Информация как объект защиты на различных уровнях ее представления

Носители информации

- Информация заключена только в материальных (вещественных или энергетических) носителях.
- Носители – это материальные объекты, обеспечивающие запись, хранение и передачу информации в пространстве и времени.

Виды носителей

- вещественные носители (бумага, фото- и кинопленка, машинные носители информации, материалы и образцы технологии);
- электрические сигналы в виде напряжений и токов.

Семантическая информация

- является продуктом абстрактного мышления и отображает объекты, явления, образы и модели с помощью символов на языках людей.
- содержание и смысл семантической информации не изменяются при копировании с одного носителя на другой.

Признаковая информация

- видовые признаки объекта (носителя) – его форма, размеры, составные части, цвет, структура;
- вещественные признаки – физический и химический состав, структура и свойства вещества объекта;
- энергетические признаки – параметры электрических сигналов и полей.

Уровни информации

- уровень материальных носителей;
- уровень средств взаимодействия с носителями;
- логический уровень;
- синтаксический уровень;
- семантический уровень;
- прагматический уровень.

Уровень материальных носителей

- вещественные носители придают информации свойство статичности, относительной неизменности во времени;
- используются для хранения информации;
- обладают относительной прочностью запечатления информации.

Уровень материальных носителей

- вещественные носители подвержены естественному старению, необратимой потере своих свойств;
- для хранения ценной информации следует использовать надежные, долговременные носители;
- если для защиты информации от несанкционированного перехвата требуется ее мгновенно уничтожить, следует выбирать такие носители, которые мгновенно можно испортить;
- если защищаемая информация содержится в самом вещественном носителе, то процесс разрушения носителя должен воздействовать на те компоненты, которые содержат признаковую информацию.

Уровень материальных носителей

- информация на вещественных носителях чаще страдает от нераспорядительности и халатности людей;
- традиционные меры защиты - обучение правильным способам эксплуатации машинных носителей информации и поддержание высокой ответственности пользователей за их сохранность ;
- для противодействия старению и разрушению носителей единственный разумный метод – резервирование информации.

Уровень материальных носителей

- наличие нескольких экземпляров одной и той же конфиденциальной информации, тем более хранимых в разных местах, делает информацию уязвимее для несанкционированного доступа;
- вещественный носитель информации можно похитить, для защиты хранимой информации его необходимо изолировать от досягаемости чужих рук;
- необходимо предусмотреть защиту технического средства обработки информации с фиксированными машинными носителями от несанкционированного доступа.

Уровень материальных носителей

- для скрытия визуальной информации следует предусмотреть защиту носителей;
- для защиты от непреднамеренной утраты вещественные носители конфиденциальной информации регистрируют и учитывают;
- зарегистрированные носители в течение всего времени, когда с ними не работают, должны размещаться в надежных хранилищах

Уровень материальных носителей

- программа для ЭВМ имеет двойственную природу: она создается как инструмент воздействия на информацию, и при этом сама, как совокупность команд и данных, является информацией;
- все сменные машинные носители необходимо периодически проверять на наличие вредоносных сигнатур и не допускать их необоснованного использования на других ЭВМ.

Виды копирования информации

- Смысловое копирование означает, что на другой носитель переносится только семантическая информация
- Логическое копирование осуществляется с сохранением не только содержания, но и логической формы представления информации.
- Детальное копирование предусматривает копирование не только содержания и формы семантической информации, но и перенос признаковых свойств.

Энергетические носители информации

- Большинство проблем для защиты доставляет существование энергетических носителей информации.
- Обмен информацией всегда сопровождается выделением энергии.

Энергия для передачи и копирования информации

- Акустическая и электромагнитная (передача семантической информации осуществляется методами модуляции информативных параметров сигнала по закону передаваемого сообщения).
- В форме электромагнитного или акустического сигнала информация существует одномоментно.
- Наиболее распространенной формой передачи информации являются электрический сигнал.

Перехват информации

- Энергия, несущая информацию, передается от источника к получателю по каналу связи.
- Область распространения электромагнитной (акустической) энергии определяется мощностью источника сигнала, чувствительностью приемников, физикой волновых и корпускулярных явлений, а также свойствами среды.
- Для перехвата информации достаточно получить хотя бы незначительную часть передаваемой энергии, позволяющую усилить сигнал и демодулировать его информативный параметр при наличии шумов.

Утечка информации

- Бесконтрольность процессов рассеивания энергии и ее преобразования в иные энергетические формы является основной причиной утечки информации по техническим каналам.
- От обычной утечки информации в форме разглашения, подслушивания и наблюдения, техническая утечка отличается необходимостью использования нарушителем технических (чаще – радиоэлектронных) средств перехвата.

Защита компьютерной информации

- Компьютерная информация – это данные или набор команд, предназначенные для использования в ЭВМ или управления ею, зафиксированные на машинном носителе или передаваемые по телекоммуникационным каналам в форме электромагнитных сигналов.

Особенности компьютерной информации

- может создаваться, изменяться, копироваться, использоваться только с помощью ЭВМ;
- скрыта от непосредственного восприятия человеком по причине использования сложных способов кодирования, больших плотностей размещения на машинных носителях, значительных скоростей передачи данных;
- сосредоточивается в памяти компьютеров в больших объемах и очень быстро обрабатывается;

Особенности компьютерной информации

- легко копируется с одного машинного носителя на другой и передается по телекоммуникационным каналам на любое расстояние;
- отличается «хрупкостью» и может быть легко уничтожена или модифицирована в процессе обработки (в ходе технологических операций из-за некомпетентности персонала, при выполнении обычных процедур открытия или копирования файлов);
- может быть заблокирована из-за неисправности оборудования, сбоя в работе программ, вредоносного аппаратно-программного воздействия.

Персонал и защита информации

- Защищать необходимо источники, преобразователи и приемники информации, т. е. технические средства обработки информации (ТСОИ), и персонал.
- По отношению к информации человек может быть носителем тех или иных прав на эту информацию и быть ее собственником, владельцем или пользователем, генератором новой информации (ученым, автором), секретоносителем, распространителем информации, информационным нарушителем или администратором информационной безопасности.

Понятие об информационных угрозах

Модель: 3 «У»

- Угрозы
- Уязвимости
- Ущерб

Угроза информации

- совокупность условий и факторов, которые потенциально могут нанести вред (ущерб) собственнику, владельцу путем раскрытия, модификации или разрушения информации либо отказа в обслуживании.
- потенциально возможные опасные действия, приводящие к ущербу.

Классификация угроз

- по носителям
- по целям
- по причиненному ущербу
- по наличию умысла
- по степени подготовленности нарушителей
- по скрытности исполнения
- по удаленности от объекта защиты

Пространство угроз

- угрозы конфиденциальности
- угрозы целостности – вредят полноте и достоверности информации
- угрозы доступности

Характер потенциальных угроз

- с помощью одного и того же набора средств и методов защитить информацию от всех трех типов угроз невозможно;
- в практической деятельности собственнику информации приходится применять варианты ее защиты, предпочитая одни угрозы другим.

Уязвимости

- угрозы становятся возможными по причине уязвимостей в информационной системе;
- уязвимостью называют некоторую неудачную характеристику системы;
- уязвимости являются следствием сложности информационных систем.

Ущерб

- реальный или прогнозируемый результат реализации угроз в натуральном или денежном выражении
- затраты на охрану материальных ценностей зависят от
  - характера угроз
  - вероятности нанесения ущерба
  - прогнозируемых потерь
- Обобщенный параметр, учитывающий ценность ресурса, уровень угрозы и степень уязвимости, называется **уровнем риска**

Нормативная основа защиты информации

Справочник законодательства РФ в области информационной безопасности

https://habr.com/ru/post/432466/

Разработка нормативной основы защиты информации

- Принадлежность информации
- Определение важности информации
- Значение секретности

Содержание нормативной документации

- Какие информационные ресурсы защищаются;
- Какие программы можно использовать на служебных компьютерах;
- Что происходит при обнаружении нелегальных программ или данных;
- Дисциплинарные взыскания и общие указания о проведении служебных расследований;

Содержание нормативной документации (2)

- На кого распространяются правила;
- Кто разрабатывает общие указания;
- Кто имеет право изменять указания;
- Точное описание полномочий и привилегий должностных лиц;
- Кто может предоставлять полномочия и привилегии;

Содержание нормативной документации (3)

- Порядок предоставления и лишения привилегий в области безопасности;
- Полнота и порядок отчетности о нарушениях безопасности и преступной деятельности;
- Особые обязанности руководства и служащих по обеспечению безопасности;
- Объяснение важности правил;
- Даты ввода в действие и пересмотра правил.

План защиты информации

- Назначение ИС;
- Перечень решаемых задач;
- Конфигурация;
- Характеристики и размещение технических средств и программного обеспечения;
- Перечень категорий информации, подлежащих защите в ИС;
- Требования по обеспечению доступности , конфиденциальности, целостности различных категорий информации;

План защиты информации (2)

- Список пользователей и их полномочий по доступу к ресурсам системы;
- Цель защиты системы и пути обеспечения безопасности ;
- Перечень угроз безопасности ИС, от которых требуется защита, наиболее вероятных путей нанесения ущерба;
- Основные требования к организации процесса функционирования ИС и мерам обеспечения безопасности обрабатываемой информации;

План защиты информации (3)

- Требования к условиям применения и определение зон ответственности, установленных в системе технических средств защиты от несанкционированного доступа;
- Основные правила, регламентирующие деятельность персонала по вопросам обеспечения безопасности ИС;
- Цель обеспечения непрерывности процесса функционирования ИС, своевременность восстановления ее работоспособности и пути ее достижения;

План защиты информации (4)

- Перечень и классификация возможных кризисных ситуаций;
- Требования, меры и средства обеспечения непрерывной работы и восстановления процесса обработки информации (порядок создания, хранения и использования резервных копий информации и дублирующих ресурсов);

План защиты информации (5)

- Обязанности и порядок действий различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий, минимизации наносимого ущерба и восстановлению нормального процесса функционирования системы;
- Разграничение ответственности субъектов, участвующих в процессах обмена электронными документами;

План защиты информации (6)

- Определение порядка подготовки, оформления, передачи, приема, проверки подлинности и целостности электронных документов;
- Определение порядка генерации, сертификации и распространения ключевой информации (ключей, паролей и т.д.);
- Определение порядка разрешения споров в случае возникновения конфликтов.

Стратегии защиты

- Оборонительная – защита от уже известных угроз, осуществляемая автономно, т.е. без оказания существенного влияния на информационно-управляющую систему;
- Наступательная – защита от всего множества потенциально возможных угроз, при осуществлении которой в архитектуре информационно-управляющей системы и технологии ее функционирования должны учитываться условия, продиктованные потребностями защиты;

Стратегии защиты (2)

- Упреждающая – создание информационной среды, в которой угрозы информации не имели бы условий для проявления.

Принципы построения систем защиты информации

Основные принципы построения систем защиты

- Простота механизма защиты
- Постоянство защиты
- Всеобъемлющий контроль
- Несекретность проектирования
- Идентификация

Основные принципы построения систем защиты (2)

- Разделение полномочий
- Минимальные полномочия
- Надежность
- Максимальная обособленность механизма защиты

Основные принципы построения систем защиты (3)

- Защита памяти
- Удобство для пользователей
- Контроль доступа
  - К ресурсам рабочих станций
  - К областям жестких дисков
  - К ресурсам и серверам сети
  - К модулям выполнения авторизации пользователей

Основные принципы построения систем защиты (4)

- Авторизация
- Отчетность
- Наличие механизмов защиты от
  - Несанкционированного чтения информации
  - Модификации хранящейся и циркулирующей в сети информации
  - Несанкционированного отказа от авторства переданной информации

Основные принципы построения систем защиты (5)

- Системный подход к защите информации
- Возможность наращивания защиты
- Адекватность
- Минимизация привилегий
- Полнота контроля

Основные принципы построения систем защиты (6)

- Экономичность механизма
- Специализация
- Гибкость
- Непрерывность мероприятий
- Наказуемость нарушений

Уровни защиты в системе

- Внешний
- Сооружений, помещений и устройств
- Компонентов системы (технических средств, программного обеспечения, элементов баз данных)
- Технологических процессов обработки данных (ввод/вывод, внутренняя обработка и т.д.)

Гарантируемые свойства защищенной системы

- Полная свобода доступа каждого пользователя и независимость его работы в пределах предоставленных ему прав и полномочий
- Удобство работы с информацией для групп взаимосвязанных пользователей
- Возможность пользователям допускать друг друга к своей информации

Основные правила защиты

- Обеспечение безопасности – непрерывный процесс, состоящий в систематическом контроле защищенности, в выявлении узких мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты
- Безопасность информации в системе обработки данных может быть обеспечена лишь при комплексном использовании всех имеющихся средств защиты

Основные правила защиты (2)

- Никакая система защиты не обеспечит безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех правил защиты
- Никакую систему защиты нельзя считать абсолютно надежной

Технические средства защиты

- Техническими называются такие средства защиты, которые реализуются в виде электрических, электромеханических, электронных устройств
  - Аппаратные – устройства, внедряемые непосредственно в аппаратуру обработки данных, или устройства, которые сопрягаются с ней по стандартному интерфейсу
  - Физические устройства – реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранных сигнализаций и наблюдения, замки и т.д.)

Программные средства защиты

- Программы, специально предназначенные для выполнения функций, связанных с защитой информации

Первоначально программные механизмы защиты включались в состав операционных систем или систем управления базами данных

Встроенные в ОС механизмы защиты

- Динамическое распределение ресурсов вычислительной системы и запрещение задачам пользователей использовать чужие ресурсы
- Разграничение доступа пользователей к ресурсам системы по паролям
- Разграничение доступа к полям оперативной и долговременной памяти по ключам защиты
- Защита таблицы паролей

Определения защищенности ИС

- Совокупность средств и технологических приемов, обеспечивающих защиту компонентов ИС
- Минимизация риска, которому могут быть подвергнуты компоненты и ресурсы ИС
- Комплекс процедурных, логических и физических мер, направленных на предотвращение угроз информации и компонентам ИС

Защищенная ИС

- Защищенная ИС – та, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов
- Механизмы выполнения данных правил реализуются в виде системы защиты информации

Этапы построения защищенной ИС

- Анализ угроз информации
- Составление перечня требований к защите
- Формулирование правил организации непосредственной защиты
- Реализация выполнения правил путем создания комплексной системы защиты информации

Характеристики, влияющие на уровень безопасности информации

- Категории обрабатываемой в ИС информации
- Общая структурная схема и состав ИС
- Тип ИС (по количеству пользователей, открытости, количеству уровней и т.д.)
- Объемы основных информационных массивов и потоков
- Скорость обмена информацией

Характеристики, влияющие на уровень безопасности информации (2)

- Продолжительность процедуры восстановления работоспособности после сбоев, наличие средств повышения надежности и живучести и т.п.
- Технические характеристики используемых каналов связи
- Территориальное положение компонентов ИС

Модель угроз безопасности информации должна содержать описание информационной системы

- описание информационной системы;
- структурно-функциональные характеристики;
- описание угроз безопасности;
- модель нарушителя;
- возможные уязвимости;
- способы реализации угроз;
- последствия от нарушения свойств безопасности информации.

Защита компьютерной информации

- Компьютерная информация – это данные или набор команд, предназначенные для использования в ЭВМ или управления ею, зафиксированные на машинном носителе или передаваемые по телекоммуникационным каналам в форме электромагнитных сигналов.

Особенности компьютерной информации

- может создаваться, изменяться, копироваться, использоваться только с помощью ЭВМ;
- скрыта от непосредственного восприятия человеком по причине использования сложных способов кодирования, больших плотностей размещения на машинных носителях, значительных скоростей передачи данных;
- сосредоточивается в памяти компьютеров в больших объемах и очень быстро обрабатывается;

Особенности компьютерной информации

- легко копируется с одного машинного носителя на другой и передается по телекоммуникационным каналам на любое расстояние;
- отличается «хрупкостью» и может быть легко уничтожена или модифицирована в процессе обработки (в ходе технологических операций из-за некомпетентности персонала, при выполнении обычных процедур открытия или копирования файлов);
- может быть заблокирована из-за неисправности оборудования, сбоя в работе программ, вредоносного аппаратно-программного воздействия.

Персонал и защита информации

- Защищать необходимо источники, преобразователи и приемники информации, т. е. технические средства обработки информации (ТСОИ), и персонал.
- По отношению к информации человек может быть носителем тех или иных прав на эту информацию и быть ее собственником, владельцем или пользователем, генератором новой информации (ученым, автором), секретоносителем, распространителем информации, информационным нарушителем или администратором информационной безопасности.

Информационная система (ИС)

Организационно-техническая система, реализующая информационные технологии и предусматривающая аппаратное, программное и другие виды **обеспечения**, а также соответствующий **персонал**, предназначенная для организации, хранения, пополнения, поддержки и предоставления пользователям информации в соответствии с их запросами

ИС характеризуют

- Наличие прямых, обратных, многоканальных и разветвленных **связей**, а также процессов управления
- **Сложность**, понимаемая как принципиальная невозможность в полной мере, без дополнительных условий и ограничений, иметь адекватное формализованное описание
- Обилие разнообразных **составляющих информационного процесса**, распределенных в пространстве, непрерывно сменяющих друг друга по времени

Особенности сетевой архитектуры ИС

- Применяемые методы распределения информации и установления связи между взаимодействующими системами
- Виды предоставляемых услуг
- Способы управления процессами
- Наличие средств **защиты** и обеспечения **целостности** данных и **сохранности** ресурсов
- Возможность организации **связи** с другими сетями и осуществления межсетевых переходов

Критерии качества ИС

- Общее число связей ИС
- Временные характеристики качества ИС (например, среднее время доступа)
- Среднее время обслуживания
- Надежность обслуживания
- Достоверность передачи, сохранность и целостность информации
- Возможность доступа к информационным и вычислительным ресурсам

Компоненты ИС

- Локальная сеть
- Каналы и средства связи
- Узлы коммутации
- Рабочее место удаленного легального пользователя системы
- Рабочее место постороннего пользователя
- Носители информации
- Оргтехника
- Рабочие станции
- Непосредственно пользователи

Особенности распределенных систем

- Территориальная удаленность компонентов системы друг от друга и интенсивный обмен информацией между ними
- Широкий спектр используемых информационных технологий
- Интеграция данных различного назначения, принадлежащих разным субъектам в рамках единых баз данных, и, наоборот, размещение необходимых некоторым субъектам данных в удаленных узлах сети

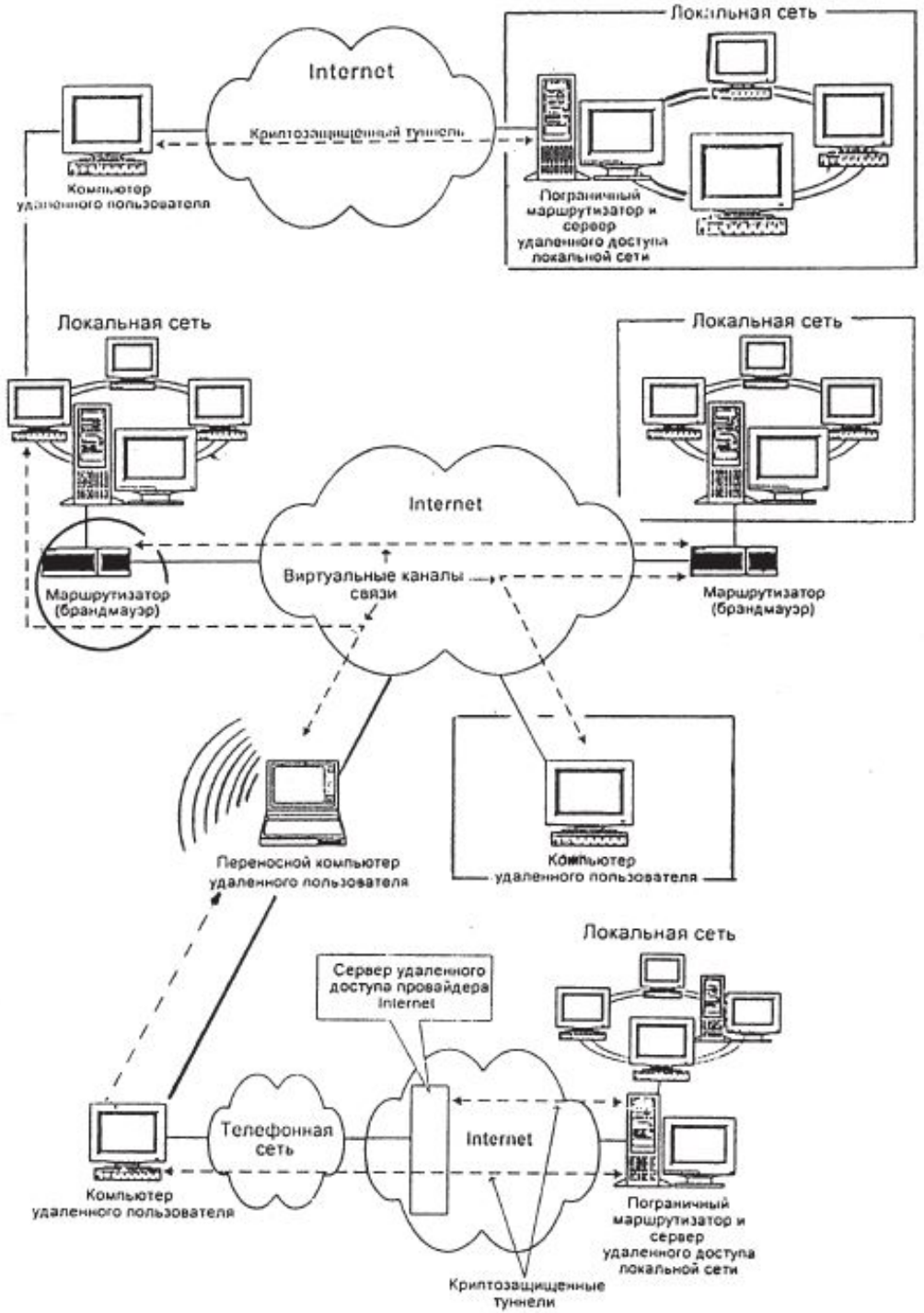
Особенности распределенных систем (2)

- Абстрагирование пользователей и владельцев данных от физических структур и места размещения данных
- Использование режимов распределенной обработки данных
- Участие в процессе функционирования ИС большого количества пользователей и персонала

Особенности распределенных систем (3)

- Одновременный доступ к ресурсам ИС большого количества пользователей различных категорий
- Высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения
- Отсутствие специальной аппаратной поддержки средств защиты в большинстве типов технических средств, широко используемых в ИС

Структурная схема распределенной ИС



Основные типовые компоненты ИС

Рабочие места пользователей и персонала ИС

- пользователя, который может функционировать в режиме обмена информации с сопряженной ЭВМ и в автономном режиме
- оператора, предназначенное для обслуживания серверов
- программиста, предназначенное для отладки программы
- администратора, предназначенное для управления и контроля за использованием каких-либо ресурсов ИС, например администраторы сети, базы данных, службы безопасности

Основные типовые компоненты ИС (2)

- Коммуникационные компоненты:
  - межсетевые мосты (шлюзы, центры коммутации пакетов, коммуникационные ЭВМ, маршрутизаторы) – элементы, обеспечивающие соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия
  - каналы связи с узлами коммутации
  - аппаратура связи типа «мультиплексор»
  - каналы связи выделенные и коммутируемые

Вспомогательные элементы ИС

- помещения, в которых размещены внешние запоминающие устройства больших ЭВМ
- помещения, в которых размещены устройства предварительной подготовки данных
- хранилище машинных носителей информации
- хранилища документов на бумажных носителях
- служебные помещения пользователей и персонала ИС

Проблемы защиты ИС

- Все компоненты ИС должны рассматриваться как объекты защиты
- Проблемы:
  - в качестве базового уровня ИС применяются бытовые рабочие станции
  - открытость систем
- Необходима централизация систем, применение особых методов защиты

Основные цели в процессе защиты информации в ИС

- предотвращение утечки, хищения, утраты, искажения, подделки информации
- предотвращение угроз безопасности личности, общества, государства
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы

Основные цели в процессе защиты информации в ИС (2)

- обеспечение правового режима обработки документированной информации как объекта собственности
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством
- гарантия прав субъектов в информационных процессах и при разработке, производстве, применении информационных систем, технологий и средств их обеспечения

Проблемы в процессе защиты информации в ИС

Проблемы в процессе защиты информации в ИС (2)

- Интеграция закрытых вычислительных систем с локальными сетями и серверами баз данных влечет за собой множество проблем, связанных с использованием различных технологий защиты без их синхронизации и с фрагментацией ответственности.
- Уровень защиты всей системы определяется степенью защиты ее самого уязвимого звена, которым, как правило, являются включенные в сеть персональные компьютеры

Защита открытых ИС

ИС можно рассматривать как сочетание двух видов сервисов:

- Основные сервисы (собственно ИС)
- Вспомогательные сервисы (серверы баз данных, почтовые серверы, сетевые сервисы, оборудование, операционные системы и т.д.)

В защите нуждаются все сервисы и коммуникационные пути между ними

Защита сервисов ИС

- Межсетевые экраны контролируют попытки доступа к наиболее уязвимым сервисам
- Файловые серверы могут контролировать доступ к различным частям файловой системы (но только на уровне каталога)
- Защита данных на локальных рабочих станциях может быть минимальной или вообще отсутствовать.
- Удаленные вычисления должны контролироваться при помощи аутентификации пользователей

Угрозы при передаче информации по каналам связи

Современные топологии и протоколы подразумевают работу через транзитные коммуникационные узлы, в связи с чем появляется угроза активного или пассивного перехвата сообщений, передаваемых по каналам связи

- Пассивный перехват заключается в чтении информации и анализе трафика
- Активный перехват изменяет поток сообщений

Прочие проблемы безопасности ИС

- Неадекватная политика управления и безопасности ИС
- Отсутствие обучения особенностям использования ИС и защиты
- Неадекватные механизмы защиты для рабочий станций
- Неадекватная защита в процессе передачи информации

Политика безопасности

- Политика безопасности является сжатой формулировкой позиции высшего руководства по вопросам информационных ценностей, ответственности по их защите и организационным обязательствам. Политика должна определять роль каждого служащего при обеспечении адекватной защиты ИС и передаваемой в ней информации

Надежность информации

Интегральный показатель, характеризующий качество информации с точки зрения

- Физической целостности
- Доверия к информации (аутентичности)
- Безопасности информации (конфиденциальности)
- Недопущения несанкционированного размножения информации

Объект защиты

- Структурный компонент системы, в котором находится или может находиться подлежащая защите информация

Удовлетворяет условиям:

- Принадлежность к одному и тому же организационному компоненту ИС
- Участие в осуществлении одних и тех же функций, связанных с автоматизированной обработкой информации в ИС
- Локализация (ограничение) с точки зрения территориального расположения ИС

Объекты защиты

- вещественные носители информации
- технические средства обработки информации
- каналы связи

Объекты защиты

- Рабочие станции пользователей
- Рабочие станции администраторов
- Серверы
- Аппаратура связи
- Каналы связи
- Периферийные устройства коллективного пользования
- Помещения, связанные с автоматизированной обработкой информации

Элемент защиты

- Находящаяся в ИС совокупность данных, которая может содержать подлежащие защите сведения
- Элементы защиты специфицируются для каждого отдельного объекта защиты

Данные как элементы защиты

- обрабатываемые в ЭВМ
- на переносных носителях
- на постоянных носителях на рабочей станции
- на постоянных носителях на сервере
- обрабатываемые в аппаратуре связи
- передаваемые по каналу связи
- выводимые из ЭВМ на периферийные устройства

Сложность решения задач защиты информации

Сложность данных задач характеризуется факторами:

- Предъявляются высокие требования к целостности системного и прикладного ПО, СУБД и ряда электронных документов
- Работа в территориально-распределенной сети предъявляет высокие требования к аутентичности информации и источников данных

Сложность решения задач защиты информации (2)

- Переход на безбумажную технологию требует обеспечения юридической значимости электронных документов
- Распределенное использование ресурсов ИС требует обеспечения безопасности информации на уровне разграничения доступа
- Ряд электронных документов требует обеспечения безопасности на уровне скрытия смыслового содержания, а в некоторых случаях и недопущения несанкционированного размножения

Распространенные пути утечки информации

- Хищение носителей информации и документов, получаемых в результате работы ИС
- Копирование информации на ПК
- Несанкционированное подключение к аппаратуре и линиям связи
- Перехват электромагнитных излучений в процессе обработки информации
- Непреднамеренные ошибки легальных пользователей

Принципы государственной политики обеспечения информационной безопасности

- Обеспечение равенства всех участников информационного взаимодействия
- Информационные ресурсы являются объектом собственности
- Развитие современных информационных и телекоммуникационных технологий и средств
- Согласованность решений в плане обеспечения информационной безопасности в рамках единого информационного пространства

Организационные меры защиты

Организационные меры разрабатываются для исключения:

- доступа к аппаратуре обработки информации
- бесконтрольного выноса персоналом различных носителей информации
- несанкционированного введения данных в память, изменения или стирания хранящейся в ней информации
- незаконного пользования системами обработки информации и полученными данными
- доступа в системы обработки информации посредством самодельных устройств

Организационные меры защиты (2)

- неправомочной передачи данных по каналам связи из информационно-вычислительного центра
- бесконтрольного ввода данных в систему
- обработки данных без соответствующего требования заказчика
- неправомочного считывания, изменения или стирания данных в процессе их передачи или транспортировки носителей информации

Защита данных и обеспечение конфиденциальности

Доступ в компьютерную систему

- любая форма проникновения, позволяющая манипулировать информацией
- неправомерным доступом считается доступ к информации постороннего лица, не санкционированный ее обладателем или произведенный ее пользователем с нарушением установленного порядка

Категории информационных нарушителей

- «Внешние» нарушители – это лица, неизвестные системе и желающие стать собственниками или, по меньшей мере, пользователями защищаемой информации.
- «Внутренние» нарушители – это пользователи системы, которые желают приобрести дополнительные полномочия с целью свободной манипуляции защищаемой информацией

Операции в системе управления доступом

- Санкционирование – процедура присвоения пользователю персонального идентификатора, регистрация его в системе, задание для него прав доступа (по времени и уровню полномочий)
- Авторизация – проверка полномочий (времени и уровня доступа), установленных в процессе санкционирования
- Аутентификация – установление подлинности идентифицированного пользователя
- Идентификатор – некое уникальное количество информации, позволяющее различать субъекты и объекты доступа

Операции в системе управления доступом

- Идентификация – процедура опознавания пользователя по предъявленному идентификатору
- Пароль – некоторое количество секретной информации, известной пользователю и парольной системе, которое пользователь может на определенное время запомнить и предъявить для прохождения процедуры аутентификации
- Парольная система – аппаратно-программный комплекс, реализующий идентификацию и аутентификацию
- Реагирование – реакция системы или персонала охраны на несанкционированные действия пользователя (нарушителя)

Операции в системе управления доступом

- Регистрация – процедура ввода идентифицирующей и аутентифицирующей информации с протоколированием действий
- Учетная запись – совокупность идентификатора и пароля

Идентификация и аутентификация

- Идентификация – это требование назвать свое имя
- Аутентификация – это требование подтвердить свою подлинность
  - вещественное доказательство, подтверждающее личность (документ, ключ, носитель ключевой информации)
  - парольная информация, известная только пользователю и проверяющей системе
  - уникальный индивидуальный признак, свойственный лишь этому пользователю

Человеческий фактор

- выбор простого пароля, который злоумышленник может легко подобрать или угадать
- запись сложного пароля в доступных местах
- открытый ввод пароля при наличии посторонних
- намеренная или по заблуждению передача пароля другому лицу

Атаки нарушителя на парольные системы

- угадывание пароля
- подбор пароля путем «лобовой» атаки
- подбор пароля по словарю и частоте символов
- подбор, оптимизированный благодаря использованию сведений о конкретном пользователе
- исследование программы, содержащей пароль, с последующей подменой или обходом этого фрагмента кода
- использование специальных программ для «взлома» парольной системы
- подмену подсистемы аутентификации операционной системы

Универсальная система управления доступом

- аппаратное или программно-аппаратное устройство считывания идентифицирующей информации (датчик), которое оценивает представленный ему для опознавания носитель признаковой или семантической информации
- база данных учетных записей известных объектов распознавания
- устройство сравнения, обработки и хранения результатов
- устройство управления физическим или логическим барьером
- управляемый барьер

Стратегии информационного нарушителя

- подбор паролей или математически преобразованной аутентифицирующей информации;
- перехват парольной информации в ходе сеансов, организуемых полномочными пользователями;
- сканирование узлов сети с получением информации о версиях сервисных программ;
- атаки сервисных программ с переполнением буфера памяти.

Объекты распознавания в компьютерных системах

- человек (должностное лицо, пользователь, оператор);
- техническое средство (персональный компьютер, консоль, терминал);
- документы (данные, сообщения);
- компьютерные программы;
- машинные носители информации;
- информация, выводимая на дисплей, табло.

Комплексная идентификация устанавливает

- имеет ли человек необходимые права доступа к информации;
- действительно ли информация, вводимая полномочным пользователем, попадет по своему адресу и будет обработана доверенным устройством;
- принадлежат ли электронные документы определенному доверенному лицу (владельцу), не производилось ли их намеренное или случайное искажение;
- не содержит ли запускаемая компьютерная программа посторонних вредоносных фрагментов.

Способы идентификации данных

- кодирование с обнаружением ошибок;
- кодирование с устранением одиночных и групповых ошибок;
- электронная цифровая подпись

Способы проверки аппаратуры и каналов связи

- использование протоколов приема-передачи с квитированием (подтверждением полученных данных);
- идентификация аппаратных узлов удаленной информационной системы на программном уровне;
- контроль за маршрутом сообщений в компьютерных сетях;
- использование виртуальных защищенных каналов;
- процедуры «рукопожатий» при установлении и завершении сеансов связи.

Защита компьютерной информации и компьютерных систем от вредоносных программ

Объекты защиты

- локальный компьютер с периферийными устройствами;
- компьютерные сети.

Вредоносное программное воздействие

- ввод в компьютерную систему посторонним лицом или программой таких команд или данных, которые будут восприняты как инструкции законного пользователя или управляющей операционной системы.
- перехват управления, выполненный с необходимыми привилегиями, позволяет информационному нарушителю реализовать в отношении компьютерной информации или компьютерной системы любые угрозы.

Способы получения управления

- Узнать (подобрать, перехватить) имя и пароль полномочного пользователя, занять его рабочее место (в отсутствие пользователя) и зарегистрироваться в системе под чужим именем.
- Дождаться, когда пользователь, не прерывая сеанса, сделает перерыв в работе и покинет на время свое рабочее место, чтобы занять его.
- Использовать запущенный сетевой сервис на удаленном компьютере, ожидающий ввода команд по сети, и подобрать пароль для входа.
- Написать компьютерную программу (или использовать готовую) и создать предпосылки для ее запуска либо руками самого пользователя, либо операционной системой атакуемого

Компьютерные вирусы

- программа, которая может заражать другие программы, модифицируя их посредством добавления своей, возможно, измененной, копии. При этом копии вируса могут структурно и функционально отличаться между собой
- при вирусном заражении копируется код (бинарный или текстовый), причем созданный или модифицированный файл также должен уметь «размножаться» и иметь шансы на запуск отличаться между собой.

Признаки компьютерных вирусов

- размещение внутри файла с исполняемым или интерпретируемым кодом либо в ином программном фрагменте (например, в загрузочном секторе машинного носителя);
- способность к саморазмножению через внедрение в другие программы;
- выраженные деструктивные действия;
- наличие латентного (скрытого) периода между инфицированием и выполнением деструктивных действий.

Программные закладки

- Это программы слежения за пользователем и клавиатурные перехватчики.
- Универсальные многозадачные операционные системы неплохо защищают ресурсы компьютера от возможного деструктивного воздействия со стороны прикладных программ, но вот самим прикладным программам по умолчанию может быть разрешено «наблюдать» за чужими процессами и получать доступ в чужое адресное пространство.

Логические бомбы

- программа в определенное время или в определенной ситуации «взрывается»;
- представляют собой единичные строки в безусловно полезной программе, которые могут быть написаны программистом, разработавшим основную программу;

Программы «удаленного администрирования»

- Вредоносные клоны программ этого типа позволяют злоумышленнику получать удаленный сетевой доступ на чужие компьютеры.

Сетевые черви

- заражают не отдельные файлы, а сетевые узлы;
- сложная программа, использующая изъяны в операционных системах, почтовых программах, Интернет-браузерах для проникновения на другие сетевые узлы.

«Жадные» программы

- программы захватывают все ресурсы, которые им может предоставить операционная система, оставляя остальные работающие приложения на «голодном пайке».
- также используют «протоколы вежливости» и непрерывно бомбардирует систему многочисленными и бессмысленными запросами на обслуживание, в которых последняя по определению не может отказать.

Особенности вредоносных программ

- Самые объемные вредоносные программы (серверные модули программ удаленного администрирования) не превышают полутора сотен килобайт.
- Весь арсенал потенциально опасных действий содержится в операционной системе и в некоторых программируемых пользовательских приложениях.
- Вредоносной программе достаточно обратиться с вызовом нужной функции к системе, и опасные действия будут выполнены «чужими руками».

Внедрение вредоносных программ

- внедрение в атакованную компьютерную систему в форме записи вредоносного кода в адресное пространство компьютерной памяти.
- открытые телекоммуникационные сети.
- обман пользователя, в результате которого он своими руками запускает незнакомую и явно небезопасную программу («троянские кони»)

Противодействие вредоносным программам

- Определение сигнатуры вирусов при помощи программ-сканеров.
- Использование мониторов - антивирусные программы, постоянно находящиеся в памяти и контролирующие операции, которые можно считать подозрительными.
- Обеспечение нормально функционирующей изолированной программной среды.

Изолированная программная среда

- все необходимое программное обеспечение, включая библиотеки функций, тщательно протестировано на предмет выполнения только документированных функций;
- программы доступны пользователям только на исполнение;
- программы периодически контролируются на целостность посредством контрольной суммы;
- при обнаружении несоответствия контрольных сумм файл программы перед запуском заменяется резервным.

Безопасная компьютерная система

- пользователи не имеют права на разработку программ и должны использовать существующее прикладное программное обеспечение;
- на компьютере, обрабатывающем защищаемую информацию, не допускается создавать и отлаживать компьютерные программы, что исключает работу с программами типа отладчиков и дизассемблеров, мониторами файлов и реестра (тем не менее универсальная операционная среда в избытке содержит программы, позволяющие работать с оперативной памятью, редактировать файловую систему и др.);
- инсталляция (установка) и запуск новых программ в компьютерной системе должны производиться под контролем администратора и при включенной системе аудита.

Требования к безопасной системе

- Потенциально опасные программы и функции операционной системы должны быть недоступны для пользователей.
- Вызов потенциально опасных системных функций из прикладных программ должен производиться только от имени администратора или самой системы.
- Штатное программное обеспечение должно располагаться в каталогах, создание и изменение файлов в которых обычным пользователям запрещены.
- В системе должны предусматриваться меры против случайного запуска программ-двойников.
- Должен осуществляться контроль за открытием файлов с конфиденциальной информацией и конфигурационных файлов.

Семантическое сокрытие информации

Методы семантического сокрытия информации

- Скремблирование – скрывает различимость и разборчивость речевой (аналоговой) информации, передаваемой по открытым каналам связи
- Криптография - скрывает смысл дискретных сообщений как при передаче по открытым каналам связи, так и при их хранении на потенциально доступных нарушителю вещественных носителях
- Стеганография - скрывает не только смысл сообщений (дискретных и аналоговых), но и факт их передачи и хранения (факт присутствия защищаемой информации).

Категории нарушителей

- перехватывают открыто передаваемую конфиденциальную информацию в каналах связи
- осуществляют несанкционированный доступ к открыто хранимой информации

применение методов семантического сокрытия при высокой ценности информации заставляет нарушителя менять тактику действий и наряду с перехватом сообщений принимать меры по установлению наличия и извлечению скрываемой семантической информации

методы семантического сокрытия должны противодействовать подготовленному нарушителю в его попытках извлечь открытое сообщение в течение того срока, пока конфиденциальная информация имеет ценность в силу неизвестности ее третьим лицам.

Скремблирование

- В результате аналогового скремблирования из обычного речевого сигнала требуется получить преобразованный сигнал, занимающий ту же полосу частот, но обладающий свойствами неузнаваемости и неразборчивости.
- С двух сторон телефонного канала должны стоять одинаковые приемо-передающие устройства, производящие прямое и обратное преобразование сигнала

Скремблирование

- Аналоговый сигнал последовательно передается путем изменения (модуляции) одного из параметров по времени. Сигналы сложной формы, к которым относится и речь, состоят из большого числа гармонических составляющих.
- Принципы аналогового скремблирования заключаются в «перемешивании» элементов сообщения без добавления посторонней информации.

Формы скремблирования

- Временное скремблирование - сообщение делится на временные кванты, которые вначале запоминаются, а затем передаются в другом порядке. При этом происходит общая задержка сообщения
- Частотное скремблирование - спектр сигнала с помощью полосовых фильтров делится на отдельные полосы частот, которые по определенному закону меняются местами
- Комбинированное скремблирование использует временные и частотные перестановки

Особенности аналогового скремблирования

- Все перестановки фрагментов речевого сообщения производятся по псевдослучайному закону.
- Генераторы псевдослучайной последовательности в аппаратах на обоих концах линии связи одинаковы, но сама последовательность может от сообщения к сообщению меняться (переключаться).
- Обычные аналоговые скремблеры могут обеспечить низкую или среднюю стойкость к вскрытию.

Цифровое скремблирование

- вначале аналоговый сигнал превращается в цифровой код (аналого-цифровое преобразование), а дальнейшие преобразования осуществляются криптографическими методами

Особенности защиты

- Скремблирование защищает сообщения только в канале связи.
- Защита от перехвата этой же речевой информации, распространяющейся в виде акустических волн из пространственной области, в которой находится говорящий, производится иными методами

Криптографические методы

- шифрование и расшифровка передаваемых сообщений и хранимых блоков данных с помощью единственного секретного ключа (симметричные криптосистемы);
- шифрование и расшифровка передаваемых сообщений (точнее – передаваемых сеансовых ключей) с помощью двух взаимосвязанных ключей – открытого и закрытого (асимметричные криптосистемы);
- подтверждение авторства и целостности передаваемого сообщения, а также неоспоримости факта его передачи методами симметричной или асимметричной криптографии (электронная цифровая подпись).

Допущение криптографии

- при разработке и применении шифра надо исходить из того, что весь механизм шифрования, множество правил или алгоритмов рано или поздно становится известным оппоненту, поэтому стойкость шифра должна определяться только секретностью ключа
- вещественные носители с зашифрованной информацией, а также каналы связи, по которым передаются энергетические носители зашифрованной информации, доступны нарушителю.

Симметричное шифрование

- Симметричные криптосистемы используют многократно повторяемые операции замены, перестановки, аддитивные методы и их комбинации.
- При замене символы открытого текста или их комбинации заменяются символами из других словарей

Операции в симметричном шифровании

- Перестановка – это совершаемое по определенным правилам перемещение символов внутри шифруемого блока.
- Аналитические методы заключаются в использовании матричных преобразований над строками и столбцами шифруемых символов.
- Гаммирование – это операция «исключающего или» над двумя последовательностями: символами шифруемой последовательности и псевдослучайной последовательностью – гаммой

Криптоанализ

- Атака на криптозащиту производится методами криптоанализа.
- Для расшифровки чужих сообщений криптоаналитик должен по меньшей мере располагать множеством перехваченных криптограмм и некоторыми сведениями о зашифрованных сообщениях (отдельные фразы, тематика сообщений)

Слабые места симметричного шифрования

- Передающей и приемной стороне нужно знать и использовать один и тот же ключ.
- Реальные ключи шифрования, обеспечивающие гарантированную стойкость, должны быть сложными и достаточно длинными
- Машинные носители ключевой информации необходимо надежно хранить
- В тайне должна содержаться процедура шифрования – расшифровки. Если этот процесс происходит в компьютерной системе, он должен быть закрыт от перехвата информации со стороны программных закладок

Проблема скрытой передачи ключей

- Лица, обменивающиеся зашифрованными сообщениями, вначале должны договориться о способе создания, генерации и передачи секретного ключа.
- Если для этого используется открытый канал связи, то такой ключ может быть перехвачен и использован злоумышленником для расшифровки перехваченных сообщений.
- Требуется защита от фальсификации.
- Надо уничтожить ключ после его использования.

Проверка подлинности сообщений

- Если получателю удается расшифровать полученную криптограмму и он уверен, что второй экземпляр секретного ключа находится только у отправителя сообщения, значит, расшифрованный документ подлинный и действительно принадлежит отправителю.

Асимметричные криптосистемы

- Один из корреспондентов, пользуясь программно или аппаратно реализованными математическими алгоритмами, генерирует парные ключи шифрования.
- Ключи являются разными, и, зная один из них, невозможно определить другой. Нарушитель, пытающийся по известному ключу подобрать второй, должен столкнуться с непреодолимой вычислительной проблемой.
- Секретность можно обеспечить без засекречивания одного из ключей, а именно ключа шифрования.

Асимметричные криптосистемы

- Генерируются ключи парой, после чего открытый ключ можно послать корреспонденту, поместить его на сетевом сервере, опубликовать и т.д.
- Генератор ключей целесообразно располагать на стороне получателя, чтобы в дальнейшем не пришлось посылать закрытый ключ по открытому каналу.
- Асимметричные системы работают с очень длинными ключами, поэтому скорость криптопреобразований оказывается низкой.

Гибридные способы шифрования

- задействованы симметричная и асимметричная криптография
- отправитель шифрует свое сообщение по симметричному алгоритму сеансовым (одноразовым) ключом
- затем он же шифрует сеансовый ключ по асимметричному алгоритму с использованием открытого ключа
- зашифрованное сообщение и зашифрованный ключ передаются по открытому каналу связи получателю
- с помощью закрытого ключа получатель вначале восстанавливает сеансовый ключ, а затем расшифровывает само сообщение.

Системы с электронной цифровой подписью

- документ, как правило, не является секретным, но получателю требуется доказать, что он подписан определенным лицом и в пути следования не изменялся
- пользователь, подписывающий документ, генерирует два ключа. Открытый ключ он предоставляет получателю и всем лицам, которые нуждаются в доказательстве аутентичности и целостности информации
- документ шифруется закрытым ключом (точнее, документ вначале «сжимается» в хэш-образ, который и шифруется)
- документ вместе с «подписью» посылается адресату

Системы с электронной цифровой подписью

- Получатель частично повторяет действия отправителя: он тоже сжимает документ в хэш-образ, с помощью своего открытого ключа расшифровывает «подпись» и сравнивает две хэш-функции
- Если они идентичны, то документ действительно подписан лицом, имеющим закрытый ключ, и в пути не изменялся
- Если отправитель откажется от своего отправления, любое третье лицо, имеющее открытый ключ (например, судья), может легко установить истину

Проблемы криптозащиты

- совершенствование средств и методов криптоанализа
- необходимость защиты ключей
- возможности компьютеров непрерывно растут, и то, что десять лет назад считалось практически абсолютной защитой, сегодня вскрывается за несколько дней

Стеганография

- Файловая
- Поточная
- Дисковая

Файловая стеганография

- скрываемый файл предварительно сжимается, шифруется методами криптографии и помещается в стегоконтейнер, который тоже является файлом произвольного формата
- файл-контейнер может как увеличиться в объеме, так и сохранить свои прежние параметры.
- в зависимости от конкретных свойств файла-контейнера можно установить минимальный объем скрываемого сообщения, которое в принципе нельзя будет обнаружить.

Способы файловой стеганографии

- информацию можно «растворить» в элементах форматирования. Незаметные на глаз различия в межсимвольном и межстрочном расстоянии могут скрывать биты сообщения
- многие файлы, используемые для хранения комбинированных документов (.doc, .pdf и др.), имеют очень сложный и недокументированный формат, в элементах которого тоже можно скрыть предварительно зашифрованное сообщение
- предварительно зашифрованное сообщение можно разместить в свободных промежутках обычного исполняемого файла или «наложить» его на какой-нибудь сжатый файл большого размера, который выбран в качестве контейнера

Способы файловой стеганографии

- Чаще всего применяется техника наименее значащих бит. Человеческий глаз не способен уловить разницу в цветопередаче одиночных пикселов. Цветная фотографию размером 1024 x 768 пикселов и цветопередачей 3 байта на пиксел может содержать предварительно сжатый текст, первоначальным объемом более 700 килобайт
- Аналогичные возможности для сокрытия данных представляют звуковые файлы. Так, одна секунда «живого» звука имеет объем 88 килобайт и может скрывать до 10 килобайт информации

Стеганоанализ

- Проводится статистическая обработка наименее значимых бит в «подозреваемом» файле.
- Предварительно сжатый и зашифрованный файл характеризуется примерно равной вероятностью нулей и единиц в младших разрядах байт, и по этому признаку можно установить файл-контейнер

Поточная стеганография

- скрытая передача сообщений в потоке данных
- скрытную передачу сообщений в потоке данных
- 20-байтные заголовки IP/TCP-пакетов содержат в себе неиспользуемые поля общим объемом в несколько байт
- к часто используемым ICMP-пакетам (известная команда ping для установления присутствия нужного IP-адреса в сети) можно «прицепить» довольно длинное зашифрованное сообщение

Дисковая стеганография

- Информацию можно записать в микросхемы энергонезависимой памяти, расположенные на материнской плате, в видеоадаптере, на сетевой плате
- В связи с тем, что содержимое этой памяти, во-первых, не используется современными операционными системами, а во-вторых, не подлежит просмотру штатными программными средствами, вместе с аппаратурой (под видом комплектующих, запасных частей) можно хранить и передавать огромное количество информации