искусства охраняются бессрочно.
- Имущественные права действуют в течение всей жизни автора и 50 лет после его смерти.
- Имущественные права на произведение, созданное в соавторстве, действуют в течение всей жизни и 50 лет после смерти последнего автора, пережившего других соавторов. Исчисление сроков начинается с 1 января года, следующего за годом, в котором имел место юридический факт, являющийся основанием для начала течения срока.
- Истечение срока действия исключительного права на объекты авторского права или смежных прав означает переход этих объектов в общественное достояние. Объекты авторского права или смежных прав, которым на территории Республики Беларусь охрана никогда не предоставлялась, также считаются перешедшими в общественное достояние.
- Объекты авторского права или смежных прав, перешедшие в общественное достояние, могут свободно использоваться

любым физическим или юридическим лицом без выплаты вознаграждения. При этом должны соблюдаться личные неимущественные права.

- В целях обеспечения имущественных прав авторов или иных правообладателей в случаях, когда их практическое осуществление в индивидуальном порядке затруднительно, а также в случаях, когда законодательством предусмотрена выплата вознаграждения за использование произведений или объектов смежных прав, осуществляемое без согласия авторов или иных правообладателей, могут создаваться организации по коллективному управлению имущественными правами.