

# Компьютерные вирусы



# 1. Введение

- Массовое использование ПК в автономном и сетевом режиме, включая выход в глобальную сеть Интернет, породило проблему заражения их компьютерными вирусами.

Компьютерным вирусом принято называть специально написанную, небольшую по размерам программу. Способную самопроизвольно присоединяться к другим программам (т.е. заражать их), создавать свои копии и внедрять их в файлы, системные области компьютера и в другие, объединенные с ним компьютеры с целью нарушения нормальной работы программ, порчи файлов и каталогов, создания различных помех при работе на компьютере.

## 2.История происхождения

- ▣ Такое упоминание относится к концу 60-х - началу 70-х годов, когда на машине Univac 1108 появилась программа «Pervading Animal». Собственно, вирусом ее назвать было нельзя, однако это была первая программа, выполнявшая не те действия, которых ожидал от нее оператор, и пытающаяся создавать свои копии. Мысли о создании саморазмножающихся программ начали приходить в голову некоторым людям еще в конце 40-х, когда появилось несколько теорий, связанных с созданием таких программ. Однако первая успешная реализация относится лишь к концу 60-х годов. Доступ к ЭВМ в те годы имели немногие, писать программы для них могли лишь избранные, поэтому впереди у компьютерного сообщества было больше десяти лет спокойствия. Но вот в середине 80-х компьютеры, теперь уже персональные, становятся общедоступными. С тех пор и ведет свое начало вирусная история.

# 3. Преступность в сфере КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

- Лиц, использующих свои знания и опыт для несанкционированного доступа к информационным и вычислительным ресурсам, к получению конфиденциальной и секретной информации, к совершению вредоносных действий, в литературе называют хакерами и кракерами. Действия хакеров, или компьютерных хулиганов, могут наносить существенный вред владельцам компьютеров и владельцам (создателям) информационных ресурсов, так как приводят к простоям компьютеров, необходимости восстановления испорченных данных либо к дискредитации юридических или физических лиц, например, путем искажения информации на электронных досках объявлений или на WEB-серверах в Интернет. Мотивы действий компьютерных злоумышленников самые различные: стремление к финансовым приобретениям; желание навредить и отомстить руководителю организации, из которой по тем или иным причинам уволился сотрудник; психологические черты человека (зависть, тщеславие, желание как-то проявить себя, просто хулиганство и др.).



# 4. Признаки появления

## вирусов

- Для маскировки вируса его действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении каких-либо условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и ее работа некоторое время не отличается от работы незараженной. Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователь часто и не замечает, что компьютер работает со "странностями". К признакам появления вируса можно отнести:
  - замедление работы компьютера;
  - невозможность загрузки операционной системы;
  - частые "зависания" и сбои в работе компьютера;
  - прекращение работы или неправильная работа ранее успешно функционировавших программ;
  - увеличение количества файлов на диске;
  - изменение размеров файлов;
  - периодическое появление на экране монитора неуместных системных сообщений;
  - уменьшение объема свободной оперативной памяти;
  - заметное возрастание времени доступа к жесткому диску.
- Надо заметить, что названные симптомы необязательно вызываются компьютерными вирусами, они могут быть следствием других причин, поэтому компьютер следует периодически диагностировать.

## 5. Классификация вирусов

- Основными путями заражения компьютеров вирусами являются съемные диски (дискеты и CD-ROM) и компьютерные сети. Заражение жесткого диска компьютера может произойти при загрузке компьютера с дискеты, содержащей вирус. Для усиления безопасности необходимо обращать внимание на то, как и откуда получена программа (из сомнительного источника, имеется ли наличие сертификата, эксплуатировалась ли раньше и т.д.). Однако главная причина заражения компьютеров вирусами - отсутствие в операционных системах эффективных средств защиты информации от несанкционированного доступа. По данным специальной литературы, к концу 1998 г. в мировой практике было зарегистрировано более 20 тыс. компьютерных вирусов (на сегодняшний день известно около 50 000 вирусов) и каждую неделю появляется около десяти новых вирусов.

# П я т ь с а м ы х о п а с н ы х в и р у с о в

1. Вирус Anna Kournikova

2. Melissa

3. MyDoom

4. Sasser-Netsky

5. 2007 Storm Worm



### Вирус Anna Kournikova

Этот вирус был приписан датскому программисту Яну де Виту 11 февраля 2001 года. Вирус был спроектирован для того, чтобы обманом заставить пользователя открыть письмо, сообщая, что в нём содержится фотография Анны Курниковой, но вместо неё получатель инициировал вредоносную программу

Это был ещё один вирус, который эксплуатировал адресную книгу в Microsoft Outlook пользователя. Тема сообщения гласила: «Привет: посмотри на это!», а в самом письме было нечто, напоминающее графический файл с названием “AnnaKournikova.jpg.vbs” Очевидно, что аттачмент не был JPG файлом, но схема в целом удачно использовала социальную инженерию и эффективный механизм передачи.



### Melissa

Макровирус, названный в честь стриптизёрши из Майами, показал себя настолько эффективным в 1999 году, что приливная волна емейл-траффика, который он генерировал, заставил компании вроде Intel и Microsoft закрыть свои почтовые сервера.

Вирус содержал в себе документ Ворд, озаглавленный List.doc, открывавший доступ на порносайты.

Этот емейл первоначально был нацелен на членов Usenet, но быстро вышел из-под контроля. Когда пользователь открывал сообщение в емейле, инфицированный Ворд документ рассылался первым пятидесяти адресатам из адресной книги владельца. Схема была достаточно успешна, поскольку емейл содержал имя того, кого пользователь знал, и ссылался на документ, который он предположительно запрашивал.

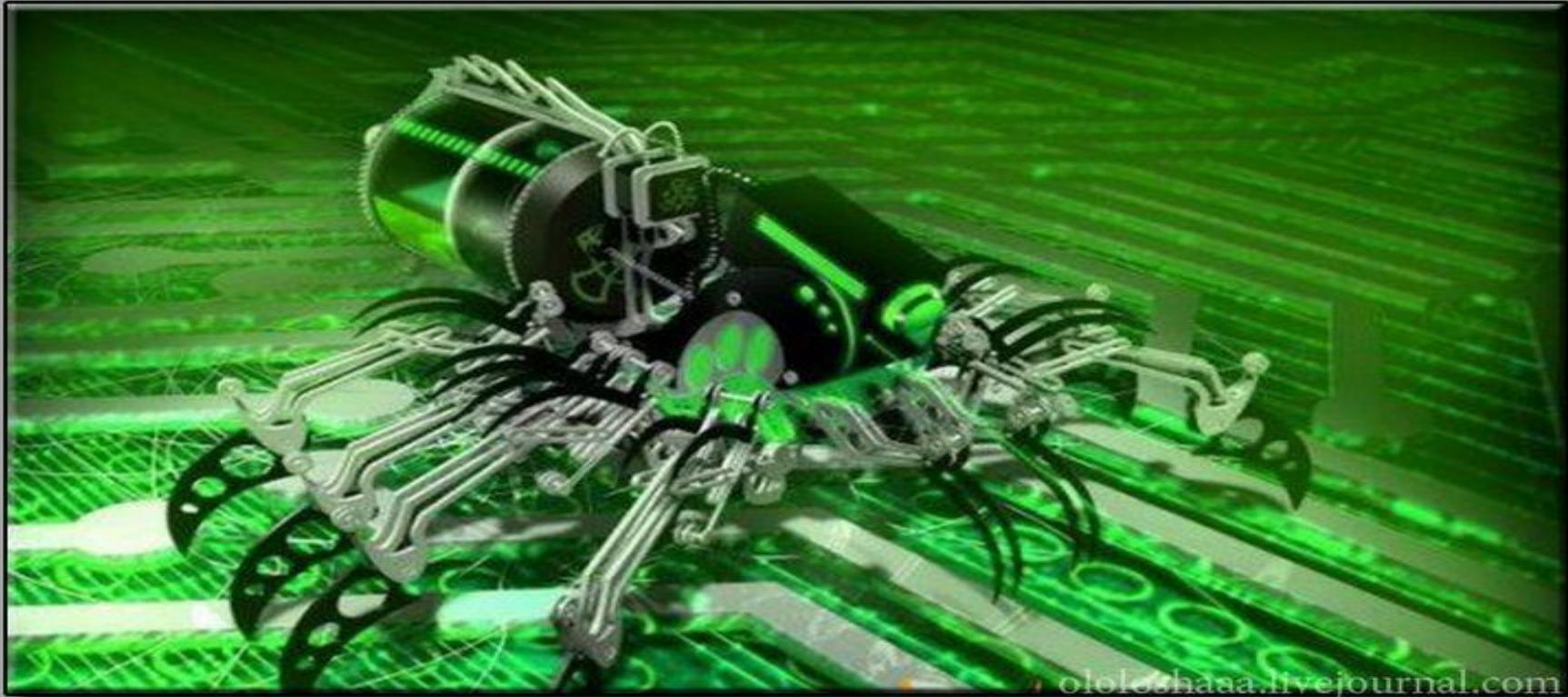


### MyDoom

MyDoom впервые появился в 2004 году и скоро стал самым быстрораспространяющимся червём, который когда-либо поражал сеть, перекрыв предыдущие рекорды червей Sobig и ILOVEYOU.

Причина эффективности MyDoom заключалась в том, что реципиент получал емейл с предупреждением об ошибке в доставке – сообщение, которое все мы видим время от времени. Письмо предлагало пользователю разобраться с проблемой и его действия инициировали запуск червя.

Как только запускался прикрепленный файл, червь рассылал себя по электронным адресам, найденным в адресной книге, и помещал свою копию в расшаренную папку (KaZaA). Подобно Klez, MyDoom мог имитировать емейл, но также имел возможность генерировать трафик через поисковые запросы, что давало существенную нагрузку на поисковые системы вроде Yahoo и Google.



### Sasser-Netsky

Одни из самых знаменитых и плодотворных вариаций компьютерных червей, известных за свою эффективность, и тот факт, что они были написаны семнадцатилетним подростком из Германии Свенном Яшаном, который признался в создании и других червей.

Netsky врезался в память тем, что он открыто оскорблял авторов других вирусов. В нём упоминались семейства червей Bagle и MyDoom, и в некоторых случаях Netsky даже включал в себя код, который удалял конкурирующие вирусы.

Другая причина, по которой этот вирус запал в память людей, заключается в том, что его автора сдал властям его друг, который захотел получить награду в 250 тысяч долларов, которую Microsoft пообещала выплатить тому, кто сможет раскрыть информацию о вирусной эпидемии.



[ololoshaaa.livejournal.com](http://ololoshaaa.livejournal.com)

### 2007 Storm Worm

Этот вирус, известный под многими именами, представлял собой троян, который поражал компьютеры под управлением Windows.

В данном случае дистрибуция вредоносного содержимого опять происходила через емейл, озаглавленный «230 человек погибло в поразившем Европу шторме». Storm Worm был трояном, который присоединял инфицированный компьютер к ботнету – сети удалённо управляемых компьютеров. И хотя считалось, что этот ботнет состоит из миллионов компьютеров, точное число так никогда и не было установлено.

# Действия при заражении вирусом

- При заражении компьютера вирусом (или при подозрении на это) важно соблюдать 4-е правила:
- 1) Прежде всего не надо торопиться и принимать опрометчивых решений. Непродуманные действия могут привести не только к потере части файлов, но к повторному заражению компьютера.
- 2) Надо немедленно выключить компьютер, чтобы вирус не продолжал своих разрушительных действий.
- 3) Все действия по обнаружению вида заражения и лечению компьютера следует выполнять при загрузке компьютера с защищенной от записи дискеты с ОС (обязательное правило).
- 4) Если Вы не обладаете достаточными знаниями и опытом для лечения компьютера, попросите помочь более опытных коллег.

# Заключение

- Компьютерный вирус - специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе компьютера.

В настоящее время известно более 50000 программных вирусов, число которых непрерывно растет. Известны случаи, когда создавались учебные пособия, помогающие в написании вирусов.

Основные виды вирусов: загрузочные, файловые, файлово-загрузочные. Наиболее опасный вид вирусов - полиморфные.

Из истории компьютерной вирусологии ясно, что любая оригинальная компьютерная разработка заставляет создателей антивирусов приспособляться к новым технологиям, постоянно усовершенствовать антивирусные программы.

Причины появления и распространения вирусов скрыты с одной стороны в психологии человека, с другой стороны - с отсутствием средств защиты у операционной системы.

Основные пути проникновения вирусов - съемные диски и компьютерные сети. Чтобы этого не случилось, соблюдайте меры по защите. Также для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, называемых антивирусными.