
**Введение**

Компьютеры стали настоящими помощниками человека и без них уже не может обойтись ни коммерческая фирма, ни государственная организация. Однако в связи с этим особенно обострилась проблема защиты информации.

Вирусы, получившие широкое распространение в компьютерной технике, взбудоражили весь мир. Многие пользователи компьютеров обеспокоены слухами о том, что с помощью компьютерных вирусов злоумышленники взламывают сети, грабят банки, крадут интеллектуальную собственность.

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных саморазмножающихся программ. Совсем недавно заражение вирусом текстовых файлов считалось абсурдом - сейчас этим уже никого не удивишь. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

**1. Компьютерные вирусы**

**Компьютерным вирусом** называется программа (некоторая совокупность выполняемого кода/инструкций), которая способна создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты/ресурсы компьютерных систем, сетей и т.д. без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

**Классификация вирусов:**

**1) по среде обитания вируса**

Файловые вирусы чаще всего внедряются в исполняемые файлы, имеющие расширения .exe и .com (самые распространенные вирусы), но могут внедряться и в файлы с компонентами операционных систем, драйверы внешних устройств, объектные файлы и библиотеки, в командные пакетные файлы, программные файлы на языках процедурного программирования (заражают при трансляции исполняемые файлы).

Загрузочные вирусы внедряются в загрузочный сектор дискеты (boot-sector) или в сектор, содержащий программу загрузки системного диска (master boot record). При загрузке DOS с зараженного диска такой вирус изменяет программу начальной загрузки либо модифицируют таблицу размещения файлов на диске, создавая трудности в работе компьютера или даже делая невозможным запуск операционной системы.

Файлово-загрузочные вирусы интегрируют возможности двух предыдущих групп и обладают наибольшей "эффективностью" заражения.

Сетевые вирусы используют для своего распространения команды и протоколы телекоммуникационных систем (электронной почты, компьютерных сетей).

Документные вирусы (их часто называют макровирусами) заражают и искажают текстовые файлы (.doc) и файлы электронных таблиц некоторых популярных редакторов.

Комбинированные сетевые макровирусы не только заражают создаваемые документы, но и рассылают копии этих документов по электронной почте.

**2) по способу заражения среды обитания;**

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

**3) по деструктивным возможностям**

Безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

Неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;

**4) по особенностям алгоритма вируса.**

Компаньон-вирусы (companion) - это вирусы, не изменяющие файлы.

Вирусы-“черви” (worm) - вирусы, которые распространяются в компьютерной сети и, так же как и компаньон-вирусы, не изменяют файлы или сектора на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

**2. Создатели вредоносных программ**

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. 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. Из-под пера подобных «умельцев» часто выходят вирусы крайне примитивные и с большим числом ошибок («студенческие» вирусы). Жизнь подобных вирусописателей стала заметно проще с развитием интернета и появлением многочисленных веб-сайтов, ориентированных на обучение написанию компьютерных вирусов. Часто здесь же можно найти готовые исходные тексты, в которые надо всего лишь внести минимальные «авторские» изменения и откомпилировать рекомендуемым способом.

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», которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т. д. Часто авторы подобных вирусов не распространяют свои творения, однако активно пропагандируют свои идеи через многочисленные интернет-ресурсы, посвященные созданию вирусов. При этом опасность, исходящая от таких «исследовательских» вирусов, тоже весьма велика -- попав в руки «профессионалов» из предыдущей группы, эти идеи очень быстро появляются в новых вирусах.

## 3. Описание вредоносных программ

К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

### 3.1Полиморфные вирусы

Полиморфные вирусы - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите. Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным. Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

### 3.2Стелс-вирусы

Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными. Тем не менее, существует простой способ отключить механизм маскировки стелс-вирусов. Достаточно загрузить компьютер с не зараженной системной дискеты и сразу, не запуская других программ с диска компьютера (которые также могут оказаться зараженными), проверить компьютер антивирусной программой. При загрузке с системной дискеты вирус не может получить управление и установить в оперативной памяти резидентный модуль, реализующий стелс-механизм. Антивирусная программа сможет прочитать информацию, действительно записанную на диске, и легко обнаружит вирус.

### 3.3Троянские вирусы

Троянский конь - это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. «Троянские кони» представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Списки таких программ широко публикуются в зарубежной печати. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку.

Программные закладки также содержат некоторую функцию, наносящую ущерб ВС, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

**3.4Черви**

Червями называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т. к. ему в любой момент может подвергнуться любой из 40 миллионов компьютеров, подключенных к этой сети.

**4. Признаки появления вирусов**

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

1.прекращение работы или неправильная работа ранее успешно функционировавших программ

2. медленная работа компьютера

3. невозможность загрузки операционной системы

4. исчезновение файлов и каталогов или искажение их содержимого

5. изменение даты и времени модификации файлов

6. изменение размеров файлов

7. неожиданное значительное увеличение количества файлов на диске

8. существенное уменьшение размера свободной оперативной памяти

9. вывод на экран непредусмотренных сообщений или изображений

10. подача непредусмотренных звуковых сигналов

11. частые зависания и сбои в работе компьютера

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

**5. Борьба с антивирусами**

Во все времена существовали вредоносные программы, защищающие себя достаточно активно. В качестве такой защиты может выступать:

- целенаправленный поиск в системе антивируса, файервола или другой защитной утилиты и нарушение ее работы. В качестве примера можно привести поиск вредоносной программой имени конкретного антивируса в списке процессов и попытку выгрузить этот антивирус;

- блокирование файлов и открытие их с эксклюзивным доступом в качестве меры противодействия файловым антивирусам;

- модификация файла hosts с целью блокирования доступа к сайтам антивирусных обновлений;

- обнаружение окон запросов от системы безопасности и имитация нажатия кнопки «Разрешить».

Фактически, целевое нападение на средства защиты — это больше «вынужденная мера», защита прижатого к стенке, чем активное нападение. В современных условиях, когда антивирусы анализируют не только код вредоносных программ, но и их поведение, последние оказываются в большей или меньшей степени безоружны: полной защиты им не обеспечивает ни полиморфизм, ни упаковка, ни

даже технологии сокрытия в системе. Поэтому вредоносным программам остается только прицельно отстреливать отдельные проявления или функции «врага». Вне неизбежной необходимости этот способ самозащиты не был бы так популярен, поскольку он является слишком невыгодным с точки зрения максимально широкой защиты.

# Заключение

Из всего вышесказанного можно сделать вывод, что компьютерный вирус - это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам, а также выполнять различные нежелательные действия на компьютере. 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-нибудь вредные действия (например, портит файлы или таблицу размещения файлов на диске, «засоряет» оперативную память и т. д.). Вирус - это программа, обладающая способностью к самовоспроизведению. Такая способность является единственным свойством, присущим всем типам вирусов. Вирус не может существовать в «полной изоляции». Это означает, что сегодня нельзя представить себе вирус, который бы так или иначе не использовал код других программ, информацию о файловой структуре или даже просто имена других программ. Причина этого довольно понятна: вирус должен каким-нибудь способом обеспечить передачу себе управления.

Самым эффективным способом защиты от компьютерных вирусов является не внесение информации в компьютер извне. Но, к сожалению, на 100% защититься от вирусов практически невозможно (подразумевается, что пользователь меняется дискетами с друзьями и играет в игры, а также получает информацию из других).

**Список используемой литературы**

1. Леонтьев В.П. Новейшая энциклопедия персонального компьютера 2003.- 5-е изд., перераб. и доп. - М.: ОЛМА-ПРЕСС, 2003

**2.** Левин А.Ш. Самоучитель работы на компьютере.- 9-е изд.,-СПб.:Питер,2006

3. www.yandex. ru

4. www.google. ru

4. CD-ROM. Лучшее из лучшего: рефераты, курсовые, дипломы, 2007

**Компьютерные вирусы, их свойства и классификация**

**Свойства компьютерных вирусов**

Сейчас применяются персональные компьютеры, в которых пользователь имеет свободный доступ ко всем ресурсам машины. Именно это открыло возможность для опасности, которая получила название компьютерного вируса.

Что такое компьютерный вирус? Формальное определение этого понятия до сих пор не придумано, и есть серьезные сомнения, что оно вообще может быть дано. Многочисленные попытки дать «современное» определение вируса не привели к успеху. Чтобы почувствовать всю сложность проблемы, попробуйте, к примеру, дать определение понятия «редактор». Вы либо придумаете нечто очень общее, либо начнете перечислять все известные типы редакторов. И то и другое вряд ли можно считать приемлемым. Поэтому мы ограничимся рассмотрением некоторых свойств компьютерных вирусов, которые позволяют говорить о них как о некотором определенном классе программ.

Прежде всего, вирус - это программа. Такое простое утверждение само по себе способно развеять множество легенд о необыкновенных возможностях компьютерных вирусов. Вирус может перевернуть изображение на вашем мониторе, но не может перевернуть сам монитор. К легендам о вирусах-убийцах, «уничтожающих операторов посредством вывода на экран смертельной цветовой гаммы 25-м кадром» также не стоит относиться серьезно. К сожалению, некоторые авторитетные издания время от времени публикуют «самые свежие новости с компьютерных фронтов», которые при ближайшем рассмотрении оказываются следствием не вполне ясного понимания предмета.

Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но и могут вообще с ним не совпадать!

Вирус не может существовать в «полной изоляции»: сегодня нельзя представить себе вирус, который не использует код других программ, информацию о файловой структуре или даже просто имена других программ. Причина понятна: вирус

должен каким-нибудь способом обеспечить передачу себе управления.

**Классификация вирусов**

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

- среде обитания
- способу заражения среды обитания
- воздействию
- особенностям алгоритма

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. *Сетевые вирусы* распространяются по различным компьютерным сетям. *Файловые вирусы* внедряются главным образом в исполняемые модули, т. е. В файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. *Загрузочные вирусы* внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord). *Файлово-загрузочные* вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные. *Резидентный вирус* при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. *Нерезидентные вирусы* не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

- *неопасные*, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах
- *опасные* вирусы, которые могут привести к различным нарушениям в работе компьютера

- *очень опасные*, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. *Простейшие вирусы* - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить *вирусы-репликаторы*, называемые *червями*, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.

Известны *вирусы-невидимки*, называемые *стелс-вирусами*, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить *вирусы-мутанты*, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые *квазивирусные* или *«троянские»* программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Теперь поподробнее о некоторых из этих групп.

**Загрузочные вирусы**

Рассмотрим схему функционирования очень простого загрузочного вируса, заражающего дискеты.

Что происходит, когда вы включаете компьютер? Первым делом управление передается *программе начальной загрузки*, которая хранится в постоянно запоминающем устройстве (ПЗУ) т.е. ПНЗ ПЗУ.

Эта программа тестирует оборудование и при успешном завершении проверок пытается найти дискету в дисководе A:

Всякая дискета размечена на т.н. секторы и дорожки. Секторы объединяются в кластеры, но это для нас несущественно.

Среди секторов есть несколько служебных, используемых операционной системой для собственных нужд (в этих секторах не могут размещаться ваши данные). Среди служебных секторов нас интересует сектор начальной загрузки (boot-sector).

В секторе начальной загрузки хранится информация о дискете - количество поверхностей, количество дорожек, количество секторов и пр. Но нас сейчас интересует не эта информация, а небольшая программа начальной загрузки (ПНЗ), которая должна загрузить саму операционную систему и передать ей управление.

Таким образом, нормальная схема начальной загрузки следующая:

ПНЗ (ПЗУ) - ПНЗ (диск) - СИСТЕМА

Теперь рассмотрим вирус. В загрузочных вирусах выделяют две части: голову и т.н. хвост. Хвост может быть пустым.

Пусть у вас имеются чистая дискета и зараженный компьютер, под которым мы понимаем компьютер с активным резидентным вирусом. Как только этот вирус обнаружит, что в дисководе появилась подходящая жертва - в нашем случае не защищенная от записи и еще не зараженная дискета, он приступает к заражению. Заражая дискету, вирус производит следующие действия:

- выделяет некоторую область диска и помечает ее как недоступную операционной системе, это можно сделать по-разному, в простейшем и традиционном случае занятые вирусом секторы помечаются как сбойные (bad)
- копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор
- замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой
- организует цепочку передачи управления согласно схеме.

Таким образом, голова вируса теперь первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору. В цепочке

ПНЗ (ПЗУ) - ПНЗ (диск) - СИСТЕМА

появляется новое звено:

ПНЗ (ПЗУ) - ВИРУС - ПНЗ (диск) - СИСТЕМА

Мы рассмотрели схему функционирования простого бутового вируса, живущего в загрузочных секторах дискет. Как правило, вирусы способны заражать не только загрузочные секторы дискет, но и загрузочные секторы винчестеров. При этом в отличие от дискет на винчестере имеются два типа загрузочных секторов,

содержащих программы начальной загрузки, которые получают управление. При загрузке компьютера с винчестера первой берет на себя управление программа начальной загрузки в MBR (Master Boot Record - главная загрузочная запись). Если ваш жесткий диск разбит на несколько разделов, то лишь один из них помечен как загрузочный (boot). Программа начальной загрузки в MBR находит загрузочный раздел винчестера и передает управление на программу начальной загрузки этого раздела. Код последней совпадает с кодом программы начальной загрузки, содержащейся на обычных дискетах, а соответствующие загрузочные секторы отличаются только таблицами параметров. Таким образом, на винчестере имеются два объекта атаки загрузочных вирусов - программа начальной загрузки в MBR и программа начальной загрузки в бут-секторе загрузочного диска

Литература: 1.https://works.doklad.ru/view/7pcslaWAL5Y.html

2.https://works.doklad.ru/view/A7v8ooMEpOw.html

3.https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%

4.https://nsportal.ru/ap/library/nauchno-tekhnicheskoe-tvorchestvo/2014/09/06/referat-kompyuternye-virusy-i-zashchita-ot

5. https://www.bestreferat.ru/referat-42967.html