Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/.

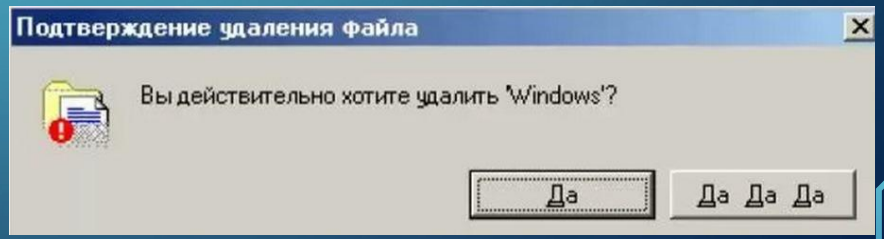
Компьютерные вирусы. Антивирусные программы.

Автор: Бобошко Екатерина, 8А класс,
Руководитель: Александрова З.В., учитель физики и информатики
МБОУ СОШ №5 пгт Печенга, Мурманская область

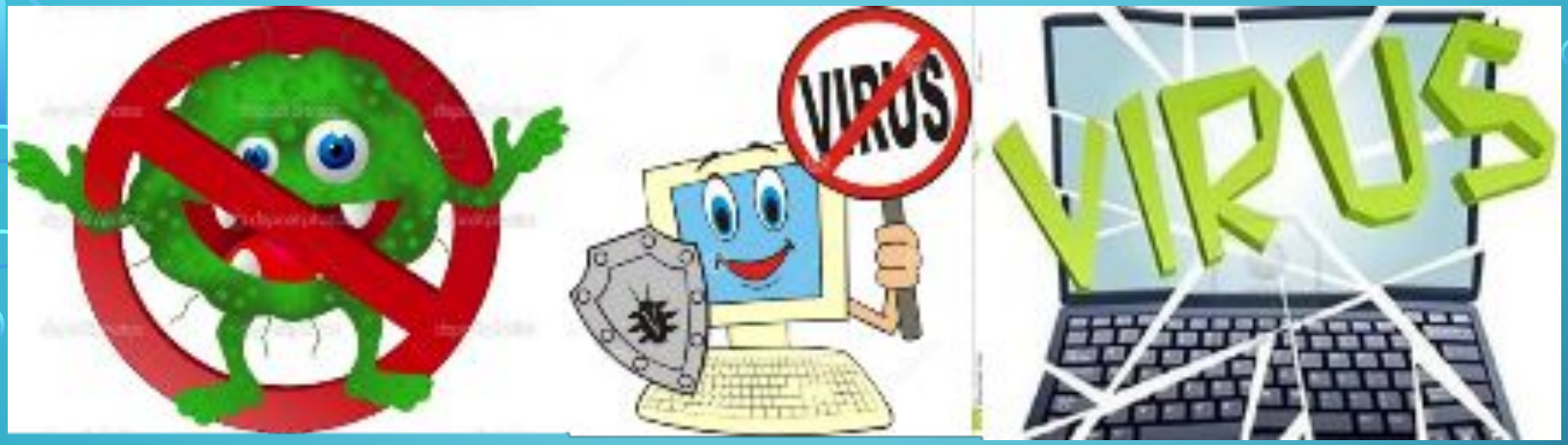
Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в 1951 году предложил метод создания таких механизмов. С 1961 года известны рабочие примеры таких программ.

Первыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Зимой 1984 года появились первые антивирусные утилиты - CHK4BOMB и BOMBSQAD авторства Энди Хопкинса (англ. Andy Hopkins).

В начале 1985 года Ги Вонг (англ. Gee Wong) написал программу DPROTECT - первый резидентный антивирус.

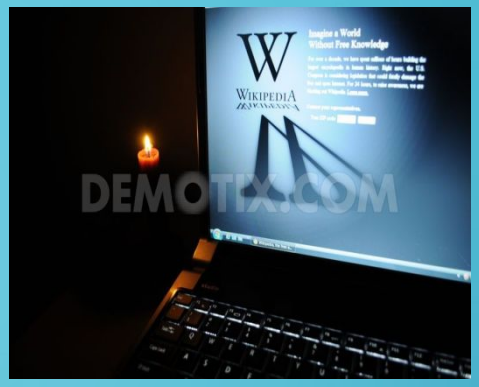


- Первые вирусные эпидемии относятся к 1986—1989 годам: Brain.A[en] (распространялся в загрузочных секторах дискет, вызвал крупнейшую эпидемию), Jerusalem[en] (проявился в пятницу 13 мая 1988 года, уничтожая программы при их запуске[3]), червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах).
- Тогда же оформились основные классы двоичных вирусов: сетевые черви (червь Морриса, 1987), «троянские кони» (AIDS, 1989[4]), полиморфные вирусы (Chameleon, 1990), стелс-вирусы (Frodo, Whale, 2-я половина 1990).



В 1992 году появились первый конструктор вирусов для PC-VCL (для Amiga конструкторы существовали и ранее), а также готовые полиморфные модули (MtE, DAME и TPE) и модули шифрования для встраивания в новые вирусы.

В несколько последующих лет были окончательно отточены стелс- и полиморфные технологии (SMEG.Pathogen, SMEG.Queeg, OneHalf, 1994; NightFall, Nostradamus, Nutcracker, 1995), а также испробованы самые необычные способы проникновения в систему и заражения файлов (Dir II - 1991, PMBS, Shadowgard, Cruncher - 1993). Кроме того, появились вирусы, заражающие объектные файлы (Shifter, 1994) и исходные тексты программ (SrcVir, 1994). С распространением пакета Microsoft Office получили распространение макровирусы (Concept, 1995).



- **В 1996 году появился первый вирус для Windows 95 - Win95.Boza, а в декабре того же года - первый резидентный вирус для неё - Win95. Punch.**

- **С распространением сетей и Интернета файловые вирусы всё больше ориентируются на них как на основной канал работы (ShareFun, 1997 - макровирус MS Word, использующий MS - Mail для распространения; Win32.HLLP.DeTroie, 1998 - семейство вирусов-шпионов; Melissa, 1999 - макровирус и сетевой червь, побивший все рекорды по скорости распространения). Эру расцвета «троянских коней» открывает утилита скрытого**

- **В конце 1990-х - начале 2000-х годов с усложнением ПО и системного окружения, массовым переходом на сравнительно защищенные Windows семейства NT, закреплением сетей как основного канала обмена данными, а также успехами антивирусных технологий в обнаружении вирусов, построенных по сложным алгоритмам, последние стали всё больше заменять внедрение в файлы на внедрение в операционную систему (необычный автозапуск, руткиты) и подменять**

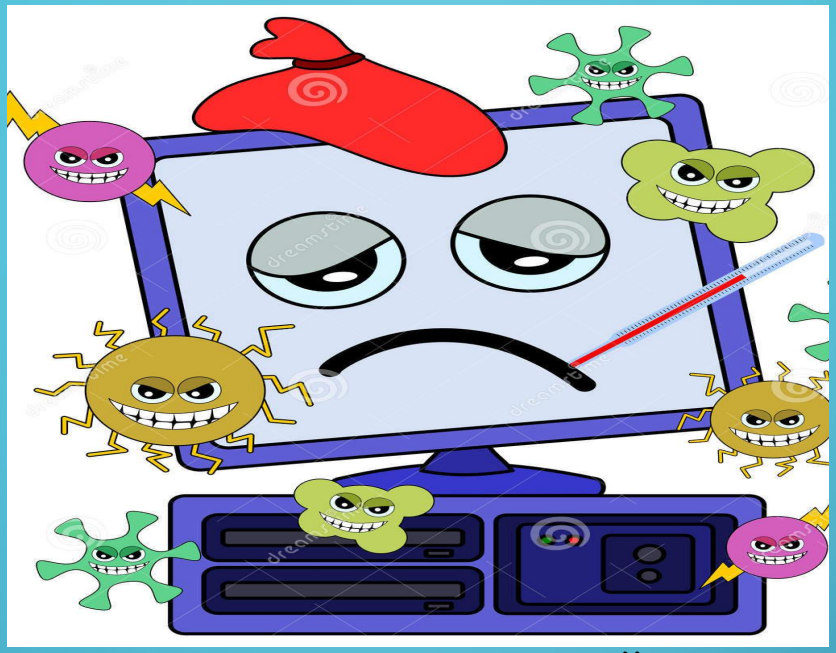
- Кроме того, монолитные вирусы в значительной мере уступают место комплексам вредоносного ПО с разделением ролей и вспомогательными средствами (троянские программы, загрузчики/ дропперы, фишинговые сайты, спам-боты и пауки). Также расцветают социальные технологии - спам и фишинг - как средство заражения в обход механизмов защиты ПО.

- В начале на основе троянских программ, а с развитием технологий p2p-сетей - и самостоятельно — набирает обороты самый современный вид вирусов - черви- ботнеты (Rustock, 2006, ок. 150 тыс. ботов; Conficker, 2008—2009, более 7 млн ботов; Kraken, 2009, ок. 500 тыс. ботов). Вирусы в числе прочего вредоносного ПО окончательно оформляются как средство киберпреступности.

Этимология названия

Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения. По-видимому, впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом (Gregory Benford) в фантастическом рассказе «Человек в шрамах», опубликованном в журнале Venture в мае 1970 года.

Термин «компьютерный вирус» впоследствии не раз «открывался» и переоткрывался. Так, переменная в подпрограмме PERVADE (1975), от значения которой зависело, будет ли программа ANIMAL распространяться по диску, называлась VIRUS. Также, вирусом назвал свои программы Джо Деллинджер и, вероятно, это и было то, что впервые было правильно обозначено как вирус.

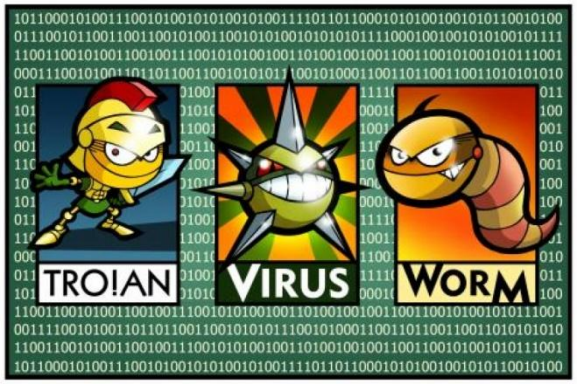


Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

Механизм

Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение; внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с э



Каналы заражения вирусами

- Флеш -накопители (флешки).
- Электронная почта. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код.
- Системы обмена мгновенными сообщениями. Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.
- Веб-страницы. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX - компонент.
- Интернет и локальные сети (черви). Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.

Профилактика и лечение

- **В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:**
- **Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)**
- **Не запускать незнакомые программы из сомнительных источников.**
- **Стараться блокировать возможность несанкционированного изменения системных файлов.**
- **Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).**

Профилактика и лечение

- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

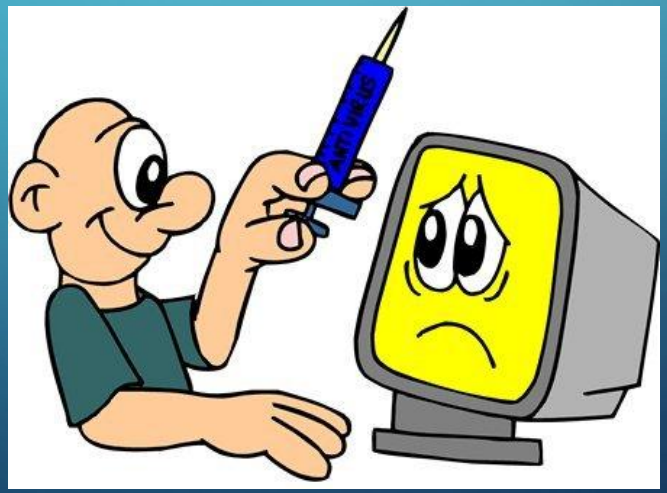
Экономика

Некоторые производители антивирусов утверждают, что сейчас создание вирусов превратилось из одиночного хулиганского занятия в серьёзный бизнес, имеющий тесные связи с бизнесом спама и другими видами противозаконной деятельности.

Также называются миллионные и даже миллиардные суммы ущерба от действий вирусов и червей. К подобным утверждениям и оценкам следует относиться осторожно: суммы ущерба по оценкам различных аналитиков различаются (иногда на три-четыре порядка), а методики подсчёта не приводятся.

Криминализация

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в некоторых странах как отдельный вид правонарушений: в России согласно Уголовному кодексу РФ (глава 28, статья 273), в США согласно Computer Fraud and Abuse Act, в Японии. Во многих странах, однако, создание вирусов само по себе не является преступлением, и нанесенный ими вред подпадает под более общие законы о компьютерных правонарушениях



СПАСИБО ЗА ВНИМАНИЕ!