Компьютерные вирусы и их классификация

Хроники «чумы» компьютерного века

«Лаборатория Касперского» подвела «вирусные» итоги 2005 г. Е.Касперский констатировал двойное увеличение количества вредоносных программ в 2005 г. В месяц их появляется более 50 тыс., и все чаще создаются они не хакерами-самоучками, а организованными преступными группами с целью извлечения коммерческой выгоды.
Источник: http://www.osp.ru

Более четырех тысяч компакт-дисков с компьютерными вирусами изъяты у продавца на радио-рынке. Цены за компакт-диски с обложками «Все для хакеров» стоили не дороже, чем диски с фильмами или музыкой.
Источник: RUpor.info

Ежегодно американский Институт компьютерной безопасности совместно с компьютерным подразделением Федерального бюро расследований проводит весьма подробное исследование компьютерной преступности По итогам 2005 г. первое место по убыткам традиционно занимают вирусы. В сумме они нанесли потери в 42 757 767 долларов (38,86% от всех убытков из-за ИТ-угроз).
Источник: http://www.infobez.ru

- **Компьютерный вирус - это специально написанная небольшая по размерам программа, имеющая специфический алгоритм, направленный на тиражирование копии программы, или её модификацию и выполнению действий развлекательного, пугающего или разрушительного характера.**
- Тем или иным способом вирусная программа попадает в компьютер и заражает их. Программа, внутри которой находится вирус, называется **зараженной**. Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и заражает другие программы, а также выполняет какие-либо вредоносные действия. Например, портит файлы или таблицу размещения файлов на диске, занимает оперативную память и т. д. После того, как вирус выполнит свои действия, он передает управление той программе, в которой он находится, и она работает как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Поэтому далеко не сразу пользователь узнаёт о присутствии вируса в машине.

- Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус остается в памяти компьютера и время от времени заражает программы и выполняет нежелательные действия на компьютере. Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметным.

К числу наиболее характерных **признаков заражения компьютера вирусами** относятся следующие:

- **некоторые ранее исполнявшиеся программы перестают запускаться или внезапно останавливаются в процессе работы;**
- **увеличивается длина исполняемых файлов;**
- **быстро сокращается объём свободной дисковой памяти;**
- **на носителях появляются дополнительные сбойные кластеры, в которых вирусы прячут свои фрагменты или части повреждённых файлов;**
- **замедляется работа некоторых программ;**
- **в текстовых файлах появляются бессмысленные фрагменты;**
- **наблюдаются попытки записи на защищённую дискету**;
- **на экране появляются странные сообщения, которые раньше не наблюдались;**
- **появляются файлы со странными датами и временем создания (несуществующие дни несуществующих месяцев, годы из следующего столетия, часы, минуты и секунды, не укладывающиеся в общепринятые интервалы и т. д.);**
- **операционная система перестаёт загружаться с винчестера;**
- **появляются сообщения об отсутствии винчестера;**
- **данные на носителях портятся.**

- Любая дискета, не защищённая от записи, находясь в дисководе заражённого компьютера, может быть заражена. Дискеты, побывавшие в зараженном компьютере, являются разносчиками вирусов. Существует ещё один канал распространения вирусов, связанный с компьютерными сетями, особенно всемирной сетью Internet. Часто источниками заражения являются программные продукты, приобретённые нелегальным путем

Существует несколько **классификаций компьютерных вирусов**:

- 1. **По среде обитания** различают вирусы сетевые, файловые, загрузочные и файлово-загрузочные.
- 2. **По способу заражения** выделяют резидентные и нерезидентные вирусы.
- 3. **По степени воздействия** вирусы бывают неопасные, опасные и очень опасные;
- 4. **По особенностям алгоритмов** вирусы делят на паразитические, репликаторы, невидимки, мутанты, троянские, макро-вирусы.

Классификация вирусов

Компьютерные вирусы подразделяются по следующим признакам:

- Среде обитания
- Способу заражения среды обитания
- Воздействию
- Особенностям алгоритма

- **Загрузочные вирусы** заражают загрузочный сектор винчестера или дискеты и загружаются каждый раз при начальной загрузке операционной системы.
- **Резидентные вирусы** загружается в память компьютера и постоянно там находится до выключения компьютера.
- **Самомодифицирующиеся вирусы (мутанты)** изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать.
- **Стелс-вирусы (невидимки)** перехватывает обращения к зараженным файлам и областям и выдают их в незараженном виде.
- **Троянские вирусы** маскируют свои действия под видом выполнения обычных приложений.


по особенностям алгоритма
вирусы-«спутники»
макровирусы
вирусы-«черви»
вирусы-призраки
«паразитические» вирусы
вирусы-мутанты
«стелс»-вирусы
«студенческие» вирусы

2. Классификация вредоносного программного обеспечения

Вирусом могут быть заражены следующие объекты:

- **1. Исполняемые файлы**, т.е. файлы с расширениями имен .com и .exe, а также оверлейные файлы, загружаемые при выполнении других программ. Вирусы, заражающие файлы, называются **файловыми.** Вирус в зараженных исполняемых файлах начинает свою работу при запуске той программы, в которой он находится. Наиболее опасны те вирусы, которые после своего запуска остаются в памяти резидентно - они могут заражать файлы и выполнять вредоносные действия до следующей перезагрузки компьютера. А если они заразят любую программу из автозапус , то и при перезагрузке с жесткого дис а начнет свою работу.

- **2. Загрузчик операционной системы и главная загрузочная запись жесткого диска**. Вирусы, поражающие эти области, называются **загрузочными**. Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентным, т.е. постоянно находится в памяти компьютера. Механизм распространения загрузочных вирусов - заражение загрузочных записей вставляемых в компьютер дискет. Часто такие вирусы состоят из двух частей, поскольку загрузочная запись имеет небольшие размеры и в них трудно разместить целиком программу вируса. Часть вируса располагается в другом участке диска, например, в конце корневого каталога диска или в кластере в области данных диска. Обычно такой кластер объявляется дефектным, чтобы исключить затирание вируса при записи данных на диск.

- **3. Файлы документов, информационные файлы баз данных, таблицы табличных процессоров** и другие аналогичные файлы могут быть заражены **макро-вирусами**. Макро-вирусы используют возможность вставки в формат многих документов макрокоманд.
- Если не принимать мер по защите от вирусов, то последствия заражения могут быть очень серьезными. Например, в начале 1989 г. вирусом, написанным американским студентом Моррисом, были заражены и выведены из строя тысячи компьютеров, в том числе принадлежащих министерству обороны США. Автор вируса был приговорен судом к трем месяцам тюрьмы и штрафу в 270 тыс. дол. Наказание могло быть и более строгим, но суд учел, что вирус не портил данные, а только размножался.

Рис. 15.1. Классификация компьютерных вирусов по среде обитания

Основные методы защиты от компьютерных вирусов

Для защиты от вирусов можно использовать:

- Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов.
Имеются две основные разновидности этих средств:

- копирование информации — создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо применять специализированные программы **АНТИВИРУСЫ**. Эти программы можно разделить на несколько видов:

- **Программы - детекторы** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
- **Программы - доктора**, или фаги, "лечат" зараженные программы или диски, "выкусывая" из зараженных программ тело вируса, т.е. восстанавливая программу в том состоянии, в котором она находилась до заражения вирусом.
- **Программы - ревизоры** сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий, об этом сообщается пользователю.
- **Программы - фильтры** располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.
- **Программы - вакцины**, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но вирус, от которого производится вакцинация, считает эти программы и диски уже зараженными. Эти программы неэффективны, хотя и могут использоваться для защиты от некоторых типов вирусов, например **autorun – вирусы.**

Необходимо отметить, что, на сегодняшний день, антивирусные программы часто объединяют все эти виды

Источник

- http://inf.e-alekseev.ru/text/Virus.html
- **Алексеев Е.Г., Богатырев С.Д. Информатика. Мультимедийный электронный учебник**