ТЕМА УРОКА:
«БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННОЙ СРЕДЕ. ОСНОВНЫЕ УГРОЗЫ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФ. БЕЗОПАСНОСТИ»

План:

1.Цели защиты информации

2.Меры обеспечения информационной безопасности

3. Программно-технические меры информационной безопасности

ЦЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ:

Федеральный закон «Об информации, информационных технологий и о защите информации» определяет цели защиты информации следующим образом:

- предотвращение утечки, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- защита прав граждан на сохранение личной тайны и персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ ПОДРАЗДЕЛЯЮТСЯ НА 3 УРОВНЯ:

законодательный

административный

программно-технический

ЗАКОНОДАТЕЛЬНЫЙ УРОВЕНЬ.

В России действует закон РФ **«О правовой охране программ для электронных вычислительных машин и баз данных»** и Закон РФ **«Об авторском праве и смежных правах».**

Уголовный кодекс содержит статьи:

•Статья 272. Неправомерный доступ к компьютерной информации **(2 года);**

•Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ; (4 года)

•Статья 274. Нарушение правил эксплуатации ЭВМ, системы (2 года)

АДМИНИСТРАТИВНЫЙ УРОВЕНЬ

На административном уровне формируется политика безопасности и комплекс процедур, определяющих действия персонала в штатных и критических условиях.

Этот уровень защиты информации зафиксирован в руководящих документах, выпущенных Гос-техкомиссией РФ.

ПРОГРАММНО-ТЕХНИЧЕСКИЙ УРОВЕНЬ.

К этому уровню защиты информации относятся программные и аппаратные средства, которые составляют технику информационной безопасности.

Программно-технические меры защиты информации

1.Шифрование (криптография) информации

Преобразование (кодирование) слов и т.д. с помощью специальных алгоритмов

2.Контроль доступа к аппаратуре

Вся аппаратура закрыта и в местах доступа к ней установлены датчики, которые срабатывают при вскрытии аппаратуры

3. Защита от компьютерных вирусов

4.Контроль внешнего трафика с помощью межсетевых экранов

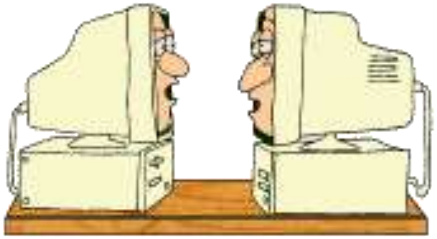
Брандмауэры- программы, предназначенные для фильтрации трафика между компьютером и Интернетом

5.Ограничение доступа к информации

На уровне среды обитания человека: выдача документов, установка сигнализации или системы видеонаблюдения

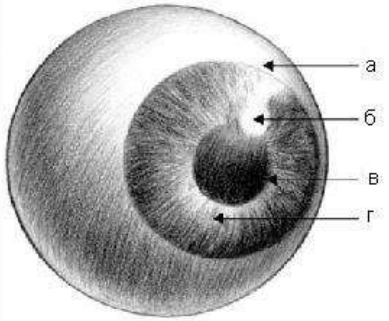
На уровне защиты компьютерных систем: введение паролей для пользователей

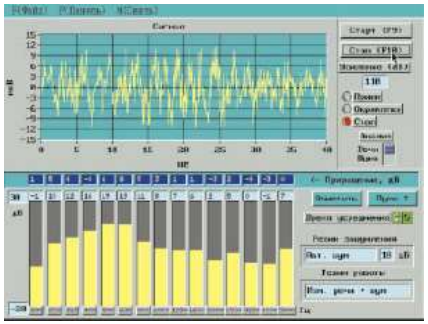
По отпечаткам пальцев



Биометрические системы защиты

По радужной оболочке глаза

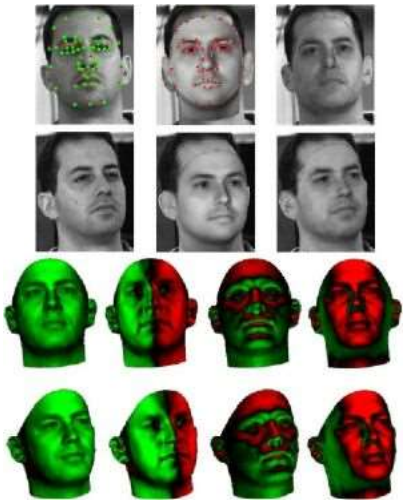




По характеристикам речи

X = ширина ладони, Y = длина ладони, Z = длина пальца

По геометрии ладони руки



По изображению лица

Вредоносные программы

Вирусы, черви, троянские и хакерские программы

Шпионское, рекламное программное обеспечение

Потенциально опасное программное обеспечение

- Загрузочные вирусы
- Файловые вирусы
- Макровирусы
- Троянские программы-шпионы
- Руткиты
- Почтовые черви

Методы борьбы:
антивирусные программы, межсетевой экран, своевременное обновление системы безопасности операционной системы и приложений, проверка скриптов в браузере

К источникам основных внешних угроз для России относятся

политика стран, противодействующая доступу к мировым достижениям в области информационных технологий

«информационная война», нарушающая функционирование информационной среды в стране

преступная деятельность, направленная против национальных интересов

К источникам основных внутренних угроз для России относятся

отставание от ведущих стран мира по уровню информатизации

технологическое отставание электронной промышленности в области производства информационной и телекоммуникационной техники

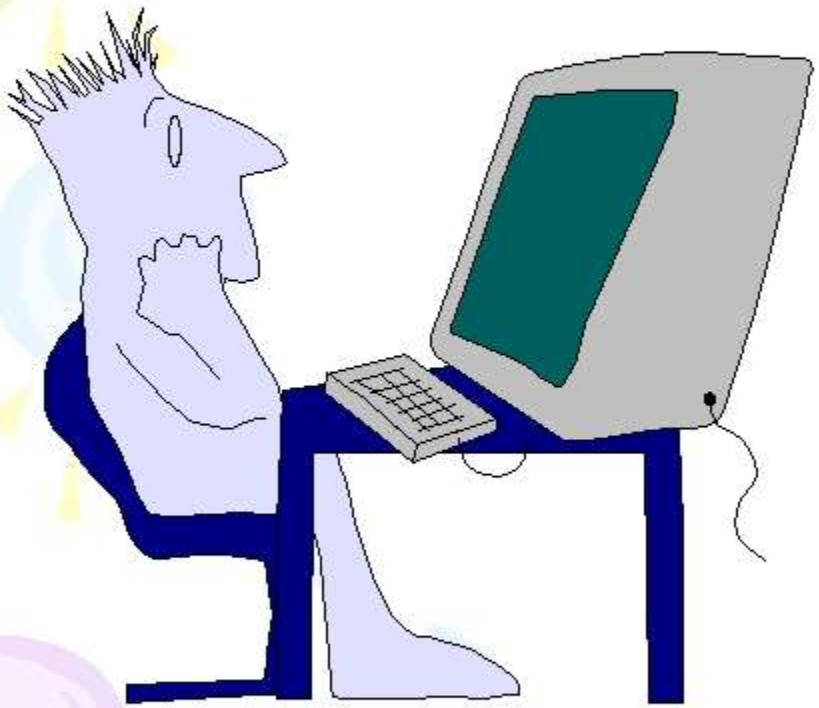
снижение уровня образованности граждан, препятствующее работе в информационной среде

А на последок я скажу…

Знайте, вирусы живут
И болезни создают,
Вирусят рождают.
Болезни размножают.
Вы вируса не бойтесь,
Отпор ему давайте.
Компьютер раз в неделю
Касперским проверяйте

Спасибо за внимание и понимание!

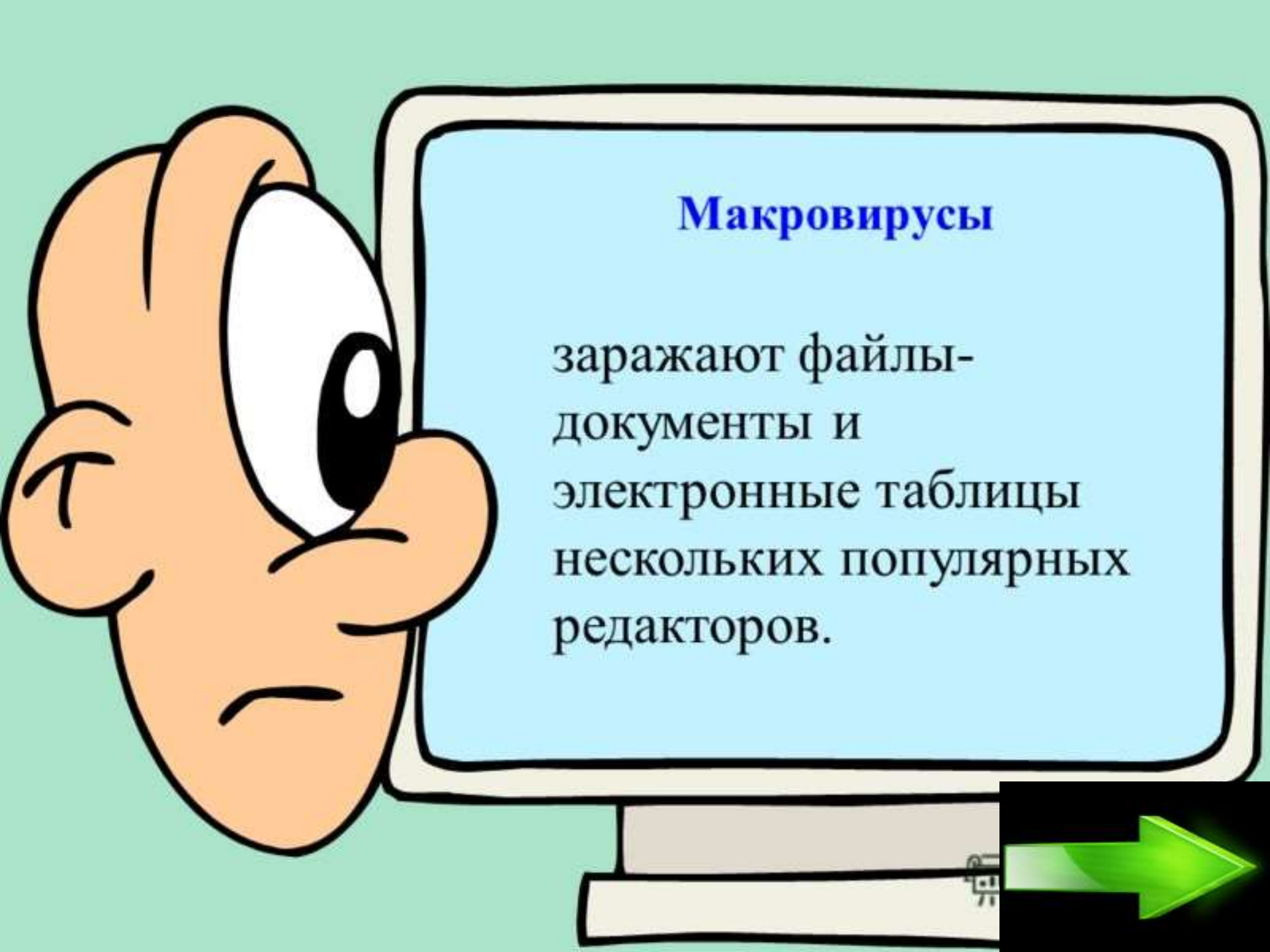
Загрузочные вирусы.



Загрузочные вирусы заражают загрузочный сектор гибкого или жёсткого диска.

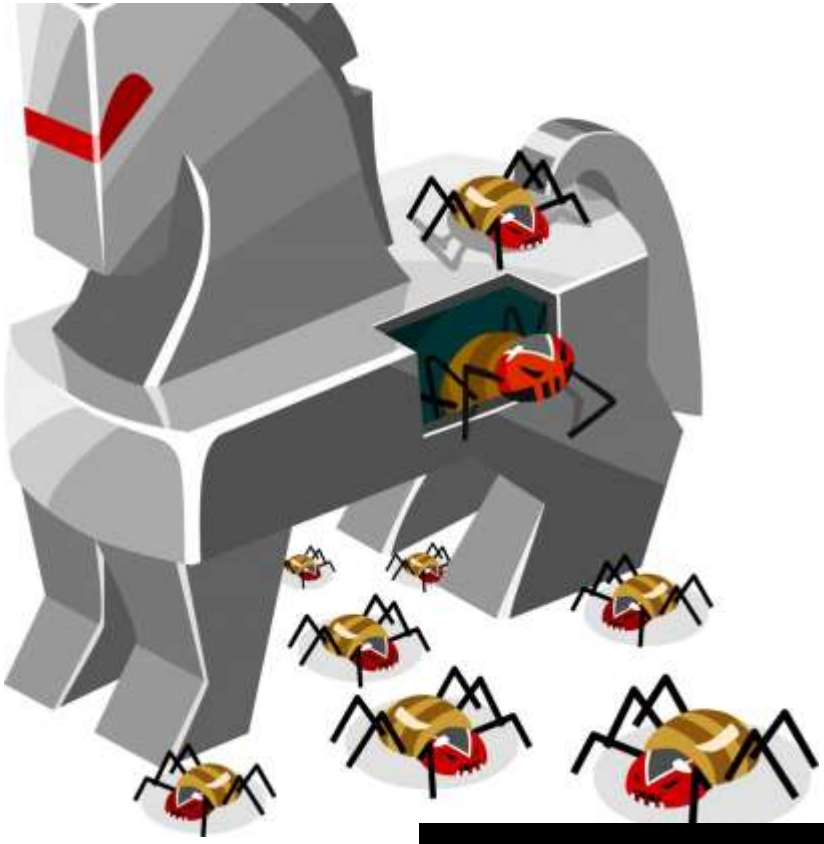
Файловые вирусы

Файловые вирусы Внедряются в Программы и Активизируются При их запуске.


Макровирусы
заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

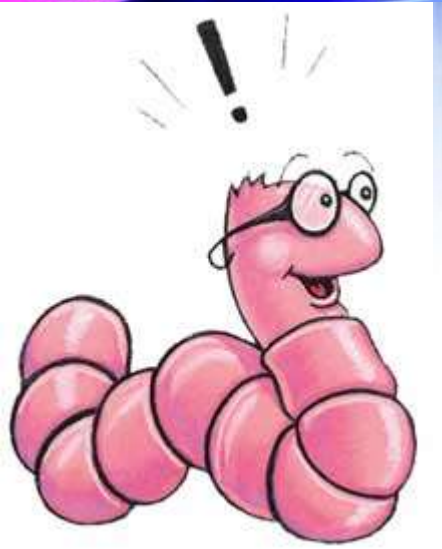
ТРОЯНСКАЯ ПРОГРАММА

(Троян, троянец, троянский конь)- вредоносная программа, используемая злоумышленниками для сбора информации, ее разрушения или модификации, нарушения работоспособности ее ресурсов в неблаговидных целях.



РУТКИТЫ

Руткиты- попросту говоря, это то, что внедряется в ваш компьютер и скрывает следы своего присутствия (скрывает файлы, процессы, самого себя) так, что вы не замечаете, что в вашем компьютере без вашего ведома и согласия кто-то что-то делает.



Почтовый червь (Email-Worm) – *червь, который распространяет электронную почту с прикрепленным кодом* или в письме присутствует ссылка на заражённый ресурс