Лекция 6
Защита информации в информационных системах управления

Изучаемые вопросы

1. Актуальность проблемы информационной безопасности (ИБ).

2. Способы и средства защиты информации (СЗИ). Электронная цифровая подпись.

3. Архитектура и организационное построение системы защиты информации в ИСУ предприятия.

1. Актуальность проблемы информационной безопасности (ИБ).

Вместе с развитием способов и методов преобразования передачи информации постоянно развиваются и методы обеспечения ее безопасности. Современный этап развития этой проблемы характеризуется переходом от традиционного ее представления как проблемы защиты информации к более широкому пониманию — проблеме **информационной безопасности** (ИБ), заключающейся в комплексном ее решении по двум основным направлениям.

- К **первому направлению** можно отнести защиту государственной тайны и конфиденциальных сведений, обеспечивающую главным образом невозможность несанкционированного доступа к ним. При этом под конфиденциальными сведениями понимаются сведения ограниченного доступа общественного характера (*коммерческая тайна*, *партийная тайна* и т.д.), а также личная конфиденциальная информация (*персональные данные*, *интеллектуальная собственность* и т.д.).
- Ко **второму направлению** относится защита от информации, которая в последнее время приобретает международный масштаб и стратегический характер. При этом выделяются три основных направления защиты от так называемого информационного оружия (воздействия):
  - на технические системы и средства;
  - общество;
  - психику человека.

Основные понятия

Информационная безопасность (ИБ)	-	состояние защищенности потребностей личности, общества и государства, при котором обеспечиваются их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз. (соответствии с «ГОСТ Р 50922-96. Защита информации. Основные термины и определения»)
Угроза безопасности	-	совокупности условий, факторов, создающих опасность жизненно важным интересам личности, общества и государства. (закон РФ «О безопасности» №2446-1 от 5 марта 1992 года)
Угроза информационной безопасности	-	воздействие дестабилизирующих факторов на состояние информированности, подвергающее опасности жизненно важные интересы личности, общества и государства.

Категории информации

ИНФОРМАЦИЯ
(ст. 1 ФЗ 27.08.2006 N 149-ФЗ)
сведения (сообщения, данные) независимо от формы их представления

ОБЩЕДОСТУПНАЯ
(ст. 7 ФЗ 27.08.2006 N 149-ФЗ)

- общеизвестные сведения и иная информация, доступ к которой не ограничен;
- обладатель информации установил общедоступный режим доступа

(ст. 8 ФЗ 27.08.2006 N 149-ФЗ)

- нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления,
- информация о состоянии окружающей среды;
- информация о деятельности государственных органов и органов местного самоуправления (за исключением сведений, составляющих государственную или служебную тайну);
- информация, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан и организаций такой информацией;
- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами

ОГРАНИЧЕННОГО ДОСТУПА
(ст. 5 ФЗ 27.08.2006 N 149-ФЗ)
доступ к информации ограничен федеральными законами

КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ
Перечень сведений отнесенных к конфиденциальной информации содержится в Указе Президента РФ N 188 6.03.1997

ГОСУДАРСТВЕННАЯ ТАЙНА
(ст. 1 Закона РФ от 21.07.1993 N 54-85-1)
защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации,

ПЕРСОНАЛЬНЫЕ ДАННЫЕ
(ФЗ 27.07.2006 N 152-ФЗ)
Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

ТАЙНА СЛЕДСТВИЯ И СУДОПРОИЗВОДСТВА
(Указ Президента РФ N 188 6.03.1997)
Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" и другими нормативными правовыми актами Российской Федерации.

СЛУЖЕБНАЯ ТАЙНА
(Указ Президента РФ N 188 6.03.1997)
Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.

ПРОФЕССИОНАЛЬНАЯ ТАЙНА
(Указ Президента РФ N 188 6.03.1997)
Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

КОМЕРЧЕСКАЯ ТАЙНА
(ФЗ 29.07.2004 N 98-ФЗ)
Сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

НОУ-ХАУ
(Указ Президента РФ N 188 6.03.1997)
Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Классификация угроз информационной безопасности

№	Угроза ИБ	Описание
1	Компрометация информации	Внесение несанкционированных изменений в базы данных, которое вынуждает потребителя либо отказаться от нее, либо предпринимать дополнительные усилия для выявления сделанных изменений и восстановления истинных сведений.
2	Несанкционированное использование ресурсов	С одной стороны, является средством доступа к информации с целью ее получения или искажения, кроме того нарушитель, используя ресурсы, сокращает поступление финансовых средств за их использование.
3	Несанкционированный обмен информацией	Возможность получения пользователем сведений, доступ к которым ему закрыт, что равносильно раскрытию информации.
4	Ошибочное использование ресурсов	Может привести к их разрушению или раскрытию конфиденциальной информации. Данная угроза чаще всего является следствием ошибок программного обеспечения.
5	Отказ от информации	Состоит в непризнании получателем или отправителем этой информации факта ее получения или отправления соответственно.
6	Отказ в обслуживании	Опасен в ситуациях, когда задержка с предоставлением ресурсов информационной системы ее пользователю может привести к тяжелым последствиям. Источником этой угрозы является сама вычислительная система, возможные отказы аппаратуры или ошибки в программном обеспечении.

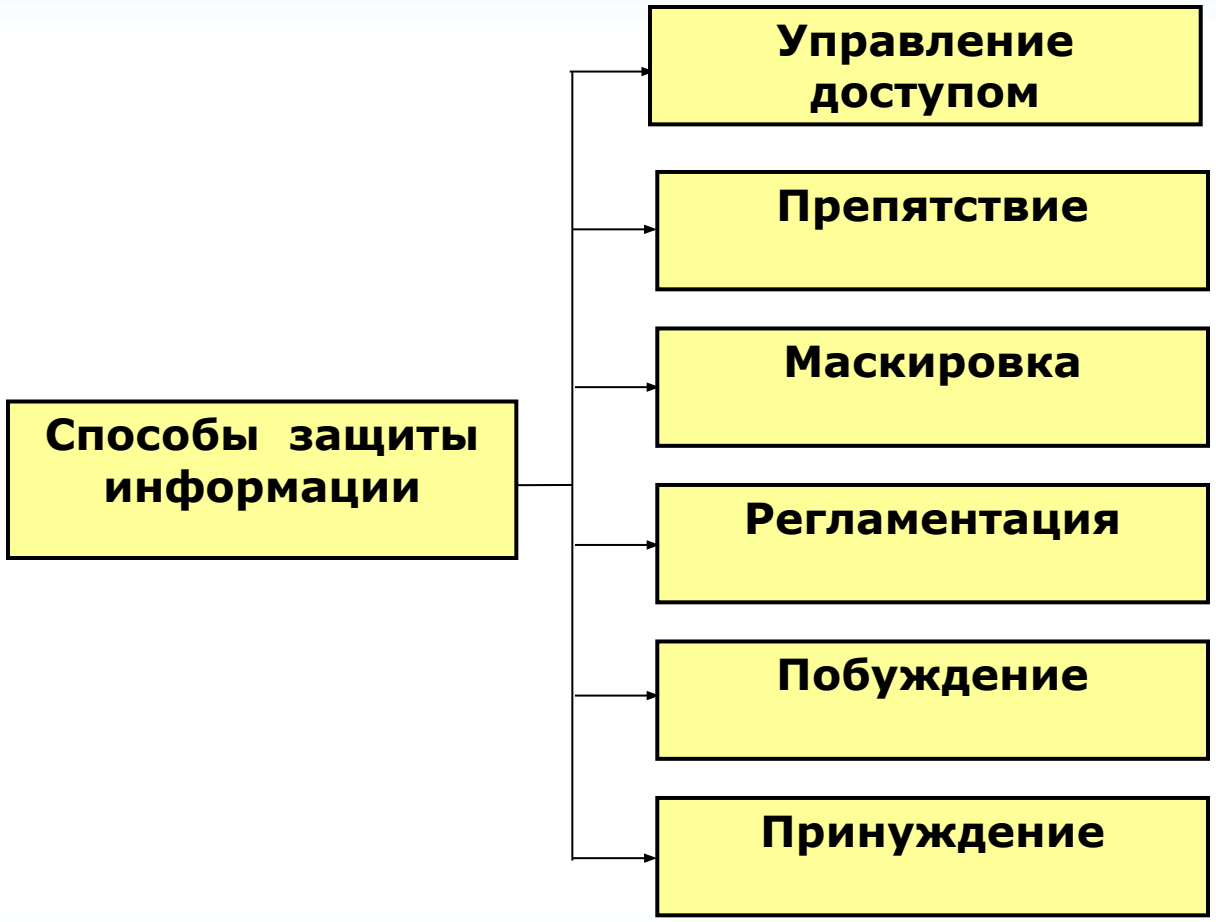
Примеры угроз ИБ, связанные с утечкой информации и несанкционированным доступом

Цели и задачи информационной безопасности

ЦЕЛИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ		
1. Обеспечение защиты системы от обнаружения	2. Обеспечение защиты содержания информации	3. Обеспечение защиты системы от информационного воздействия

КЛАССЫ ЗАДАЧ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ		
1.1. Скрытие 1.2. Дезинформация 1.3. Легендирование	2.1. Введение избыточности 2.2. Регулирование доступа 2.3. Регулирование использования 2.4. Маскировка 2.5. Регистрация 2.6. Уничтожение 2.7. Сигнализация	3.1. Защита от воздействия на технические средства 3.2. Защита от воздействия на общество 3.3. Защита от воздействия на человека

2. Способы и средства защиты информации (СЗИ). Электронная цифровая подпись.


Способы защиты информации
Управление доступом
Препятствие
Маскировка
Регламентация
Побуждение
Принуждение

Способы защиты информации

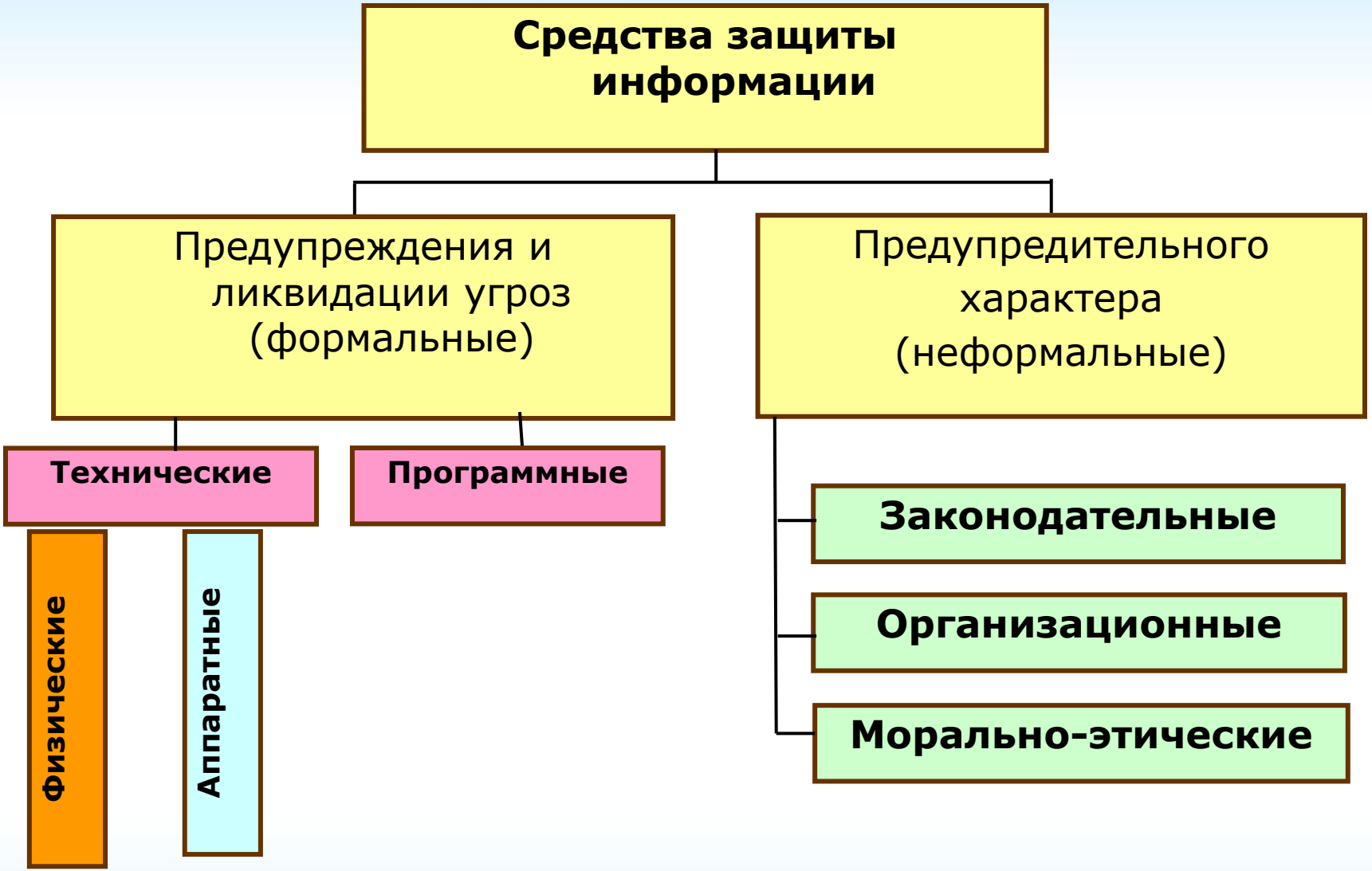
№	Способ	Описание	Пример
1	Препятствие	Заключается в создании на пути возникновения или распространения дестабилизирующего фактора некоторого барьера, не позволяющего соответствующему фактору принять опасные размеры.	Типичными примерами препятствий являются блокировки, не позволяющие техническому устройству или программе выйти за опасные границы; создание физических препятствий на пути злоумышленников, экранирование помещений и технических средств и т. п.
2	Маскировка	Предполагает такие преобразования информации, вследствие которых она становится недоступной для злоумышленников или такой доступ существенно затрудняется, также комплекс мероприятий по уменьшению степени распознавания самого объекта.	К маскировке относятся криптографические методы преобразования информации, скрытие объекта, дезинформация и легендирование, а также меры по созданию шумовых полей, маскирующих информационные сигналы.
3	Регламентация	Заключается в разработке и реализации в процессе функционирования объекта комплекса мероприятий, создающих такие условия, при которых существенно затрудняются проявление и воздействие угроз.	Регламентация обращения с документами в процессе защищенного документооборота заключается в разработке таких правил их учета, хранения, перемещения и уничтожения, которые обеспечивают высокую степень защиты сведений.

Способы защиты информации

№	Способ	Описание	Пример
4	Управление доступом	Определение на каждом шаге функционирования систем обработки информации таких управляющих воздействий на элементы системы, следствием которых будет решение (или способствование решению) одной или нескольких задач по защите информации. Такими управляющими воздействиями являются задачи, обозначенные выше как реагирование на проявление дестабилизирующих воздействий. При этом управление включает в себя в соответствии с законами кибернетики сбор, передачу, обобщение и анализ данных, то есть достигается решением задач класса «Сигнализация» и «Оценка».	Например, управление доступом на объект включает следующие функции защиты: ▪ опознавание (установление подлинности) объекта или субъекта по предъявленному им идентификатору; ▪ проверку полномочий (проверку соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту); ▪ регистрацию (протоколирование) обращений к защищаемым ресурсам; ▪ реагирование (сигнализацию, отключение, задержку работ, отказ в запросе) при попытках несанкционированных действий.

Способы защиты информации

№	Способ	Описание
5	Принуждение	Пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.
6	Побуждение	Пользователи и персонал объекта внутренне (то есть материальными, моральными, этическими, психологическими и другими мотивами) побуждаются к соблюдению всех правил обработки информации.


Средства защиты информации
Предупреждения и ликвидации угроз (формальные)
Предупредительного характера (неформальные)
Технические
Программные
Физические
Аппаратные
Законодательные
Организационные
Морально-этические

Технические средства защиты информации

Технические средства защиты информации

Технические средства защиты – это средства, в которых основная защитная функция реализуется некоторым техническим устройством (комплексом, системой).

К **достоинствам** технических средств относятся: широкий круг задач, достаточно высокая надежность, возможность создания развитых комплексных систем защиты, гибкое реагирование на попытки несанкционированных действий.

Недостатками являются высокая стоимость многих средств, необходимость регулярного проведения регламентных работ и контроля, возможность подачи ложных тревог.

В зависимости от цели и места применения, выполняемых функций и физической реализуемости технические средства можно условно разделить на аппаратные и физические:

а) **аппаратные средства защиты**:

- нейтрализация технических каналов утечки информации (ТКУИ) выполняет функцию защиты информации от ее утечки по техническим каналам;
- поиск закладных устройств – защита от использования злоумышленником закладных устройств съема информации;
- маскировка сигнала, содержащего конфиденциальную информацию – защита информации от обнаружения ее носителей (стеганографические методы) и защита содержания информации от раскрытия (криптографические методы);

б) физические средства защиты:

- внешняя защита – защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств объекта;
- внутренняя защита – защита от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации;
- опознавание – специфическая группа средств, предназначенная для опознавания людей и идентификации технических средств по различным индивидуальным характеристикам.

Средства защиты информации

Все средства защиты можно разделить на две группы — формальные и неформальные.

Формальные средства защиты информации

№	Средство	Описание
1	Физические	Механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.
2	Аппаратные	Различные электронные, электронно-механические и тому подобные устройства, встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач по защите информации. Например, для защиты от утечки по техническим каналам используются генераторы шума.
3	Программные	Специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения автоматизированных систем с целью решения задач по защите информации. Это могут быть различные программы по криптографическому преобразованию данных, контролю доступа, защите от вирусов и др.

Технические средства защиты информации

Аппаратные средства поиска закладных устройств

№	Средство	Описание
1	Индикаторы электромагнитного поля	Позволяют обнаруживать излучающие закладные устройства, использующие для передачи информации практически все виды сигналов, включая широкополосные шумоподобные и сигналы с псевдослучайной скачкообразной перестройкой несущей частоты.
2	Интерсепторы	Дальнейшее развитие индикаторов поля – широкополосные радиоприемные устройства, автоматически настраивающиеся на частоту наиболее мощного радиосигнала (как правило, уровень этого сигнала на 15-20 дБ превышает все остальные) и осуществляющие его детектирование.
3	Радиочастотомеры	Позволяют «захватывать» частоты радиосигнала с максимальным уровнем с последующим анализом его характеристик микропроцессором.
4	Детекторы диктофонов	Принцип действия приборов основан на обнаружении слабого магнитного поля, создаваемого генератором подмагничивания или работающим двигателем диктофона в режиме записи.
5	Сканерные приемники	Могут работать в одном из следующих режимов: ▪ автоматического сканирования в заданном диапазоне частот; ▪ автоматического сканирования по фиксированным частотам; ▪ ручном.
6	Портативные анализаторы спектра	Позволяют не только принимать сигналы, но и анализировать их структуру.
7	Средства контроля проводных линий	Предназначены для выявления, идентификации и определения местоположения закладных устройств, подключаемых к проводным линиям. К ним относятся в том числе, электросеть, телефонные кабели, линии селекторной связи, пожарной сигнализации и т. п.
8	Нелинейные локаторы	Обнаруживают радиоэлектронные устройства путем излучения сигналов и приема отраженных гармоник высших порядков.
9	Металлоискатели и металлодетекторы	Для поиска закладных устройств в экранированных корпусах используются металлоискатели.
10	Технические средства обнаружения пустот	Позволяют повысить достоверность выявления пустот в сплошных средах (кирпичных и бетонных стенах, в деревянных конструкциях и др.).

Средства физической защиты информации

Аппаратные средства защиты информации

средства идентификации и установления подлинности

Идентификация (присвоение объекту уникального кода) и установление подлинности объекта заключаются в проверке его соответствия истинному объекту, производятся с целью определения возможности допуска объекта к информации ограниченного пользования. В основе процесса идентификации личности лежит анализ его **биометрических особенностей** или специально предъявляемых **носителей ключа**.

Основные способы идентификации

№	Способ	Описание
1	Геометрия руки	Современные методы предусматривают оценку нескольких параметров руки, в том числе ширины и толщины ладони в различных местах, длины пальцев, их толщины и формы.
2	Почерк	Разработаны автоматические системы подтверждения подписи, измеряющие характеристики движения руки при письме (усилия при нажатии на перо, скорость, ускорение). Преобразователи, измеряющие характеристики почерка, могут устанавливаться как в пишущем устройстве, так и под пластиной, на которой ставится подпись.
3	Дактилоскопия	Идентификация происходит по папиллярным узорам пальцев руки, которые формируются еще в утробе матери, являются строго индивидуальными и остаются неизменными на протяжении всей жизни.
4	Рисунок сетчатки глаз	Участок сетчатки глаза сканируется неполяризованным светом низкой интенсивности, испускаемым инфракрасными светодиодами. Различная интенсивность света, отраженного от различных точек сетчатки в процессе сканирования, отражает индивидуальное расположение кровеносных сосудов сетчатки глаза.
5	Радужная оболочка глаза	Источником информации является трабекулярная сетка радужной оболочки глаза, имеющая различные бороздки, кольца, ореол, маленькие точки и т. д.
6	Характеристики речи	Один из бурно развивающихся методов. Современные системы анализируют несколько характеристик речи, среди которых огибающая формы сигнала, период высоты тона, относительный спектр амплитуды, резонансные частоты речевого тракта (форманты) и т. д.
7	Инфракрасная карта лица	Источником информации является тепловой образ лица — своего рода комбинация термальных свойств сосудистых структур, их формы и плотности, свойств подкожных тканей, хрящей, кожи и т. д., остающаяся постоянной даже после пластической операции.

Программные средства защиты информации

Для нейтрализации угроз информации необходимо на программном уровне решить две основные группы задач по защите информации:

- обеспечение целостности информации (физической логической);
- защита от несанкционированного доступа (для предупреждения несанкционированной модификации, получения и копирования информации).

Программные средства обеспечения целостности информации

№	Способ	Описание
1	Программы-детекторы	Проверяют, имеется ли в файлах специфическая для данного вируса комбинация байтов. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать лишь те вирусы, которые им известны. То есть они не обнаруживают новые вирусы или модифицированные версии старого вируса.
2	Программы-доктора (фаги)	«Лечат» зараженные программы, «выкусывая» из зараженных программ тело вируса. Большинство программ-докторов умеют «лечить» только от некоторого фиксированного набора вирусов, поэтому они быстро устаревают. Но некоторые программы могут обучаться не только способам обнаружения, но и способам лечения новых вирусов.
3	Программы-ревизоры	Запоминают сведения о состоянии программ и системных дисков. После этого можно в любой момент сравнить состояние программ и системных областей дисков с исходными. О выявленных несоответствиях сообщается пользователю.
4	Доктора-ревизоры	Гибриды ревизоров и докторов (не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние). Это позволяет вылечивать файлы даже от тех вирусов, которые не были созданы на момент написания программы. Однако они могут лечить не от всех вирусов, а только от тех, которые используют «стандартные», известные на момент написания программы, механизмы заражения файлов.
5	Программы-фильтры	Программы-фильтры располагаются оперативной памяти компьютера и перехватывают все обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда. При каждом запросе на «подозрительное» действие на экран компьютера выводится сообщение о том, какое действие затребовано и какая программа желает его выполнить.
6	Программы-вакцины (иммунизаторы)	Модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными.

Программные средства защиты информации

Программные средства защиты от несанкционированного доступа (НСД)

1. Опознавание (аутентификация) пользователей и используемых компонентов обработки информации;
2. Разграничение доступа к элементам защищаемой информации;
3. Криптографическое закрытие защищаемой информации;
4. Регистрация всех обращений к защищаемой информации.

1. Опознавание (аутентификация)пользователей и используемых компонентов обработки информации

При решении этой задачи система защиты должна надежно определять законность каждого обращения к ресурсам, а законный пользователь должен иметь возможность убедиться, что ему предоставляются именно необходимые компоненты. Для опознавания пользователей к настоящему времени разработаны следующие основные способы:

№	Способ	Описание
1	С использованием простого пароля	Каждому зарегистрированному пользователю выдается персональный пароль, который он должен держать в тайне. При каждом обращении к ЭВМ специальная программа сравнивает введенный пользователем пароль с эталоном, и при совпадении запрос пользователя принимается к исполнению.
2	Опознавание в диалоговом режиме	В файлах механизмов защиты заблаговременно создаются записи, содержащие персонифицирующие пользователя данные (дата рождения, рост, вес, имена и даты рождения родных и т. п.) или достаточно большой и упорядоченный набор паролей. При обращении пользователя к системе программа механизма защиты предлагает ему назвать некоторые данные из указанных файлов. По результатам сравнения принимается решение о допуске.
3	Опознавание по индивидуальным особенностям и физиологическим характеристикам	Данный способ является весьма надежным, но требует применения специальных устройств для съема и ввода соответствующих параметров и программ их обработки и сравнения с эталоном. Одним из вариантов, использующим только программное обеспечение и удешевляющим процесс опознавания, является опознавание пользователя по параметрам его работы с клавиатурой (скорость набора текста, интервалы между нажатием клавиш и др.)
4	Опознавание по радиокодовым устройствам	Пользователь имеет устройство, генерирующее индивидуальные для каждого пользователя радиосигналы.
5	Опознавание по идентификационным карточкам	На карточки наносятся данные, персонифицирующие пользователя (персональный номер, специальный шифр или код и т. п.).

Программные средства защиты информации

Программные средства защиты от несанкционированного доступа

3. Криптографическое закрытие защищаемой информации

Данный механизм защиты можно подразделить на:

№	Способ	Описание
1	Криптографическое закрытие информации, хранимой на носителях	При этом достигаются две цели защиты информации: во-первых, с помощью известных алгоритмов шифрования обеспечивается требуемая криптографическая стойкость защиты; во-вторых, как правило, криптографические преобразования информации сопровождаются архивацией данных с уменьшением их объемов (сжатие данных);
2	Криптографическое преобразование информации в процессе ее обработки и передачи	Данный механизм предполагает засекречивание информации непосредственно в процессе ее обработки, практически полностью исключая тем самым возможность НСД к ней. Для этого дополнительно к программным используются специализированные аппаратные средства защиты.

4. Регистрация всех обращений к защищаемой информации

Данный механизм позволяет решить следующие задачи:

- контроль использования защищаемой информации;
- выявление попыток НСД к информации;
- накопление статистических данных о функционировании систем защиты с целью повышения ее эффективности.

Как правило, это реализуется соответствующими программами регистрации, позволяющими накапливать данные о попытках доступа к информации в определенных «спрятанных» файлах.

Криптографические средства защиты информации

Криптография («тайнопись») учит, как сохранить информацию в тайне, обозначает защиту информации с помощью шифрования.

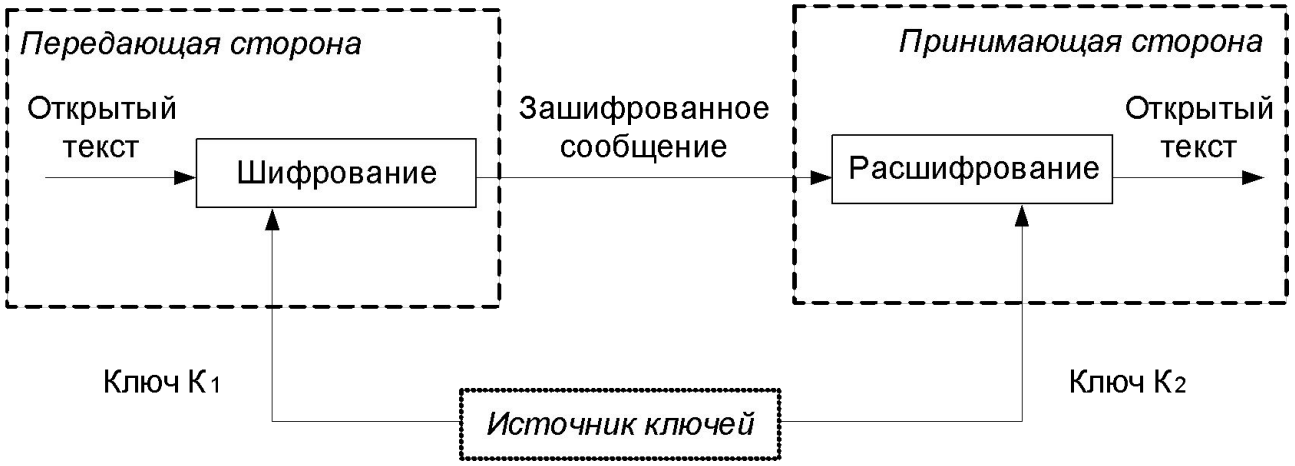
Шифрование – это преобразование «открытого текста» с целью сделать непонятным его смысл. В результате преобразования получается шифротекст. Процесс обратного преобразования - **расшифровка** (расшифрование, дешифрация) – восстановление исходного текста из шифротекста.

Шифрование используется для обеспечения защиты паролей, применяемых для аутентификации пользователей, защиты системной информации, защиты информации, передаваемой по линиям связи, защиты данных в файлах и базах данных и т.д.

Криптографический алгоритм (шифр или алгоритм шифрования) – это математические функции, используемые для шифрования и расшифрования (используется две функции: одна - для шифрования, другая - для расшифрования).

В современной криптографии надежность криптографического алгоритма обеспечивается с помощью использования ключей. Зашифрованный текст всегда можно восстановить (расшифровать) в исходном виде, зная соответствующий ключ. Некоторые алгоритмы шифрования используют различные ключи для шифрования и расшифрования.

Под **криптосистемой** понимается алгоритм шифрования, а также множество всевозможных ключей, открытых и шифрованных текстов.



Криптографические средства защиты информации

Существует две разновидности алгоритмов шифрования с использованием различных типов ключей: криптосистемы с открытым ключом и симметричные криптосистемы.

- **Симметричным** называют криптографический алгоритм, в котором ключ, используемый для шифрования сообщения, может быть получен из ключа расшифрования и наоборот. В большинстве симметричных систем используют всего один ключ, который должен храниться в секрете. Такие алгоритмы называют **одноключевыми**, или алгоритмами с **секретным ключом**.
- Алгоритмы шифрования с **открытым ключом** называют еще **асимметричными** алгоритмами шифрования. Они устроены так, что ключ, используемый для шифрования, отличается от ключа, применяемого для расшифровки сообщения, и ключ расшифрования не может быть за приемлемое время вычислен через ключ шифрования. Поэтому ключ шифрования не требуется держать в тайне и его называют открытым. Ключ же расшифрования является тайным, или секретным.

Симметричную криптосистему можно сравнить с сейфом, а ключ - с комбинацией, позволяющей открыть сейф каждому, кто эту комбинацию знает. Алгоритм шифрования с открытым ключом можно сравнить с почтовым ящиком: в него просто опустить почту (зашифровать сообщение с помощью открытого ключа), но сложно сообщение извлечь - это может сделать только человек, имеющий специальный ключ {расшифровать сообщение может только тот, кто знает соответствующий тайный ключ).

Электронная цифровая подпись

Цифровая сигнатура (электронная, электронно-цифровая подпись) — это строка символов, зависящая как от идентификатора отправителя, так и от содержания сообщения.

- Никто (кроме самого отправителя информации) не может вычислить его цифровую подпись для конкретного передаваемого им сообщения.
- Никто (и даже сам отправитель!) не может изменить уже отправленное сообщение так, чтобы сигнатура (электронная подпись под сообщением) осталась неизменной.
- Получатель должен быть способен проверить, является ли электронно-цифровая подпись (сигнатура), присвоенная сообщению, подлинной.
- В конфликтной ситуации внешнее лицо (арбитр, судья) должно быть способно проверить, действительно ли цифровая сигнатура, приписанная сообщению, выполнена его отправителем. Для верификации используется информация, предоставляемая арбитру отправителем и получателем.

Цифровые подписи могут быть реализованы на основе **шифрования с секретными ключами** (при симметричном шифровании), кроме того, допускается возможность подтверждения фактов передачи сообщений с помощью посредников, участвующих в процессе обмена информацией.

Классическим примером схемы электронно-цифровой подписи является алгоритм DSA (Digital Signature Algorithm), использованный как основа для опубликованного в 1991 г. в США стандарта на цифровые подписи DSS (Digital Signature Standard). Алгоритм DSA реализует схему на основе использования хэш-функций и асимметричного шифрования.

Отечественным стандартом на процедуры выработки к проверки электронно-цифровых подписей является ГОСТ Р 34.10-94. Схема, предложенная в данном стандарте, напоминает алгоритм DSA.

Средства защиты информации (СЗИ)

Неформальные средства защиты информации

№	Средство	Описание
1	Организационные	Специально предусматриваемые в технологии функционирования объекта организационно-технические мероприятия для решения задач по защите информации, осуществляемые в виде целенаправленной деятельности людей.
2	Законодательные	Существующие в стране или специально издаваемые нормативно-правовые акты, с помощью которых регламентируются права и обязанности, связанные с обеспечением защиты информации, всех лиц и подразделений, имеющих отношение к функционированию системы, а так же устанавливается ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации.
3	Морально-этические нормы	Сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

3. Архитектура и организационное построение системы защиты информации в организации.

Система защиты информации (СЗИ) – организованная совокупность всех средств, методов и мероприятий, выделяемых (предусматриваемых) на объекте информатизации (ОИ) для решения в ней выбранных задач по защите.

Архитектура системы защиты информации

Основные методологические принципы построения Система защиты информации

№	Принцип	Описание
1	Концептуальное единство	Архитектура, технология, организация и обеспечение функционирования как СЗИ в целом, так и составных ее компонентов должны объединяться в единую, целостную систему, которая является функционально самостоятельной подсистемой любого объекта информатизации.
2	Адекватность требованиям	СЗИ должна строиться в строгом соответствии с требованиями к защите, которые определяются категорией соответствующего объекта и значениями параметров, влияющих на защиту информации.
3	Гибкость (адаптируемость)	Такое построение и такую организацию функционирования, при которых функции защиты осуществлялись бы достаточно эффективно при изменении в некотором диапазоне структуры ОИ, технологических схем или условий функционирования каких-либо ее компонентов.
4	Функциональная самостоятельность	СЗИ должна быть самостоятельной обеспечивающей подсистемой системы обработки информации и при осуществлении функций защиты не должна зависеть от других подсистем.
5	Удобство использования	СЗИ не должна создавать дополнительных неудобств для пользователей и персонала ОИ.
6	Минимизация предоставляемых прав	Каждому пользователю и каждому лицу из состава персонала ОИ должны предоставляться лишь те полномочия на доступ к ресурсам ОИ и находящейся в ней информации, которые ему действительно необходимы для выполнения своих функций в процессе автоматизированной обработки информации.
7	Полнота контроля	Все процедуры автоматизированной обработки защищаемой информации должны контролироваться системой защиты в полном объеме, причем основные результаты контроля должны фиксироваться в специальных регистрационных журналах.
8	Активность реагирования	СЗИ должна реагировать на любые попытки несанкционированных действий.
9	Экономичность	При условии соблюдения основных требований всех предыдущих принципов расходы на СЗИ должны быть минимальными.

Структура системы защиты информации

№	Подсистемы	Описание
1	Подсистема ограничения доступа	Подсистема должна выполнять функции идентификации, проверки подлинности (аутентификации) и контроля доступа пользователей конфиденциально» информацией и программ (процессов) к ресурсам.
2	Подсистема криптографической защиты	Подсистема реализует функцию шифрования конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, а также на съемные носители данных (ленты, диски, дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа, а также информации, передаваемой по линиям связи. Доступ к операциям шифрования и/или криптографическим ключам контролируется посредством подсистемы управления доступом.
3	Подсистема обеспечения целостности	Включает организационные, программно-аппаратные и другие средства и методы, обеспечивающие: ▪ контроль целостности программных средств на предмет их несанкционированного изменения; ▪ периодический и/или динамический контроль на предмет несанкционированного доступа; ▪ наличие администратора (службы) защиты информации; ▪ восстановление системы защиты информации при отказе и/или сбое; ▪ резервирование информационных ресурсов на других типах носителей; ▪ применение сертифицированных (аттестованных) средств и методов защиты, сертификация которых проводится специальными и испытательными центрами.
4	Подсистема регистрации и учета	Включает средства регистрации учета событий и/или ресурсов с указанием времени и инициатора: ▪ входа/выхода пользователей в/из системы; ▪ выдачи печатных (графических) выходных документов; ▪ запуска/завершения программ и процессов (заданий, задач), использующих защищаемые файлы; ▪ доступа программ пользователей к защищаемым файлам, включая их создание и удаление; ▪ и др.
5	Подсистема управления	Предназначена для объединения всех подсистем СЗИ в единую целостную систему, для организации обеспечения управления ее функционированием.

Организационное построение системы защиты информации

Служба защиты информации

В организациях, использующих в своей деятельности сведения с ограниченным доступом, требуется наличие специальной **службы защиты информации**.

Служба защиты информации, как правило, является самостоятельным структурным подразделением, подчиненным непосредственно руководителю и (при наличии) заместителю по безопасности (режиму).

Проведение любых мероприятий и работ с использованием сведений с ограниченным доступом без принятия необходимых мер защиты **не допускается**.

Основными **задачами** службы защиты информации являются:

- обеспечение и организация разработки перечней сведений конфиденциального характера;
- выявление, локализация и оперативное пресечение возможных каналов утечки защищаемой информации в процессе повседневной деятельности и в экстремальных ситуациях;
- анализ возможностей возникновения новых каналов утечки и разработка методов и рекомендаций по их пресечению;
- профилактическая деятельность, направленная на предотвращение открытия потенциальных каналов и источников утечки информации;
- анализ и оценка реальной опасности перехвата информации техническими средствами негласного съема информации, предотвращение возможных несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;
- обеспечение режима конфиденциальности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, связанные с деловым сотрудничеством как на национальном, так и на международном уровнях;
- изучение, анализ и оценка состояния системы технической защиты информации, разработка предложений и рекомендаций по ее совершенствованию.

Организационно-правовое обеспечение

Законодательные меры по защите процессов переработки информации заключаются в исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц — пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

Цель законодательных мер — предупреждение и сдерживание потенциальных нарушителей.

Поскольку информационная безопасность должна быть связующим звеном между политикой национальной безопасности и информационной политикой страны, то логично было бы проводить их по единым принципам, выделяя как общие положения и принадлежности для информационной политики.

Проблема обеспечения безопасности носит комплексный характер. Для ее решения необходимо сочетание как правовых мер, так и организационных (например, в компьютерных информационных системах на управленческом уровне руководство каждой организации должно выработать политику безопасности, определяющую общее направление работ и выделить на эти цели соответствующих ресурсы) и программно-технических (идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование).