# Вредоносные программы
# Методы профилактики и защиты


**План презентации**

1. **Понятие вредоносного программного обеспечения.**
2. **Классификация вредоносного программного обеспечения.**
3. **Компьютерные вирусы.**
4. **Признаки появления и способы заражения вирусами.**
5. **Программные антивирусные средства.**
6. **Темы самостоятельных исследований.**

Больше не выводить это сообщение

OK Справка

# 1. Понятие вредоносного программного обеспечения

К вредоносному программному обеспечению относятся сетевые черви, компьютерные вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие какой-либо вред компьютеру, на котором они запускаются, или другим компьютерам в сети.

(*http://www.viruslist.com/ru*)

# 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 ком-пьютерными 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 безопасностиЕжегодно американский Институт компьютерной безопасности совместно с компьютерным подраз-делением Федерального бюро расследований проводит весьма подроб-ное исследование ком-пьютерной преступности По итогам 2005 г. первое место по убыткам тради-ционно 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

# 2. Классификация вредоносного программного обеспечения

## Классические компьютерные вирусы

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью: последующего запуска своего кода при каких-либо действиях пользователя; дальнейшего внедрения в другие ресурсы компьютера.

## Троянские программы

В данную категорию входят программы, осуществляющие несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

.

## Сетевые черви

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

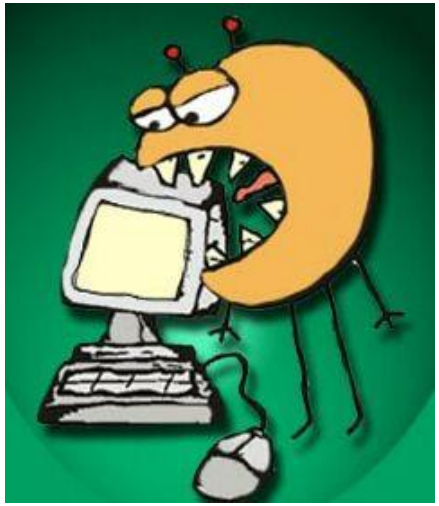
- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры сети.

## Прочие вредоносные программы

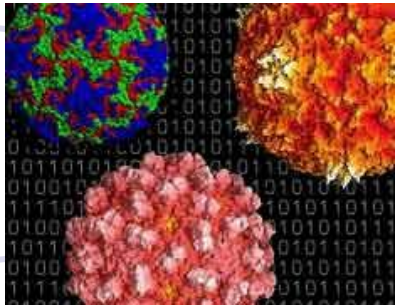
К данной категории относятся:

утилиты автоматизации создания сетевых червей, вирусов и троянских программ

- библиотеки, разработанные для создания вредоносного ПО;
- утилиты скрытия кода зараженных файлов от антивирусной проверки



# 3. Компьютерные вирусы



Существует несколько определений компьютерных вирусов.

- «Компьютерный вирус — это специально написанная, небольшая по размерам программа (т. е. некоторая совокупность выполняемого кода), которая может «приписывать» себя к другим программам «заражать» их), создавать свои копии и внедрять их в файлы, системные области компьютера и т. д., а также выполнять различные нежелательные действия на компьютере» (3, 208).
- «Компьютерным вирусом называется способная к самовоспроизводству и размножению программа, внедряющаяся в другие программы» (2, 145)
- «Компьютерный вирус - фрагмент исполняемого кода, который копирует себя в другую программу (главную программу), модифицируя ее при этом. Дублируя себя, вирус заражает другие программы. Вирус выполняется только при запуске главной программы и вызывает ее непредсказуемое поведение, приводящее к уничтожению и искажению данных и программ» (http://www.glossary.ru).
- «Компьютерный вирус - программа, имеющая возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие объекты с целью искажения и уничтожения данных и программ.(Словарь прикладной интернетики / Нехаев С.А., Кривошеин Н.В., Андреев И.Л., Яскевич Я.С.) При этом дубликаты сохраняют способность к дальнейшему распространению. Такие программы, как правило, составляются на языке ассемблера, никаких сообщений на экран дисплея не выдают. Переносятся при копировании с диска на диск либо по сети Интернет.(Словарь прикладной интернетики / Нехаев С.А., Кривошеин Н.В., Андреев И.Л., Яскевич Я.С.)

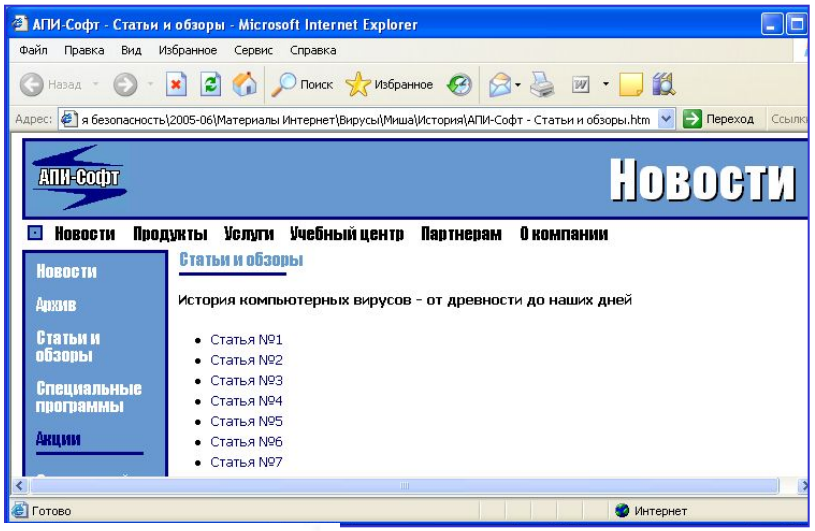
# Первый вирус для PC

- Первый вирус для PC был обнаружен ровно 20 лет назад - в январе 1986 года. Назывался он Brain.A и распространялся "перекрестным опылением" - через дискеты.
- Инфицируя загрузочный сектор машины, вирус приступал к копированию себя во все доступные файлы. Вирус был безопасен, не причинял никакого особого вреда, но именно он стал родоначальником длинной вереницы своих последователей, за прошедшие 20 лет успевших "эволюционировать" в порой весьма агрессивные "особи".
- Вирусы же, поражающие загрузочный сектор, благополучно "вымерли" уже с 1995 года, когда против них появились достаточно эффективные средства борьбы, а сами дискеты почти перестали использоваться - появилась технология оптических носителей.
- (Itnews.com.ua)

# История компьютерных вирусов - от древности до наших дней

на сайте http://apisoft.nnov.ru

«О появлении первого компьютерного вируса много разных мнений. Доподлинно только известно, что на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, его не было, а на Univax 1108 и IBM 360/370, в середине 1970-х годов они уже были. Интересно, что идея компьютерных виру-сов появилась намного раньше самих персональных компьютеров ». (http://apisoft.nnov.ru)




# Классификация вирусов

Один из авторитетнейших «вирусологов» страны Евгений Касперский предлагает условно классифицировать вирусы по следующим признакам:

- по среде обитания вируса;
- по способу заражения среды обитания;
- по деструктивным возможностям;
- по особенностям алгоритма вируса.

KASPERSKY lab

# Среда существования вирусов

- Операционная система или приложение может подвергнуться вирусному нападению в том случае, если она имеет возможность запустить программу, не являющуюся частью самой системы. Данному условию удовлетворяют все популярные «настольные» операционные системы, многие офисные приложения, графические редакторы, системы проектирования и прочие программные комплексы, имеющие встроенные скриптовые языки.

- Компьютерные вирусы, черви, троянские программы существуют для десятков операционных систем и приложений. В то же время существует огромное количество других операционных систем и приложений, для которых вредоносные программы пока не обнаружены. Что является причиной существования вредных программ в одних системах и отсутствия их в других?

- Причиной появления подобных программ в конкретной операционной системе или приложении является одновременное выполнение следующих условий:
  - популярность, широкое распространение данной системы;
  - наличие разнообразной и достаточно полной документации по системе;
  - незащищенность системы или существование известных уязвимостей в системе безопасности.

- Каждое перечисленное условие является необходимым, а выполнение всех трех условий одновременно является достаточным для появления разнообразных вредоносных программ.

# Кто создает вирусы ?


- **Кто и почему создает вредоносные программы?**

- *Основная масса вирусов* и троянских программ в прошлом создавалась студентами и школьниками, которые только что изучили язык программирования, хотели **попробовать свои силы**, но не смогли найти для них более достойного применения. Отраден тот факт, что значительная часть подобных вирусов их авторами не распространялась и вирусы через некоторое время умирали сами вместе с дисками, на которых хранились. Такие вирусы писались и пишутся по сей день только для самоутверждения их авторов.

- *Вторую группу* создателей вирусов также составляют молодые люди (чаще — студенты), которые еще не полностью овладели искусством программирования. Единственная причина, толкающая их на написание вирусов, это комплекс неполноценности, который компенсируется компьютерным хулиганством. Из-под пера подобных «умельцев» часто выходят **вирусы крайне примитивные** и с большим числом ошибок («студенческие» вирусы).

- Став старше и опытнее, многие из подобных вирусописателей попадают *в третью*, наиболее опасную группу, которая создает и запускает в мир **«профессиональные» вирусы**. Эти тщательно продуманные и отлаженные программы создаются профессиональными, часто очень талантливыми программистами. Такие вирусы нередко используют достаточно оригинальные алгоритмы проникновения в системные области данных, ошибки в системах безопасности операционных сред, социальный инжиниринг и прочие хитрости.

- Отдельно стоит *четвертая группа* авторов вирусов — **«исследователи»**, довольно сообразительные программисты, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т. д. Они же придумывают способы внедрения в новые операционные системы. Эти программисты пишут вирусы не ради собственно вирусов, а скорее ради исследования потенциалов «компьютерной фауны». Часто авторы подобных вирусов не распространяют свои творения, однако активно пропагандируют свои идеи через многочисленные интернет-ресурсы, посвященные созданию вирусов.

# 4. Признаки появления и способы заражения вирусами

Непрофессионалу сложно обнаружить присутствие вирусов на компьютере, поскольку они умело маскируются среди обычных файлов.

**Признаки заражения**

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- произвольный, без вашего участия, запуск на компьютере каких-либо программ;
- при наличии на вашем компьютере межсетевого экрана, появление предупреждений о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя вы это никак не инициировали.

# Если ваш компьютер заражен

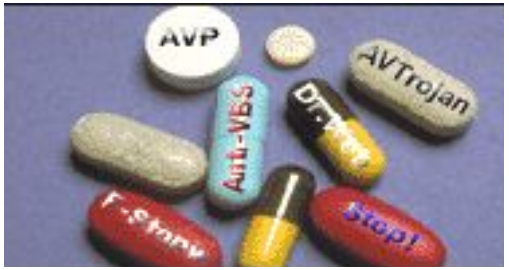
- Не паникуйте! Не поддаваться панике — золотое правило, которое может избавить вас от потери важных данных и лишних переживаний.
- Отключите компьютер от интернета.
- Отключите компьютер от локальной сети, если он к ней был подключен.
- Если симптом заражения состоит в том, что вы не можете загрузиться с жесткого диска компьютера (компьютер выдает ошибку, когда вы его включаете), попробуйте загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows, который вы создавали при установке операционной системы на компьютер.
- Прежде чем предпринимать какие-либо действия, сохраните результаты вашей работы на внешний носитель (дискету, CD-диск, флэш-карту и пр.).
- Скачайте и установите пробную или же купите полную версию Антивируса, если вы этого еще не сделали и на вашем компьютере не установлено других антивирусных программ.
- Получите последние обновления антивирусных баз. Если это возможно, для их получения выходите в интернет не со своего компьютера, а с незараженного компьютера друзей, интернет-кафе, с работы. Лучше воспользоваться другим компьютером, поскольку при подключении к интернету с зараженного компьютера есть вероятность отправки вирусом важной информации злоумышленникам или распространения вируса по адресам вашей адресной книги. Именно поэтому при подозрении на заражение лучше всего сразу отключиться от интернета.
- Установите рекомендуемый уровень настроек антивирусной программы.
- Запустите полную проверку компьютера.

# 5. Программные антивирусные средства

- Программный пакет, предназначенный для эффективной защиты, перехвата и удаления из операционной системы компьютера максимального количества вредоносных (или потенциально вредоносных) программ.

- В настоящее время большинство ведущих антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

- Постоянная антивирусная защита запускается автоматически при старте операционной системы и работает в качестве фонового системного процесса, проверяя на вредоносность совершаемые другими программами действия. Постоянная антивирусная защита проверяет не только файлы на различных носителях информации, но и оперативную память компьютера. Основная задача постоянной антивирусной защиты компьютера: обеспечивать максимальную безопасность при минимальном замедлении работы проверяемых на вредоносные действия программ.



# Примеры антивирусных программ


- **Антивирусные программы Dr.Web®** выполняют поиск и удаление известных компьютерных вирусов из памяти и с жестких дисков компьютера. Кроме того, используя уникальную технологию определения вирусоподобных ситуаций, они способны с высочайшей степенью вероятности обнаруживать ранее неизвестные компьютерные вирусы. Эту способность не раз очень высоко оценивали специалисты и отмечали ведущие журналы. В частности английский журнал “Virus Bulletin ”, ежегодно проводящий тестирование сильнейших антивирусных программ мира неоднократно присваивал престижный знак VB100% антивирусным программам Dr.Web®, т.к. программы Dr.Web® при тестировании на имеющейся у журнала вирусной коллекции определили 100 % компьютерных вирусов. Данная коллекция собрана специалистами журнала из реально распространенных вирусов.


- Предтече антивируса **Eset NOD32** появился на свет примерно в то же время, что и первый компьютерный вирус. А было это в мае 1988 года. Тогда же на чехословацком телевидении огромной популярностью пользовался сериал "Больница на окраине города" (или "Nemocnica na Okraji Mesta". Как мы помним, первые вирусы атаковали исключительно boot-сектора, тоже расположенные на "окраине" диска. А поскольку антивирус вполне мог сойти за больницу, решено было обыграть название с почти одноименным сериалом. В результате получился антивирус "Больница на краю диска" (или "Nemocnica na Okraji Disku", т.е. NOD)


- Годы упорной работы позволили Лаборатории Касперского стать лидером в разработке средств защиты от вирусов. Основной продукт, Антивирус Касперского®, регулярно занимает высшие места в тестах международных исследовательских центров и компьютерных изданий.
- Антивирусные программные модули "Лаборатории Касперского" обеспечивают надежную защиту всех потенциальных объектов вирусных атак - рабочих станций, файловых и веб-серверов, почтовых шлюзов, межсетевых экранов и карманных компьютеров. Удобные средства управления позволяют максимально автоматизировать антивирусную защиту компьютеров и корпоративных сетей.


**ПРОВЕРЯЛ СВОЙ КОМПЬЮТЕР НА ВИРУС?**