|  |
| --- |
| Федеральное государственное образовательное бюджетное учреждение  высшего образования  «Финансовый университет при Правительстве Российской Федерации»  **КОЛЛЕДЖ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ**  **ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих**  **УП.04.01 Учебная практика (оператор ЭВМ)**  **ПРАКТИЧЕСКАЯ РАБОТА №1 «MS WORD»**  Вариант № … |

Выполнил:

Студент группы 2ПКС – 115

Деменчук Г.М.

Проверил:

Пестов А.И.

Москва 2017

**Содержание**

[Введение 3](#_Toc474404759)

[Глава 1. Компьютерные вирусы 4](#_Toc474404760)

[1.1. Понятие «Компьютерный вирус» 4](#_Toc474404761)

[1.2. Авторы компьютерных вирусов 5](#_Toc474404762)

[1.3. История компьютерных вирусов 5](#_Toc474404763)

[1.4. Механизм работы вирусов 7](#_Toc474404764)

[Глава 2. Классификация компьютерных вирусов 9](#_Toc474404765)

[Глава 3. Профилактика и лечение 13](#_Toc474404766)

[3.1. Антивирусные программы 13](#_Toc474404767)

[3.2. Виды антивирусных программ 13](#_Toc474404768)

[2.2.1 Программы-детекторы 14](#_Toc474404769)

[2.2.2 Программы-доктора 14](#_Toc474404770)

[2.2.3 Программы-ревизоры (инспектора) 14](#_Toc474404771)

[3.4. Альтернатива платным программам 14](#_Toc474404772)

[Заключение 17](#_Toc474404773)

[Библиография 18](#_Toc474404774)

Введение

Компьютеры в наше время выполняют множество задач. Практически никто сейчас не работает без компьютера. Рынок IT процветает и развивается, появляются новые интернет-проекты и сервисы, люди все больше времени проводят в сети. Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

В связи с этим защита личной информации и нормальной работоспособности персональных компьютеров сейчас, как никогда, актуальна. Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных вредоносных программ.

Борьбой с компьютерными вирусами профессионально занимаются тысячи специалистов в десятках, а может быть, сотнях компаний, ведь именно компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации.

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.

Поэтому, ***цель данной работы***: выяснить пути проникновения и влияние вирусов на работу компьютера и определить методы защиты от них.

Исходя из цели реферата, были сформулированы следующие задачи:

* определить, что является компьютерным вирусом;
* выделить виды вирусов по способам проникновения их в компьютер и влиянию на работу и безопасность;
* ознакомиться с существующими методами защиты от компьютерных вирусов.

Глава 1. Компьютерные вирусы

## Понятие «Компьютерный вирус»

Компьютерный вирус был назван по аналогии с биологическими вирусами за сходный механизм распространения: процесс захвата компьютера вирусом полностью соответствует процессу захвата вирусом человеческого организма. Человеческий вирус внедряется в клетку, после чего начинает размножаться. Так и компьютерный: попав в программу, вирус действует аналогичным образом.

Считается, что впервые слово «вирус» по отношению к программе было употреблено Грегори Бенфордом (GregoryBenford) в фантастическом рассказе «Человек в шрамах», опубликованном в журнале Venture в мае 1970 года.

***Компьютерный вирус***— разновидность компьютерных программ или вредоносный код, отличительным признаком которых является способность к размножению (саморепликация).

Проникнув в компьютерную систему, вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае компьютерная система, пораженная вирусом, становится неработоспособной или же окажется под полным контролем злоумышленника.

Даже если автор вируса не программировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы обычно занимают некоторое место, иногда довольно значительное, в оперативной памяти или на накопителях информации и отбирают некоторые другие ресурсы системы.

Поэтому вирусы относят к вредоносным программам.

## Авторы компьютерных вирусов

Вирусы не возникают сами по себе, а создаются людьми. Наиболее вероятными причинами, толкающими вирусо-писателей на создание и распространение вредоносного программного обеспечения являются:

- обычное *юношеское хулиганство*, попытки самоутверждения на основе достигнутого интеллектуального уровня. Фактически подобное компьютерное хулиганство ничем не отличается от обычного уличного хулиганства, за исключением того, что "самоутверждение" происходит либо в подворотне, либо в сети;

- *мошенничество* с целью присвоения ресурсов жертвы: незаметное управление пораженным компьютером, воровство паролей доступа в Интернет, средств с "кошельков" WebMoney и кодов доступа к персональным банковским счетам (в том случае, если жертва использует данный сервис). В случае, если атакой подверглись корпоративные сети, то речь идет уже о шпионаже: как правило, это проникновение в сеть с целью присвоения конфиденциальной информации, представляющей финансовую ценность.

Основную массу вирусов создают студенты и школьники, которые только что изучили язык программирования и хотят попробовать свои силы. Значительная часть таких вирусов их авторами часто не распространяется.

Вторую группу составляют также молодые люди (чаще - студенты), которые решили посвятить себя написанию и распространению вирусов. Как правило, они создают многочисленные модификации "классических" вирусов, либо вирусы крайне примитивные и с большим числом ошибок. Часто они используют конструкторы вирусов, при помощи которых можно создавать новые вирусы даже при минимальных знаниях об операционной системе.

Став старше и опытнее, многие из этих вирусописателей попадают в третью, наиболее опасную группу, которая создает и запускает в мир "профессиональные" вирусы. Это тщательно продуманные и отлаженные программы.

Четвертая группа авторов вирусов - "исследователи". Эта группа состоит из талантливых программистов, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т.д. Эти программисты пишут вирусы не ради собственно вирусов, а скорее ради "исследования" потенциалов "компьютерной вирусологии".

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (гл. 28, ст.273).

## История компьютерных вирусов

На сегодняшний день компьютерному вирусу уже более тридцати лет.

Первыми известными вирусами являются *Virus 1,2,3* и *ElkCloner*для ПК Apple II, появившиеся в 1981 году.Первые вирусные эпидемии относятся к 1987 - 1989 годам: *Brain*(более 18 тысяч зараженных компьютеров, по данным *McAfeeJerusalem* (проявился в пятницу 13 мая 1988 года, уничтожая программы при их запуске), *червь Морриса* (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), *DATACRIME* (около 100 тысяч зараженных ПЭВМ только в Нидерландах).

В 1990 году появляется первый коммерческий антивирус Symantec NortonAntiVirus.

В несколько последующих лет были 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 MicrosoftOffice получили распространение макровирусы (*Concept*, 1995).

С распространением сетей и Интернета файловые вирусы всё больше ориентируются на них как на основной канал работы (*Melissa*, 1999 - макровирус и сетевой червь, побивший все рекорды по скорости распространения).

В 2004 году беспрецедентные по масштабам эпидемии вызывают черви-эксплоиты[[1]](#footnote-1)*MsBlast* (по данным Microsoft - более 16 млн систем), *Sasser и Mydoom* (оценочные ущербы 500 млн и 4 млрд долл. соответственно).

Кроме того, монолитные вирусы в значительной мере уступают место комплексам вредоносного ПО с разделением ролей и вспомогательными средствами. Также расцветают социальные технологии — спам[[2]](#footnote-2) и фишинг[[3]](#footnote-3) — как средство заражения в обход механизмов защиты программного обеспечения.

Самый современный вид вирусов  - черви-[ботнеты](http://ru.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82" \o "Ботнет) всё больше набирают обороты (*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.

## Механизм работы вирусов

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 MicrosoftWord и Excel, содержащие макросы. Кроме того, для проникновения на компьютер, вирус может использовать уязвимости в популярном программном обеспечении (например, AdobeFlash, InternetExplorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплоитом, использующим уязвимость.



XTAL2

XTAL1

PB 7..0

GND

RESET

PA 7..0

VCC

JTAG/  
отладочная система

УСАПП 1

Порт C (8)

Порт D (8)

УСАПП 0

16-разр. T/C 2

16-разр. T/C 1

8-разр. T/C 0

Стат. ОЗУ

Флеш-память

2-пров. интерфейс

ЦПУ AVR

SPI

Порт В (8)

Аналоговый компаратор

ИОН

ЭСППЗУ

АЦП

Порт А (8)

Генератор/ схема синхронизации

Генератор ст. таймера

с

Сторожевой таймер

Супервизор питания/ схема сброса

Глава 2. Классификация компьютерных вирусов

На сегодняшний день известны десятки тысяч различных вирусов. Несмотря на такое изобилие, число типов вирусов, отличающихся друг от друга механизмом распространения и принципом действия, весьма ограниченно. Существуют и комбинированные вирусы, которые можно отнести одновременно к нескольким типам. Таким образом, вирусы можно классифицировать по следующим признакам:

* среда обитания;
* способ заражения;
* степень воздействия;
* особенности алгоритма работы.

В зависимости **от среды обитания** вирусы делят на:

* ***сетевые*** – распространяются по различным компьютерным сетям;
* ***файловые*** - поражают файлы с расширением .com, .ехе, реже .sys или оверлейные модули .ехе файлов. Эти вирусы дописывают своё тело в начало, середину или конец файла и изменяют его таким образом, чтобы первыми получить управление. Получив управление, вирус может заразить другие программы, внедриться в оперативную память компьютера и т.д. Некоторые из этих вирусов не заботятся о сохранение заражаемого файла, в результате чего он оказывается неработоспособным и не подлежащим восстановлению;
* ***загрузочные*** - получают управление на этапе инициализации компьютера, еще до начала загрузки ОС. При заражении дискеты или жесткого диска загрузочный вирус заменяет загрузочную запись BR или главную загрузочную запись MBR. При начальной загрузке компьютера BIOS считывает загрузочную запись с диска или дискеты, в результате чего вирус получает управление еще до загрузки ОС. Затем он копирует себя в конец оперативной памяти и перехватывает несколько функций BIOS. В конце процедуры заражения вирус загружает в память компьютера настоящий загрузочный сектор и передает ему управление. Далее все происходит, как обычно, но вирус уже находится в памяти и может контролировать работу всех программ и драйверов;
* ***файлово–загрузочные*** – комбинированные вирусы, объединяющие свойства файловых и загрузочных. В качестве примера можно привести широко распространенный когда-то файлово-загрузочный вирус OneHalf. Проникая в компьютер с ОС MS-DOS, этот вирус заражает главную загрузочную запись. Во время загрузки вирус постепенно шифрует секторы жесткого диска, начиная с самых последних секторов.

**По способу заражения среды обитания** вирусы делятся на:

* ***резидентные*** - 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:

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

**По особенностям алгоритма**:

* ***простейшие вирусы*** - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены;
* ***вирусы-невидимки (стелс-вирусы)*** – пытаются скрыть свое присутствие в компьютере. Если ОС или другая программа считывают файл зараженной программы, то вирус подставляет настоящий, незараженный, файл программы. Для этого резидентный модуль может временно удалять вирус из зараженного файла. После окончания работы с файлом он заражается снова. Загрузочныестелс-вирусы действуют по такой же схеме. Когда какая-либо программа считывает данные из загрузочного сектора, вместо зараженного подставляется настоящий загрузочный сектор.
* ***Макрокомандные вирусы***. Файлы документов MicrosoftOffice могут содержать в себе небольшие программы для обработки этих документов, составленные на языке VisualBasicforApplications. Это относится и к базам данных Access, а также к файлам презентаций PowerPoint. Такие программы создаются с использованием макрокоманд, поэтому вирусы, живущие в офисных документах, называются макрокомандными. Такие вирусы распространяются вместе с файлами документов. Чтобы заразить компьютер таким вирусом, достаточно просто открыть файл документа в соответствующем приложении. Распространенности данного вида вирусов в немалой степени способствует популярность MicrosoftOffice. Они могут изменять зараженные документы, оставаясь незамеченными долгое время.

Кроме вирусов принято выделять еще, по крайней мере, три вида вредоносных программ:

* ***Троянские программы*** - по основному назначению троянские программы совершенно безобидны или даже полезны. Но когда пользователь запишет программу в свой компьютер и запустит ее, она может незаметно выполнять вредоносные функции. Чаще всего троянские программы используются для первоначального распространения вирусов, для получения удаленного доступа к компьютеру через Интернет, кражи данных или их уничтожения.
* ***Логические бомбы*** - программа или ее отдельные модули, которые при определенных условиях выполняют вредоносные действия, например, может сработать по достижении определенной даты или тогда, когда в базе данных появится или исчезнет запись, и т. д. Такая бомба может быть встроена в вирусы, троянские программы и даже в обычные программы.
* ***Программы-черви*** нацелены на выполнение определенной функции, например, на проникновение в систему и модификацию данных, могут подсматривать пароль для доступа к банковской системе и изменять базу данных. Некоторые вирусы-черви (например, *CodeRed*) существуют не внутри файлов, а в виде процессов в памяти зараженного компьютера. Это исключает их обнаружение антивирусами, сканирующими файлы и оставляющими без внимания оперативную память компьютера.
* ***Вирусы в системах документооборота***- документы, хранящиеся в базах данных таких систем документооборота, как LotusNotes и MicrosoftExchange, тоже могут содержать вирусы, точнее, вредоносные макрокоманды. Они могут активизироваться при выполнении каких-либо действий над документом (например, когда пользователь щелкает кнопку мышью). Поскольку такие вирусы расположены не в файлах, а в записях баз данных, для защиты от них требуются специализированные антивирусные программы;
* ***новые и экзотические вирусы.*** По мере развития компьютерных технологий совершенствуются и компьютерные вирусы, приспосабливаясь к новым для себя сферам обитания. Новые вирусы могут использовать неизвестные или не существовавшие ранее каналы распространения, а также новые технологии внедрения в компьютерные системы.



Видео стример

Приемники

Кодер

ADSL

STB

Hub

Hub

Hub

LAN

Видео сервер

Видео сервер

Система распределения

Web  
Server

Middleware

CAS

Контент от провайдера

Спутниковый контент

Местный контент

IP Network

Глава 3. Профилактика и лечение

## 3.1. Антивирусные программы

Главным оружием в борьбе с вирусами являются антивирусные программы. Они позволяют не только обнаружить вирусы, но и удалить их из компьютера.

Итак, что же такое антивирус? Почему-то многие считают, что антивирус может обнаружить любой вирус, то есть, запустив антивирусную программу, можно быть абсолютно уверенным в их надежности. Такая точка зрения не совсем верна. Дело в том, что антивирус - это тоже программа, написанная профессионалом. Но эти программы способны распознавать и уничтожать только известные вирусы. То есть антивирус против конкретного вируса может быть написан только в том случае, когда у программиста есть в наличии хотя бы один экземпляр этого вируса. Но существует большое количество вирусов, алгоритм которых практически скопирован с алгоритма других вирусов.

Современные антивирусные технологии позволяют выявить практически все уже известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе. Кроме того, разработаны технологии моделирования поведения, позволяющие обнаруживать вновь создаваемые вирусные программы. Обнаруживаемые объекты могут подвергаться лечению, изолироваться (помещаться в карантин) или удаляться. Защита от вирусов может быть установлена на рабочие станции, файловые и почтовые сервера, межсетевые экраны, работающие под практически любой из распространенных операционных систем, на процессорах различных типов.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

## 3.2. Виды антивирусных программ

Существует несколько основополагающих методов поиска вирусов, которые применяются антивирусными программамиДля обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов антивирусных программ:

1. программы-детекторы

2. программы-доктора или фаги

3. программы-ревизоры (инспектора)

4. программы-фильтры (мониторы)

5. программы-вакцины или иммунизаторы

6. сканер

### 2.2.1 Программы-детекторы

Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

### 2.2.2 Программы-доктора

Программы-доктора или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, то есть программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

### 2.2.3 Программы-ревизоры (инспектора)

Программы-ревизоры (инспектора) относятся к самым надежным средствам защиты от вирусов. Ревизоры (инспектора) проверяют данные на диске на предмет вирусов-невидимок, изучают, не забрался ли вирус в файлы, нет ли посторонних в загрузочном секторе жесткого диска, нет ли несанкционированных изменений реестра Windows. Причем инспектор может не пользоваться средствами операционной системы для обращения к дискам (а значит, активный вирус не сможет это обращение перехватить).

## 3.4. Альтернатива платным программам

Нередко встречается сегодня практика, когда производители антивирусных программ предлагают версии своих продуктов без оплаты, которые менее функциональны, чем их платные аналоги. Это делается по многим причинам, одна из главных это продвижение и популяризация своего бренда среди пользователей.

Как правило, для того чтобы продукт без оплаты полноценно работал, необходима его регистрация. Обычно она заключается в заполнении регистрационной формы, с внесением своих контактных данных.

Также в некоторых антивирусах встречается назойливая реклама, которая постоянно напоминает о необходимости купить платную версию программы. Помимо всего этого антивирус без оплаты имеет урезанный функционал. Все это можно получить, если скачать бесплатный антивирус. Но ведь и использование таких продуктов не требует денег!

Нужно отметить, что некоторые программы подобного рода смогут защитить систему не хуже коммерческих антивирусов от неизвестных или малоизвестных производителей**.** Так что скачать антивирус бесплатно или использовать пробную версию антивируса за оплату это решать уже пользователю.

Примеры бесплатных программ-антивирусов:

Антивирус **BitDefenderFreeEdition** - программа, которая поможет защитить систему, периодически проводя проверки и сканирование. При работе антивирус использует те же сертифицированные технологии обнаружения, что и платные продукты от BitDefender.

**AVG Anti-VirusFreeEdition 2013** из раздела бесплатных антивирусов позволит обеспечить базовую защиту компьютера. Хороший вариант для домашнего пользователя, который много времени проводит в социальных сетях благодаря встроенной функции защиты AVG SocialNetworkingProtection.

Антивирус **avast! FreeAntivirus -** это один из лучших антивирусов среди бесплатных программ для защиты. Новое эвристическое ядро и высокая эффективность обнаружения сделали популярным avast среди пользователей всего мира.

**AviraFreeAntivirus** это антивирус от немецкого производителя, который обеспечивает надежную защиту, как от вирусов, так и от программ руткитов, использующих маскировку в своей работе.

**Comodo** защитит систему от вирусов, шпионских программ, руткитов, а также от иных вредоносных программ. В антивирусе отсутствуют некоторые незначимые функции, поэтому он бесплатный. Имеется встроенная автоматическая функция песочница (AutoSandbox).

**BitDefenderFreeEdition -** это бесплатная программа, которая поможет защитить систему, периодически проводя проверки и сканирование. При работе антивирус использует те же сертифицированные технологии обнаружения, что и платные продукты от BitDefender.

Антивирус от**Microsoft**под названием **SecurityEssentials** предоставит защиту от вирусов, шпионов и других вредоносных программ. Наличие журнала проверки, планировщика, а также интуитивно понятный интерфейс для пользователей сделали этот антивирус, который распространяется бесплатно, популярным среди многих пользователей.

**RisingAntivirusFreeEdition** это бесплатная программа для защиты системы, которая поможет как при ежедневной работе, так и при работе в сети Интернет. Антивирус имеет простой и удобный интерфейс, а также множество настроек.

**Zillya** представлен на рынке украинскими экспертами по безопасности. Эвристическая проверка файлов, сканирование почты, большая антивирусная база и простой пользовательский интерфейс сделали этот довольно молодой антивирус популярным среди многих пользователей.

**Ad-Aware FREE InternetSecurity** это антивирус, который распространяется бесплатно и который сможет обеспечить полноценную защиту при работе в сети Интернет. Помимо функции антивируса, программа имеет встроенный модуль обнаружения программ-шпионов.

**PandaCloudAntivirus** это возможность использовать передовую защиту отПанда, ничего при этом не потратив. Антивирус оказывает минимальное воздействие на систему и обеспечивает максимальную защиту.

Если у вас нет времени или желания разбираться со всеми этими вопросами по выбору домашнего антивируса, то, основываясь на результаты тестов, проведенных авторитетными независимыми лабораториями можно выделить два лидера, которые подходят под понятие домашний антивирус. Эти антивирусы бесплатны, не нагружают систему, имеют высокую скорость сканирования и обеспечивают высокую степень защиты. Это антивирус **Avast** и антивирус **Avira**.

# Заключение

Пожалуй, самым страшным кошмаром любого пользователя сети Интернет являются компьютерные вирусы, которыепостоянно совершенствуются. Вирусы попадают на компьютеры часто, причем иногда не сразу понятно, что же произошло с системой.

Хочется сразу заметить, что слишком уж бояться вирусов не стоит, особенно если компьютер приобретен совсем недавно, и много информации на жестком диске еще не накопилось. Вирус компьютер не взорвет. Ныне известен только один вирус (*Win95.CIH*), который способен испортить "железо" компьютера. Другие же могут лишь уничтожить информацию, не более того.

Зачем надо защищаться? Все зависит от конкретного профиля рода занятий. Для одних главной задачей является предотвращение утечки информации к конкурентам. Другие могут уделять главное внимание целостности информации. Для третьих на первое место поднимается задача безотказной работы информационных систем (например, для провайдеров Интернет). Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека - в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

Из всего вышесказанного можно смело сделать вывод, что необходимость защиты от компьютерных вирусов на данный момент стоит на первом месте.

Для предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.

Библиография

1. Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов. – М.: «СОЛОН-Р», 2001.
2. Левин А.Ш. Самоучитель полезных программ. 4-е издание. – СПБ.: Питер, 2005.
3. Мостовой Д.Ю. Современные технологии борьбы с вирусами - Мир ПК. - №8. 2001.
4. Островский С. Компьютерные вирусы Информатика, январь 2002.
5. [http://www.bytemag.ru](http://www.bytemag.ru/) – BYTE/Россия – Что нужно знать о компьютерных вирусах.
6. [http://www.wasm.ru](http://www.wasm.ru/) – Вирусология.
7. [http://abisoft.ru](http://abisoft.ru/1/cid/2201_2813/ANTIVIRUSY._BEZOPASNOST/) - Интернет-магазин пограммного обеспечения.
8. <http://antivibest.ru> – Антивирусные программы.

1. ## Эксплойт [exploit] - компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на компьютерную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

   [↑](#footnote-ref-1)
2. **Спам** (англ. *spam*) — рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выражавшим желания их получать. [↑](#footnote-ref-2)
3. **Фи́шинг** (англ. *phishing*, от *fishing* — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведениямассовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков, сервисов (Rambler, Mail.ru) или внутри социальных сетей (Facebook,Вконтакте, Одноклассники.ru). [↑](#footnote-ref-3)