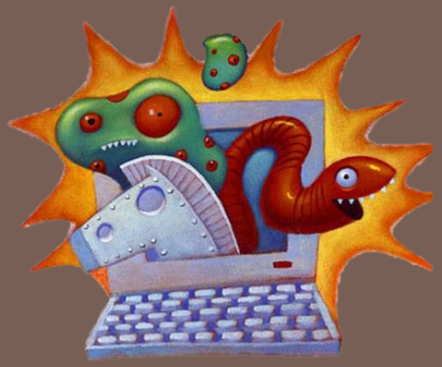
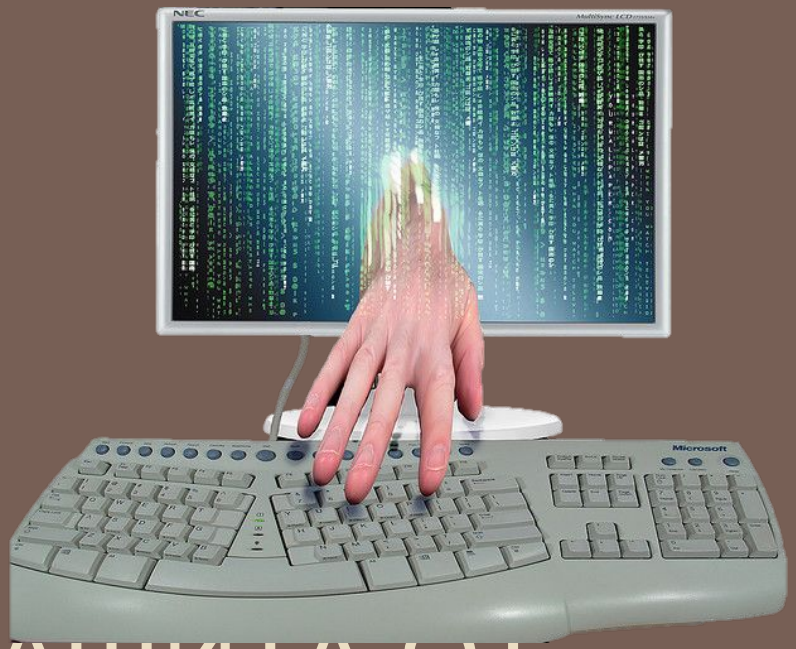
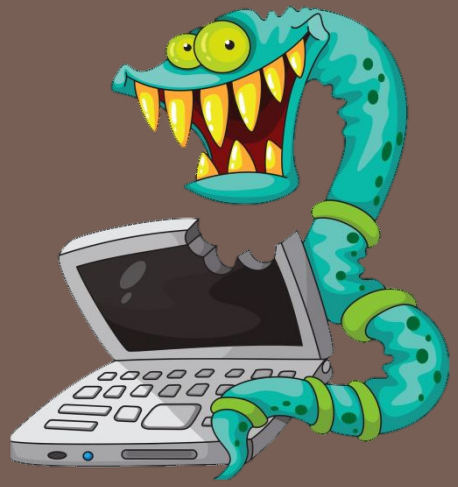




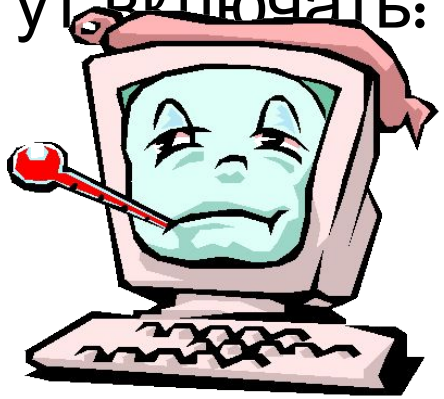


ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Троянские программы и защита от них

Что такое троянская программа?

- **Троянские программы** — это вредоносные программы, выполняющие несанкционированные пользователем действия. Такие действия могут включать:
- удаление данных;
- блокирование данных;
- изменение данных;
- копирование данных;
- замедление работы компьютеров и компьютерных сетей



Различия

В отличие от компьютерных вирусов и червей троянские программы неспособны к самовоспроизведению.

- **Компьютерный вирус и компьютерный червь —** это вредоносные программы, которые способны воспроизводить себя на компьютерах или через компьютерные сети. При этом пользователь не подозревает о заражении своего компьютера. Так как каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению, заражение распространяется очень быстро. Существует очень много различных типов компьютерных вирусов и компьютерных червей, большинство кот[illegible]адают высокой способностью к ра[illegible].

Что нужно знать о троянских программах

- **Троянские программы классифицируются в соответствии с типом действий, выполняемых ими на компьютере.**
- **Бэкдоры**
- Троянская программа бэкдор предоставляет злоумышленникам возможность удаленного управления зараженными компьютерами. Такие программы позволяют автору выполнять на зараженном компьютере любые действия, включая отправку, получение, открытие и удаление файлов, отображение данных и перезагрузку компьютера. Троянцы-бэкдоры часто используются для объединения группы компьютеров-жертв в ботнет или зомби-сеть для использования в криминальных целях.
- **Руткиты**
- Руткиты — это программы, предназначенные для сокрытия в системе определенных объектов или действий. Часто основная их цель — предотвратить обнаружение вредоносных программ, чтобы увеличить время работы этих программ на зараженном компьютере.
- **Банковские троянцы**
- Банковские троянцы (Trojan-Banker) предназначены для кражи учетных данных систем интернет-банкинга, систем электронных платежей и кредитных или дебетовых карт.

Как защититься от троянских программ

- Установив эффективное программное обеспечение для защиты от вредоносных программ, или просто, **антивирус**, можно защитить от троянских программ свои мобильные устройства, включая ПК, ноутбуки, компьютеры Mac, планшеты и смартфоны. Тщательно разработанный антивирус, такой как Антивирус Касперского, обнаруживает и предотвращает троянские атаки на ПК, а Kaspersky Internet Security для Android обеспечивает антивирусную защиту смартфонов и планшетов на базе Android. В «Лаборатории Касперского» созданы антивирусные продукты, которые защищают от троянских программ следующие устройства:

- ПК на базе Windows;
- компьютеры Mac;
- смартфоны;
- планшеты

Антивирусные программы

- **Антивирусная программа** - программа, предназначенная для борьбы с компьютерными вирусами.
- В своей работе эти программы используют различные принципы для поиска и лечения зараженных файлов. Для нормальной работы на ПК каждый пользователь должен следить за обновлением антивирусов. Если антивирусная программа обнаруживает вирус в файле, то она удаляет из него программный код вируса. Если лечение невозможно, то зараженный файл удаляется целиком.
- **Типы антивирусных программ:**
- •Антивирусные сканеры – после запуска проверяют файлы и оперативную память и обеспечивают нейтрализацию найденного вируса.
- •Антивирусные сторожа – постоянно находятся в ОП и обеспечивают проверку файлов в процессе их загрузки в ОП.
- •Полифаги – самые универсальные и эффективные антивирусные программы. Проверяют файлы, загрузочные сектора дисков и ОП на поиск новых и неизвестных вирусов. Занимают много места, работают не быстро.
- •Ревизоры – проверяют изменение длины файла. Не могут обнаружить вирус в новых файлах (на дискетах, при распаковке), т.к. в базе данных нет сведений о этих файлах
- •Блокировщики – способны обнаружить и остановить вирус на самой ранней стадии его развития (при записи в загрузочные сектора дисков).