

МЕТОДЫ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

...Today after sleepless 80 hours I have finished the contest!
WOW, I am so satisfied, dunno what is better, sex or hacking.
(... Сегодня после восьмидесяти бессонных часов я наконец-то
хакнул это! Вау, я чувствую себя таким удовлетворенным, что
начинаю сомневаться, что лучше – секс или хакинг.)

MoD

Содержание:

Введение

Глава 1. Компьютерный вирус

1.1. Понятие «Компьютерный вирус»

1.2. Пути попадания вирусов на компьютер

1.3. Классификация вредоносных программ

1.4. Признаки заражения вирусом

Глава 2. Методы защиты от компьютерных вирусов

2.1. Виды антивирусных программ

2.2. Защита от несанкционированного воздействия

Заключение

Библиографический список

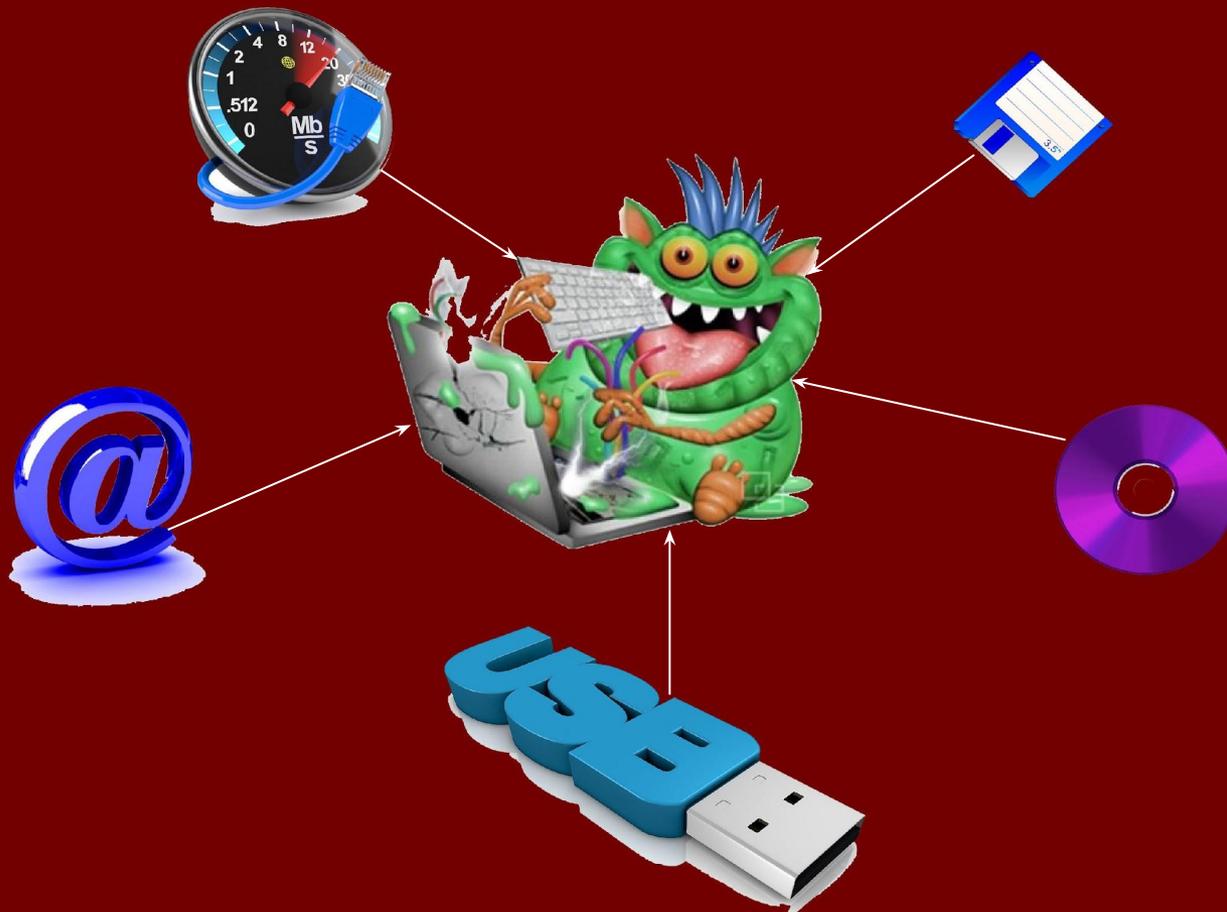
Компьютерный вирус

машинный код, созданный программистами для нанесения ущерба пользователям персональных компьютеров.

Термин «компьютерный вирус» появился в 1984 году на конференции.



Пути попадания вирусов на компьютер



Классификация вредоносных программ



Признаки заражения вирусом

- - прекращение работы или неправильная работа ранее функционировавших программ;
- - значительное увеличение количества файлов на диске;
- - подача непредусмотренных звуковых сигналов;
- - отсутствие возможности загрузки операционной системы;
- - искажение одержимых на диске файлов и папок;
- - изменение даты и времени модификации файлов;
- - изменение размера файлов;
- - уменьшение размера свободной оперативной памяти;
- - вывод на экран непредусмотренных сообщений или изображений;
- - медленная работа компьютера;
- - частые зависания и сбои в работе компьютера.

Виды антивирусных программ

- детекторы - позволяют обнаружить на компьютере файлы, зараженные только известными им вирусами;
- доктора или фаги – обеспечивают проверку компьютера, на наличие зараженных файлов, выполняет их лечение;
- ревизоры (инспекторы) - собирают сведения о состоянии программ и загрузочных секторов;
- программы-фильтры (мониторы) – помогают обнаружить вирусы на самой ранней стадии когда вирус еще не успел размножиться и что-либо испортить;
- программы-вакцины или иммунизаторы - отслеживают потенциально опасные операции;
- сканер – быстро и эффективно проверяет и лечит зараженную систему.

Защита от несанкционированного воздействия



Заключение

Методы защиты от компьютерных вирусов:

- 1) резервное копирование всех программ, файлов и системных областей дисков на дискеты, чтобы можно было восстановить данные в случае вирусной атаки. Создание системной и аварийной дискеты;
- 2) ограничение доступа к машине путём введения пароля, администратора, закрытых дисков;
- 3) включение антивирусного протектора от загрузочных вирусов. Защита дискет от записи;
- 4) использование только лицензионного программного обеспечения, а не «пиратских» копий, в которых могут находиться вирусы;
- 5) проверка всей поступающей извне информации на вирусы, как на дискетах, CD-ROM, так и по сети;
- 6) применение антивирусных программ и обновление их версий;
- 7) подготовка ремонтного набора дискет (антивирусы и программы по обслуживанию дисков);
- 8) периодическая проверка компьютера на наличие вирусов при помощи антивирусных программ.

Библиографический список

1. Крис Касперски – Компьютерные вирусы изнутри и снаружи. – Спб.: Питер, 2006.-527 с.:ил.;
2. Бабин С.А. – Инструментарий хакера. – СПб.: БХВ-Петербург.ю 2014.- 240 с.:ил. – (Глазами хакера);
3. http://www.informatika.edusite.ru/lezione8_24.htm;
4. Закон Российской Федерации от 23 сентября 1992 года №3523-1 «О правовой охране программ для электронно-вычислительных машин и баз данных»