ОСНОВНЫЕ УГРОЗЫ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА. АНТИВИРУСНАЯ ЗАЩИТА ИНФОРМАЦИИ

ИНФОРМАТИКА ДЛЯ СПО

ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ?

Информационная безопасность — это защищённость информации от любых действий, в результате которых владельцам или пользователям информации может быть нанесён **недопустимый** ущерб.

Причины ущерба:

- **искажение** информации
- **утеря** информации
- **неправомерный доступ** к информации

Защита не должна стоить дороже возможных потерь!

© К.Ю. Поляков, Е.А. Ерёмин, 2013

ЧТО ТАКОЕ ЗАЩИТА ИНФОРМАЦИИ?

Защита информации — это меры, направленные на то, чтобы не потерять информацию, не допустить её искажения и неправомерного доступа к ней.

Нужно обеспечить:

- **доступность** информации — отказ оборудования или сайта
- **целостность** — кража или искажение
- **конфиденциальность** — доступ посторонних

Проблемы **в сетях**:

- много пользователей
- возможность незаконного подключения к сети
- уязвимости сетевого ПО
- атаки взломщиков и вредоносных программ

ЗАЩИТА ИНФОРМАЦИИ

Закон «**Об информации, информационных технологиях и о защите информации**» от 27 июля 2006 г. № 149-ФЗ.

Средства защиты информации:

- **организационные**: распределение помещений и прокладку линий связи; политика безопасности организации
- **технические**: замки, решётки на окнах, системы сигнализации и видеонаблюдения и т.п.
- **программные**: доступ по паролю, шифрование, удаление временных файлов, защита от вредоносных программ и др.

ОГРАНИЧЕНИЕ ПРАВ ДОСТУПА

Сотрудники

- имеют право доступа только к тем **данным**, которые им **нужны** для работы
- не имеют права **устанавливать ПО**
- раз в месяц должны менять **пароли**

Один человек не должен иметь возможности причинить серьёзный вред!

инсайдеры!

Вирусы

ПОНЯТИЕ ВИРУСА

ОСНОВНАЯ ОТЛИЧИТЕЛЬНАЯ ХАРАКТЕРИСТИКА КОМПЬЮТЕРНОГО ВИРУСА — СПОСОБНОСТЬ К САМОРАСПРОСТРАНЕНИЮ. ПОДОБНО БИОЛОГИЧЕСКОМУ ВИРУСУ ДЛЯ ЖИЗНИ И РАЗМНОЖЕНИЯ ОН АКТИВНО ИСПОЛЬЗУЕТ ВНЕШНЮЮ СРЕДУ - ПАМЯТЬ КОМПЬЮТЕРА, ОПЕРАЦИОННУЮ СИСТЕМУ.

УВЕЛИЧЕНИЕ СКОРОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ, ОБЪЕМОВ И ЗНАЧИМОСТИ ОБРАБАТЫВАЕМЫХ В ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ДАННЫХ ОТКРЫВАЕТ ПЕРЕД ВИРУСОПИСАТЕЛЯМИ ВСЕ БОЛЕЕ ШИРОКИЕ ВОЗМОЖНОСТИ - РАСПРОСТРАНЕНИЕ ПО ВСЕМУ МИРУ НАПИСАННЫХ ПРОГРАММ ЗАНИМАЕТ СЧИТАННЫЕ ДНИ ИЛИ ДАЖЕ ЧАСЫ. СОТНИ МЕГАБАЙТ ОПЕРАТИВНОЙ ПАМЯТИ ПОЗВОЛЯЮТ ВЫПОЛНЯТЬ ПРАКТИЧЕСКИ ЛЮБЫЕ ДЕЙСТВИЯ НЕЗАМЕТНО ОТ ПОЛЬЗОВАТЕЛЯ. СПЕКТР ВОЗМОЖНЫХ ЦЕЛЕЙ, ТАКИХ КАК ПАРОЛИ, КАРТОЧНЫЕ СЧЕТА, РЕСУРСЫ УДАЛЕННЫХ КОМПЬЮТЕРОВ ПРЕДСТАВЛЯЕТ ОГРОМНОЕ ПОЛЕ ДЛЯ ДЕЯТЕЛЬНОСТИ. УСЛОЖНЕНИЕ ОПЕРАЦИОННЫХ СИСТЕМ ВЕДЕТ К ПОЯВЛЕНИЮ ВСЕ НОВЫХ ДЫР, КОТОРЫЕ МОГУТ БЫТЬ ИСПОЛЬЗОВАНЫ ДЛЯ ПРОНИКНОВЕНИЯ НА УДАЛЕННЫЙ КОМПЬЮТЕР.

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!

ПОНЯТИЕ ВИРУСА

ОДНАКО ИЗНАЧАЛЬНО КОМПЬЮТЕРНЫЕ ВИРУСЫ БЫЛИ ПРИДУМАНЫ С СОВЕРШЕННО ИНОЙ ЦЕЛЬЮ.

ИСТОРИЯ НАЧИНАЕТСЯ В 1983 ГОДУ, КОГДА АМЕРИКАНСКИЙ УЧЕНЫЙ ФРЕД КОЭН (FRED COHEN) В СВОЕЙ ДИССЕРТАЦИОННОЙ РАБОТЕ), ПОСВЯЩЕННОЙ ИССЛЕДОВАНИЮ САМОВОСПРОИЗВОДЯЩИХСЯ КОМПЬЮТЕРНЫХ ПРОГРАММ ВПЕРВЫЕ ВВЕЛ ТЕРМИН КОМПЬЮТЕРНЫЙ ВИРУС. ИЗВЕСТНА ДАЖЕ ТОЧНАЯ ДАТА - 3 НОЯБРЯ 1983 ГОДА, КОГДА НА ЕЖЕНЕДЕЛЬНОМ СЕМИНАРЕ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ В УНИВЕРСИТЕТЕ ЮЖНОЙ КАЛИФОРНИИ (США) БЫЛ ПРЕДЛОЖЕН ПРОЕКТ ПО СОЗДАНИЮ САМОРАСПРОСТРАНЯЮЩЕЙСЯ ПРОГРАММЫ, КОТОРУЮ ТУТ ЖЕ ОКРЕСТИЛИ ВИРУСОМ. ДЛЯ ЕЕ ОТЛАДКИ ПОТРЕБОВАЛОСЬ 8 ЧАСОВ КОМПЬЮТЕРНОГО ВРЕМЕНИ НА МАШИНЕ VAX 11/750 ПОД УПРАВЛЕНИЕМ ОПЕРАЦИОННОЙ СИСТЕМЫ UNIX И РОВНО ЧЕРЕЗ НЕДЕЛЮ, 10 НОЯБРЯ СОСТОЯЛАСЬ ПЕРВАЯ ДЕМОНСТРАЦИЯ. ФРЕДОМ КОЭНОМ ПО РЕЗУЛЬТАТАМ ЭТИХ ИССЛЕДОВАНИЙ БЫЛА ОПУБЛИКОВАНА РАБОТА "COMPUTER VIRUSES: THEORY AND EXPERIMENTS"2) С ПОДРОБНЫМ ОПИСАНИЕМ ПРОБЛЕМЫ.

ПОНЯТИЕ ВИРУСА

ТЕОРЕТИЧЕСКИЕ ЖЕ ОСНОВЫ САМОРАСПРОСТРАНЯЮЩИХСЯ ПРОГРАММ БЫЛИ ЗАЛОЖЕНЫ В 40-Х ГОДАХ ПРОШЛОГО СТОЛЕТИЯ В ТРУДАХ ПО ИЗУЧЕНИЮ САМОВОСПРОИЗВОДЯЩИХСЯ МАТЕМАТИЧЕСКИХ АВТОМАТОВ АМЕРИКАНСКОГО УЧЕНОГО ДЖОНА ФОН НЕЙМАНА (JOHN VON NEUMANN), КОТОРЫЙ ТАКЖЕ ИЗВЕСТЕН КАК АВТОР БАЗОВЫХ ПРИНЦИПОВ РАБОТЫ СОВРЕМЕННОГО КОМПЬЮТЕРА. В 1951 ГОДУ ФОН НЕЙМАНОМ БЫЛ РАЗРАБОТАН МЕТОД, КОТОРЫЙ ДЕМОНСТРИРОВАЛ ВОЗМОЖНОСТЬ СОЗДАНИЯ ТАКИХ АВТОМАТОВ, А В 1959 ЖУРНАЛ "SCIENTIFIC AMERICAN" ОПУБЛИКОВАЛ СТАТЬЮ Л. С. ПЕНРОУЗА (L. S. PENROSE) "SELF-REPRODUCING MACHINES", ПОСВЯЩЕННУЮ САМОВОСПРОИЗВОДЯЩИМСЯ МЕХАНИЧЕСКИМ СТРУКТУРАМ. В ОТЛИЧИЕ ОТ РАНЕЕ ИЗВЕСТНЫХ РАБОТ, ЗДЕСЬ БЫЛА ОПИСАНА ПРОСТЕЙШАЯ ДВУМЕРНАЯ МОДЕЛЬ ПОДОБНЫХ СТРУКТУР, СПОСОБНЫХ К АКТИВАЦИИ, РАЗМНОЖЕНИЮ, МУТАЦИЯМ, ЗАХВАТУ. ПОЗДНЕЕ, ПО СЛЕДАМ ЭТОЙ СТАТЬИ ДРУГОЙ УЧЕНЫЙ Ф. Ж. ШТАЛЬ (F. G. STAHL) РЕАЛИЗОВАЛ МОДЕЛЬ НА ПРАКТИКЕ С ПОМОЩЬЮ МАШИННОГО КОДА НА IBM 650.

ПОНЯТИЕ ВИРУСА

ПЕРВЫЕ САМОРАСПРОСТРАНЯЮЩИЕСЯ ПРОГРАММЫ НЕ БЫЛИ ВРЕДОНОСНЫМИ В ПОНИМАЕМОМ НЫНЕ СМЫСЛЕ. ЭТО БЫЛИ СКОРЕЕ ПРОГРАММЫ-ШУТКИ ЛИБО ПОСЛЕДСТВИЯ ОШИБОК В ПРОГРАММНОМ КОДЕ, НАПИСАННОМ В ИССЛЕДОВАТЕЛЬСКИХ ЦЕЛЯХ. СЛОЖНО ПРЕДСТАВИТЬ, ЧТО ОНИ БЫЛИ СОЗДАНЫ С КАКОЙ-ТО КОНКРЕТНОЙ ВРЕДОНОСНОЙ ЦЕЛЬЮ.

ПЕРВЫЕ ВИРУСЫ

PERVADING ANIMAL (КОНЕЦ 60-Х - НАЧАЛО 70-Х) — ТАК НАЗЫВАЛСЯ ПЕРВЫЙ ИЗВЕСТНЫЙ ВИРУС-ИГРА ДЛЯ МАШИНЫ UNIVAC 1108. С ПОМОЩЬЮ НАВОДЯЩИХ ВОПРОСОВ ПРОГРАММА ПЫТАЛАСЬ ОПРЕДЕЛИТЬ ИМЯ ЖИВОТНОГО, ЗАДУМАННОГО ИГРАЮЩИМ. БЛАГОДАРЯ НАЛИЧИЮ ФУНКЦИИ ДОБАВЛЕНИЯ НОВЫХ ВОПРОСОВ, КОГДА МОДИФИЦИРОВАННАЯ ИГРА ЗАПИСЫВАЛАСЬ ПОВЕРХ СТАРОЙ ВЕРСИИ ПЛЮС КОПИРОВАЛАСЬ В ДРУГИЕ ДИРЕКТОРИИ, ЧЕРЕЗ НЕКОТОРОЕ ВРЕМЯ ДИСК СТАНОВИЛСЯ ПЕРЕПОЛНЕННЫМ.

ПЕРВЫЕ ВИРУСЫ

ПЕРВЫЙ СЕТЕВОЙ ВИРУС CREEPER ПОЯВИЛСЯ В НАЧАЛЕ 70-Х В ВОЕННОЙ КОМПЬЮТЕРНОЙ СЕТИ ARPANET3), ПРОТОТИПЕ ИНТЕРНЕТ. ПРОГРАММА БЫЛА В СОСТОЯНИИ САМОСТОЯТЕЛЬНО ВЫЙТИ В СЕТЬ ЧЕРЕЗ МОДЕМ И СОХРАНИТЬ СВОЮ КОПИЮ НА УДАЛЕННОЙ МАШИНЕ. НА ЗАРАЖЕННЫХ СИСТЕМАХ ВИРУС ОБНАРУЖИВАЛ СЕБЯ СООБЩЕНИЕМ: "I'M THE CREEPER : CATCH ME IF YOU CAN". ДЛЯ УДАЛЕНИЯ НАЗОЙЛИВОГО, НО В ЦЕЛОМ БЕЗОБИДНОГО ВИРУСА НЕИЗВЕСТНЫМ БЫЛА СОЗДАНА ПРОГРАММА REAPER. ПО СУТИ ЭТО БЫЛ ВИРУС, ВЫПОЛНЯВШИЙ НЕКОТОРЫЕ ФУНКЦИИ, СВОЙСТВЕННЫЕ АНТИВИРУСУ: ОН РАСПРОСТРАНЯЛСЯ ПО ВЫЧИСЛИТЕЛЬНОЙ СЕТИ И В СЛУЧАЕ ОБНАРУЖЕНИЯ ТЕЛА ВИРУСА CREEPER УНИЧТОЖАЛ ЕГО.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

ВОЗМОЖНОСТИ ПЕРВЫХ ВИРУСОВ БЫЛИ СИЛЬНО ОГРАНИЧЕНЫ МАЛОЙ ФУНКЦИОНАЛЬНОСТЬЮ СУЩЕСТВУЮЩИХ НА ТОТ МОМЕНТ ВЫЧИСЛИТЕЛЬНЫХ МАШИН. ТОЛЬКО В КОНЦЕ СЕМИДЕСЯТЫХ, ВСЛЕД ЗА ВЫПУСКОМ НОВОГО ПОКОЛЕНИЯ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ APPLE (APPLE II) И ВПОСЛЕДСТВИИ IBM PERSONAL COMPUTER (1981 ГОД), СТАЛИ ВОЗМОЖНЫ ВИРУСНЫЕ ЭПИДЕМИИ. ПОЯВЛЕНИЕ BBS (BULLETIN BOARD SYSTEM) ОБЕСПЕЧИЛО БЫСТРЫЙ ОБМЕН ИНФОРМАЦИЕЙ МЕЖДУ ДАЖЕ САМЫМИ ОТДАЛЕННЫМИ ТОЧКАМИ ПЛАНЕТЫ.

ELK CLONER (1981 ГОД) ИЗНАЧАЛЬНО ИСПОЛЬЗОВАЛ ДЛЯ РАСПРОСТРАНЕНИЯ ПИРАТСКИХ КОПИЙ КОМПЬЮТЕРНЫХ ИГР.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

ПОСКОЛЬКУ ЖЕСТКИХ ДИСКОВ ТОГДА ЕЩЕ НЕ БЫЛО, ОН ЗАПИСЫВАЛСЯ В ЗАГРУЗОЧНЫЕ СЕКТОРА ДИСКЕТ И ПРОЯВЛЯЛ СЕБЯ ПЕРЕВОРАЧИВАНИЕМ ИЗОБРАЖЕНИЯ НА ЭКРАНЕ И ВЫВОДОМ ТЕКСТА:

ELK CLONER:

THE PROGRAM WITH A PERSONALITY

IT WILL GET ON ALL YOUR DISKS

IT WILL INFILTRATE YOUR CHIPS

YES, IT'S CLONER

IT WILL STICK TO YOU LIKE GLUE

IT WILL MODIFY RAM, TOO

SEND IN THE CLONER!

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

BRAIN (1986 ГОД) — ПЕРВЫЙ ВИРУС ДЛЯ IBM-СОВМЕСТИМЫХ КОМПЬЮТЕРОВ, ВЫЗВАВШИЙ ГЛОБАЛЬНУЮ ЭПИДЕМИЮ. ОН БЫЛ НАПИСАН ДВУМЯ БРАТЬЯМИ-ПРОГРАММИСТАМИ БАСИТОМ ФАРУК И АМЖАДОМ АЛВИ (BASIT FAROOQ ALVI И AMJAD ALVI) ИЗ ПАКИСТАНА С ЦЕЛЬЮ ОПРЕДЕЛЕНИЯ УРОВНЯ ПИРАТСТВА У СЕБЯ В СТРАНЕ: ВИРУС ЗАРАЖАЛ ЗАГРУЗОЧНЫЕ СЕКТОРА, МЕНЯЛ МЕТКУ ДИСКА НА "(C) BRAIN" И ОСТАВЛЯЛ СООБЩЕНИЕ С ИМЕНАМИ, АДРЕСОМ И ТЕЛЕФОНОМ АВТОРОВ. ОТЛИЧИТЕЛЬНОЙ ЧЕРТОЙ ЕГО БЫЛА ФУНКЦИЯ ПОДМЕНЫ В МОМЕНТ ОБРАЩЕНИЯ К НЕМУ ЗАРАЖЕННОГО СЕКТОРА НЕЗАРАЖЕННЫМ ОРИГИНАЛОМ. ЭТО ДАЕТ ПРАВО НАЗВАТЬ BRAIN ПЕРВЫМ ИЗВЕСТНЫМ СТЕЛС-ВИРУСОМ. В ТЕЧЕНИЕ НЕСКОЛЬКИХ МЕСЯЦЕВ ПРОГРАММА ВЫШЛА ЗА ПРЕДЕЛЫ ПАКИСТАНА И К ЛЕТУ 1987 ГОДА ЭПИДЕМИЯ ДОСТИГЛА ГЛОБАЛЬНЫХ МАСШТАБОВ. НИЧЕГО ДЕСТРУКТИВНОГО ВИРУС НЕ ДЕЛАЛ.

09.11.2020

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

В ЭТОМ ЖЕ ГОДУ ПРОИЗОШЛО ЕЩЕ ОДНО ЗНАМЕНАТЕЛЬНОЕ СОБЫТИЕ. НЕМЕЦКИЙ ПРОГРАММИСТ РАЛЬФ БЮРГЕР (RALF BURGER) ОТКРЫЛ ВОЗМОЖНОСТЬ СОЗДАНИЯ ПРОГРАММОЙ СВОИХ КОПИЙ ПУТЕМ ДОБАВЛЕНИЯ СВОЕГО КОДА К ВЫПОЛНЯЕМЫМ DOS-ФАЙЛАМ ФОРМАТА COM. ОПЫТНЫЙ ОБРАЗЕЦ ПРОГРАММЫ, ПОЛУЧИВШЕЙ НАЗВАНИЕ VIRDEM, БЫЛ ПРОДЕМОНСТРИРОВАН НА ФОРУМЕ КОМПЬЮТЕРНОГО АНДЕГРАУНДА - CHAOS COMPUTER CLUB (ДЕКАБРЬ 1986 ГОДА, ГАМБУРГ, ФРГ). ПО РЕЗУЛЬТАТАМИ ИССЛЕДОВАНИЙ БЮРГЕР ВЫПУСТИЛ КНИГУ "COMPUTER VIRUSES. THE DISEASE OF HIGH TECHNOLOGIES", ПОСЛУЖИВШУЮ ТОЛЧКОМ К НАПИСАНИЮ ТЫСЯЧ КОМПЬЮТЕРНЫХ ВИРУСОВ, ЧАСТИЧНО ИЛИ ПОЛНОСТЬЮ ИСПОЛЬЗОВАВШИХ ОПИСАННЫЕ АВТОРОМ ИДЕИ.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

LEHIGH (1987 ГОД) — ПЕРВЫЙ ПО-НАСТОЯЩЕМУ ВРЕДОНОСНЫЙ ВИРУС, ВЫЗВАВШИЙ ЭПИДЕМИЮ В ЛЕХАЙСКОМ УНИВЕРСИТЕТЕ (США), ГДЕ В ТО ВРЕМЯ РАБОТАЛ ФРЕД КОЭН. ОН ЗАРАЖАЛ ТОЛЬКО СИСТЕМНЫЕ ФАЙЛЫ COMMAND.COM И БЫЛ ЗАПРОГРАММИРОВАН НА УДАЛЕНИЕ ВСЕЙ ИНФОРМАЦИИ НА ТЕКУЩЕМ ДИСКЕ. В ТЕЧЕНИЕ НЕСКОЛЬКИХ ДНЕЙ БЫЛО УНИЧТОЖЕНО СОДЕРЖИМОЕ СОТЕН ДИСКЕТ ИЗ БИБЛИОТЕКИ УНИВЕРСИТЕТА И ЛИЧНЫХ ДИСКЕТ СТУДЕНТОВ. ВСЕГО ЗА ВРЕМЯ ЭПИДЕМИИ БЫЛО ЗАРАЖЕНО ОКОЛО ЧЕТЫРЕХ ТЫСЯЧ КОМПЬЮТЕРОВ. ОДНАКО ЗА ПРЕДЕЛЫ УНИВЕРСИТЕТА LEHIGH НЕ ВЫШЕЛ.

СЕМЕЙСТВО РЕЗИДЕНТНЫХ ФАЙЛОВЫХ ВИРУСОВ SURIV (1987 ГОД) — ТВОРЕНИЕ НЕИЗВЕСТНОГО ПРОГРАММИСТА ИЗ ИЗРАИЛЯ. САМАЯ ИЗВЕСТНАЯ МОДИФИКАЦИЯ, JERUSALEM, СТАЛА ПРИЧИНОЙ ГЛОБАЛЬНОЙ ВИРУСНОЙ ЭПИДЕМИИ, ПЕРВОЙ НАСТОЯЩЕЙ ПАНДЕМИЕЙ, ВЫЗВАННОЙ MS-DOS-ВИРУСОМ.

09.11.2020

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

ДЕЙСТВИЕ ВИРУСОВ SURIV СВОДИЛОСЬ К ЗАГРУЗКЕ КОДА В ПАМЯТЬ КОМПЬЮТЕРА, ПЕРЕХВАТЫВАНИИ ФАЙЛОВЫХ ОПЕРАЦИЙ И ЗАРАЖЕНИИ ЗАПУСКАЕМЫХ ПОЛЬЗОВАТЕЛЕМ COM- И/ИЛИ EXE-ФАЙЛОВ. ЭТО ОБСТОЯТЕЛЬСТВО ОБЕСПЕЧИВАЛО ПРАКТИЧЕСКИ МГНОВЕННОЕ РАСПРОСТРАНЕНИЕ ВИРУСА ПО МОБИЛЬНЫМ НОСИТЕЛЯМ. JERUSALEM ОТЛИЧАЛСЯ ОТ СВОИХ ПРЕДШЕСТВЕННИКОВ ДОПОЛНИТЕЛЬНОЙ ДЕСТРУКТИВНОЙ ФУНКЦИЕЙ - УНИЧТОЖЕНИЕМ ВСЕХ ЗАПУСКАЕМЫХ ПРОГРАММ В ПЯТНИЦУ, 13. ТАКОЙ ЧЕРНОЙ ДАТОЙ СТАЛО 13 МАЯ 1988 ГОДА, КОГДА В ОДНОЧАСЬЕ ПЕРЕСТАЛИ РАБОТАТЬ КОМПЬЮТЕРЫ МНОГИХ КОММЕРЧЕСКИХ ФИРМ, ГОСУДАРСТВЕННЫХ ОРГАНИЗАЦИЙ И УЧЕБНЫХ ЗАВЕДЕНИЙ, В ПЕРВУЮ ОЧЕРЕДЬ АМЕРИКИ, ЕВРОПЫ И БЛИЖНЕГО ВОСТОКА.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

ПРИМЕЧАТЕЛЬНО, ЧТО В ТОМ ЖЕ 1988 ГОДУ ИЗВЕСТНЫЙ ПРОГРАММИСТ ПИТЕР НОРТОН (PETER NORTON) ВЫСКАЗАЛСЯ РЕЗКО ПРОТИВ СУЩЕСТВОВАНИЯ ВИРУСОВ. ОН ОФИЦИАЛЬНО ОБЪЯВИЛ ИХ НЕСУЩЕСТВУЮЩИМ МИФОМ И СРАВНИЛ СО СКАЗКАМИ О КРОКОДИЛАХ, ЖИВУЩИХ В КАНАЛИЗАЦИИ НЬЮ-ЙОРКА. ЭТО ПОКАЗЫВАЕТ СКОЛЬ НИЗКА БЫЛА КУЛЬТУРА АНТИВИРУСНОЙ БЕЗОПАСНОСТИ В ТО ВРЕМЯ.

MIKE ROCHENLE — ПСЕВДОНИМ АВТОРА ПЕРВОЙ ИЗВЕСТНОЙ ВИРУСНОЙ МИСТИФИКАЦИИ. В ОКТЯБРЕ 1988 ГОДА ОН РАЗОСЛАЛ НА СТАНЦИИ BBS БОЛЬШОЕ КОЛИЧЕСТВО СООБЩЕНИЙ О ВИРУСЕ, КОТОРЫЙ ПЕРЕДАЕТСЯ ОТ МОДЕМА К МОДЕМУ СО СКОРОСТЬЮ 2400 БИТ/С. В КАЧЕСТВЕ ПАНАЦЕИ ПРЕДЛАГАЛОСЬ ПЕРЕЙТИ НА ИСПОЛЬЗОВАНИЕ МОДЕМОВ СО СКОРОСТЬЮ 1200 БИТ/С. КАК ЭТО НИ СМЕШНО, МНОГИЕ ПОЛЬЗОВАТЕЛИ ДЕЙСТВИТЕЛЬНО ПОСЛЕДОВАЛИ ЭТОМУ СОВЕТУ.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

ЧЕРВЬ МОРРИСА (НОЯБРЬ 1988) — С НИМ СВЯЗАНА ПЕРВАЯ ЭПИДЕМИЯ, ВЫЗВАННАЯ СЕТЕВЫМ ЧЕРВЕМ. 60000-БАЙТНАЯ ПРОГРАММА, НАПИСАННАЯ 23-ЛЕТНИМ СТУДЕНТОМ КОРНЕЛЬСКОГО УНИВЕРСИТЕТА (США) РОБЕРТОМ МОРРИСОМ, ИСПОЛЬЗОВАЛА ОШИБКИ В СИСТЕМЕ БЕЗОПАСНОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ UNIX ДЛЯ ПЛАТФОРМ VAX И SUN MICROSYSTEMS. С ЦЕЛЬЮ НЕЗАМЕТНОГО ПРОНИКНОВЕНИЯ В ВЫЧИСЛИТЕЛЬНЫЕ СИСТЕМЫ, СВЯЗАННЫЕ С СЕТЬЮ ARPANET, ИСПОЛЬЗОВАЛСЯ ПОДБОР ПАРОЛЕЙ (ИЗ СПИСКА, СОДЕРЖАЩЕГО 481 ВАРИАНТ). ЭТО ПОЗВОЛЯЛО МАСКИРОВАТЬСЯ ПОД ЗАДАЧУ ЛЕГАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ. ОДНАКО ИЗ-ЗА ОШИБОК В КОДЕ БЕЗВРЕДНАЯ ПО ЗАМЫСЛУ ПРОГРАММА НЕОГРАНИЧЕННО РАССЫЛАЛА СВОИ КОПИИ ПО ДРУГИМ КОМПЬЮТЕРАМ СЕТИ, ЗАПУСКАЛА ИХ НА ВЫПОЛНЕНИЕ И ТАКИМ ОБРАЗОМ ЗАБИРАЛА ПОД СЕБЯ ВСЕ СЕТЕВЫЕ РЕСУРСЫ.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

ЧЕРВЬ МОРРИСА ЗАРАЗИЛ ПО РАЗНЫМ ОЦЕНКАМ ОТ 6000 ДО 9000 КОМПЬЮТЕРОВ В США (ВКЛЮЧАЯ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР NASA) И ПРАКТИЧЕСКИ ПАРАЛИЗОВАЛ ИХ РАБОТУ НА СРОК ДО ПЯТИ СУТОК. ОБЩИЕ УБЫТКИ БЫЛИ ОЦЕНЕНЫ В МИНИМУМ 8 МИЛЛИОНОВ ЧАСОВ ПОТЕРИ ДОСТУПА И СВЫШЕ МИЛЛИОНА ЧАСОВ ПРЯМЫХ ПОТЕРЬ НА ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ СИСТЕМ. ОБЩАЯ СТОИМОСТЬ ЭТИХ ЗАТРАТ ОЦЕНИВАЕТСЯ В 96 МИЛЛИОНОВ ДОЛЛАРОВ. УЩЕРБ БЫЛ БЫ ГОРАЗДО БОЛЬШЕ, ЕСЛИ БЫ ЧЕРВЬ ИЗНАЧАЛЬНО СОЗДАВАЛСЯ С РАЗРУШИТЕЛЬНЫМИ ЦЕЛЯМИ.

4 МАЯ 1990 ГОДА ВПЕРВЫЕ В ИСТОРИИ СОСТОЯЛСЯ СУД НАД АВТОРОМ КОМПЬЮТЕРНОГО ВИРУСА, КОТОРЫЙ ПРИГОВОРИЛ РОБЕРТА МОРРИСА К 3 ГОДАМ УСЛОВНО, 400 ЧАСАМ ОБЩЕСТВЕННЫХ РАБОТ И ШТРАФУ В 10 ТЫСЯЧ ДОЛЛАРОВ США.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

ЭПИДЕМИЯ ЧЕРВЯ МОРРИСА СТАЛА ПРИЧИНОЙ СОЗДАНИЯ ОРГАНИЗАЦИИ CERT (COMPUTER EMERGENCY RESPONSE TEAM), В ФУНКЦИИ КОТОРОЙ ВХОДИТ ОКАЗАНИЕ СОДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯМ В ПРЕДОТВРАЩЕНИИ И РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ, ИМЕЮЩИХ ОТНОШЕНИЕ К ИНФОРМАЦИОННЫМ РЕСУРСАМ. НА САЙТЕ ЭТОЙ ОРГАНИЗАЦИИ (HTTP://WWW.CERT.ORG) ОПЕРАТИВНО ПУБЛИКУЮТСЯ САМЫЕ ПОСЛЕДНИЕ СВЕДЕНИЯ О НОВЫХ ВРЕДОНОСНЫХ ПРОГРАММАХ, ОБНАРУЖЕННЫХ УЯЗВИМОСТЯХ В ПО, МЕТОДАХ ЗАЩИТЫ КОРПОРАТИВНЫХ СЕТЕЙ, АНАЛИТИЧЕСКИЕ СТАТЬИ, А ТАКЖЕ РЕЗУЛЬТАТЫ РАЗЛИЧНЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

DATACRIME (1989) — ВИРУС, КОТОРЫЙ НЕСМОТРЯ НА СРАВНИТЕЛЬНО НЕБОЛЬШОЕ РАСПРОСТРАНЕНИЕ, ВЫЗВАЛ ПОВАЛЬНУЮ ИСТЕРИЮ В МИРОВЫХ СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ. ОН ОТЛИЧАЛСЯ ТЕМ, ЧТО С 13 ОКТЯБРЯ ПО 31 ДЕКАБРЯ ИНИЦИИРОВАЛ НИЗКОУРОВНЕВОЕ ФОРМАТИРОВАНИЕ НУЛЕВОГО ЦИЛИНДРА ЖЕСТКОГО ДИСКА, ЧТО ПРИВОДИЛО К УНИЧТОЖЕНИЮ ТАБЛИЦЫ РАЗМЕЩЕНИЯ ФАЙЛОВ (FAT) И БЕЗВОЗВРАТНОЙ ПОТЕРЕ ДАННЫХ.

В ОТВЕТ КОРПОРАЦИЯ IBM ВЫПУСТИЛА (4 ОКТЯБРЯ 1989 ГОДА) КОММЕРЧЕСКИЙ АНТИВИРУС VIRSCAN ДЛЯ MS-DOS, ПОЗВОЛЯЮЩИЙ ИСКАТЬ ХАРАКТЕРНЫЕ ДЛЯ РЯДА ИЗВЕСТНЫХ ВИРУСОВ СТРОКИ В ФАЙЛОВОЙ СИСТЕМЕ. СТОИМОСТЬ ПРОГРАММЫ СОСТАВИЛА ВСЕГО 35 ДОЛЛАРОВ США.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

AIDS INFORMATION DISKETTE (ДЕКАБРЬ 1989) — ПЕРВАЯ ЭПИДЕМИЯ ТРОЯНСКОЙ ПРОГРАММЫ. ЕЕ АВТОР РАЗОСЛАЛ ОКОЛО 20000 ДИСКЕТ С ВИРУСОМ ПО АДРЕСАМ В ЕВРОПЕ, АФРИКЕ И АВСТРАЛИИ, ПОХИЩЕННЫМ ИЗ БАЗ ДАННЫХ ОРГАНИЗАЦИИ ВСЕМИРНОГО ЗДРАВООХРАНЕНИЯ И ЖУРНАЛА PC BUSINESS WORLD. ПОСЛЕ ЗАПУСКА ВРЕДОНОСНАЯ ПРОГРАММА АВТОМАТИЧЕСКИ ВНЕДРЯЛАСЬ В СИСТЕМУ, СОЗДАВАЛА СВОИ СОБСТВЕННЫЕ СКРЫТЫЕ ФАЙЛЫ И ДИРЕКТОРИИ И МОДИФИЦИРОВАЛА СИСТЕМНЫЕ ФАЙЛЫ. ЧЕРЕЗ 90 ЗАГРУЗОК ОПЕРАЦИОННОЙ СИСТЕМЫ ВСЕ ФАЙЛЫ НА ДИСКЕ СТАНОВИЛИСЬ НЕДОСТУПНЫМИ, КРОМЕ ОДНОГО - С СООБЩЕНИЕМ, ПРЕДЛАГАВШИМ ПРИСЛАТЬ $189 НА УКАЗАННЫЙ АДРЕС. АВТОР ТРОЯНЦА, ДЖОЗЕФ ПОПП (JOSEPH POPP), ПРИЗНАННЫЙ ПОЗДНЕЕ НЕВМЕНЯЕМЫМ, БЫЛ ЗАДЕРЖАН В МОМЕНТ ОБНАЛИЧИВАНИЯ ЧЕКА И ОСУЖДЕН ЗА ВЫМОГАТЕЛЬСТВО. ФАКТИЧЕСКИ, AIDS INFORMATION DISKETTE - ЭТО ПЕРВЫЙ И ЕДИНСТВЕННЫЙ ВИРУС, ДЛЯ МАССОВОЙ РАССЫЛКИ ИСПОЛЬЗОВАВШИЙ НАСТОЯЩУЮ ПОЧТУ.

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

CASCADE (1989) — РЕЗИДЕНТНЫЙ ЗАШИФРОВАННЫЙ ВИРУС, ВЫЗЫВАЮЩИЙ ХАРАКТЕРНЫЙ ВИДЕОЭФФЕКТ - ОСЫПАНИЕ БУКВ НА ЭКРАНЕ. ПРИМЕЧАТЕЛЕН ТЕМ, ЧТО ПОСЛУЖИЛ ТОЛЧКОМ ДЛЯ ПРОФЕССИОНАЛЬНОЙ ПЕРЕОРИЕНТАЦИИ ЕВГЕНИЯ КАСПЕРСКОГО НА СОЗДАНИЕ ПРОГРАММ-АНТИВИРУСОВ, БУДУЧИ ОБНАРУЖЕННЫМ НА ЕГО РАБОЧЕМ КОМПЬЮТЕРЕ. УЖЕ ЧЕРЕЗ МЕСЯЦ ВТОРОЙ ИНЦИДЕНТ (ВИРУС VACSINA) БЫЛ ЗАКРЫТ ПРИ ПОМОЩИ ПЕРВОЙ ВЕРСИИ АНТИВИРУСА — V, КОТОРЫЙ НЕСКОЛЬКИМИ ГОДАМИ ПОЗЖЕ БЫЛ ПЕРЕИМЕНОВАН В AVP — ANTIVIRAL TOOLKIT PRO

ПЕРВЫЕ ВИРУСНЫЕ ЭПИДЕМИИ

EDDIE (ТАКЖЕ ИЗВЕСТЕН КАК DARK AVENGER, 1989 ГОД) — ПЕРВЫЙ ВИРУС, ПРОТИВОДЕЙСТВУЮЩИЙ АНТИВИРУСНОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ: ОН ЗАРАЖАЕТ НОВЫЕ ФАЙЛЫ, ПОКА АНТИВИРУС ПРОВЕРЯЕТ ЖЕСТКИЙ ДИСК КОМПЬЮТЕРА. ЭТО ДОСТИГАЛОСЬ ПРИМЕНЕНИЕМ ОСОБОЙ ТЕХНОЛОГИИ, ПОЗВОЛЯЮЩЕЙ ЗАРАЖАТЬ НЕ ТОЛЬКО COM/EXE- ПРОГРАММЫ В МОМЕНТ ИХ ЗАПУСКА, НО И ЛЮБЫЕ ФАЙЛЫ ПРИ ПОПЫТКЕ ПРОЧТЕНИЯ.

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.

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

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

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)

ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ

ПЕРВЫЕ АНТИВИРУСНЫЕ УТИЛИТЫ

ПЕРВЫЕ АНТИВИРУСНЫЕ УТИЛИТЫ (1984 ГОД) БЫЛИ НАПИСАНЫ АНДИ ХОПКИНСОМ (ANDY HOPKINS). ПРОГРАММЫ CHK4BOMB И BOMBSQAD ПОЗВОЛЯЛИ ПРОИЗВОДИТЬ АНАЛИЗ ЗАГРУЗОЧНОГО МОДУЛЯ С ПОМОЩЬЮ КОНТЕКСТНОГО ПОИСКА И ПЕРЕХВАТЫВАТЬ ОПЕРАЦИИ ЗАПИСИ И ФОРМАТИРОВАНИЯ, ВЫПОЛНЯЕМЫЕ ЧЕРЕЗ BIOS. НА ТО ВРЕМЯ ОНИ БЫЛИ ОЧЕНЬ ЭФФЕКТИВНЫ И БЫСТРО ЗАВОЕВАЛИ ПОПУЛЯРНОСТЬ.

ПЕРВЫЕ АНТИВИРУСНЫЕ УТИЛИТЫ

DR. SOLOMON'S ANTI-VIRUS TOOLKIT (1988) — ПЕРВАЯ ШИРОКО ИЗВЕСТНАЯ АНТИВИРУСНАЯ ПРОГРАММА. СОЗДАННАЯ АНГЛИЙСКИМ ПРОГРАММИСТОМ АЛАНОМ СОЛОМОНОМ (ALAN SOLOMON), ОНА ЗАВОЕВАЛА ОГРОМНУЮ ПОПУЛЯРНОСТЬ И ПРОСУЩЕСТВОВАЛА ДО 1998 ГОДА, КОГДА КОМПАНИЯ DR. SOLOMON БЫЛА ПОГЛОЩЕНА ДРУГИМ ПРОИЗВОДИТЕЛЕМ АНТИВИРУСОВ - АМЕРИКАНСКОЙ NETWORK ASSOCIATES (NAI).

ПЕРВЫЕ АНТИВИРУСНЫЕ УТИЛИТЫ

КРОМЕ ОФИЦИАЛЬНОГО ПЕРЕИМЕНОВАНИЯ ARPANET В ИНТЕРНЕТ, СЛЕДУЮЩИЙ ГОД ОЗНАМЕНОВАЛСЯ ВЫХОДОМ В СВЕТ ПЕРВОГО НОМЕРА VIRUS BULLETIN (ИЮЛЬ 1989) — САМОГО ПОПУЛЯРНОГО НА СЕГОДНЯШНИЙ ДЕНЬ ИЗДАНИЯ, СОДЕРЖАЩЕГО ПОСЛЕДНИЕ НОВОСТИ В СФЕРЕ ВИРУСНЫХ И АНТИВИРУСНЫХ ТЕХНОЛОГИЙ: ПОДРОБНУЮ ИНФОРМАЦИЮ О НОВЫХ ВРЕДОНОСНЫХ ПРОГРАММАХ, МЕТОДАХ ЗАЩИТЫ ОТ ВИРУСОВ И УСТРАНЕНИЯ ПОСЛЕДСТВИЙ ЗАРАЖЕНИЯ. ОСНОВАТЕЛЯМИ ЖУРНАЛА ВЫСТУПИЛИ РУКОВОДИТЕЛИ АНГЛИЙСКОЙ АНТИВИРУСНОЙ КОМПАНИИ SOPHOS ЯН ХРАСКЕ (JAN HRUSKA), ПИТЕР ЛЭММЕР (PETER LAMMER) И ЭД УАЙЛДИНГ (ED WILDING). ВПОСЛЕДСТВИИ РЕДАКЦИЯ VIRUS BULLETIN (1991) НАЧАЛА ПРОВОДИТЬ ЕЖЕГОДНЫЕ КОНФЕРЕНЦИИ ДЛЯ АНТИВИРУСНЫХ ЭКСПЕРТОВ, ГДЕ КОРПОРАТИВНЫЕ ЗАКАЗЧИКИ ИМЕЮТ ВОЗМОЖНОСТЬ НАПРЯМУЮ ОБЩАТЬСЯ С ВЕДУЩИМИ СПЕЦИАЛИСТАМИ В ЭТОЙ ОБЛАСТИ. В ЯНВАРЕ 1998 ГОДА БЫЛА УЧРЕЖДЕНА НАГРАДА VB 100%, ПРИСУЖДАЕМАЯ АНТИВИРУСНЫМ ПРОГРАММАМ ПО РЕЗУЛЬТАТАМ ПРОВОДИМОГО РЕДАКЦИЕЙ VIRUS BULLETIN ТЕСТИРОВАНИЯ. КОЛИЧЕСТВО НАГРАД VB 100%, ПОЛУЧЕННЫХ В РЕЗУЛЬТАТЕ ТЕСТИРОВАНИЯ СЕГОДНЯ ЗАЧАСТУЮ ЯВЛЯЕТСЯ ОДНИМ ИЗ ОСНОВНЫХ КРИТЕРИЕВ В ВЫБОРЕ СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ.

ПЕРВЫЕ АНТИВИРУСНЫЕ УТИЛИТЫ

В КАЧЕСТВЕ ОТВЕТА ЧЕРЕЗ ПАРУ МЕСЯЦЕВ DR. SOLOMON'S ЗАПУСТИЛА СВОЙ СОБСТВЕННЫЙ ИЗДАТЕЛЬСКИЙ ПРОЕКТ - VIRUS FAX INTERNATIONAL, ВПОСЛЕДСТВИИ ПЕРЕИМЕНОВАННЫЙ В SECURE COMPUTING. СЕГОДНЯ ЭТОТ ЖУРНАЛ ЯВЛЯЕТСЯ ОДНИМ ИЗ НАИБОЛЕЕ ПОПУЛЯРНЫХ ИЗДАНИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ, СПЕЦИАЛИЗИРУЯСЬ НА АНАЛИЗЕ НЕ ТОЛЬКО АНТИВИРУСНЫХ ПРОГРАММ, НО ТАКЖЕ ВСЕГО СПЕКТРА ПРОГРАММНЫХ И АППАРАТНЫХ СРЕДСТВ, ПРИМЕНЯЕМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ.

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

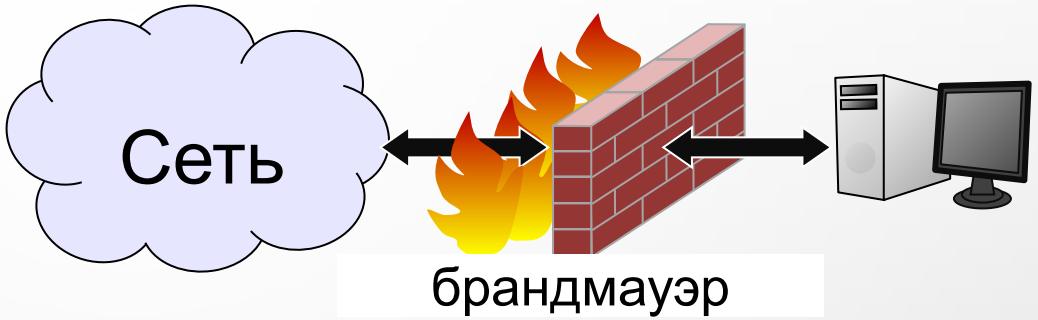
чаще всего не умеют лечить, предлагает купить антивирус

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)

© К.Ю. Поляков, Е.А. Ерёмин, 2013