# Тема 5. Компьютерные вирусы и антивирусные программы

# Термин «компьютерный вирус»

впервые употребил сотрудник Лехайского университета (США) Ф.Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США.

С тех пор прошло немало времени, однако строгого определения, что же такое компьютерный вирус, так и не дано, несмотря на то, что попытки дать такое определение предпринимались неоднократно.

# Компьютерные вирусы

**Компьютерные вирусы -** это класс программ способных к саморазмножению и самомодификации в работающей вычислительной среде и вызывающих нежелательные для пользователей действия. Действия могут выражаться в нарушении работы программ, выводе на экран посторонних сообщений или изображений, порче записей, файлов, дисков, замедлении работы ЭВМ и др.

# Краткая история вредоносных программ

- Первые вредоносные программы появились через несколько лет после появления персональных компьютеров серии IBM PC. Это случилось в начале 80-х годов двадцатого века. К 2005 году вредоносных программ зарегистрировано уже более 100000.
- Основная масса компьютерных вирусов - это так называемые студенческие вирусы.

  Их пишут студенты-подростки, изучающие программирование на компьютере. Они делают это в форме игры для самоутверждения. Часто такие вирусы только издают разные звуки, видеоэффекты, тормозят работу компьютера. Опасность студенческих вирусов в том, что в них много ошибок. Поэтому их воздействие на компьютер может быть непредвиденным.

# Начало пути

Те, кто начал работать на IBM-PC в середине 80-х, не забыли повальную эпидемию вирусов. Буквы сыпались на экранах, а толпы пользователей неслись к специалистам по ремонту дисплеев (сейчас все наоборот: винчестер сдох от старости, а валят на неизвестный передовой науке вирус). Затем компьютер заиграл чужеземный гимн «Yankee Doodle», но чинить динамики уже никто не бросился - очень быстро разобрались, что это - вирус, да не один, а целый десяток.

Так вирусы начали заражать файлы. Вирус «Brain» и скачущий по экрану шарик вируса «Ping-pong» ознаменовали победу вируса и над Boot-сектором. Все это очень не нравилось пользователям IBM-PC, и - появились противоядия. Первым антивирусом был отечественный ANTI-KOT: это легендарный Олег Котик выпустил в свет первые версии своей программы, которая уничтожала целых 4 (четыре) вируса (американский SCAN появился у нас в стране несколько позднее).

**Полиморфизм - мутация вирусов.** Первый полиморфик-вирус появился в начале 90-х годов. К счастью, первый MtE-вирус не попал в «живую природу» и не вызвал эпидемии, а разработчики антивирусных программ, соответственно, имели некоторый запас времени для подготовки к отражению новой напасти.

**За пределы DOS.** В конце 1992 года появился первый вирус для Windows, открывший, таким образом, новую страницу в истории вирусописания. Небольшого размера (менее 1K), совершенно безвредный и нерезидентный вирус вполне грамотно заражал выполняемые файлы нового формата Windows (NewEXE) и своим появлением пробил для вирусов окно в мир Windows.
Через некоторое время появились вирусы для OS/2, а в январе 1996 - и первый вирус для Windows95. Коль скоро все существующие DOS-приложения будут замещены их аналогами для Windows, Win95 и OS/2, проблема DOS-вирусов сойдет на нет и оставит после себя лишь теоретический интерес для компьютерного социума.

**Эпидемия макро-вируса.** Год 1995-й, август. Все прогрессивное человечество, компания Microsoft и Билл Гейтс лично празднуют выход новой операционной системы Windows95. На фоне шумного торжества практически незамеченным прошло сообщение о появлении вируса, использующего принципиально новые методы заражения, вируса, заражающего документы Microsoft Word.

**Отличительными особенностями компьютерных вирусов** являются:

- маленький объем;
- самостоятельный запуск;
- многократное копирование кода;
- создание помех для корректной работы компьютера

## **Классификация компьютерных вирусов**

**Вирусы** можно разделить на классы по следующим основным признакам:

- среда обитания;
- операционная система (ОС);
- особенности алгоритма работы;
- деструктивные возможности.

# По **СРЕДЕ ОБИТАНИЯ** вирусы можно разделить на:

- файловые;
- загрузочные;
- макро;
- сетевые.

**Файловые вирусы** заражают выполняемые файлы (это наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).
**Загрузочные вирусы** заражают загрузочные сектора дисков (boot-сектор), либо главную загрузочную запись (Master Boot Record), либо меняют указатель на активный boot-сектор.
**Макро-вирусы** - разновидность файловых вирусов встраивающиеся в документы и электронные таблицы популярных редакторов.
**Сетевые вирусы** используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Заражаемая **ОПЕРАЦИОННАЯ СИСТЕМА** (вернее, ОС, объекты которой подвержены заражению) является вторым уровнем деления вирусов на классы.

Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких OS - DOS, Windows, Win95/NT, OS/2 и т.д.

Макро-вирусы заражают файлы форматов Word, Excel, Office97.

Загрузочные вирусы также ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков.

# Среди **ОСОБЕННОСТЕЙ АЛГОРИТМА РАБОТЫ** вирусов выделяются следующие пункты

- резидентность;
- использование стелс-алгоритмов;
- самошифрование и полиморфичность;
- использование нестандартных приемов.

# **РЕЗИДЕНТНЫЙ** вирус

**РЕЗИДЕНТНЫЙ** вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время.

# Использование **СТЕЛС**

Использование **СТЕЛС** - алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс - алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов. Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации.

# **САМОШИФРОВАНИЕ** и **ПОЛИМОРФИЧНОСТЬ**

используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса.

Полиморфик - вирусы (polymorphic) - это достаточно трудно обнаружимые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода.

В большинстве случаев два образца одного и того же полиморфик - вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

# По **ДЕСТРУКТИВНЫМ ВОЗМОЖНОСТЯМ** вирусы можно разделить на:

- **безвредные**, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- **неопасные**, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
- **опасные вирусы**, которые могут привести к серьезным сбоям в работе компьютера;
- **очень опасные**, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов - вводить в резонанс и разрушать головки некоторых типов винчестеров.

# Boot-вирусы

При загрузке операционной системы компьютер может самостоятельно прочитать только нулевой Boot-сектор дискеты или винчестера. Считанная оттуда программа затем полностью управляет загрузкой операционной системы. В Boot-сектор достаточно грамотно вписать несколько команд, вызывающих на выполнение вирус, расположенный на винчестере компьютера. И тогда при каждой загрузке операционной системы в памяти компьютера уже будет находиться Boot-вирус.

Для борьбы с Boot-вирусами в установочные параметры компьютера (Setup компьютера) ввели запрет загрузки с дискеты и запрет редактирования Boot-сектора винчестера.

# Психологические вирусы

- Есть и нестандартные способы нанесения вреда чужим компьютерам. Не обязательно уметь программировать вирусы. Периодически по электронной почте приходят ложные предупреждения о вирусных атаках. В них запугивают появлением нового страшного вируса.
- Иногда авторы страшилок останавливаются на запугиваниях. Но иногда советуют для борьбы с вирусом удалить один или несколько файлов на Вашем компьютере, где "прячется" вирус. Но если Вы последуете их совету, то своими руками выведете свой компьютер из строя. Чаще всего он просто перестанет загружаться. Рассчитаны эти страшилки на людей, которые недавно подключились к сети Интернет и ещё не уверены в своих действиях.
- Другой распространённый способ обмана - это ложные письма от администрации провайдера. В этих письмах обычно сообщается о реорганизации работы или о сбоях на серверах провайдера, и Вас просят сообщить свой логин и пароль, под которыми Вы выходите в Интернет. Таким способом воруют пароли.

# Почтовые черви

- В настоящее время 90% вредоносных и вирусных программ проникают на компьютеры из сети Интернет с электронными письмами и во время посещения сайтов.
- Почтовый червь - это вредоносная программа, находящаяся в файле, присоединённом к электронному письму. Авторы червя всячески побуждают Вас запустить на выполнение присоединённый файл с вирусом. Его маскируют под новую игру, обновление популярных программ (в том числе, например, под обновление антивирусной программы), фотографии и так далее. В ход идёт всё. Вплоть до расчёта ширины поля, в котором почтовая программа показывает имена присоединённых файлов. Длину имени файла подбирают так, чтобы она не помещалась полностью в этом поле и не было видно истинного расширения файла "EXE" или "COM". А в видимой части поля присоединённый файл может иметь ложное расширение, соответствующее графическому, звуковому или текстовому файлу.

# Программы-шпионы (троянские кони)

- Обычно шпионские программы - это коммерческие программы очень высокого качества и большой сложности. Часто они направлены на получение секретной информации о кодах электронных банковских карточек. Программа-шпион не должна себя обнаруживать в компьютере. Она должна отслеживать момент выхода компьютера в Интернет и по возможности незаметно передавать данные своему хозяину.
- Программа-шпион может иметь функции управления компьютером. Тогда по командам хозяина, получаемым во время сеансов связи с Интернет, шпион может передавать в Интернет какие-то файлы с Вашего компьютера или интересующую его хозяина информацию о Вашем компьютере.

# Структура и функционирование антивирусных программ (Типы антивирусных программ):

**Антивирусный монитор**

Монитор работает в компьютере постоянно. Он отслеживает ситуации, при которых может произойти заражение компьютера вирусом. Это запуск программ на выполнение, обращения к дискам с целью модифицировать файлы, открытие приложений к электронным письмам, загрузка программ и файлов из сети Интернет и тому подобные действия. Обычно антивирусный монитор можно настраивать, включая и отключая различные его возможности.

# Антивирусный сканер

Антивирусный сканер предназначен для проверки оперативной памяти и дисков компьютера на наличие вирусов. В настройках антивирусного сканера можно указывать, какие типы файлов, архивов, баз хранения электронных писем нужно проверять во время антивирусного сканирования.

***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). Антивирусные блокировщики могут входить в BIOS Setup

# Защита от компьютерных вирусов

Основными мерами защиты от вирусов считаются:

- резервирование (копирование FAT, ежедневное ведение архивов измененных файлов);
- профилактика (раздельное хранение вновь полученных программ и эксплуатирующихся, хранение неиспользуемых программ в архивах, использование специального диска для записи новых программ);
- ревизия (анализ вновь полученных программ специальными средствами и их запуск в контролируемой среде, систематическая проверка *BOOT*-сектора используемых дискет и содержимого системных файлов (прежде всего *command.com*) и др.);

# Основными мерами защиты от вирусов считаются:

- фильтрация (использование специальных сервисных программ для разбиения диска на зоны с установленным атрибутом *read only*,);
- вакцинация (специальная обработка файлов, дисков, каталогов, запуск специальных резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса для определения, заражена уже программа, диск, ЭВМ или нет, т.е. обманывающих вирус);
- лечение (дезактивацию конкретного вируса с помощью специальной программы или восстановление первоначального состояния программ путем удаления всех экземпляров вируса в каждом из зараженных файлов или дисков).

**Антивирусные программы** предназначены для предотвращения заражения компьютера вирусом и ликвидации последствий заражения.

# В зависимости от назначения и принципа действия различают следующие антивирусные программы:

- **сторожа или детекторы** – предназначены для обнаружения файлов зараженных известными вирусами, или признаков указывающих на возможность заражения.
- **доктора** – предназначены для обнаружения и устранения известных им вирусов, удаляя их из тела программы и возвращая ее в исходное состояние. Наиболее известными представителями являются Dr.Web, AidsTest, Norton Anti Virus.

# В зависимости от назначения и принципа действия различают следующие антивирусные программы:

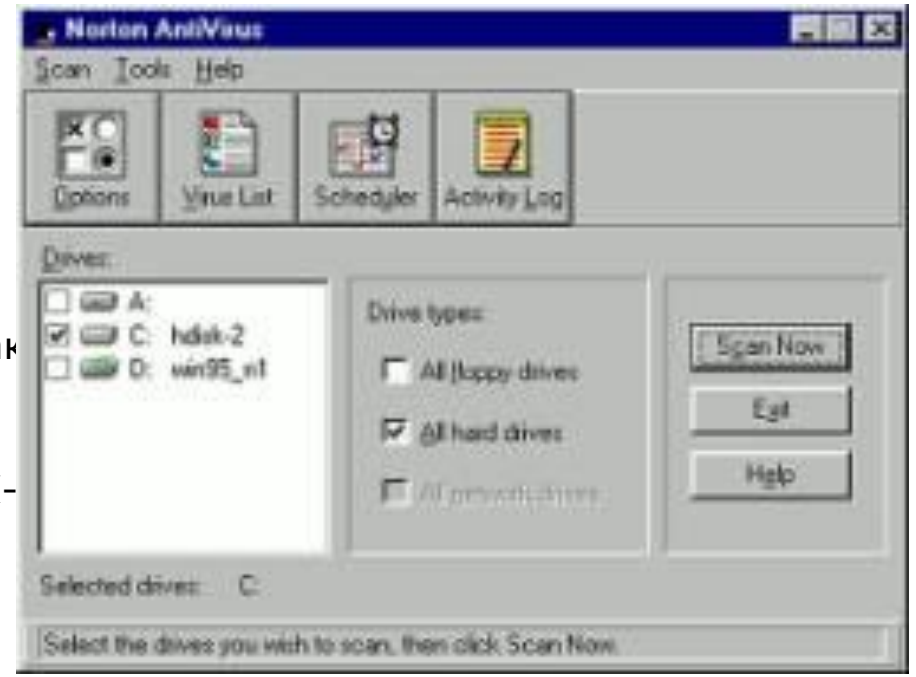
- **ревизоры** – они контролируют уязвимые и поэтому наиболее атакуемые компоненты компьютера, запоминают состояние служебных областей и файлов, а в случае обнаружения изменений сообщают пользователю.
- **резидентные мониторы или фильтры** – постоянно находятся в памяти компьютера для обнаружения попыток выполнить несанкционированные действия. В случае обнаружения подозрительного действия выводят запрос пользователю на подтверждение операций.
- **вакцины** – имитируют заражение файлов вирусами. Вирус будет воспринимать их зараженными и не будет внедряться.

Среди антивирусных программных продуктов можно отметить, прежде всего, пакеты: Norton Antivirus (Symantec), Vims Scan (McAfee), Dr.Solomon AV Toolkit (S&S IntL), AntiVirus (IBM), InocuLAN (Computer Associates) и AntiViral Toolkit Pro (Лаборатория Касперского).

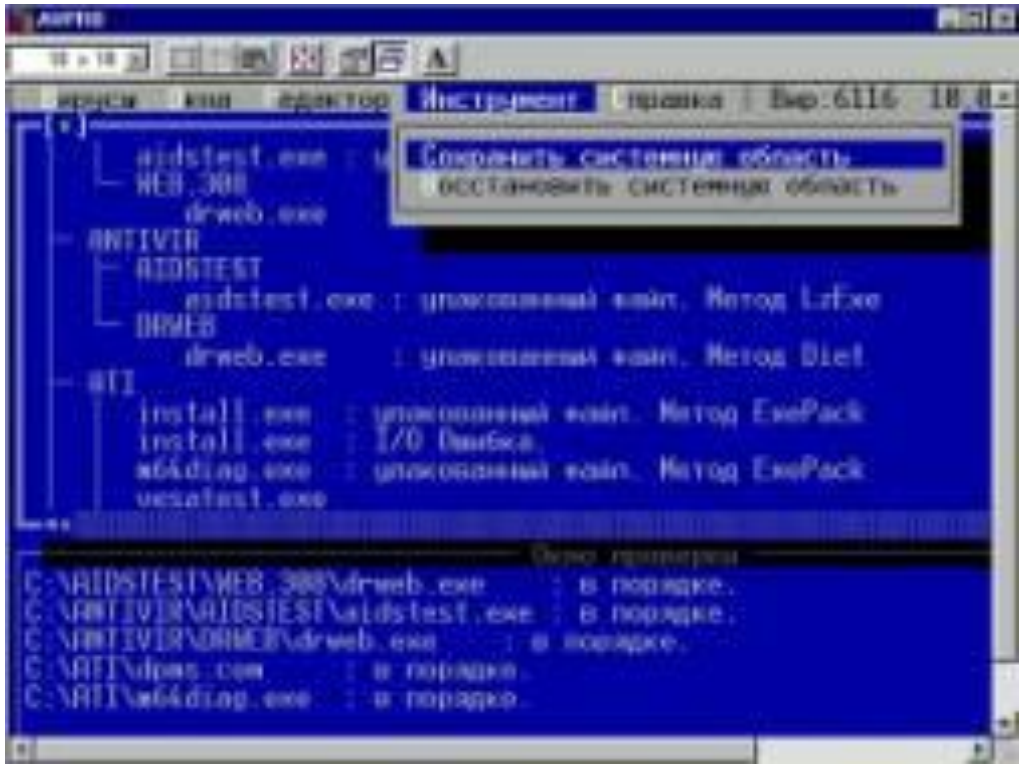
Данные программные продукты отвечают требованиям ICSA, отслеживая 300 наиболее распространённых и хотя бы 9 из каждых 10 остальных вирусов.
В той или иной степени данные антивирусные программы обладают функциями проверки на вирусы и удаления их в реальном времени, отключения заражённых рабочих станций от сети, определения источника заражения, проверки сжатых файлов в режимах сканирования и реального времени.

# Антивирусные программные продукты:

- **Norton AntiVirus** — пакет, предназначенный для защиты компьютера от вирусов во время работы в Интернете, обмена файлами по сети, загрузки файлов с дискет и CD. Программа может автоматически сканировать входящие почтовые сообщения, содержащие различного рода прикрепленные данные, в таких популярных почтовых программах, как MS Outlook, MS Outlook Express, Eudora Pro, Eudora Lite, Netscape Messenger, Netscape Mail. Программа защищает систему от опасных ActiveX-кодов, Java-апплетов и так называемых «троянов», а также определяет и удаляет вирусы из сжатых файлов (в том числе и из многократно сжатых файлов). Поддерживаемые форматы: MIME/UU; LHA/LZH; ARJ; CAB; PKLite; LZEXE; ZIP.



# Антивирусные программные продукты




- Антивирусный пакет **AVP**, является расширенной версией известного антивирусного комплекта «Доктор Касперский». Комплекс содержит программу-фаг, тестирующую и восстанавливающую файлы и загрузочные сектора дисков, поврежденные вирусами. В процессе работы программы производится тестирование на неизвестные вирусы. Также в комплект входит резидентная программа, отслеживающая подозрительные действия, совершаемые на компьютере, и дающая возможность просматривать карту памяти. Специальный набор утилит помогает обнаруживать новые вирусы и разбираться в них.

Наиболее популярным средством против вирусов является, как известно, **Aidstest**, но, используя его, всегда надо помнить, что он предохраняет только от вирусов, с которыми он уже знаком. Для обеспечения большей безопасности использование Aidstest необходимо сочетать с повседневным использованием ревизора диска Adinf.

Ревизор **ADinf** позволяет обнаружить появление любого вируса, включая Stealth-вирусы, вирусы-мутанты и неизвестные на сегодняшний день вирусы. При установленной программе ADinf Cure Module (лечащий блок ревизора ADinf) можно немедленно удалить до 97% из них. ADinf берет под контроль все участки винчестера, куда возможно проникновение вируса. Такой способ проверок полностью исключает маскировку Stealth-вирусов и обеспечивает весьма высокую скорость проверки диска.

**Doctor Web** борется с известными программе полиморфными вирусами. Кроме того, Doctor Web может проводить эвристический анализ файлов в целях выявления неизвестных вирусов, в том числе сложношифруемых и полиморфных вирусов. Успех такого анализа — в среднем 82%. Программа может распаковывать и проверять исполняемые файлы, обработанные архиваторами LZEXE, PKLite и Diet.

# Самостоятельная работа №5

1. Какие цифры и символы использует для обозначения числа в троичной системе счисления?
2. Для чего используется шестнадцатеричная система счисления?
3. Перевести число 567 из десятичной системы счисления в двоичную систему счисления.