Информационная безопасность

§ 76. Вредоносные программы

Что такое компьютерный вирус?

Компьютерный вирус — это программа, способная создавать свои копии (не обязательно совпадающие с оригиналом) и внедрять их в файлы и системные области компьютера.

Основная черта – способность распространяться при запуске!

Вредоносные программы — это программы, предназначенные для незаконного доступа к информации, для скрытого использования компьютера или для нарушения работы компьютера и компьютерных сетей.

malware

Зачем пишут вирусы?

- вирусы-шутки
- самоутверждение программистов
- **взлом сайтов** через заражённый компьютер
- перевод **денег** на другой счёт
- платные **SMS** для разблокировки
- рассылка **спама**
- **шпионаж** (кража паролей ⇒ кража денег)
- **DoS-атака** *(Denial of Service)* – отказ в обслуживании

ботнет – сеть из заражённых компьютеров, управляемая из единого центра

УК РФ, статья 273: **до 7 лет** лишения свободы!

Признаки заражения вирусом

- замедление работы компьютера
- уменьшение объема свободной оперативной памяти
- зависание, перезагрузка или блокировка компьютера
- ошибки при работе ОС или прикладных программ
- изменение длины файлов
- появление новых файлов
- рассылка спама

Чтобы выполнить какие-то действия, вирус должен оказаться в памяти и получить управление компьютером.

Что заражают вирусы?

Вирусы заражают программный код!

- исполняемые программы (**`*.exe`**)
- загрузочные секторы дисков (MBR = *Master Boot Record*)
- пакетные командные файлы (**`*.bat`**)
- драйверы (**`*.sys`**)
- библиотеки динамической загрузки (**`*.dll`**)
- документы с **макросами**
- веб-страницы (внедрение программы-**скрипта**)

Вирусы **НЕ** заражают файлы с **данными**: тексты, рисунки, звук, видео!

Как распространяются вирусы?

Основные источники заражения – **флэш-диски и компьютерные сети**!

- запуск заражённого файла
- загрузка с заражённого диска
- автозапуск заражённого флэш-диска (**`autorun.inf`**)
- открытие заражённого документа с макросами
- открытие сообщения электронной почты
- запуск программы, полученной в письме
- открытие веб-страницы с вирусом
- установка активного содержимого для просмотра веб-страницы
- по сетям (**вирусы-черви**, без участия человека)

Типы вредоносных программ

по среде обитания

- файловые
- загрузочные
- макровирусы
- скриптовые вирусы
- сетевые вирусы

Полиморфные вирусы: при создании копии немного изменяют код.

Сетевые черви: посылают по сети пакеты (*эксплойты*), позволяющие выполнить код удалённо.

нужно ставить «заплатки» (исправления, «патчи»)

Почтовые черви: распространяются через исполняемые программы в приложении к письму.

Google: запрет пересылки исполняемых файлов

социальная инженерия: спровоцировать на запуск файла

«Троянские» программы

Распространяются вместе с кодеками, червями, «кряками»!

- клавиатурные шпионы
- похитители паролей
- утилиты удалённого управления (*backdoor*)
- логические бомбы (уничтожают информацию на дисках)

Информационная безопасность

§ 77. Защита от вредоносных программ

Что такое антивирус?

Антивирус — это программа, предназначенная для борьбы с вредоносными программами.

Задачи:

- не допустить заражения
- обнаружить присутствие вируса
- удалить вирус без ущерба для остальных данных

Антивирусный комплекс

сканер	монитор

Антивирус-сканер («доктор»)

- защита «по требованию» (нужен запуск)
- поиск в файлах **сигнатур** вирусов, которые *есть в базе данных*

нужно обновлять!

- после обнаружения – лечение или удаление
- **эвристический анализ** – поиск кода, похожего на вирус

- лечит известные вирусы
- до запуска не занимает память и время процессора

- не может предотвратить заражение

Антивирус-монитор

- постоянная защита
- проверка файлов при файловых операциях
- проверка флэш-дисков
- перехват подозрительных действий
- проверка данных из Интернета
- защита от «фишинга» и спама

- предотвращает заражение, в том числе и неизвестными вирусами

- замедляет работу компьютера
- может мешать работе программ и ОС

Антивирусы

Коммерческие

- **AVP** = *Antiviral Toolkit Pro* (www.avp.ru) – Е. Касперский
- **DrWeb** (www.drweb.com) – И. Данилов
- **NOD32** (www.eset.com)

shareware

! Есть бесплатные пробные версии!

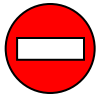
Бесплатные

- **Security Essential** (http://www.microsoft.com/security_essentials/)
- **Avast Home** (www.avast.com)
- **Antivir Personal** (free-av.com)
- **AVG Free** (free.grisoft.com)

Онлайновые антивирусы

- устанавливают на компьютер активный модуль (*ActiveX*), который проверяет файлы…
- или файл пересылается на сайт разработчика антивирусов

http://www.kaspersky.ru/virusscanner
http://www.bitdefender.com
http://security.symantec.com
http://us.mcafee.com/root/mfs/default.asp

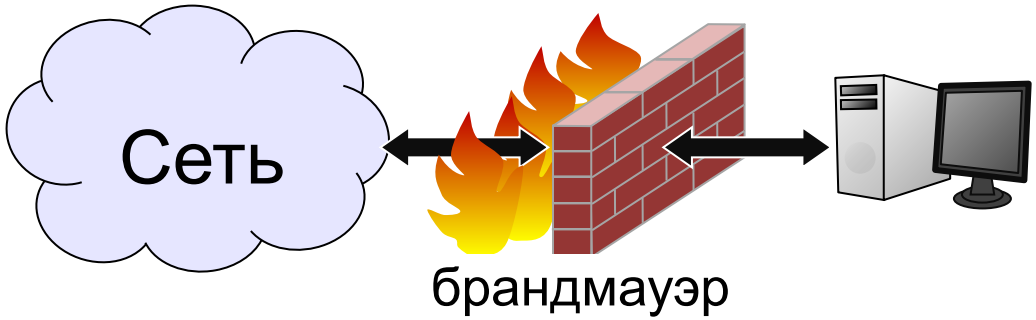


чаще всего не умеют лечить, предлагает купить антивирус

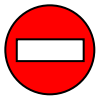
Сетевой экран

Брандмауэр (*файервол*)

Контролирует
- подключения из внешней сети
- передачу данных из внутренней сети



Фильтрация пакетов:
- по адресам источника и приёмника
- по портам (каналам подключения)


не проверяет данные

Agnitum Outpost (www.agnitum.com)


Kerio Winroute Firewall (kerio.ru)


Comodo Personal Firewall (www.personalfirewall.comodo.com)

бесплатно!

Меры безопасности

- делать резервные копии данных
- использовать сетевой экран (брандмауэр)
- использовать антивирус-монитор
- проверять флэш-диски антивирусом
- обновлять базы данных антивируса
- отключать автозапуск флэш-дисков
- не открывать подозрительные файлы (социальная инженерия!)
- не переходить по ссылкам в письмах
- использовать стойкие пароли
- менять пароли (раз в месяц)