ITCOM ACADEMY

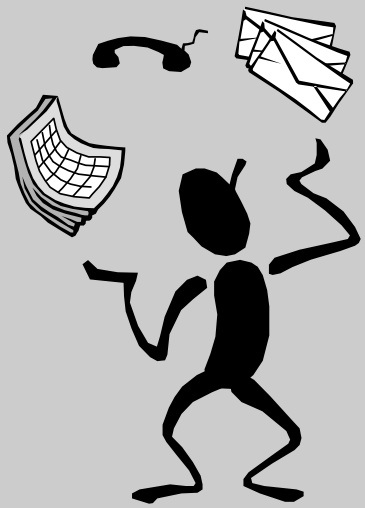
Что такое информация и как она хранится

ITCOM ACADEMY

Термин ***информация***

происходит от латинского слова ***information,***

что означает ***сведения, разъяснения, изложение.***



Понятие информации в человеческой деятельности:

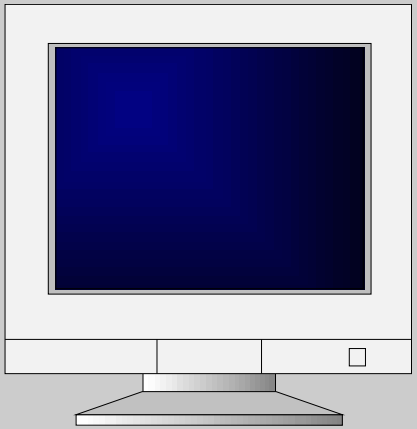
в быту информацией называют любые данные, сведения, знания, которые кого-либо интересуют. Например, сообщение о каких-либо событиях, о чьей-либо деятельности

в технике под **информацией** понимают сообщения, передаваемые в форме знаков или сигналов

в биологии понятие **«информации»** связывается с поведением живых организмов, а также в связи с исследованиями механизмов наследственности.

в информатике

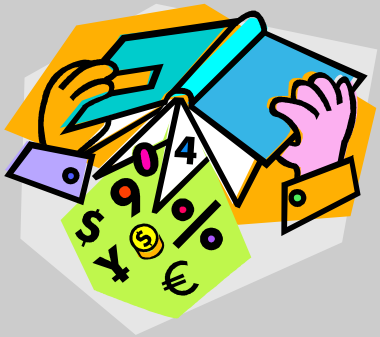
информация – это знания человека, которые он получает из окружающего мира которые реализует с помощью вычислительной техники.



Свойства информации:

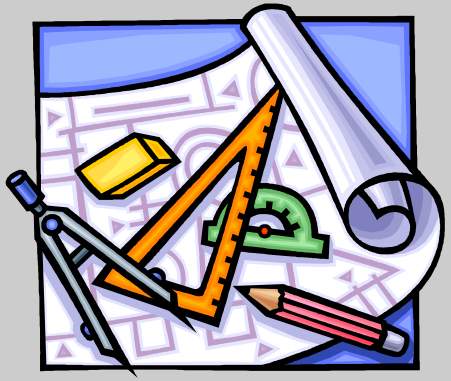
- ***Понятность*** - изложенная на доступном для получателя языке
- ***Достоверность*** - отражающая истинное положение дел
- ***Актуальность*** - существенно важная в настоящий момент
- ***Полнота и точность*** - содержание всего необходимого для понимания информации
- ***Полезность.***

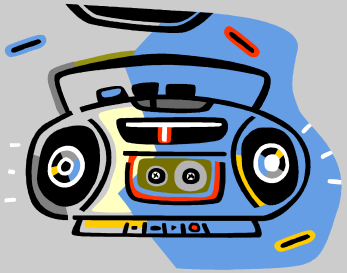
Формы представления информации:



текстовая

графическая





звуковая

символьная

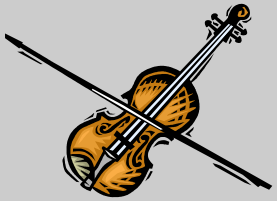
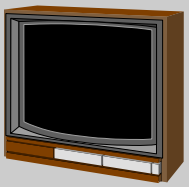
Виды информации:

Аналого-непрерывная

(воспринимается человеком)

- визуальная
- аудиальная
- тактильная
- вкусовая

Источники:

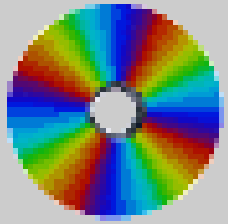
Информационные процессы:

Информационными процессами называют процессы, связанные с получением, хранением, обработкой и передачей информации.

Хранение информации – это её накопление на различных носителях.

Носитель информации – среда для записи и хранения информации.

ВНЕШНЯЯ ПАМЯТЬ



Внешняя память – это устройства, предназначенные для долговременного хранения больших объёмов информации.

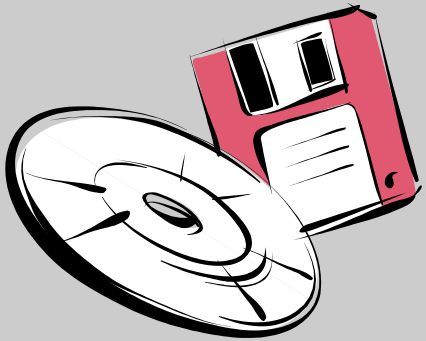
Внешняя память **энергонезависима**, характеризуется меньшим быстродействием в сравнении с внутренней памятью, но имеет намного больший информационный объём.

Устройства внешней памяти ***(накопители)*** обеспечивают запись информации на ***носители информации***, а также считывание информации с носителей.

Накопитель информации — устройство записи, воспроизведения и хранения информации, а ***носитель информации*** — это предмет, на который производится запись информации (диск, лента, твердотельный носитель).

Внешние носители информации:

- бумага;
- фото- и киноплёнка;
- компакт – диски;



Каждый человек хранит определённую информацию в собственной памяти – «в уме». Вы помните свой адрес, номер телефона, как зовут ваших родных и близких, друзей. Такую память можно назвать **оперативной**.

Но есть информация, которую трудно запомнить. Её человек записывает в записную книжку, ищет в справочнике, словаре, энциклопедии. Это внешняя память. Её можно назвать **долговременной.**

У компьютера также существует два вида памяти.

Оперативная память – предназначена для **временного хранения** информации, т.е. на момент когда компьютер работает (после выключения компьютера информация удаляется с оперативной памяти).

Долговременная память (внешняя) – для **долгого хранения** информации (при выключении компьютера информация не удаляется).

Существует память отдельного человека и память человечества. Память человечества, в отличие от памяти человека, содержит все знания, которые накопили люди за время своего существования и которыми могут воспользоваться ныне живущие люди. Эти знания представлены в книгах, запечатлены в живописных полотнах, скульптурах и архитектурах произведениях великих мастеров.

Изобретённая в 1839 году фотография позволила сохранить для потомков лица людей, пейзажи, явления природы и другие зримые свидетельства прошедших времён.

В 1895 году в Париже был продемонстрирован первый в мире кинофильм. С той поры человечество получило возможность сохранять образы, воплощенные в движении (танец, жесты, пантомимы и т.д.).

Человек научился хранить и звуковую информацию. Вначале её сохранение обеспечивалось передачей «из уст в уста» (например, напевами), позднее – с помощью записи нот.

В середине прошлого столетия в Японии было налажено производство магнитофонов. До сих пор магнитофоны применяются для записи и воспроизведение звуков информации

Бумажные носители

Бумага изобретена во II веке н.э. в Китае.
Информационный объём книги из 300 страниц по 2000 символов на странице составляет примерно 600 000 байтов, или 586 Кб.
Школьная библиотека из 5000 томов имеет информационный объём приблизительно 2861Мб=2,8 Гб
На первых компьютерах использовали бумажные носители – перфолента и перфокарта.

Магнитные носители

В XIX веке была изобретена магнитная запись (на стальной проволоке диаметром 1 мм).
В 1906 году был выдан патент на магнитный диск.
Ферро магнитная лента использовалась как носитель для ЭВМ первого и второго поколения. Её объем был 500 Кб. Появилась возможность записи звуковой и видео информации.

В начале 1960-х годов в употребление входят магнитные диски.
Винчестер компьютера — это пакет магнитных дисков, надетых на общую ось. Информационная емкость современных винчестеров измеряется в Гб.

Компакт-диск (англ. Compact Disc) — **оптический носитель** информации в виде пластикового диска с отверстием в центре, процесс записи и считывания информации которого осуществляется при помощи лазера.

Жесткий диск

Взглянув на накопитель на жестком диске, вы увидите только прочный металлический корпус. Он полностью герметичен и защищает дисковод от частичек пыли, которые при попадании в узкий зазор между головкой и поверхностью диска могут повредить чувствительный магнитный слой и вывести диск из строя. Кроме того, корпус экранирует накопитель от электромагнитных помех.

Сведения из истории:

В 1973 году на фирме IBM по новой технологии был разработан первый жесткий диск, который мог хранить до 16 Кбайт информации.

Этот диск имел 30 цилиндров (дорожек), каждая из которых была разбита на 30 секторов

По аналогии с автоматическими винтовками, имеющими калибр 30/30, такие жесткие диски получили прозвище «винчестер».

ЖЕСТКИЕ МАГНИТНЫЕ ДИСКИ

Первый накопитель на жестких дисках IBM 350 Disk File разработан в 1955 году.

Накопитель емкостью 5 Мбайт состоял из 50 дисков диаметром 24 дюйма, вращавшихся со скоростью 1200 об/мин.

Размер накопителя был сравним с двумя современными двухкамерными холодильниками.

Первый HDD емкостью 5 Мбайт

Flash – диски (карты)

Flash-память - это **энергонезависимый** тип памяти, позволяющий записывать и хранить данные в микросхемах. Устройства на основе flash-памяти **не имеют** в своём составе **движущихся частей**, что обеспечивает высокую сохранность данных при их использовании в мобильных устройствах.

Flash-память представляет собой микросхему, помещенную в миниатюрный корпус. Для записи или считывания информации накопители подключаются к компьютеру через USB-порт. Информационная емкость карт памяти до 128 Гбайт.

Еще одно неоспоримое преимущество состоит в том, что когда флэш-память сжата в сплошную карту, ее практически невозможно разрушить какими-то стандартными физическими способами, поэтому она выдерживает кипящую воду и высокое давление

Зачем нужно защищать информацию

Направления информационной защиты

- Нормативно-правовое регулирование защиты информации
- Организационно-распорядительная защита
- Инженерная защита и техническая охрана объектов информатизации
- Защита информации от утечки по техническим каналам
- Обнаружение и нейтрализация средств технической разведки

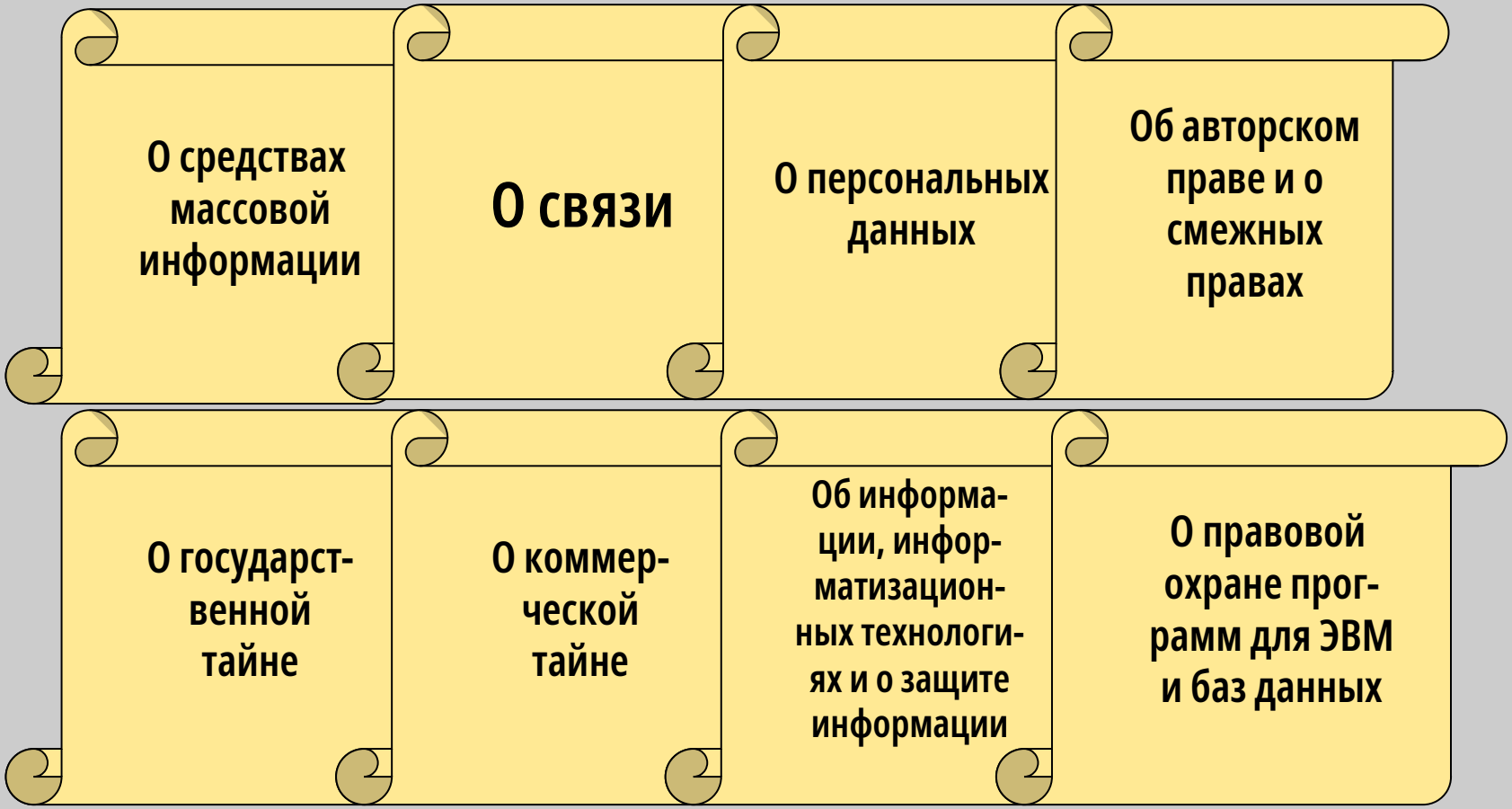
Направления информационной защиты

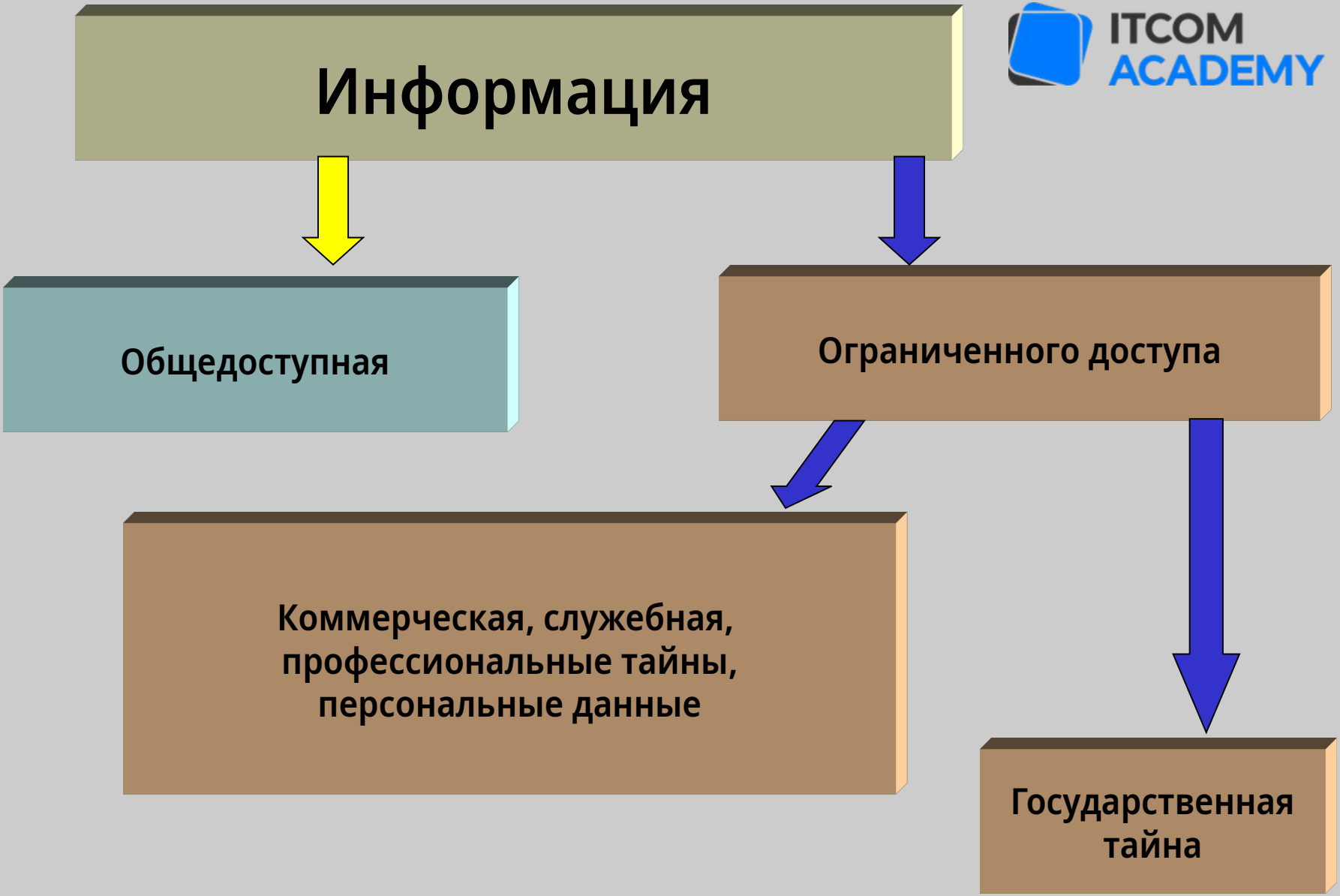
- Управление доступом к информации
- Защита компьютерных систем от вредоносных программ
- Семантическое сокрытие информации
- Обеспечение нормальных условий эксплуатации информационных систем и машинных носителей информации

Защита информации - это защита прав собственности на нее

Обладателями информации могут быть физические и юридические лица, Российская Федерация, ее субъекты и муниципальные образования

Законодательство РФ в области защиты информации




Информация
Общедоступная
Ограниченного доступа
Коммерческая, служебная, профессиональные тайны, персональные данные
Государственная тайна

Информация, общедоступная по закону

- Законодательные и другие нормативные акты
- Информация о чрезвычайных ситуациях
- Информация о деятельности органов государственной власти и местного самоуправления
- Открытые фонды библиотек и архивов

Сведения, относящиеся к государственной тайне

- Правами на распоряжение сведениями, относимыми к государственной тайне, обладает государство в лице своих институтов
- Уровень (степень) секретности - это мера ответственности лица за утечку или утерю конкретной информации
- Степени секретности: секретно, совершенно секретно, особой важности

Конфиденциальная информация

- Защита определяется собственником информации
- Государство содействует защите конфиденциальной информации, если установлена ее документированность и ценность для собственника
- Конфиденциальная информация образует набор частных тайн (личной жизни, коммерческой, врачебной, адвокатской и др.)

Виды информации ограниченного доступа

ITCOM ACADEMY

- Коммерческая тайна (научно-техническая, технологическая, производственная, финансово-экономическая и иная деловая информация)
- Персональные данные, а также личная и семейная тайна, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений
- Профессиональные тайны - адвокатская, журналистская, врачебная, нотариальная, тайна усыновления, страхования, связи, а также налоговая и банковская тайны в отношении персональной информации о клиентах
- Государственная служебная тайна
- Процессуальная тайна

Информационные преступления преследуются в соответствии с уголовным законодательством

Правонарушения в информационной сфере регулируются

Административным законодательством

Обеспечение информационной защиты достаточно противоречиво

ITCOM ACADEMY

«Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом ...».

Ст. 29 Конституции РФ

«... каждый гражданин имеет право на неприкосновенность частной жизни, личную и семейную тайну».

Ст. 23 Конституции РФ

ITCOM ACADEMY

Субъект угрозы - человек, причем не только из посторонних лиц, но и из числа своего персонала

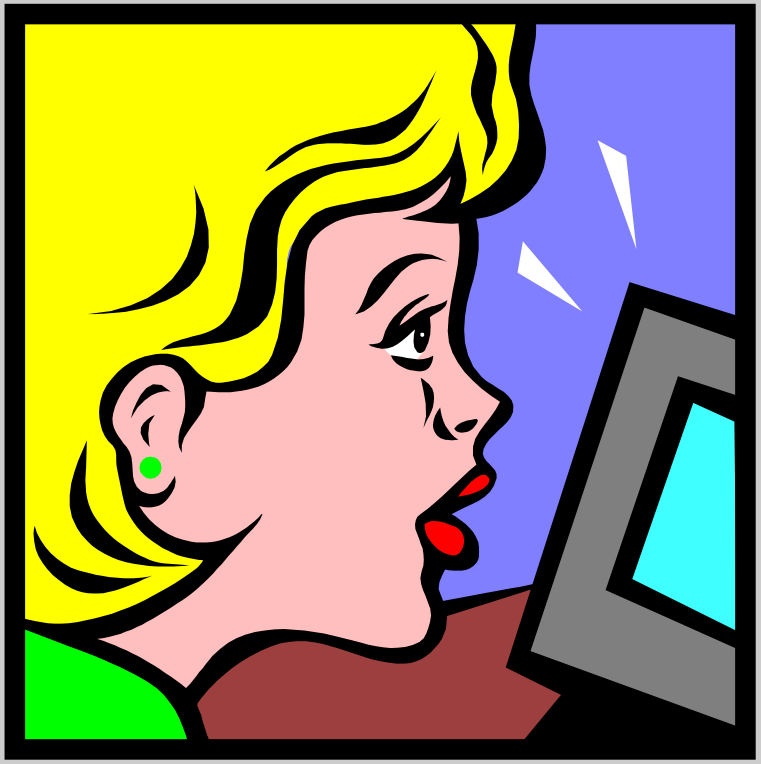
ITCOM ACADEMY

Наиболее уязвимым компонентом информационной системы является персонал.

По его вине совершается до 80% информационных преступлений

ITCOM ACADEMY

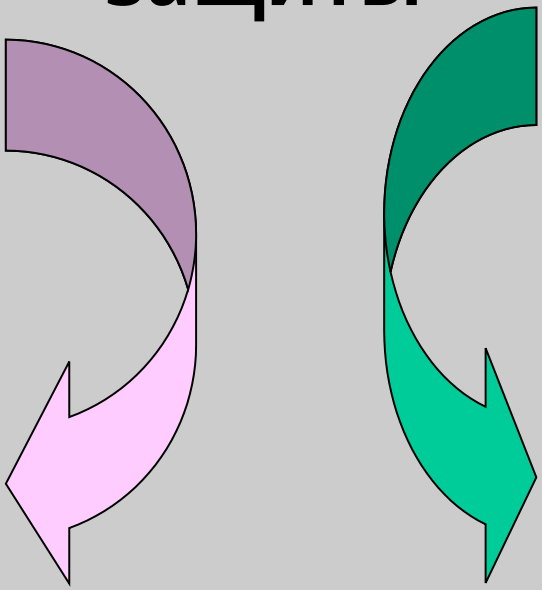
Объект защиты — это секретная и конфиденциальная информация на любых носителях



ITCOM ACADEMY

Большинство пользователей, к сожалению, являются скорее противниками любой системы защиты, чем ее союзниками до тех пор, пока жизнь сама не научит их бдительности

Направления организационно-распорядительной защиты



Работа с кадрами

Обеспечение внутриобъектового режима

ITCOM ACADEMY

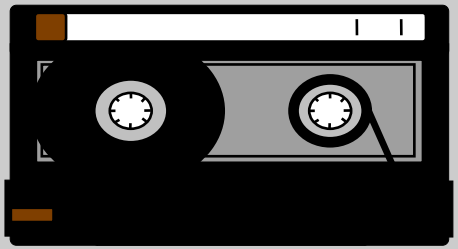
Каждый сотрудник должен знать только то, что необходимо ему для выполнения служебных обязанностей

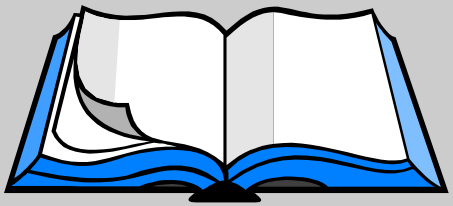
Постулаты физической охраны

ITCOM ACADEMY

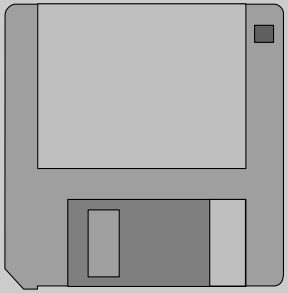
- Основная угроза - проникновение «извне»
- Субъект угрозы - человек-нарушитель
- Методы защиты: физическая изоляция ценностей, создание механических и иных препятствий нарушителю, технический контроль охраняемого пространства, реагирование на тревожные сигналы

Объекты защиты



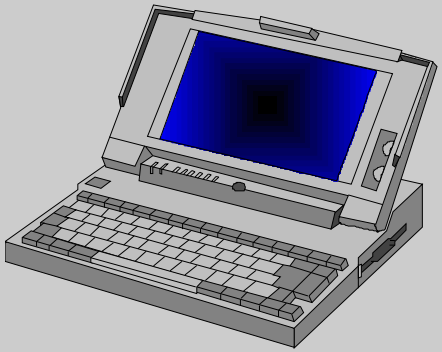


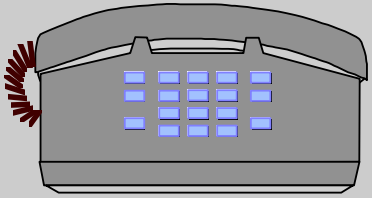
Вещественные носители информации



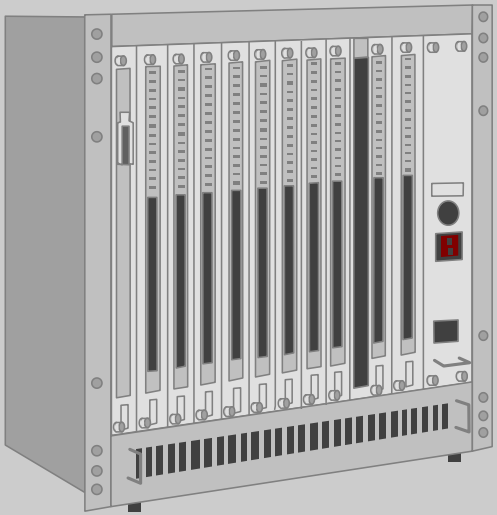
Объекты защиты

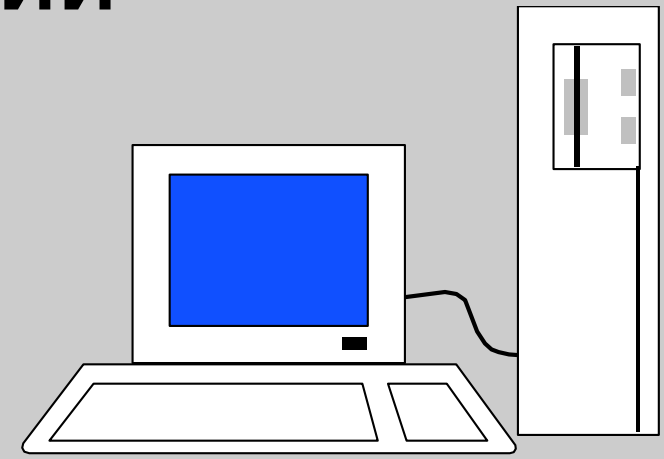
ITCOM ACADEMY





Технические средства обработки информации





Объекты защиты

Персонал объекта информатизации

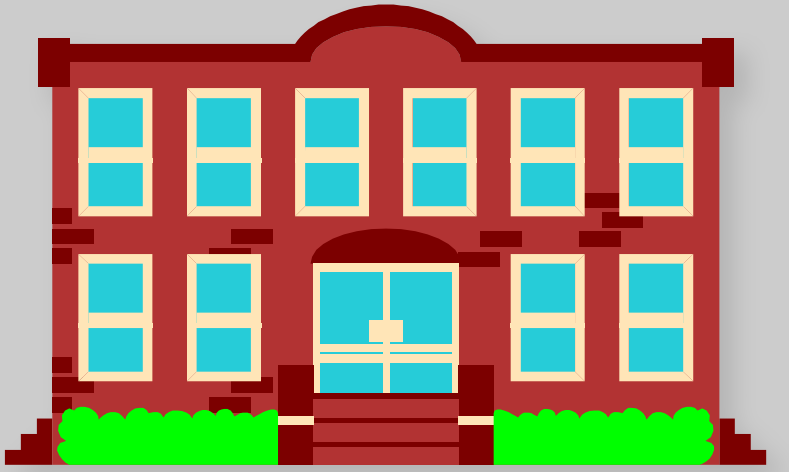
(на рабочих местах)

Объекты защиты

ITCOM ACADEMY

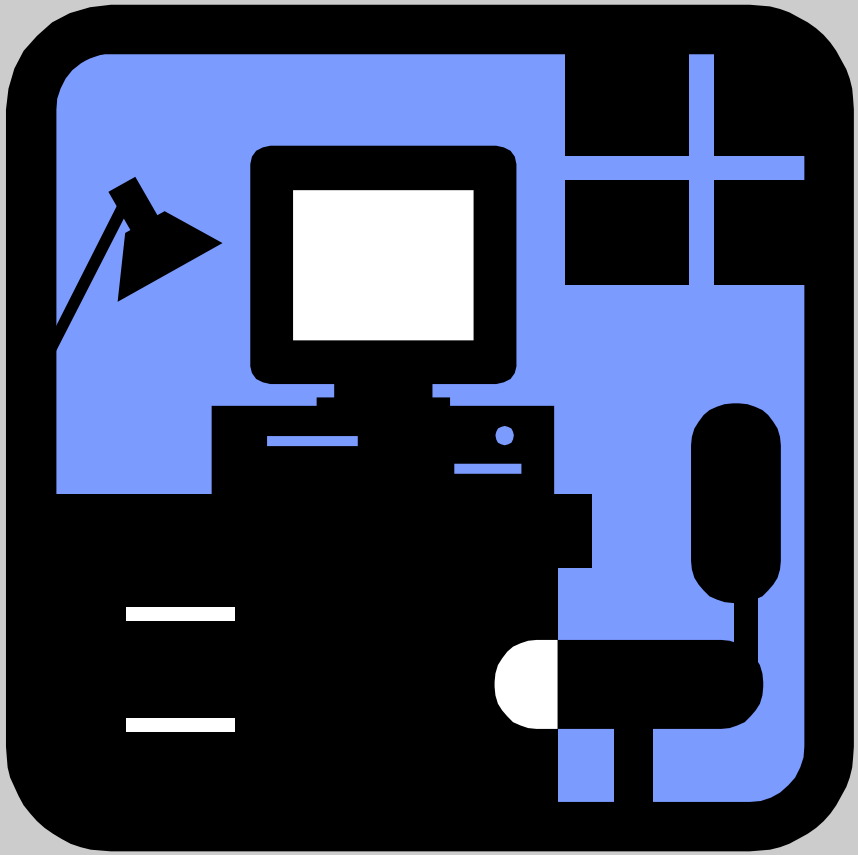
Территория с огороженным или обозначенным периметром

Объекты защиты



Здания, комплексы зданий и сооружений, к которым возможен свободный доступ

Объекты защиты



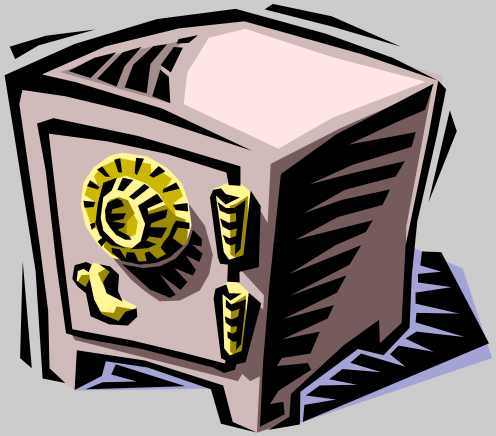
Отдельные помещения

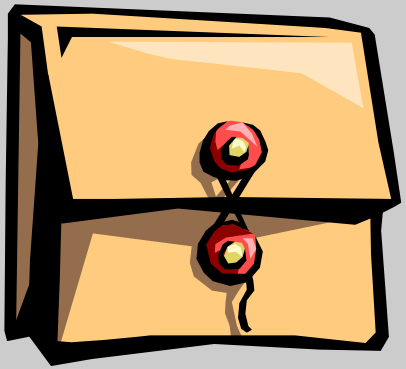
Объекты защиты

ITCOM ACADEMY

Рабочие места сотрудников

Объекты защиты





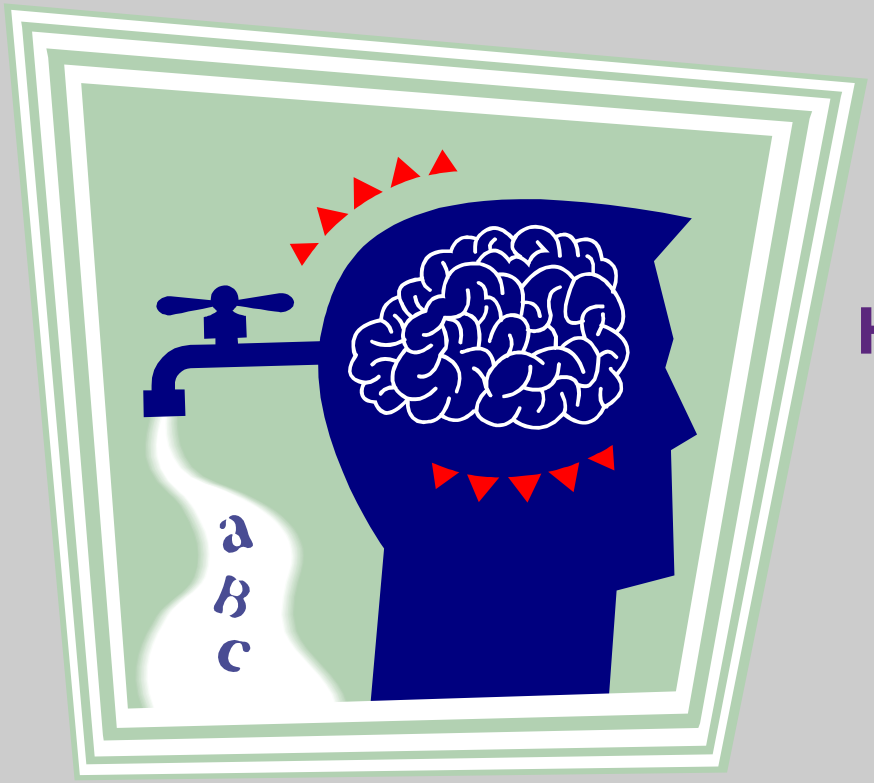
Предметы внутри помещений: сейфы, металлические шкафы и иные хранилища ценностей, документов, машинных носителей информации, компьютеры, средства связи, множительная техника, настенные схемы, карты, планы и др.

ITCOM ACADEMY

Субъектом угрозы является человек-нарушитель, проникающий на охраняемый объект извне

Как избежать утечки информации

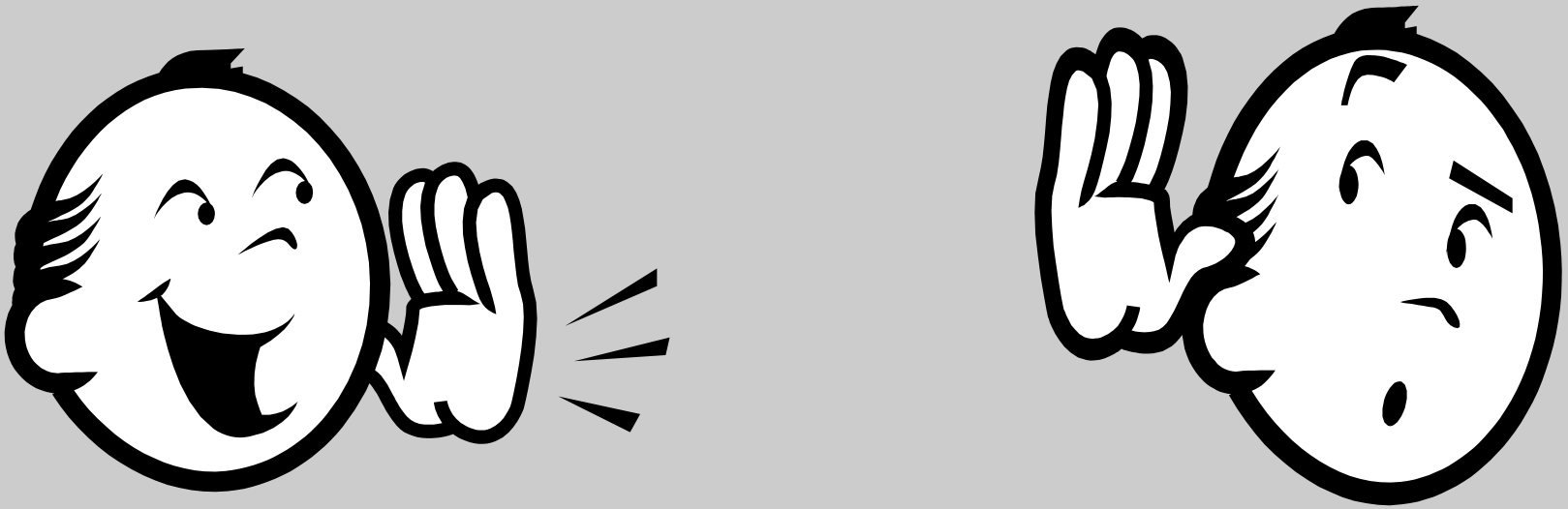
Утечка информации



Утечка информации - несанкционированный процесс переноса информации от источника к злоумышленнику

ITCOM ACADEMY

Физический путь переноса информации от ее источника к несанкционированному получателю называется каналом утечки

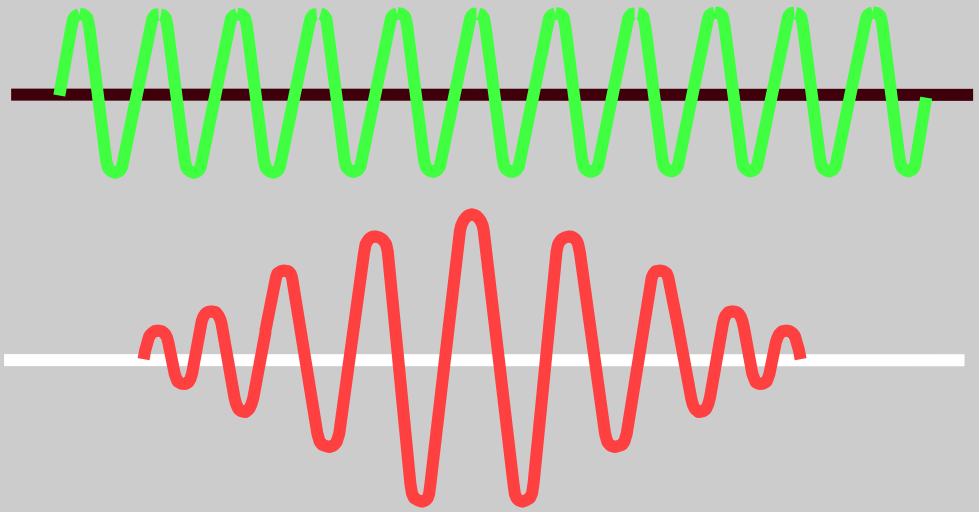


Технический канал утечки:

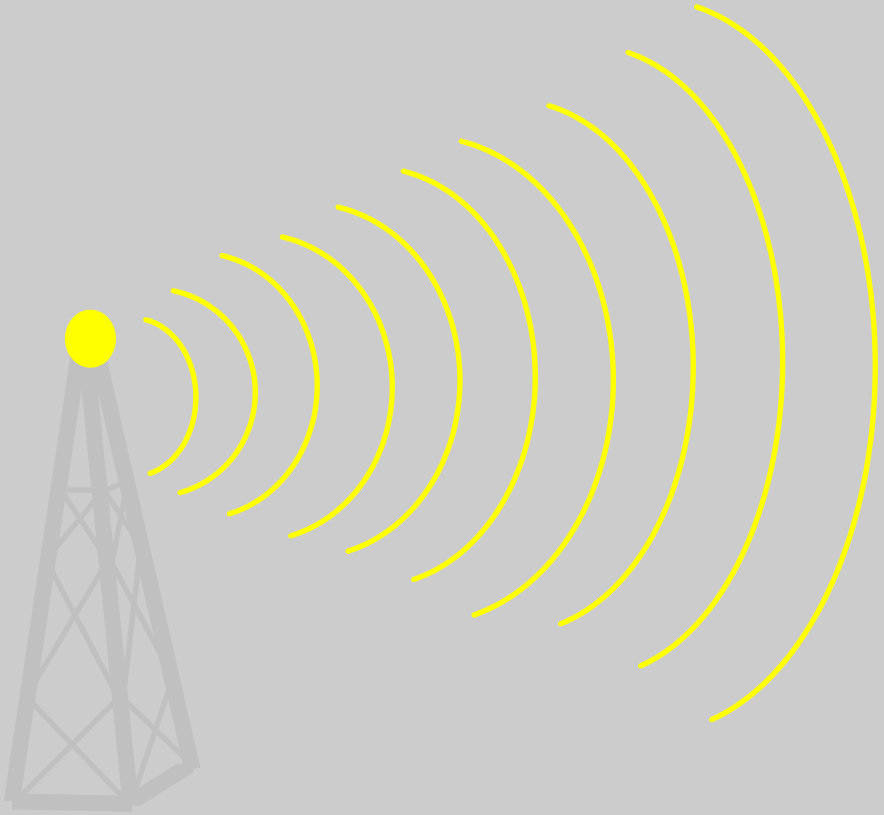
- Объект разведки
- Техническое средство перехвата информации
- Физическая среда, в которой распространяется информационный сигнал

От многих источников могут распространяться несанкционированные сигналы с защищаемой информацией.
Такие сигналы могут возникать случайно или создаваться злоумышленниками.
Эти сигналы условно называются опасными

«Опасными» являются не сами сигналы, а их параметры (амплитуда, частота, фаза, длительность, полярность и др., используемые для модуляции и кодирования



Электромагнитные каналы утечки информации

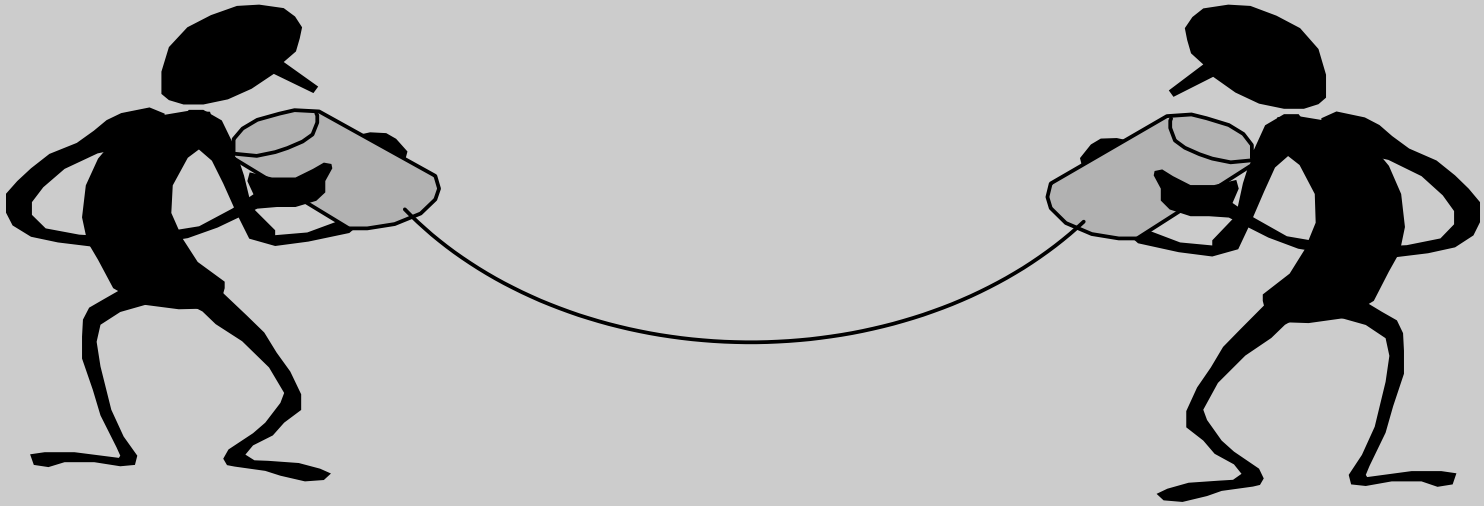


В качестве носителей используются электрические, магнитные и электромагнитные поля, а также электрические токи, распространяющиеся в проводящих средах

Акустические каналы утечки информации

ITCOM ACADEMY

Носителями информации являются механические упругие акустические волны в инфразвуковом (менее 16 Гц), звуковом (16 Гц - 20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, распространяющиеся в атмосфере, воде и твердой среде



Оптические каналы утечки информации

В качестве носителей используется электромагнитное поле в диапазоне 0.46-0.76 мкм (видимый свет) и 0.76-13 мкм (инфракрасное излучение)

Материально-вещественные каналы утечки информации

ITCOM ACADEMY

Вещественные носители с защищаемой информацией:

черновики документов, использованная копировальная бумага, неисправные машинные носители, бракованные детали и узлы, демаскирующие вещества, по которым можно определить состав, структуру, свойства и технологию получения новых материалов, демаскирующие вещества, по которым можно определить состав, структуру, свойства и технологию получения новых материалов

Использование большей части каналов утечки информации возможно лишь благодаря специальным техническим средствам

Защита компьютерных систем от вредоносных программ

- Объект защиты - компьютерная информация
- Нарушитель - вредоносная программа или управляющее воздействие
- Методы - сканирование памяти на предмет обнаружения известной сигнатуры и мониторинг обращений к ресурсам, дискам, файлам и устройствам

Поскольку компьютер является *программно управляемым устройством*, основным видом доступа к хранимой и обрабатываемой на нем информации является *программный доступ*, позволяющий манипулировать данными

Путем перехвата управления можно “заставить” компьютер выполнить действия против интересов его владельца (пользователя) информации

Способы управления компьютерной системой

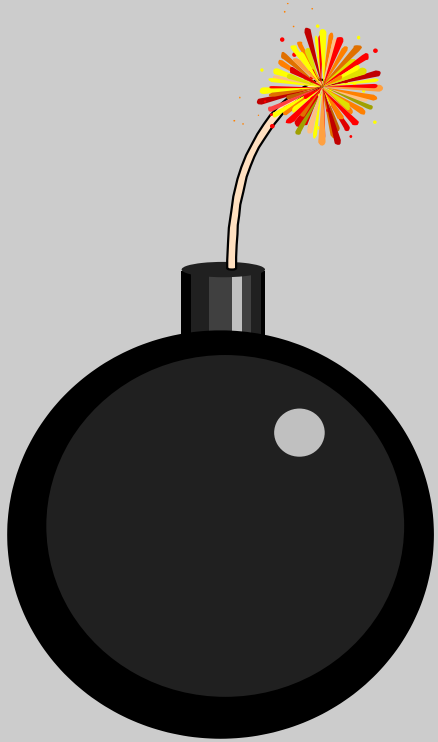
ITCOM ACADEMY

- Внедрение и автономное исполнение готовых программ
- Создание и запуск исполняемого кода непосредственно на атакуемом компьютере
- Ручное управление процессами с помощью манипуляторов и клавиатуры
- Дистанционное (удаленное) управление компьютером с использованием сетевых протоколов и специальных клиент-серверных программ

Вредоносные программы

ITCOM ACADEMY

Это программы, предназначенные для несанкционированного *копирования, модификации, блокирования и уничтожения* компьютерной информации



Методы защиты от вредоносного программного воздействия

- Защита целостности сертифицированных программ
- Антивирусная защита (сканирование, мониторинг, лечение)
- Защита от программных закладок
- Организационные формы защиты от случайного запуска

Управление доступом к информации

Объекты идентификации и аутентификации

- Человек (пользователь, оператор)
- Техническое средство (персональный компьютер, консоль, терминал)
- Документы (данные, сообщения)
- Компьютерные программы
- Машинные носители информации
- Информация, выводимая на дисплей, табло

Проверка подлинности элементов компьютерной системы

- Прав пользователя
- Персонального компьютера или терминала
- Программы идентификации и аутентификации
- Документа, с которым работает пользователь

ITCOM ACADEMY

Процедура управления доступом должна заключаться в том, чтобы легальные пользователи имели максимально простой доступ, а нелегальные - максимально сложный

Средства защиты информации

К средствам защиты информации ИС от действий субъектов относятся:

- средства защита информации от несанкционированного доступа;
- защита информации в компьютерных сетях;
- криптографическая защита информации;
- электронная цифровая подпись;
- защита информации от компьютерных вирусов

ITCOM ACADEMY

Зашифрованные данные защищены настолько, насколько защищен ключ дешифрования

Если Вы оставили ключ в дверях,
их прочность уже не имеет
никакого значения

Защита информации в сетях

Локальные сети предприятий очень часто подключаются к сети Интернет. Для защиты локальных сетей компаний, как правило, применяются межсетевые экраны - брандмауэры (файрволлы).

Экран (firewall) - это средство разграничения доступа, которое позволяет разделить сеть на две части (граница проходит между локальной сетью и сетью Интернет) и сформировать набор правил, определяющих условия прохождения пакетов из одной части в другую. Экраны могут быть реализованы как аппаратными средствами, так и программными.

Защита информации от компьютерных вирусов

Компьютерный вирус – это небольшая вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в программы (исполняемые файлы), документы, загрузочные сектора носителей данных и распространяться по каналам связи.

В зависимости от среды обитания основными типами компьютерных вирусов являются:

- Программные вирусы
- Загрузочные вирусы
- Макровирусы
- Сетевые вирусы

Источниками вирусного заражения могут быть съемные носители и системы телекоммуникаций.

Защита персональных данных

- Конституция РФ закрепила свободу поиска, получения, передачи, производства и распространения информации (ч. 4 ст. 29), гарантировала право на неприкосновенность частной жизни, личную, семейную тайну, тайну сообщений и запретила распространение информации о частной жизни лица без его согласия (ст. 23, 24).
- Жизнедеятельность человека предполагает предоставление информации о себе другим членам общества.
- Отношения по предоставлению и охране информации регулируются нормами российского права.

Персональные данные

ITCOM ACADEMY

Согласно ст. 3 Закона о персональных данных

Персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Законодательство РФ в сфере защиты персональных данных.

Основой основ является Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»

Что такое персональные данные?

Это **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.

Правовое регулирование

Правоотношения в сфере персональных данных регулируются федеральным законодательством РФ (Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»), Трудовым кодексом РФ (глава 14), а так же Гражданским кодексом РФ.

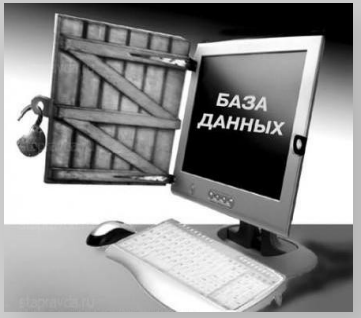
Защита персональных данных

- *Защита персональных данных* – это комплекс мероприятий, позволяющий выполнить требования законодательства РФ, касающиеся обработки, хранению и передачи персональных данных граждан.

Комплекс мероприятий по обеспечению защиты ПД

Технические меры по защите персональных данных предполагают использование программно - аппаратных средств защиты информации.

При обработке ПД с использованием средств автоматизации, применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется исходя из класса системы персональных данных.



Кто такой оператор ПД?

ITCOM ACADEMY

Оператор персональных данных - государственный орган, муниципальный орган, юр. или физ. лицо, организующие и (или) осуществляющие обработку ПД, а также определяющие цели и содержание обработки ПД.

Закон «О персональных данных» обязывает оператора принимать необходимые организационные и технические меры для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

На кого распространяется Закон?

В любой компании, вне зависимости от её организационно-правовой формы, есть информация о сотрудниках, работающих в организации, а иногда и её контрагентах.

Таким образом такая компания является оператором персональных данных, действия ФЗ-152 распространяются и на неё.

Ответственность

ITCOM ACADEMY

За нарушения законодательных актов РФ, регулирующих правоотношения в сфере ПД предусмотрены следующие санкции:

1. Привлечение к административной и гражданской ответственности
2. Направление в органы прокуратуры материалов о возбуждении уголовных дел
3. Прекращение обработки персональных данных
4. Приостановление деятельности оператора в случае осуществления ее без лицензии
5. Конфискация несертифицированных средств обеспечения безопасности и шифровальных средств

Общие принципы политики безопасности

Минимальный уровень привилегий

ITCOM ACADEMY

Одним из таких принципов является предоставление каждому сотруднику предприятия того *минимально уровня привилегий* на доступ к данным, который необходим ему для выполнения его должностных обязанностей.

Ввести четкие ограничения для всех пользователей сети, не наделяя их излишними возможностями.

Баланс надежности защиты всех уровней

Используя многоуровневую систему защиты, важно обеспечивать *баланс надежности защиты всех уровней.*

- Если в сети все сообщения шифруются, но ключи легкодоступны, то эффект от шифрования нулевой.
- Если на компьютерах установлена файловая система, поддерживающая избирательный доступ на уровне отдельных файлов, но имеется возможность получить жесткий диск и установить его на другой машине, то все достоинства средств защиты файловой системы сводятся на нет.
- Если внешний трафик сети, подключенной к Интернету, проходит через мощный брандмауэр, но пользователи имеют возможность связываться с узлами Интернета по коммутируемым линиям, используя локально установленные модемы, то деньги (как правило, немалые), потраченные на брандмауэр, можно считать выброшенными на ветер.

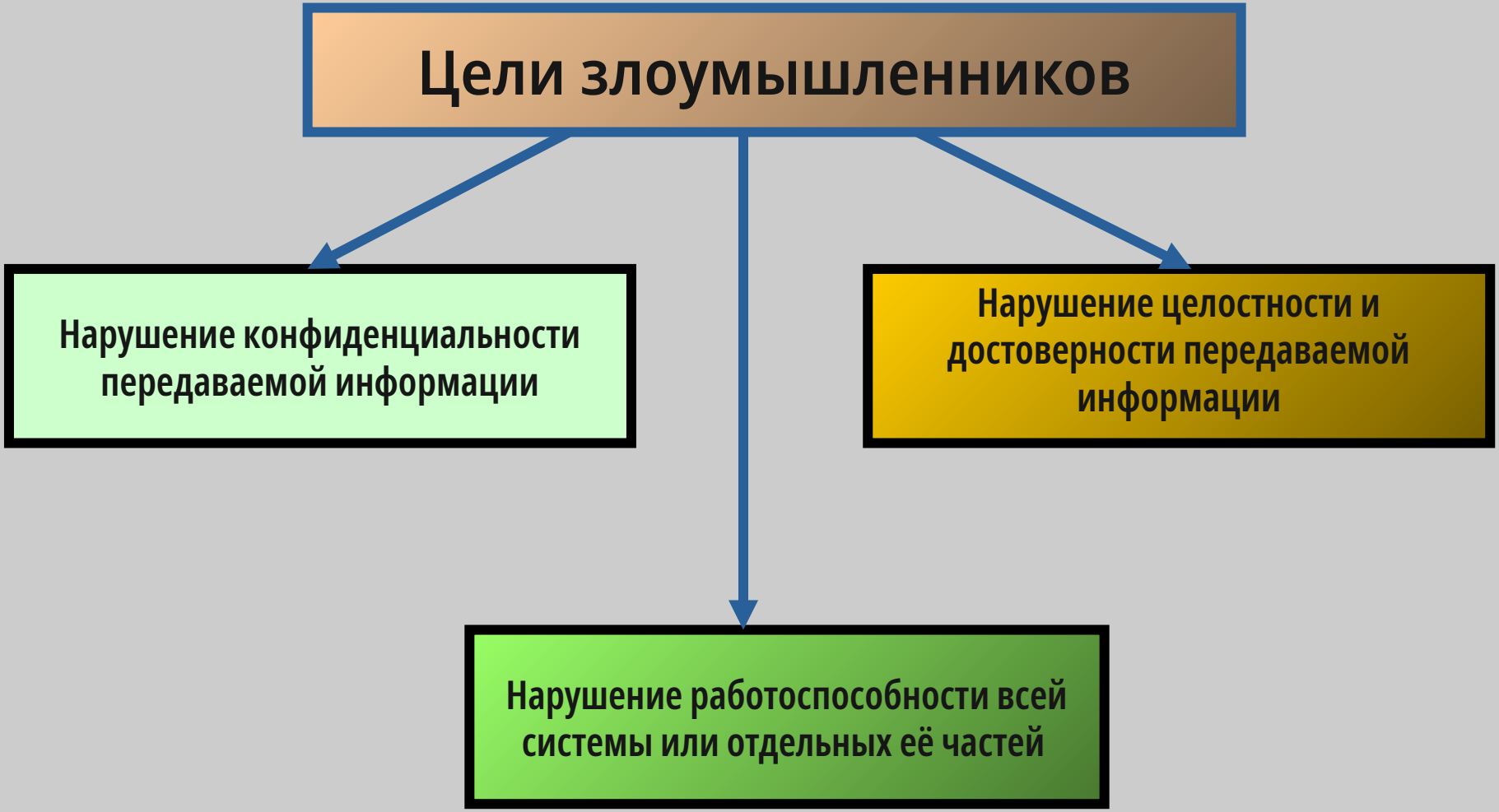
Принцип единого контрольно-пропускного пункта

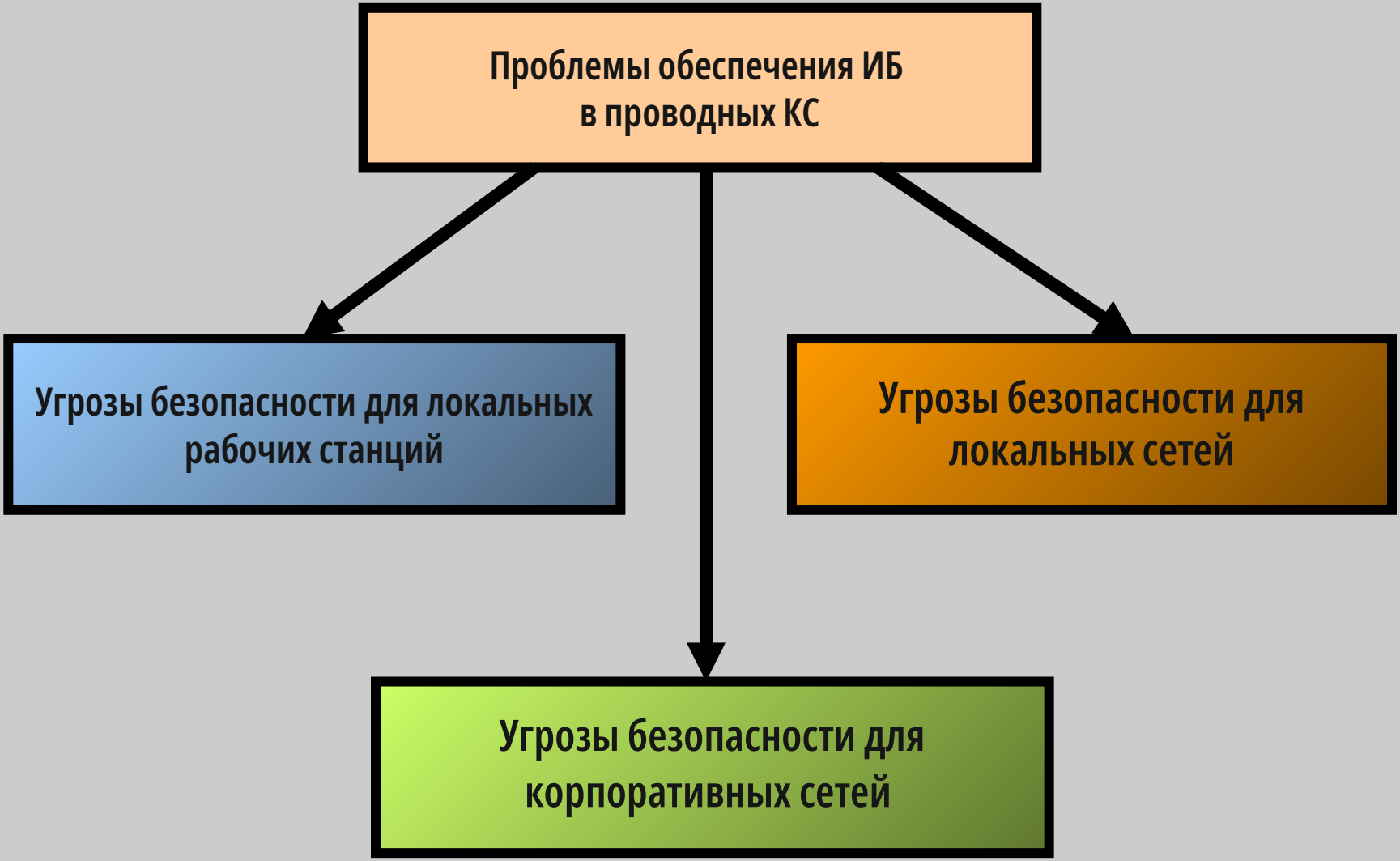
ITCOM ACADEMY

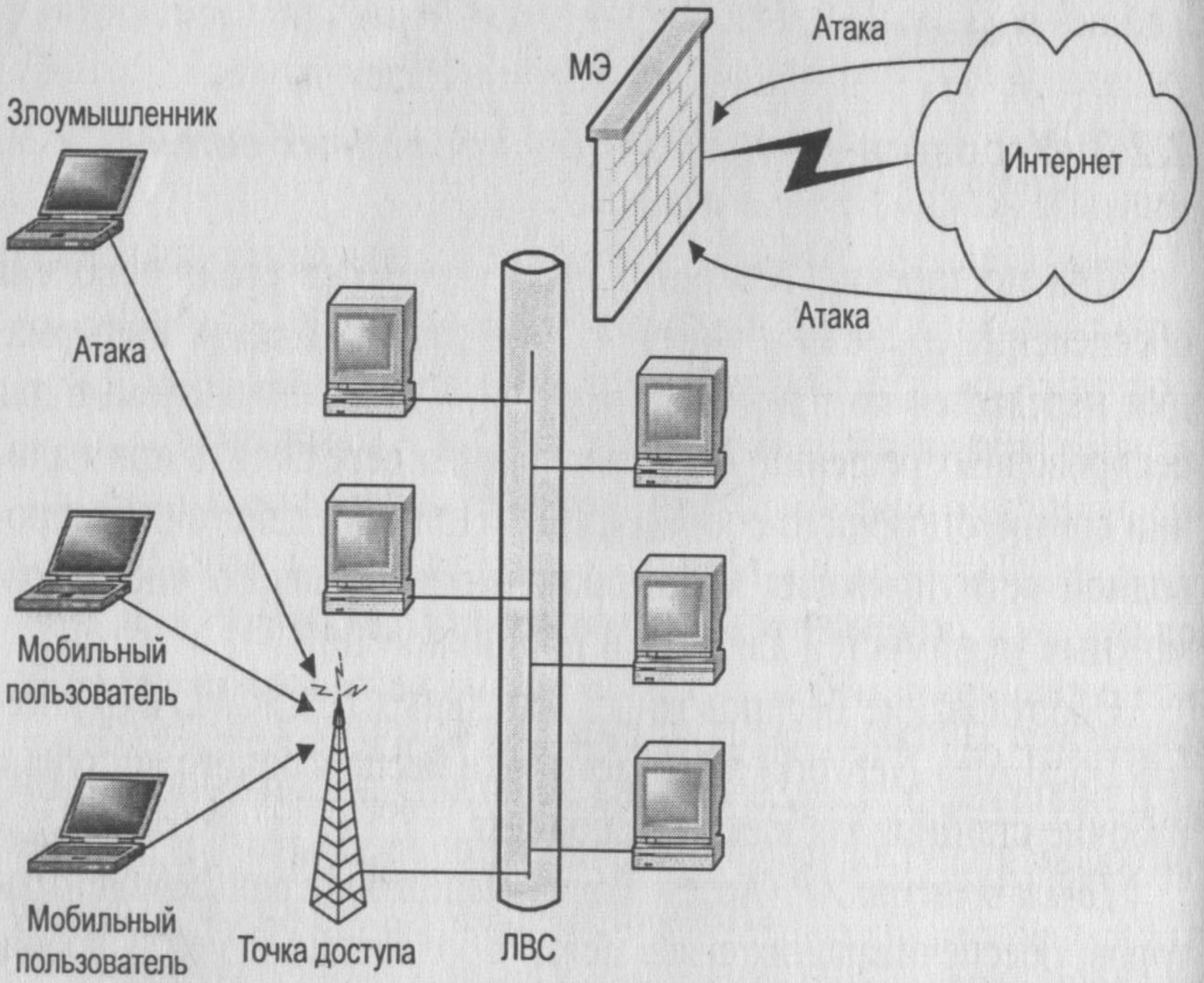
Весь входящий во внутреннюю сеть и выходящий во внешнюю сеть трафик должен проходить через единственный узел сети, например через межсетевой экран (firewall).

Только это позволяет в достаточной степени контролировать трафик.

В противном случае, когда в сети имеется множество пользовательских станций, имеющих независимый выход во внешнюю сеть, очень трудно скоординировать правила, ограничивающие права пользователей внутренней сети но доступу к серверам внешней сети и обратно — права внешних клиентов по доступу к ресурсам внутренней сети.


Цели злоумышленников
Нарушение конфиденциальности передаваемой информации
Нарушение целостности и достоверности передаваемой информации
Нарушение работоспособности всей системы или отдельных её частей


Проблемы обеспечения ИБ
в проводных КС
Угрозы безопасности для локальных
рабочих станций
Угрозы безопасности для
локальных сетей
Угрозы безопасности для
корпоративных сетей


Злоумышленник
Атака
МЭ
Атака
Интернет
Атака
Мобильный пользователь
Мобильный пользователь
Точка доступа
ЛВС

Основные угрозы в проводных КС

ITCOM ACADEMY

- Подслушивание (sniffing)
- Анализ сетевого трафика
- Посредничество
- Парольные атаки
- Атаки на уровне приложений
- Изменение данных
- Подмена доверенного субъекта (spoofing)
- Перехват сеанса
- Отказ в обслуживании
- Компьютерные вирусы

КОМПЬЮТЕРНЫЕ ВИРУСЫ

Компьютерные вирусы - это вредоносные программы, которые могут «размножаться» и скрытно внедрять свои копии в исполняемые файлы, загрузочные секторы дисков и документы.

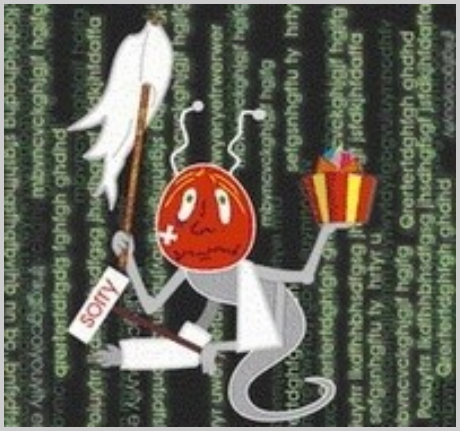
После заражения компьютера вирус может начать выполнение вредоносных действий и распространение своих копий, а также заставлять компьютер выполнять какие-либо действия.

Активация компьютерного вируса может вызывать уничтожение программ и данных и может быть связана с различными событиями (наступлением определенной даты или дня недели, запуском программ, открытием документа и т.д.).

ФАЙЛОВЫЕ ВИРУСЫ

ITCOM ACADEMY

Файловые вирусы внедряются в исполняемые файлы и обычно активируются при их запуске.



После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т.е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

По способу заражения файловые вирусы разделяют на перезаписывающие вирусы, вирусы-компаньоны и паразитические вирусы.

В 1999 году началась эпидемия файлового вируса Win95.CIH, названного «Чернобыль» из-за даты активации 26 апреля. Вирус уничтожал данные на жестком диске и стирал содержание BIOS.

Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.

МАКРО-ВИРУСЫ

ITCOM ACADEMY

Макро-вирусы заражают документы, созданные в офисных приложениях.

Макро-вирусы являются ограниченно-резидентными, т.е. они находятся в оперативной памяти и заражают документ, пока он открыт.
Макро-вирусы заражают шаблоны документов.

В 1995 году началась эпидемия первого макро-вируса «Concept» для текстового процессора Microsoft Word. Макро-вирус «Concept» до сих пор широко распространен.

Профилактическая защита от макро-вирусов состоит в предотвращении запуска вируса (запрете на загрузку макроса).

СЕТЕВЫЕ ЧЕРВИ

Сетевые черви - это вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей: Всемирную паутину, электронную почту, интерактивное общение, файлообменные сети и т.д.

Активация сетевого червя может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

АНТИВИРУСНЫЕ ПРОГРАММЫ

Принцип работы антивирусных программы основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вирусов.

Для поиска известных вирусов используются сигнатуры, т.е. некоторые постоянные последовательности двоичного кода, специфичные для конкретного вируса.

Для поиска новых вирусов используются алгоритмы эвристического сканирования, т.е. анализ последовательности команд в проверяемом объекте.

Большинство антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

МЕЖСЕТЕВОЙ ЭКРАН

Межсетевой экран (брандмауэр) – это программное или аппаратное обеспечение, которое проверяет информацию, поступающую из сети.

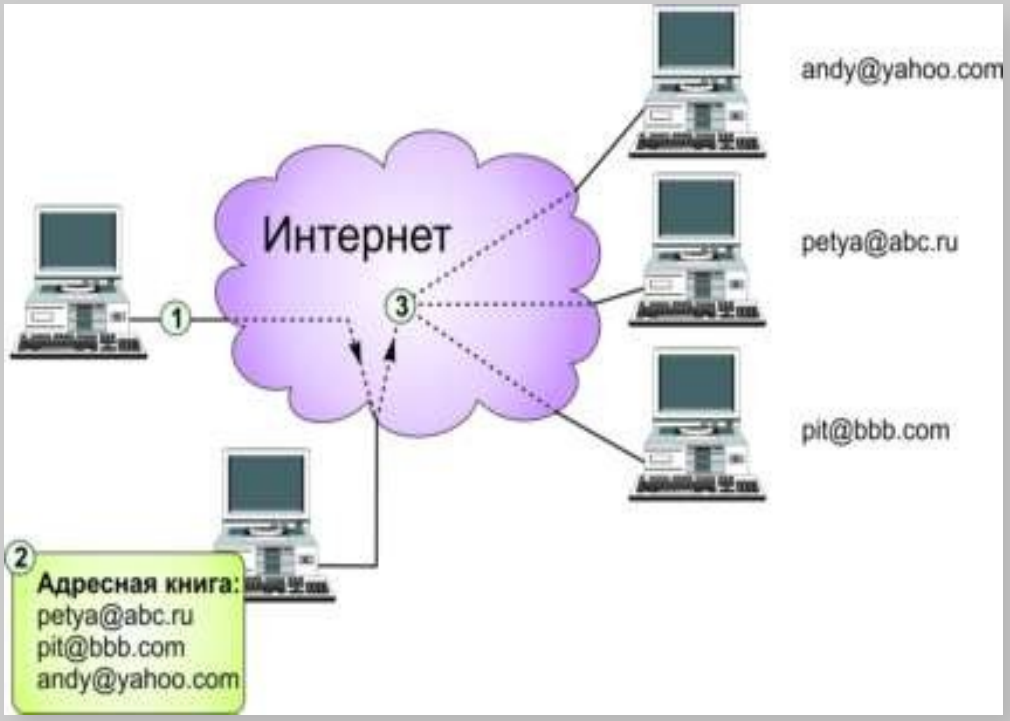
Межсетевой экран проверяет все web-страницы, поступающие на компьютер пользователя

Распознавание вредоносных программ происходит на основании баз

Если при открытии web-страницы обнаружена угроза, то загрузка web-страницы блокируется, а пользователю выдается соответствующее сообщение

ПОЧТОВЫЕ ЧЕРВИ

Почтовые черви для своего распространения используют электронную почту.



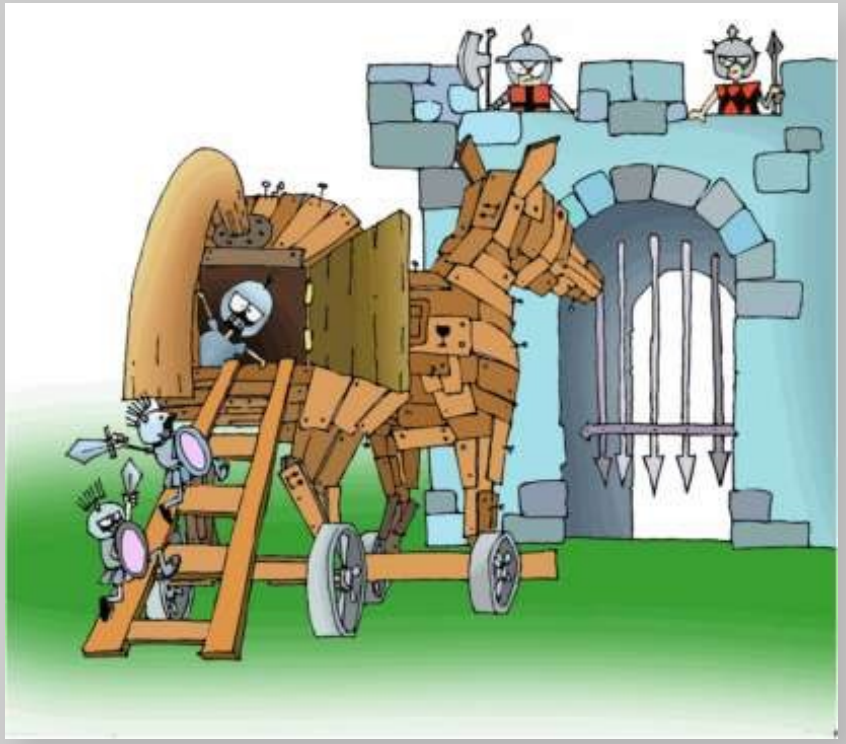
Червь отсылает либо свою копию в виде вложения в электронное письмо, либо ссылку на свой файл, расположенный на каком-либо сетевом ресурсе.

Код червя активируется при открытии (запуске) зараженного вложения или при открытии ссылки на зараженный файл.

Профилактическая защита от почтовых червей состоит в том, что не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.

ТРОЯНСКИЕ ПРОГРАММЫ

Троянская программа, троянец (от англ. trojan) – вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удаленному пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.



Троянские программы обычно проникают на компьютер как сетевые черви, а различаются между собой по тем действиям, которые они производят на зараженном компьютере.

ТРОЯНСКИЕ ПРОГРАММЫ - ШПИОНЫ

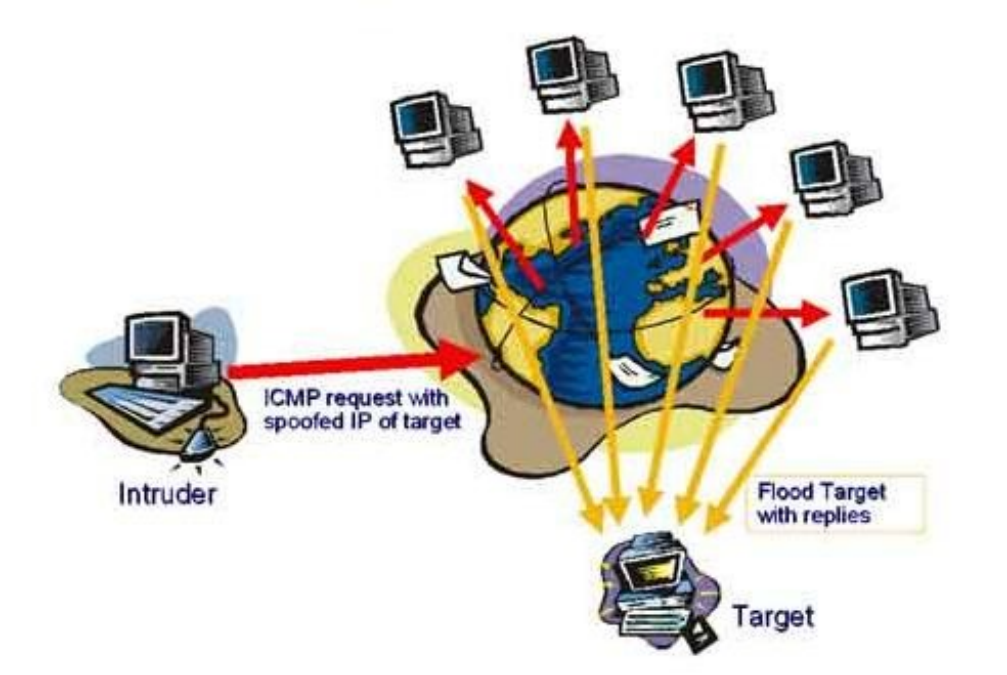
ITCOM ACADEMY

Троянские программы, ворующие информацию, при запуске ищут файлы, хранящие конфиденциальную информацию о пользователе (банковские реквизиты, пароли доступа к Интернету и др.) и отсылают ее по указанному в коде троянца электронному адресу или адресам.

Троянцы данного типа также сообщают информацию о зараженном компьютере (размер памяти и дискового пространства, версию операционной системы, IP-адрес и т. п.).

Некоторые троянцы воруют регистрационную информацию к программному обеспечению.

СЕТЕВЫЕ АТАКИ

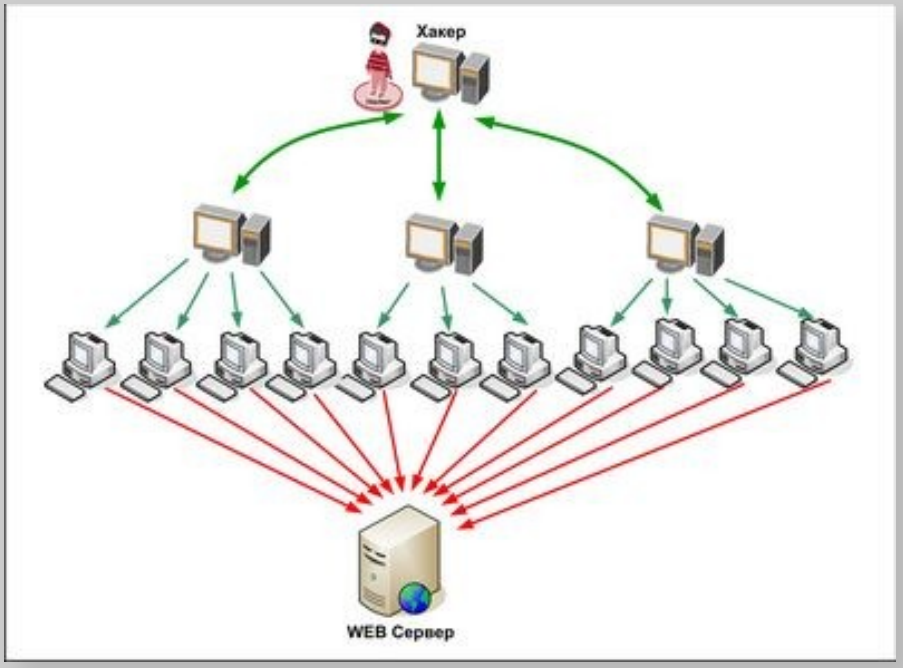


DoS-программы (от англ. Denial of Service – отказ в обслуживании) реализуют атаку с одного компьютера с ведома пользователя.

DoS-программы обычно наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера.

Некоторые сетевые черви содержат в себе DoS-процедуры, атакующие конкретные сайты. Так, червь «Codered» 20 августа 2001 года организовал успешную атаку на официальный сайт президента США, а червь «Mydoom» 1 февраля 2004 года «выключил» сайт компании – производителя дистрибутивов UNIX.

СЕТЕВЫЕ АТАКИ



DDoS-программы *(от англ. Distributed DoS – распределенный DoS)* реализуют распределенные атаки с разных компьютеров, причем без ведома пользователей зараженных компьютеров.

Для этого DDoS-программа засылается на компьютеры «жертв-посредников» и после запуска в зависимости от текущей даты или по команде от хакера начинает сетевую атаку на указанный сервер в сети.

ЗАЩИТА ОТ ХАКЕРСКИХ АТАК И СЕТЕВЫХ ЧЕРВЕЙ

ITCOM ACADEMY

Защита компьютерных сетей или отдельных компьютеров от несанкционированного доступа может осуществляться с помощью межсетевого экрана, или брандмауэра *(от англ. firewall).*

Межсетевой экран позволяет:

1. блокировать хакерские DoS-атаки, не пропуская на защищаемый компьютер сетевые пакеты с определенных серверов (определенных IP-адресов или доменных имен);

2. не допускать проникновение на защищаемый компьютер сетевых червей (почтовых, Web и др.);

3. препятствовать троянским программам отправлять конфиденциальную информацию о пользователе и компьютере.

Первые признаки заражения вирусом

ITCOM ACADEMY

- медленная работа компьютера
- зависания и сбои в работе компьютера
- изменение размеров файлов
- уменьшение размера свободной оперативной памяти
- значительное увеличение количества файлов на диске
- исчезновение файлов и каталогов или искажение их содержимого
- изменение даты и времени модификации файлов

Какой пароль самый надежный?

ITCOM ACADEMY

- Используйте разные пароли для всех важных учетных записей
- Используйте разные пароли для разных учеток. Используйте длинный пароль.
- Чем длиннее пароль, тем труднее его угадать.
- Пароль должен включать буквы, цифры и символы (желательно вперемешку).
- Гораздо сложнее взломать или подобрать пароль, состоящий из цифр, символов и букв в разных регистрах.
- Используйте словосочетание, известное только вам.
- Следите за тем, чтобы параметры восстановления пароля всегда содержали самую актуальную информацию и не были известны третьим лицам.
- Регулярно обновляйте дополнительный адрес электронной почты, чтобы в случае необходимости изменить пароль вы могли получить письмо с соответствующими инструкциями.
- Храните памятки со своими паролями там, где их трудно найти.
- Не оставляйте памятки в доступных местах, на компьютере или на столе.

Первые правила для защиты от мошенничества в Интернет.

- никогда не осуществляйте покупок через Интернет, особенно с использованием кредитных карточек (это излюбленное лакомство для многих хакеров);
- никогда и ни где не вводите каких-либо настоящих данных о себе (ФИО, адрес, E-Mail и т.д.) - все данные должны быть вымышленными!

Как осуществляется защита персональных компьютеров?

ITCOM ACADEMY

- средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;
- применение различных методов шифрования, не зависящих от контекста информации;
- средства защиты от копирования коммерческих программных продуктов;
- защита от компьютерных вирусов и создание архивов.

Что такое безопасность сети?

ITCOM ACADEMY

Безопасность беспроводной сети - это предотвращение несанкционированного доступа или повреждения компьютеров или данных с помощью беспроводных сетей, в том числе сетей Wi-Fi .

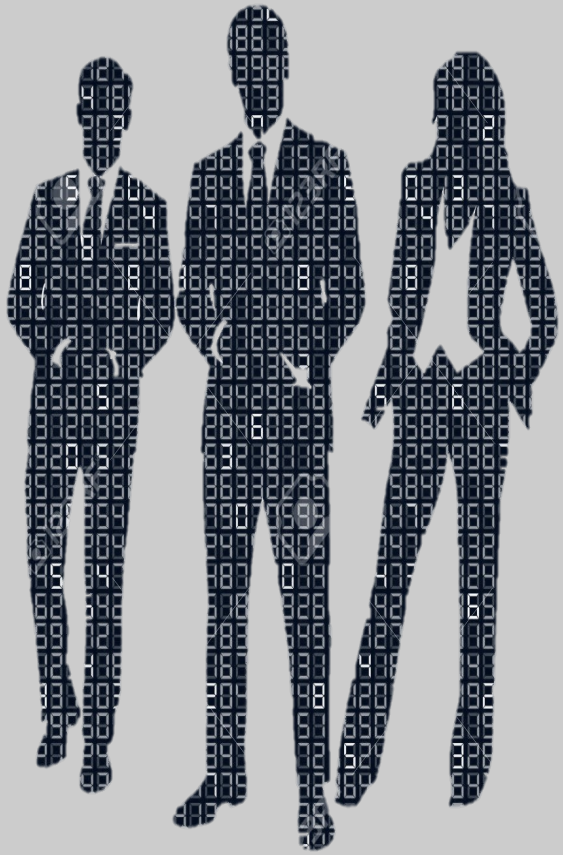
Наиболее распространенным типом является безопасность Wi-Fi , которая включает в себя эквивалентную конфиденциальность проводных сетей (WEP) и защищенный доступ Wi-Fi (WPA2).

Специфика беспроводных сетей подразумевает, что данные могут быть перехвачены и изменены в любой момент.

Для одних технологий достаточно стандартного беспроводного адаптера, для других требуется специализированное оборудование.

Но в любом случае, эти угроза реализуются достаточно просто, и для противостояния им требуются эффективные криптографические механизмы защиты данных.

Меры безопасности и правила общения в сети Интернет



Интернет представляет собой важный способ личного и профессионального общения, но он может также использоваться со злым умыслом.

Поэтому важно знать о проблемах компьютерной безопасности.

Для чего кому-то нужно взламывать ваш компьютер?

ITCOM ACADEMY

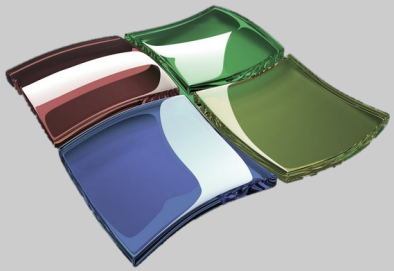
- Кража паролей от ваших электронных кошельков, почтовых ящиков и т.д.
- Организация DDoS-атак
- Организация массовых рекламных рассылок
- Прочие способы извлечения коммерческой выгоды

Использование интернета является безопасным, если выполняются три основные правила:

- Защитите свой компьютер
- Защитите себя в Интернете
- Соблюдайте правила

1. Защитите свой компьютер

- Регулярно обновляйте операционную систему.
- Используйте антивирусную программу.
- Применяйте брандмауэр.
- Создавайте резервные копии важных файлов.
- Будьте осторожны при загрузке содержимого.



2. Защитите себя в Интернете

- С осторожностью разглашайте личную информацию.
- Думайте о том, с кем разговариваете.
- Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.
- Не используйте простые пароли.

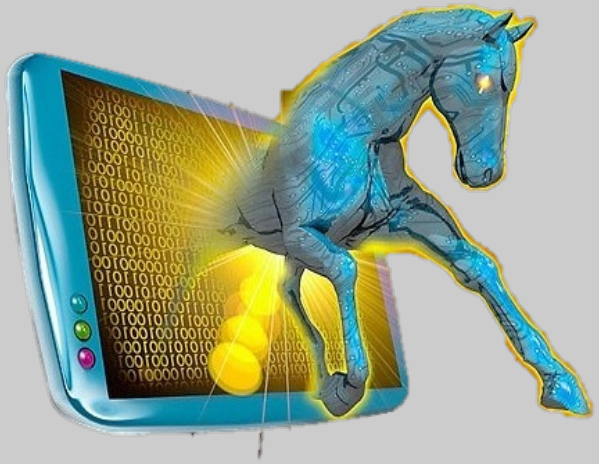
3. Соблюдайте правила

- Закону необходимо подчиняться даже в Интернете.
- При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

Вирусы

Вирусы, трояны и черви представляют собой опасные программы, которые могут распространяться через электронную почту или веб-страницы.

Вирусы могут повредить файлы или программное обеспечение, хранящиеся на компьютере.



Хакеры и взломщики

Хакерами и взломщиками называют людей, которые взламывают защиту систем данных. Они могут вторгнуться на незащищенный компьютер через Интернет и воспользоваться им со злым умыслом, а также украсть или скопировать файлы и использовать их в противозаконной деятельности.

Хакеры

Истинное происхождение термина «хакер» сейчас, наверное, установить уже невозможно: предполагается, что оно зародилось в кампусах и аудиториях Массачусетского Технологического Университета еще в 60-х годах прошлого столетия. Бытует мнение, что словечко попало в обиход компьютерщиков из жаргона хиппи, где глагол «to hack» означал отнюдь не «взламывать», как это считается сейчас, а «соображать», «врубаться».

Собственно, в 70-х «хакерами» как раз и называли тех, кто «врубается» в принципы работы компьютеров, глубоко понимает происходящие в них процессы — то есть, высококвалифицированных IT-специалистов, программистов, разработчиков.

Хакеры — это прежде всего исследователи, настоящие ученые из мира высоких технологий. Настоящие хакеры никогда не взламывали чужие приложения или серверы ради наживы, и уж тем более не совершали преступлений - разве что порой использовали свои знания для организации безобидных розыгрышей.

Расхожее слово «хакер», некогда обозначавшее просто высококлассного компьютерного специалиста, оказалось затерто до дыр не разбирающимися в вопросе журналистами, которые низвели IT-профессионалов до уровня компьютерных преступников и киберзлодеев.

Спам в интернете

Массовая рассылка нежелательных сообщений электронной почты известна как спам. Он приводит к перегрузке систем электронной почты и может заблокировать почтовые ящики. В качестве средства для рассылки спама его отправители иногда используют червей электронной почты.

Пять правил при работе с электронной почтой

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. (Вместо этого сразу удалите их)
2. Никогда не отвечайте на спам.
3. Применяйте фильтр спама поставщика услуг интернета или программы работы с электронной почтой (при наличии подключения к интернету).
4. Создайте новый или используйте семейный адрес электронной почты для интернет-запросов, дискуссионных форумов и т.д.
5. Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.

Дополнительные правила

- **Закрывайте сомнительные всплывающие окна**

Всплывающие окна — это небольшие окна с содержимым, побуждающим к переходу по ссылке.

- **Остерегайтесь мошенничества**

В интернете легко скрыть свою личность. Рекомендуется проверять личность человека, с которым происходит общение. Никогда не разглашайте в интернете личную информацию, за исключением людей, которым вы доверяете.

- **Обсуждайте использование интернета**

Большая часть материалов, доступных в интернете, является непригодной для несовершеннолетних.

Законы также применяются к интернету

ITCOM ACADEMY

Что разрешено и что запрещено в Интернете?

Интернет является общественным ресурсом. В Интернете необходимо следовать основным правилам так же, как правилам дорожного движения при вождении.

Несмотря на то, что большая часть законов была создана до широкого распространения Интернета, закон также распространяется и на него. Все, что незаконно в обычной жизни, незаконно и в Интернете. Интернет предоставляет беспрецедентные возможности свободного общения, но они также подразумевают ответственность. Например, владелец веб-сайта всегда несет ответственность за его содержимое и законность самого сайта и места его публикации

Авторское право

Авторским правом защищается способ реализации идеи, но не сама идея. Разрешается копирование материала из Интернета для личного использования, но присвоение авторства этого материала запрещено.

Например, при использовании материала в собственной презентации необходимо указать источник. Неразрешенное использование материала может привести к административному взысканию в судебном порядке, а также иметь прочие правовые последствия.

ITCOM ACADEMY

Безопасность - это не состояние, а непрекращающийся процесс

Брюс Шнайер