Котова Галина Петровна, МБОУ СОШ № 10

Ст. Новопокровская Краснодарский край

Тема:
Компьютерные вирусы. Антивирусные программы.

Цель:

- познакомить учащихся с различными видами компьютерных вирусов, способов их распространения и профилактикой и методами борьбы с ними.
- познакомить учащихся с различными видами антивирусных программ, сформировать навыки работы с ними

Требования к знаниям и умениям:

Учащиеся должны знать:

- определение термина «компьютерный вирус»;
- классификацию компьютерных вирусов;
- пути заражения;
- способы профилактики и методы борьбы с компьютерными вирусами;
- виды и назначение различных антивирусных программ.

Учащиеся должны уметь:

- проводить тестирование объектов на наличие компьютерных вирусов

В мировых электронных сетях циркулируют 55-65 тысяч различных вирусов, которые создают 10-12 тысяч программистов. Количество разрушительных программ увеличивается с каждым днем, поскольку искусство их создания несложно. Авторы вирусов живут практически во всех индустриально развитых странах, а вот эпидемии начинались в странах, доселе считавшихся не особо преуспевшими в развитии Интернета.

Действуют авторы вирусов из совершенно различных побуждений: некоторые по политическим мотивам, иногда вызывает раздражение та или иная компания и чаще всего выясняется, что вирус был создан из чистого любопытства.

Например, в 1988 г. вирус написанный аспирантом из Иерусалимского университета (в пятницу, 13-го), заразил компьютеры в Европе, Америке, на Ближнем Востоке, вывел из строя 6 тысяч ЭВМ Министерства обороны США, ущерб составил более 150 тыс. долларов.

Компьютерный вирус – специально написанная программа, как правило, небольшая по размерам, действия которой в подавляющем большинстве случаев направлены на разрушение, искажение данных и нарушение работоспособности компьютера. Это программа, способная к размножению: может записывать свои копии в программы, системные области, драйвера, документы и т. д. Вирусы попадают на ПК извне в результате несоблюдения пользователями правил антивирусной защиты.

Котова Галина Петровна, МБОУ СОШ № 10

Ст. Новопокровская Краснодарский край

Что может сделать компьютерный вирус?

- ✓ «засорить» оперативную память или жесткий диск (своими копиями или другими символами);
- ✓ испортить FAT-таблицу размещения файлов (FAT-каталог для файлов, без которых их не отыскать);
- ✓ испортить содержимое загрузочного сектора (специальной программы на диске, при повреждении которой диск становится неработоспособным);
- ✓ вывести сообщение на экран или сыграть мелодию (часто ненормативная лексика);
- ✓ отформатировать диск;
- ✓ перезагрузить ПК;
- ✓ заблокировать клавиатуру (разрушение таблицы кодов клавиш)
- ✓ изменить содержимое файлов с программами и данными (перемещения, ошибки и т. д.)

Основные источники вирусов:

- ➢ дискета с зараженными файлами;
- ➢ компьютерная сеть (почта и Интернет);
- ➢ жесткий диск с вирусом, попавшим от зараженных программ;
- ➢ вирус из оперативной памяти.

Признаки появления компьютерных вирусов:

1. перестала загружаться ОС;
2. «зависание» программ, переполнение оперативной памяти;
3. изменение числа и (или) характеристики файлов, исчезновение файлов;
4. замедление работы с МД или идет несанкционированное обращение к нему.

загрузочный сектор
заменяется головой вируса

Программа начальной загрузки (ПЗУ) → ПНЗ (диск) → система

⇩

преобразуется

ПНЗ (ПЗУ) → Вирус → ПНЗ (диск) → система

Классификация компьютерных вирусов (бывают различные классификации):

1. по среде обитания:
   - ✓ сетевые (распространяемые в компьютерной сети),
   - ✓ файловые (внедряющиеся в выполняемые файлы),
   - ✓ загрузочные (загрузочный сектор диска – Boot-сектор или системный загрузчик винчестера),

- ✓ существуют и смешанные виды вирусов и макрокомандные – в WORD или EXCEL.

2.<u>по способу заражения:</u>

- ✓ резидентный – оставляющий при инфицировании компьютера в оперативной памяти свои резидентную часть, которая затем перехватывает обращение ОС к объектам заражения и внедряется в них;
- ✓ нерезидентный- не заражает память компьютера и является активным ограниченное время.

3.<u>по деструктивным возможностям:</u>

- ✓ безвредные – никак не влияющие на память компьютера, кроме уменьшения свободного места на диске;
- ✓ неопасные – влияние их ограничивается уменьшением свободного места на диске, графическими, звуковыми и прочими эффектами;
- ✓ опасные – могут привести к серьёзным сбоям в работе компьютера (замедление и ошибки загрузки, изменения файлов, невозможность их сохранить);
- ✓ очень опасные – могут привести к потере программ и данных, стереть необходимую для работы компьютера информацию, записанную в системных областях.

4. <u>по особенностям алгоритма:</u>

- ✓ вирусы-«спутники» (companion). Не изменяют файлы, они создают для EXE-файлов файлы спутники с тем же именем, но расширением COM. При запуске система ищет файл с COM, выполняет его, вирус выполняет свои действия и запускает настоящую программу с расширением EXE.
- ✓ вирусы-«черви» (worm). Распространяются по компьютерной сети. Проникают в память, вычисляют адреса других компьютеров и рассылаются по этим адресам.
- ✓ «паразитические». При распространении своих копий изменяют содержимое дисковых секторов и файлов. Эта группа включает все вирусы, не являющиеся «червями» и «спутниками».
- ✓ «студенческие». Крайне примитивные вирусы, часть нерезидентных, содержат большое количество ошибок.
- ✓ вирусы-«невидимки» (stealth). Очень совершенные программы, перехватывающие обращение DOS к пораженным файлам или секторам диска и «подставляют» вместо себя пораженные участки.
- ✓ вирусы-«призраки». Труднообнаруживаемые вирусы, не имеющие ни одного постоянного участка кода.

Самошифрование и полиморфичность (шифрование и дешифрование различными кодами) свойственны практически всем типам вирусов, что максимально усложняет процедуру обнаружения вируса. При шифровке вирус шифрует свой код и каждый раз

используются разные ключи, модифицируется и программа-расшифровщик. Таким образом, код вируса в разных случаях заражения будет разный.

Структура компьютерного вируса

1. Программный код, обеспечивающий попадание КВ в ОЗУ 2. Программный код, обеспечивающий копирование КВ на МД, добавляя его к файлам или загрузочному сектору 3. Программный код, описывающий условия активизации КВ 4. Алгоритм несанкционированный или деструктивных действий.	Такова приблизительно структура всех КВ. Сложность различна: от инструкции DOS до очень высокой до десятков тысяч операторов.

Средства предотвращения заражения:

- ☑ Резервное копирование информации (файлов и системных областей ЖД)
- ☑ Не торопитесь запускать файл, полученный из сети (даже если на него не среагировал ни один антивирус)– выждите неделю
- ☑ Избегайте пользоваться случайными и неизвестными программами
- ☑ Перезагрузите компьютер, если до вас за ним работал другой пользователь
- ☑ Ограничение доступа к информации, в частности, физическая защита дискеты во время копирования информации с неё
- ☑ Разные антивирусные программы.

Первые вирусы – rabbits (кролики)– конец 60-х-начало 70-х гг

Creeper – первый сетевой вирус

Reeper – первый антивирус } первая половина 70-х годов

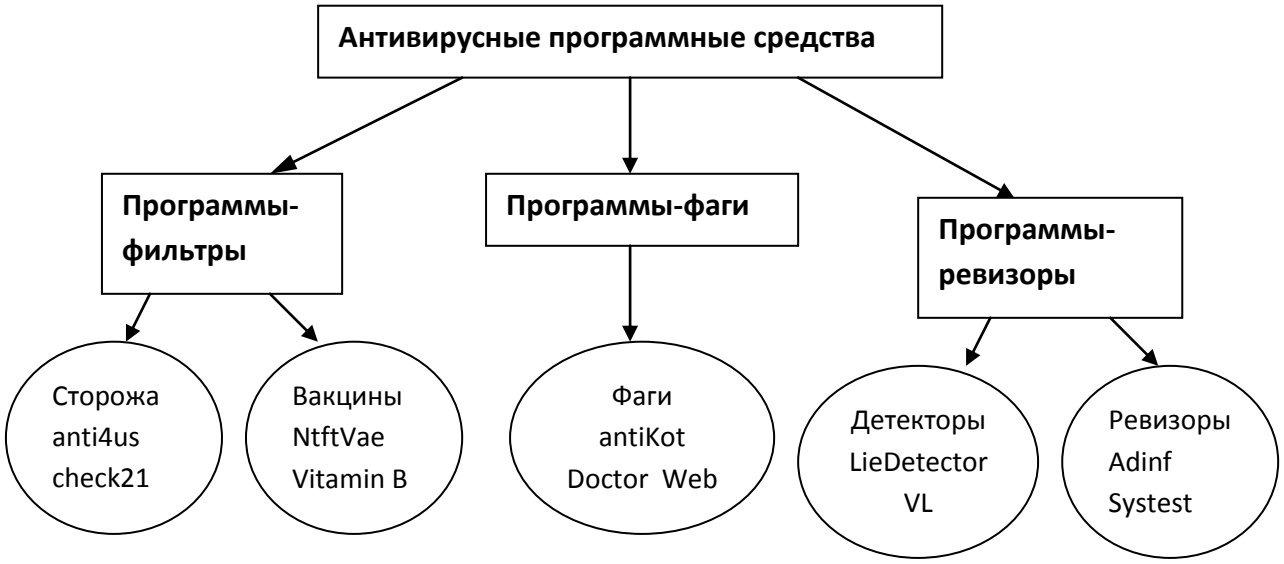
С начала 90-х годов количество вирусов растет в геометрической прогрессии; 1995 г. – первый вирус для M. Word (Concept), 1997 г. для M. Excel.

Антивирусные программы.

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы, позволяющие выявлять вирусы, лечить зараженные файлы и диски, обнаруживать и предотвращать подозрительные (характерные для вирусов) действия. Разумеется при этом не стоит пренебрегать профилактическими мерами защиты.

Котова Галина Петровна, МБОУ СОШ № 10

Ст. Новопокровская Краснодарский край



Существует несколько типов антивирусных программ, различающихся выполняемыми функциями.

1. Программы-фильтры – «сторожа» и «вакцины» - создаются для предотвращения «заражения». «Сторожа» проверяют на наличие вирусов запускаемые файлы и вставляемые в дисковод дискеты, при наличии вируса об этом сообщается пользователю. «Вакцины» выявляют попытки выполнить действия вируса для размножения и нанесения вреда – так же сообщают об этом пользователю. Эти программы ведут просмотр оперативной памяти и значений векторов прерываний в момент возникновения подозрительных действий; самопроверка и устойчивость к антифильтрам; ведение архива.
2. Программы-ревизоры – «ревизоры» и «детекторы» - запоминают сведения о состоянии файлов и системных областей дисков (подсчет контрольных сумм файлов и некоторой другой информации: длины файлов, даты их последней модификации и т. д.). «Детекторы» определяют заражена ли программа тем или иным КВ, «ревизоры» - внесены ли изменения в текст программы. Используются для локализации мест внедрения КВ путем прогонки «пустой» системы и выявления изменений в системных файлах.
3. Программы-фаги или полифаги (fag – англ., негодный конец, остаток) – создаются для уничтожения («выкусывания») КВ после их распознавания. Известные вирусы имеют некоторую постоянную последовательность программного кода, специфичную для данного вируса. Если антивирусная программа обнаруживает такую последовательность в каком-либо файле, он считается зараженным и подлежит лечению. К недостаткам можно отнести большие размеры антивирусных баз данных, которые периодически следует обновлять, что замедляет поиск вирусов.

При заражении вирусом компьютера:

1. ***отключитесь от локальной сети и проинформируйте системного администратора***

2. ***для остановки распространения вируса запустите антивирусную программу***
3. ***если антивирус не удаляет вирусы, перезагрузите его с незараженной и защищенной от записи дискеты***
4. ***если антивирус удаляет вирусы, удалите зараженные файлы или подвергните их «лечению»***
5. ***в случае обнаружения загрузочного вируса проверьте все диски, независимо от того, загрузочные они или нет.***

Задания:

1. Какие вирусы могут заразить следующие файлы (уровень понимания):
   Реферат.doc setup.exe товарооборот.xls электронное письмо чертеж в AutoCade
2. Перечислите объекты компьютерной системы, заражение которых приведет (уровень применения):
   к незначительным разрушительным последствиям
   к необратимым разрушительным последствиям
3. Составить сообщение о ваших столкновениях с компьютерными вирусами и их последствиях (творческий уровень):
   Макро-вирусы почтовые черви троянские программы и т. д.