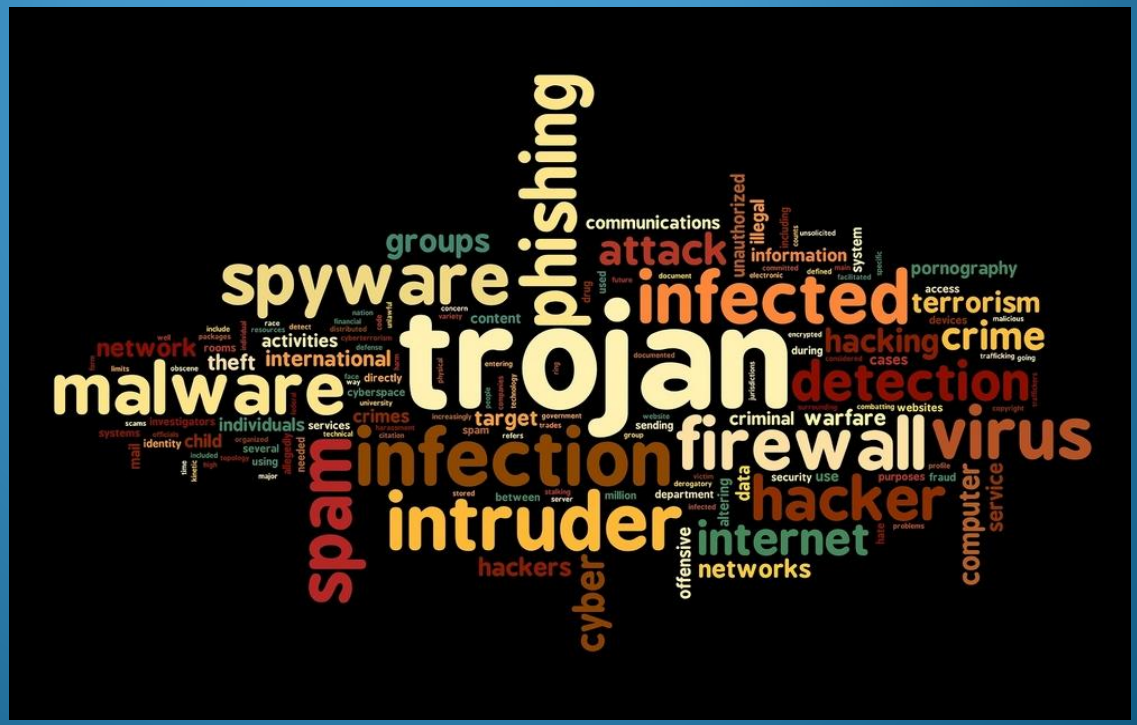
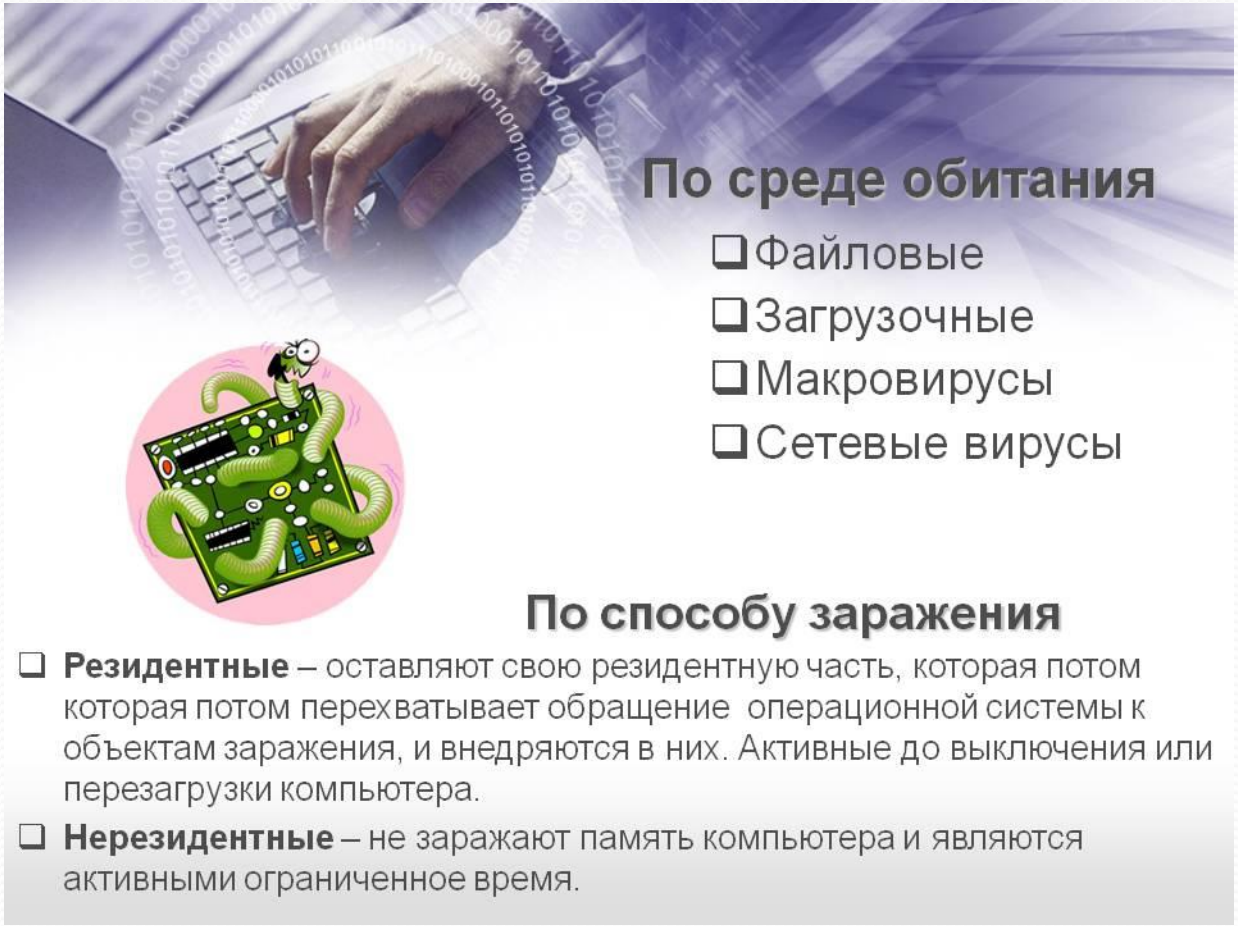
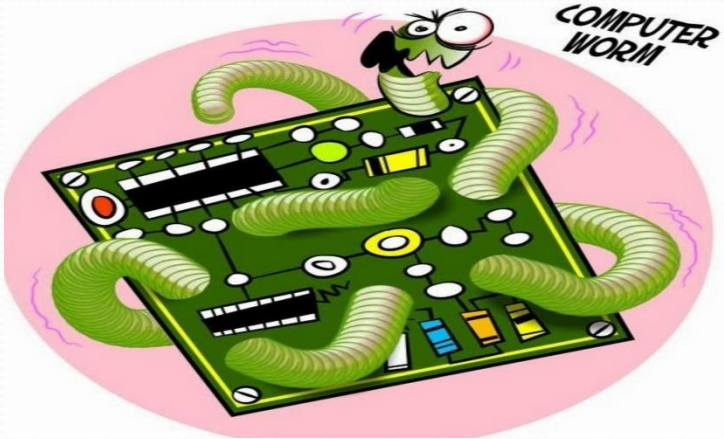
Защита от вредоносных программ



Вредоносные и антивирусные программы



- **Вредоносные программы**— это программы, предназначенные для незаконного доступа к информации, для скрытого использования компьютера или для нарушения работы.
- **Типы вредоносных программ:**
- **Файловые**– внедряются в исполняемые файлы, системные библиотеки и т.п.;
- **Загрузочные**– внедряются в загрузочный сектор диска или в главную загрузочную запись винчестера; опасны тем, что загружаются в память раньше, чем ОС и антивирусные программы;
- **Макровирусы**– поражают документы, в которых могут быть макросы;
- **Скриптовые вирусы**– внедряются в командные файлы или в веб-страницы ;
- **Червь***(сетевой червь) - это вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом.*



- Еще одна группа вредоносных программ – **троянские программы**или «троянцы» (трояны).
- **Троян** *(троянский конь) - программа, основной целью которой является вредоносное воздействие по отношению к компьютерной системе. Трояны отличаются отсутствием механизма создания собственных копий.*
- Троянские программы проникают на компьютер под видом «полезных» программ, например, кодеков для просмотра видео или экранных заставок (которые включаются, если некоторое время не работать на компьютере). В отличие от вирусов и червей, они не могут распространяться самостоятельно и часто «путешествуют» вместе с червями. Среди «троянцев» встречаются:
- **Клавиатурные шпионы**, постоянно находясь в оперативной памяти, записывают все данные, поступающие от клавиатуры с целью последующей их передачи своему автору.
- • **Похитители паролей** предназначены для кражи паролей путем поиска на зараженном компьютере специальных файлов, которые их содержат.
- • **Утилиты скрытого удаленного управления** - это трояны, которые обеспечивают несанкционированный удаленный контроль над инфицированным компьютером. Перечень действий, которые позволяет выполнять тот или иной троян, определяется его функциональностью, заложенной автором. Обычно это возможность скрыто загружать, отсылать, запускать или уничтожать файлы. Такие трояны могут быть использованы как для получения конфиденциальной информации, так и для запуска вирусов, уничтожения данных.

- **Анонимные SMTP-сервера и прокси-сервера** - такие трояны на зараженном компьютере организовывают несанкционированную отправку электронной почты, что часто используется для рассылки спама.
- • **Утилиты дозвона** в скрытом от пользователя режиме инициируют подключение к платным сервисам Интернет.
- • **Модификаторы настроек браузера** меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, открывают дополнительные окна, имитируют нажатия на рекламные баннеры и т. п.
- • **Логические бомбы** характеризуются способностью при срабатывании заложенных в них условий (в конкретный день, время суток, определенное действие пользователя или команды извне) выполнять какое-либо действие, например, удаление файлов.

Шпионское , рекламное программное обеспечение

- Это программы скрытого дозвона. Данная группа объединяет в себе потенциально опасное программное обеспечение , которое может причинить неудобство пользователю или даже нанести значительный ущерб.

Потенциально опасное программное обеспечение

- Эта группа включает программы, которые не являются вредоносными или опасными, однако при некотором стечении обстоятельств могут быть использованы для нанесения вреда вашему компьютеру.

Антивирусные программы

- Современные антивирусные программы обеспечивают **комплексную защиту** программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения(Интернет, локальная сеть, электронная почта и съемные носители информации).

Популярные антивирусные программы:

Принцип работы антивирусных программ

- Принцип основан на проверке файлов ,загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

  Недопустимо использование на одном компьютере двух разных антивирусных программ.

  Для поиска известных вредоносных программ используются сигнатуры (некоторая постоянная последовательность программного кода специфичная для конкретной вредоносной программы).Если антивирусная программа обнаружит такую последовательность в каком-либо файле ,то файл считается зараженным вирусом и подлежит лечению и удалению.

Антивирусный монитор и антивирусный сканер

- **Антивирусный монитор**(функция постоянной защиты) запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса ,проверяя на вредность совершаемые другими программами действия .Основная задача антивирусного монитора состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

- **Антивирусный сканер**(функция защиты по требованию пользователя) запускается заранее выбранному расписанию или в произвольный момент пользователем . Антивирусный сканер производит поиск вредоносных программ в оперативной памяти , а также на жестких и сетевых дисках компьютера.

Признаки заражения компьютера

Вывод на экран непредусмотренных сообщений или изображений;

Подача непредусмотренных звуковых сигналов;

Неожиданное открытие и закрытие лотка CD/DVD дисководов;

Произвольны запуск на компьютере каких-либо программ;

Частые зависания и сбои в работе компьютера ;

Медленная работа компьютера при запуске программ;

Исчезновение или изменение файлов и папок;

Частое обращение к жесткому диску(часто мигает лампочка на системном блоке);

Зависание или неожиданное поведение браузера (например, окно программы невозможно закрыть);

Друзья или знакомые говорят о полученных от вас сообщениях, которые вы не отправляли;

В вашем почтовом ящике находится большое количество сообщений без обратного адреса и заголовка;

Действия при наличии признаков заражения компьютера

- Отключить компьютер от локальной сети и Интернета, если он к ним был подключен;

  Если симптом заражения состоит в том, что невозможно загрузиться с жесткого диска компьютера(компьютер выдает ошибку , когда вы его включаете), попробовать загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows;

  Запустить антивирусную программу;

Спасибо за внимание!