**Тема: «Виды компьютерных вирусов и способы защиты от них».**

**Введение.**

Бурное развитие средств вычислительной техники открыло перед человечеством небывалые возможности по автоматизации умственного труда и привело к созданию большого числа разного рода автоматизированных информационных и управляющих систем, к возникновению принципиально новых, так называемых, информационных технологий.

К сожалению, как и любое другое достижение человеческого гения, компьютер, решая одни технические, экономические и социальные проблемы, одновременно порождает и другие, порою не менее сложные. Если в должной мере не позаботиться о нейтрализации сопутствующих прогрессу негативных факторов, то эффект от внедрения новейших достижений науки и техники может оказаться в целом отрицательным.

Актуальность проблемы защиты информационных технологий в современных условиях определяется следующими основными факторами:

• обострением противоречий между объективно существующими потребностями общества *в* расширении свободного обмена информацией и чрезмерными или наоборот недостаточными ограничениями на ее распространение и использование

• расширением сферы использования ЭВМ, многообразием и повсеместным распространением информационно-управляющих систем, высокими темпами увеличения парка средств вычислительной техники и связи

• повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности

• вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса

• концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях

• количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам

• отношением к информации, как к товару, переходом к рыночным отношениям в области предоставления информационных услуг с присущей им конкуренцией и промышленным шпионажем

• многообразием видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации

• ростом числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими нежелательных программно-математических воздействий на системы обработки информации

• увеличением потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (возрастанием уязвимости различных затрагиваемых субъектов)

• развитием рыночных отношений (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты).

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает.

***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**

1. **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.

1. **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).

1. **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 Norton AntiVirus.

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 Microsoft Office 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 *MsBlast* (по данным Microsoft - более 16 млн систем), *Sasser и Mydoom* (оценочные ущербы 500 млн и 4 млрд долл. соответственно).

Самый современный вид вирусов  - черви-[ботнеты](http://www.google.com/url?q=http%3A%2F%2Fru.wikipedia.org%2Fwiki%2F%25D0%2591%25D0%25BE%25D1%2582%25D0%25BD%25D0%25B5%25D1%2582&sa=D&sntz=1&usg=AFQjCNFftkQWktWxYGEbTuwAwq1JB3LRAw) 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.

1. **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 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 эксплоитом, использующим уязвимость.

1. **Способы распространения компьютерных вирусов**

Способы распространения компьютерных вирусов разнообразны, однако существуют все же наиболее распространенные, от которых можно уберечься, соблюдая элементарные меры предосторожности.

***Дискеты.*** Самый распространённый канал заражения в 1980-1990-е годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.

***Флеш-накопители (флешки).*** В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, портативные цифровые плееры, а с 2000-х годов всё большую роль играют мобильные телефоны, особенно смартфоны (появились мобильные вирусы).

***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. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости в ПО владельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.

***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. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

Как видно, способов распространения компьютерных вирусов немало. Для предотвращения заражения необходимо соблюдать элементарные меры предосторожности:

* стараться использовать только проверенные ресурсы в сети Интернет;
* не скачивать сомнительные программы, а также не нажимать сомнительных картинок;
* при получении писем от неизвестного адресата, обращать внимание на расширение приложенных файлов. Если они имеют такие типы как:\*.bat,\*.vbs,\*.scr,\*.exe, то не стоит скачивать эти приложения, они могут быть заражены или попросту являются вирусом трояном;
* применять лицензионные антивирусы.

И тогда с легкостью можете избежать заражения.

1. **Признаки заражения вирусом**

При заражении компьютера вирусом важно его обнаружить, для этого следует знать основные признаки его проявления:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;

- медленная работа компьютера;

- невозможность загрузки операционной системы;

- исчезновение файлов и каталогов или искажение их содержимого;

- изменение даты и времени модификации файлов;

- изменение размера файлов;

- неожиданное значительное увеличение количества файлов на диске;

- существенное уменьшение размера свободной оперативной памяти;

- вывод на экран непредусмотренных сообщений или изображений;

- подача непредусмотренных звуковых сигналов;

- 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. Заразиться компьютерным вирусом можно только в определенных случаях:

- запуск на компьютере исполняемой программы, заражённой вирусом;

- загрузка компьютера с диска (дискеты), содержащего загрузочный вирус;

- подключение к системе заражённого драйвера;

- открытие документа, заражённого макровирусом;

- установка на компьютере заражённой операционной системы.

Компьютер не может быть заражён, если:

- на него переписывались текстовые и графические файлы (за исключением файлов, предусматривающих выполнение макрокоманд);

- на нём производилось копирование с одной дискеты на другую при условии, что ни один файл с дискет не запускался;

- на компьютере производится обработка принесённых извне текстовых и графических файлов, файлов данных и информационных файлов (за исключением файлов, предусматривающих выполнение макрокоманд);

**-**переписывание на компьютер заражённого вирусом файла ещё не означает заражения его вирусом. Чтобы заражение произошло нужно либо запустить заражённую программу, либо подключить заражённый драйвер, либо открыть заражённый документ (либо, естественно, загрузиться с заражённой дискеты). Иначе говоря, заразить свой компьютер можно только в том случае, если запустить на нём непроверенные программы и (или) программные продукты, установить непроверенные драйвера и (или) операционные системы, загрузиться с непроверенной системной дискеты или открыть непроверенные документы, подверженные заражению макровирусами.

**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. Загрузочные стелс-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 Microsoft Office могут содержать в себе небольшие программы для обработки этих документов, составленные на языке Visual Basicfor Applications. Это относится и к базам данных Access, а также к файлам презентаций Power Point. 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 Microsoft Office. 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 Lotus Notes и Microsoft Exchange, 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.

**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 программами. Для 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).

**2.2.4 Программы - фильтры (мониторы)**

Программы-фильтры (мониторы) или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

1. попытки коррекции файлов с расширениями COM, EXE

2. изменение атрибутов файла

3. прямая запись на диск по абсолютному адресу

4. запись в загрузочные сектора диска

5. загрузка резидентной программы.

**2.2.5 Вакцины или иммунизаторы**

Вакцины или иммунизаторы - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

**2.2.6 Сканер**

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти, а также поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски». Маской вируса является некоторая постоянная последовательность кода, специфичная для конкретного вируса. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы.

В настоящий момент существует множество антивирусных программ, однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

1. Не работать под привилегированными учётными записями без крайней необходимости.

2. Не запускать незнакомые программы из сомнительных источников.

3. Стараться блокировать возможность несанкционированного изменения системных файлов.

4. Отключать потенциально опасный функционал системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).

5. Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.

6. Пользоваться только доверенными дистрибутивами.

7. Постоянно делать резервные копии важных данных и иметь образ системы со всеми настройками для быстрого развёртывания.

8. Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

**3.3. Лицензионные антивирусные программы**

Выбор антивируса для домашнего пользования - актуальный вопрос, особенно для начинающих пользователей. Рано или поздно у любого возникает необходимость установки антивируса. Интересный факт, но многие пользователи вообще не устанавливают программ для защиты своего компьютера. Не устанавливают, пока не возникают различные сбои в работе системы. И действительно, при заражении компьютера вирусами замедляется работа системы, компьютер "тормозит" или "подвисает". В худшем же случае троянские программы могут похитить пароли и личную информацию. Как выбрать домашний антивирус, чтобы обезопасить себя от неприятностей попробуем разобраться.

Различные фирмы-производители программных продуктов, целенаправленно занимающиеся компьютерной и информационной безопасностью предлагают сегодня большой выбор антивирусных программ.

Приобретение лицензионной антивирусной программы обеспечит относительно надежную защиту данных от несанкционированного доступа и использования компьютера во вредоносных целях.

Ниже представлены наиболее популярные лицензионные антивирусные программы, которые можно приобрести, в т.ч и через Интернет.

**Антивирус Касперского -**обеспечивает защиту в реальном времени от вирусов, червей, троянских коней, руткитов, adware, шпионских программ в том числе и неизвестных угроз используя проактивную защиту, которая включает HIPS-компоненты, в том числе, имеются версии для мобильных устройств (18 версий).

[**Eset NOD32**](http://www.google.com/url?q=http%3A%2F%2Fabisoft.ru%2F1%2Fcid%2F2724%2FEset_NOD32.html&sa=D&sntz=1&usg=AFQjCNE2uqyHhbhJpIjPnMkItnAdFtYSZw)**-**представляет полную защиту компьютера. Комплексная защита компьютера функционирует в реальном времени и обеспечивает надежную защиту от вирусов и вредоносных программ, а так же других угроз, таких как фишинг-атаки, черви, spyware, adware и другие.Отличительной особенностью является экономичное использование ресурсов и высокая скорость исполнения (31 версия)

[**Norton (Symantec)**](http://www.google.com/url?q=http%3A%2F%2Fabisoft.ru%2F1%2Fcid%2F2725%2FNorton_(Symantec).html&sa=D&sntz=1&usg=AFQjCNFkQx_LtYwV07jqQyQUpkrnVcqv9Q)**-**базовая антивирусная защита, блокирующая вирусы и программы-шпионы и позволяющая безопасно работать в Интернете и обмениваться информацией (10 версий).

**Доктор Веб -**базовая антивирусная защита, блокирующая вирусы и программы-шпионы и позволяющая безопасно работать в Интернете и обмениваться информацией (45 различных версий).

**Avira -**AAviraAntivirusPremium - защита от вирусов для персональных компьютеров, работающих под управлением ОС Windows (18 версий)

[**Аvast! -**](http://www.google.com/url?q=http%3A%2F%2Fabisoft.ru%2F1%2Fcid%2F2801%2Favast!.html&sa=D&sntz=1&usg=AFQjCNHYzQuxKFLLPCjFwPHBISyrZiM8Jw)это более эффективная защита во время просмотра страниц Интернета, полнофункциональная антивирусная программа [(23 версии)](http://www.google.com/url?q=http%3A%2F%2Fabisoft.ru%2F1%2Fcid%2F2801%2Favast!.html&sa=D&sntz=1&usg=AFQjCNHYzQuxKFLLPCjFwPHBISyrZiM8Jw).

**TrendMicro —**обновления в режиме реального времени**,** защита от новейших веб-угроз сейчас и в будущем(11 версий).

[**AVG**(24 версии)](http://www.google.com/url?q=http%3A%2F%2Fabisoft.ru%2F1%2Fcid%2F2878%2FAVG.html&sa=D&sntz=1&usg=AFQjCNHeOSBZXAA38BgiytUHabCnR3clWA).

[**McAfee -**](http://www.google.com/url?q=http%3A%2F%2Fabisoft.ru%2F1%2Fcid%2F2891%2FMcAfee.html&sa=D&sntz=1&usg=AFQjCNHTMrPLBb_WTIJEZKj4O04pVJoebg) эффективная защита от вирусов, шпионских и вредоносных программ. Защитное ПО постоянно сканирует и блокирует опасные электронные сообщения, содержимое опасных веб-страниц (3 версии).

**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 **Bit Defender Free Edition** - программа, которая поможет защитить систему, периодически проводя проверки и сканирование. При работе антивирус использует те же сертифицированные технологии обнаружения, что и платные продукты от Bit Defender.

A**VG Anti-Virus Free Edition 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 Social Networking Protection.

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

**Avira Free Antivirus** 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).

**Bit Defender Free Edition -**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 Bit Defender.

Антивирус от **Microsoft** под названием **Security Essentials** 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.

**Rising Antivirus Free Edition** 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.

**Panda Cloud Antivirus** это возможность использовать передовую защиту от Панда, 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**.

**3.5. Лучший антивирус для нетбука**

При подборе антивируса для нетбука весьма актуально изучить различные аспекты антивирусных программ, такие как скорость сканирования, ресурсоёмкость, самозащита, эффективность лечения и так далее. Не последним фактором, который может повлиять на выбор, выступает скорость реагирования разработчиков антивирусов на появление новых образцов вредоносов и внесение их в базу данных. Вышеописанные программы полностью удовлетворяют поставленным критериям. Можно остановиться на следующих антивирусах:

* бесплатный **Avira Free Antivirus**
* бесплатный **Panda Cloud Antivirus**
* платный с демо версией **ESET NOD32 Антивирус**

Можно смело скачать антивирус для нетбука бесплатно в сети Интернет без регистрации, сравнить и выбрать наиболее удобный.

**Заключение**

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.

Антивирусное обеспечение и проблема удаления вирусов играет всё большую роль, т.к. количество вирусов и вирусописателей постоянно увеличивается, а в следствии этого возрастает процент вероятности заражения вирусом, т.е. возникает постоянная необходимость в профилактике компьютера от вирусов, удаления вирусов. Следует также помнить, что вирус можно «подцепить» всего лишь несколькими способами, в любом случае, он должен быть запущен, т.е. внесен тем или иным способом в систему, т.е. должно быть запущено соответствующее приложение на вашем компьютере, т.е. , открыв картинку очень сложно, почти невозможно получить вирус, тоже относится и к музыкальным файлам и другим аналогиям, doc, exl. От того как вирус внесен и что он сделает в компьютере и будут предприняты все дальнейшие шаги по удалению вирусов. Естественно он может быть внесен вне зависимости от желания владельца компьютера, через те или иные уязвимости браузеров, уязвимостей операционной системы, для подобных вещей существуют фаерволы, которые судя по названию, являются нечто вроде блокирующей стены, отслеживающие исходящие и входящие потоки данных. Но для удаления вирусов фаервол не подходит.

Имея в своем наличие наиболее удобный и четко настроенный антивирус, возможность заражения всегда остается, т.к. антивирусы, обладают лишь базой вирусов, и если кто-то напишет вирус, только под Вас, то антивирус его не определит и даст спокойно запустить, поэтому вопрос ручного удаления вирусов всегда актуален. Антивирусы нужны лишь для отсечения большого количества вирусов , гуляющих по сети, опасность потери данных с такими вирусами невелика, однако велика вероятность испортить операционную систему, сильно её затормозить и вывести её из строя и простое удаление вируса уже не поможет, необходимо будет реанемировать пострадавшую машину. Вирусов огромное количество видов, и сказать точно, что делает тот или иной невозможно, шаги по удалению вирусов принимаются по каждому индивидуально.

**Литература:**

1. БезруковН.Н. "Классификация компьютерных вирусов MS-DOS и методы защиты от них", Москва, СП "ICE", 1990 г.
2. Алексеев А.П. «Информатика», изд. «Солон», 2002 г.
3. Острейковский В.А. «Информатика», изд. «Высшая школа», 2001 г.
4. Денисов Т.В. "Антивирусная защита"//Мой Компьютер-№4-1999 г.
5. http://www.ctc.msiu.ru/materials/Book1/contents.html