Курсовая работа

**«Сравнительный анализ современных антивирусных программ»**

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

ГЛАВА 1. Общие сведения о компьютерных вирусах

1.1 Понятие компьютерные вирусы

1.2 Разновидности компьютерных вирусов

1.3 Пути проникновения вирусов, признаки появления в компьютере

1.4 Антивирусные средства

ГЛАВА 2. Сравнительный анализ антивирусных программ

ЗАКЛЮЧЕНИЕ

Список использованных источников

**Введение**

Мы живем на стыке двух тысячелетий, когда человечество вступило в эпоху новой научно-технической революции. К концу двадцатого века люди овладели многими тайнами превращения вещества и энергии и сумели использовать эти знания для улучшения своей жизни. Но кроме вещества и энергии в жизни человека огромную роль играет еще одна составляющая - информация. Это самые разнообразные сведения, сообщения, известия, знания, умения. В середине нашего столетия появились специальные устройства - компьютеры, ориентированные на хранение и преобразование информации и произошла компьютерная революция. В связи со стремительным развитием информационных технологий и их проникновением во все сферы человеческой деятельности возросло количество преступлений, направленных против информационной безопасности. 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. 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.

С каждым днем вирусы становятся все более изощренными, что приводит к существенному изменению профиля угроз. Но и рынок антивирусного программного обеспечения не стоит на месте, предлагая множество, казалось бы, идентичных продуктов. Их пользователи, представляя проблему лишь в общих чертах, нередко упускают важные нюансы и в итоге получают иллюзию защиты вместо самой защиты.

Для написания курсовой работы были использованы следующие источники: Безруков Н.Н. «Компьютерные вирусы», Мостовой Д.Ю. "Современные технологии борьбы с вирусами», Могилев А.В. «Информатика: учебное пособие для студентов педагогических вузов». В учебном пособии Могилева содержатся обширные сведения по теоретическим основам информатики, программному обеспечению, языкам и методам программирования, вычислительной технике, информационным системам, компьютерным сетям и телекоммуникациям, компьютерному моделированию. Ясно и доступно рассказано о различных компьютерных вирусах, их разновидностях и средствах борьбы с ними.

На основеизученной литературы попробуем разобраться в том, что же надо защищать, как это сделать и на что следует обратить особое внимание.

**ГЛАВА 1. ОБЩИЕ СВЕДЕНИЯ О КОМПЬЮТЕРНЫХ ВИРУСАХ**

**1.1 Понятие компьютерные вирусы.**

Компьютерным вирусом называется программа, обычно малая по размеру (от 200 до 5000 байт), которая самостоятельно запускается, многократно копирует свой код, присоединяя его к кодам других программ («размножается») и мешает корректной работе компьютера и/или разрушает хранимую на магнитных дисках информацию (программы и данные).

Существуют вирусы и менее «злокачественные», вызывающие, например, переустановку даты в компьютере, музыкальные (проигрывающие какую-либо мелодию), приводящие к появлению на экране дисплея какого-либо изображения или к искажениям в отображении дисплеем информации, «осыпанию букв» и т.д.

Создание компьютерных вирусов можно квалифицировать с юридической точки зрения как преступление.

Интересны причины, заставляющие квалифицированных программистов создавать компьютерные вирусы, ведь это работа не оплачивается и не может принести известности. По-видимому, для создателей вирусов это способ самоутверждения, способ доказать свою квалификацию и способности. Созданием компьютерных вирусов занимаются квалифицированные программисты, по тем или иным причинам не нашедшие себе место в полезной деятельности, в разработке прикладных программ, страдающие болезненными самомнением или комплексом неполноценности. Становятся создателями вирусов и те молодые программисты, которые испытывают трудности в общении с окружающими людьми, не встречают признания со стороны специалистов, которым чужды понятие морали и этики компьютерной сферы деятельности. Также созданием вирусов могут заниматься сами производители антивирусных программ в целях наживы. Создав новый вирус или модифицировав старый, производители незамедлительно выпускают антивирусные средства для борьбы с ними, обгоняя тем самым своих конкурентов.

Существуют и такие специалисты, которые отдают свои силы и талант делу борьбы с компьютерными вирусами. В России – это известные программисты Д.Лозинский, Д.Мостовой, И.А.Данилов, Н.Безруков и др. Ими исследованы многие компьютерные вирусы, разработаны антивирусные программы, рекомендации по мерам, предотвращающим уничтожение вирусами компьютерной информации и распространение эпидемий компьютерных вирусов.

Главную опасность, по их мнению, представляют не сами по себе компьютерные вирусы, а пользователи компьютеров и компьютерных программ, не подготовленные к встрече с вирусами, ведущие себя неквалифицированно при встрече с симптомами заражения компьютера, легко впадающие в панику, что парализует нормальную работу.

**1.2 Разновидности компьютерных вирусов**

Рассмотрим подробнее основные особенности компьютерных вирусов, характеристики антивирусных программ и меры защиты программ и данных от компьютерных вирусов в наиболее распространенной системе MS DOS.

По приближенным оценкам в сегодняшние дни существует более десяти тысяч различных вирусов. Подсчет их осложняется тем, что многие вирусы мало отличаются друг от друга, являются вариантами одного и того же вируса и, наоборот, один и тот же вирус может менять свой облик, кодировать сам себя. На самом деле основных принципиальных идей, лежащих в основе вирусов, не очень много (несколько десятков).

Среди всего разнообразия компьютерных вирусов следует выделить следующие группы:

**- загрузочные (**boot**) вирусы** заражают программу начальной загрузки компьютера, хранящуюся в загрузочном секторе дискеты или винчестера, и запускающиеся при загрузке компьютера;

**- файловые вирусы**  в простейшем случае заражают пополняемые файлы, но могут распространяться и через файлы документов (системы Word for Windows) и даже вообще не модифицировать файлы, а лишь иметь к ним какое-то отношение;

**- загрузочно-файловые вирусы** имеют признаки как загрузочных, так и файловых вирусов;

- **драйверные вирусы** заражаютдрайверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки.

Из вирусов, функционирующих не на персональных компьютерах под операционной системой MS DOS, следует упомянуть **сетевые вирусы**, распространяющиеся в сетях, объединяющих многие десятки и сотни тысяч компьютеров.

Рассмотрим принципы функционирования **загрузочных вирусов.** На каждой дискете или винчестере имеются служебные сектора, используемые операционной системой для собственных нужд, в том числе сектор начальной загрузки. В нем помимо информации о дискете (число дорожек, число секторов и пр.) хранится небольшая программа начальной загрузки.

Простейшие загрузочные вирусы, резидентно находясь в памяти зараженного компьютера, обнаруживают в дисководе незараженную дискету и производят следующие действия:

- выделяют некоторую область дискеты и делают ее недоступной операционной системе (помечая, например, как сбойную - bad);

- замещают программу начальной загрузки в загрузочном секторе дискеты, копируя корректную программу загрузки, а также свой код, в выделенную область дискеты;

- организуют передачу управления так, чтобы вначале выполнялся бы код вируса и лишь затем – программа начальной загрузки.

Магнитные диски компьютеров винчестерского типа обычно бывают разбиты на несколько логических разделов. Программы начальной загрузки при этом имеются и в MBR (Master Boot Record – главная загрузочная запись) и в загрузочном разделе винчестера, заражение которых может происходить аналогично заражению загрузочного сектора дискеты. Однако, программа начальной загрузки в MBR использует при переходе к программе загрузки загрузочного раздела винчестера, так называемую таблицу разбиения (Partition table), содержащую информацию о положении загрузочного раздела на диске. Вирус может исказить информацию Partition table и таким образом передать управление своему коду, записанному на диск, формально не меняя загрузочной программы.

Теперь рассмотрим принципы функционирования **файловых вирусов**. Файловый вирус не обязательно является резидентным, он может, например, внедриться в код исполняемого файла. При запуске зараженного файла вирус получает управление, выполняет некоторые действия и возвращает управление коду, в который он был внедрен. Действия, которые выполняет вирус, включает поиск подходящего для заражения файла, внедрение в него так, чтобы получить управление файла, произведение некоторого эффекта, например, звукового или графического. Если файловый вирус резидентный, то он устанавливается в памяти и получает возможность заражать файлы и проявляться независимо от первоначального зараженного файла.

Заражая файл, вирус всегда изменит его код, но далеко не всегда производит другие изменения. В частности, может не изменяться начало файла и его длина (что раньше считалось признаком заражения). Например, вирусы могут искажать информацию о файлах, хранящуюся в служебной области магнитных дисков – таблице размещения файлов (Fat – file allocation table), - делать таким образом невозможным любую работу с файлами. Так ведут себя вирусы семейства «Dir».

**Загрузочно-файловые** вирусы используют принципы как загрузочных, так и файловых вирусов, и являются наиболее опасными.

**«Троянские кони», программные закладки и сетевые черви.**
 «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. Вирусы могут нести в себе троянских коней или "троянизировать" другие программы - вносить в них разрушающие функции. «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. Программные закладки также содержат некоторую функцию, наносящую ущерб вычислительной системе, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать. Если вирусы и «Троянские кони» наносят ущерб посредством лавинообразного саморазмножения или явного разрушения, то основная функция вирусов типа "червь", действующих в компьютерных сетях, - взлом атакуемой системы, т.е. преодоление защиты с целью нарушения безопасности и целостности. В более 80% компьютерных преступлений, расследуемых ФБР, "взломщики" проникают в атакуемую систему через глобальную сеть Internet. Когда такая попытка удается, будущее компании, на создание которой ушли годы, может быть поставлено под угрозу за какие-то секунды. Этот процесс может быть автоматизирован с помощью вируса, называемого сетевой червь. 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 миллионов компьютеров, подключенных к этой сети.

### 1.3 Пути проникновения вируса в компьютер

Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода А и перезагрузили компьютер, при этом дискета может быть и не системной. Заразить дискету гораздо проще. На нее вирус может попасть, даже если дискету просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление. Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус, прежде всего, переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов.
Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы. После заражения программы вирус может выполнить какую-нибудь диверсию, не слишком серьезную, чтобы не привлечь внимания. И, наконец, не забывает возвратить управление той программе, из которой был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом, заразится все программное обеспечение.

### 1.4 Признаки появления вируса

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие: прекращение работы или неправильная работа ранее успешно функционировавших программ

* медленная работа компьютера
* исчезновение файлов и каталогов или искажение их содержимого
* изменение даты и времени модификации файлов
* изменение размеров 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.

**1.4 Антивирусные средства**

К настоящему времени накоплен значительный опыт борьбы с компьютерными вирусами, разработаны антивирусные программы, известны меры защиты программ и данных. Происходит постоянное совершенствование, развитие антивирусных средств, которые в короткий срок с момента обнаружения вируса – от недели до месяца – оказываются способными справиться с вновь появляющимися вирусами.

Создание антивирусных программ начинается с обнаружения вируса по аномалиям в работе компьютера. После этого вирус тщательно изучается, выделяется его сигнатура – последовательность байтов, которая полностью характеризует программу вируса (наиболее важные и характерные участки кода), выясняется механизм работы вируса, способы заражения. Полученная информация позволяет разработать способы обнаружения вируса в памяти компьютера и на магнитных дисках, а также алгоритмы обезвреживания вируса (если возможно, удаления вирусного кода из файлов – «лечения»).

Известные ныне антивирусные программы можно разделить на несколько типов:

- **Детекторы.** Их назначение – лишь обнаружить вирус. Детекторы вирусов могут сравнивать загрузочные сектора дискет с известными загрузочными секторами, формируемыми операционными системами различных версий, и таким образом обнаружить загрузочные вирусы или выполнять сканирование файлов на магнитных дисках с целью обнаружения сигнатур известных вирусов. Такие программы в чистом виде в настоящее время редки.

- **Фаги.** Фаг – это программа, которая способна не только обнаружить, но и уничтожить вирус, т.е. удалить его код из зараженных программ и восстановить их работоспособность (если возможно). Известнейшим в России фагом является Aidstest, созданный Д.Н.Лозинским. Одна из последних версий обнаруживает более 8000 вирусов. Aidstest для своего нормального функционирования требует, чтобы в памяти не было резидентных антивирусов, блокирующих запись в программные файлы, поэтому их следует выгрузить, либо, указав опцию выгрузки самой резидентной программе, либо воспользоваться соответствующей утилитой.

Очень мощным и эффективным антивирусом является фаг Dr Web (созданный И.Даниловым). Детектор этого фага не просто сканирует файлы в поисках одной из известных вирусных сигнатур. Для нахождения вирусов Dr Web использует программу эмуляцию процессора, т.е. он моделирует выполнение остальных файлов с помощью программной модели микропроцессора I-8086 и тем самым создает среду для проявления вирусов и их размножения. Таким образом, программа Dr Web может бороться не только с полиморфными вирусами, но и вирусам, которые только еще могут появиться в перспективе.

Основными функциональными особенностями Dr Web 4.33 являются:

* защита от червей, вирусов, троянов, полиморфных вирусов, макровирусов, spyware, программ-дозвонщиков, adware, хакерских утилит и вредоносных скриптов;
* обновление антивирусных баз до нескольких раз в час, размер каждого обновления до 15 KB;
* проверка системной памяти компьютера, позволяющая обнаружить вирусы, не существующие в виде файлов (например, CodeRed или Slammer);
* эвристический анализатор, позволяющий обезвредить неизвестные угрозы до выхода соответствующих обновлений вирусных баз.

**Установка.** Вначале Dr Web честно предупреждает, что не собирается уживаться с другими антивирусными приложениями и просит убедиться в отсутствии таковых на компьютере. В противном случае совместная работа может привести к "непредсказуемым последствиям". Далее выбирается "Выборочную" или "Обычную" (рекомендуемую) установку и приступают к изучению представленных основных компонентов:

* сканер для Windows**.** Проверка файлов в ручном режиме;
* консольный сканер для Windows. Предназначен для запуска из командных файлов;
* SpiDer Guard. Проверка файлов "на лету", предотвращение заражений в режиме реального времени;
* SpiDer Mail. Проверка сообщений, поступающих через протоколы POP3, SMTP, IMAP и NNTP.

**Интерфейс и работа.** В глаза бросается отсутствие согласованности в вопросе интерфейса между модулями антивируса, что создает дополнительный визуальный дискомфорт при и так не слишком дружелюбном доступе к компонентам Dr Web. Большое количество всевозможных настроек явно не рассчитано на начинающего пользователя, однако довольно подробная справка в доступной форме объяснит назначение тех или иных интересующих вас параметров. Доступ к центральному модулю Dr Web – сканер для Windows – осуществляется не через трей, а только через "Пуск".

Обновление доступно как через Интернет, так и с помощью прокси-серверов, что при небольших размерах сигнатур представляет Dr Web весьма привлекательным вариантом для средних и крупных компьютерных сетей.

Задать параметры проверки системы, порядок обновления и настройку условий работы каждого модуля Dr Web можно с помощью удобного инструмента "Планировщик", который позволяет создать слаженную систему защиты из "конструктора" компонентов Dr Web.

В итоге мы получаем нетребовательную к ресурсам компьютера, достаточно несложную (при ближайшем рассмотрении) целостную защиту компьютера от всевозможных угроз, чьи возможности по противодействию вредоносным приложениям однозначно перевешивают единственный недостаток, выраженный "разношерстным" интерфейсом модулей Dr Web.

- **Ревизоры.** Программа-ревизор контролирует возможные пути распространения программ-вирусов и заражения компьютеров. Программы-ревизоры относятся к самым надежным средствам защиты от вирусов и должны входить в арсенал каждого пользователя. Ревизоры являются единственным средством, позволяющим следить за целостностью и изменениями файлов и системных областей магнитных дисков. Наиболее известна в России программа-ревизор ADinf, разработанная Д.Мостовым.

- **Сторожа.** Сторож – это резидентная программа, постоянно находящаяся в памяти компьютера, контролирующая операции компьютера, связанная с изменением информации на магнитных дисках, и предупреждающая пользователя о них. В состав операционной системы MS DOS, начиная с версии 6.0, входит сторож VSAFE. Однако, из-за того, что обычные программы выполняют операции, похожие на те, что делают вирусы, пользователи обычно не используют сторожа, так как постоянные предупреждения мешают работе.

- С**канеры** – основной элемент любого антивируса, осуществляет, если можно так выразиться, пассивную защиту. По запросу пользователя или заданному распорядку производит проверку файлов в выбранной области системы. Вредоносные объекты выявляет путем поиска и сравнения программного кода вируса. Примеры программных кодов содержатся в заранее установленных сигнатурах (наборах, характерных последовательностей байтов для известных вирусов). В первую очередь к недостаткам данных программ относится беззащитность перед вирусами, не имеющими постоянного программного кода и способными видоизменяться при сохранении основных функций. Также сканеры не могут противостоять разновидностям одного и того же вируса, что требует от пользователя постоянного обновления антивирусных баз. Однако наиболее уязвимое место этого инструмента – неспособность обнаруживать новые и неизвестные вирусы, что особенно актуально, когда посредством e-mail новоявленная угроза способна заразить тысячи компьютеров по всему миру за считаные часы;

- **Мониторы** – в совокупности со сканерами образуют базовую защиту компьютера. На основе имеющихся сигнатур проводят проверку текущих процессов в режиме реального времени. Осуществляют предварительную проверку при попытке просмотра или запуска файла. Различают файловые мониторы, мониторы для почтовых клиентов (MS Outlook, Lotus Notes, Pegasus, The Bat и другие, использующие протоколы POP3, IMAP, NNTP и SMTP) и специальные мониторы для отдельных приложений. Как правило, последние представлены модулями проверки файлов Microsoft Office. Основное их достоинство – способность обнаруживать вирусы на самой ранней стадии активности;

- **Вакцины.** Так называются антивирусные программы, ведущие себя подобно вирусам, но не наносящие вреда. Вакцины предохраняют файлы от изменений и способны не только обнаружить факт заражения, но и в некоторых случаях «вылечить» пораженные вирусами файлы. В настоящее время антивирусные программы-вакцины широко не применяются, так как в прошлые годы некоторыми некорректно работающими вакцинами был нанесен ущерб многим пользователям.

Помимо программных средств защиты от вирусов существуют и специальные дополнительные устройства, обеспечивающие надежную защиту определенных разделов винчестера. Примером такого рода устройств является плата Sheriff (разработанная Ю.Фоминым). Несмотря на кажущееся обилие программных антивирусных средств, даже все вместе они не обеспечивают полной защиты программ и данных, не дают 100%-ной гарантии от воздействия вирусных программ. Только комплексные профилактические меры защиты обеспечивают надежную защиту от возможной потери информации. В комплекс таких мер входит:

- регулярное архивирование информации (создание резервных копий важных файлов и системных областей винчестера);

- избегание использования случайно полученных программ (старайтесь пользоваться только законными путями получения программ);

- входной контроль нового программного обеспечения, поступивших дискет;

- сегментация жесткого диска, т.е. разбиение его на логические разделы с разграничением доступа к ним;

- систематическое использование программ-ревизоров для контроля целостности информации;

- при поиске вирусов (который должен происходит регулярно!) старайтесь использовать заведомо чистую операционную систему, загруженную с дискеты. Защищайте дискеты от записи, если есть хоть малая вероятность заражения.

При неаккуратной работе с антивирусными программами можно не только переносить с ними вирусы, но и вместо лечения файлов безнадежно их испортить. Полезно иметь хотя бы общее представление о том, что могут и чего не могут компьютерные вирусы, об их жизненном цикле, о важнейших методах защиты.

Любой современный антивирусный продукт - это не только набор отдельных технологий детектирования, но и сложная система защиты, построенная на собственном понимании антивирусной компанией того, как нужно обеспечивать безопасность от вредоносных программ. При этом принятые многие годы назад архитектурные и технические решения серьезно ограничивают возможности изменять соотношение проактивных и реактивных методов защиты. Например, в антивирусной системе Eset NOD32 используются как эвристические, так и сигнатурные методы борьбы с вредоносным кодом, но роли между этими двумя технологиями распределяются не так, как в других антивирусах: в то время как большинство антивирусов отталкивается от сигнатурных методов, дополняя их эвристиками, у Eset NOD32 все наоборот. Основным способом противостояния вредоносным программам здесь являются так называемые расширенные эвристики (Advanced Heuristics), представляющие собой сочетание эмуляции, эвристик, алгоритмического анализа и сигнатурного метода. В итоге расширенные эвристики Eset NOD32 позволяют проактивно детектировать почти 90% всех угроз, а остальные устраняются сигнатурными методами. Надежность такого подхода подтверждается результатами независимых тестирований.

Основными функциональными особенностями Esest NOD32 являются:

* эвристический анализ, позволяющий обнаруживать неизвестные угрозы;
* технология ThreatSense – анализ файлов для выявления вирусов, программ-шпионов (spyware), непрошенной рекламы (adware), phishing-атак и других угроз;
* проверка и удаление вирусов из заблокированных для записей файлов (к примеру, защищенные системой безопасности Windows библиотеки DLL);
* поверка протоколов HTTP, POP3 и PMTP.

**Установка** предложена в трех режимах: "Типичный" (для большинства пользователей), "Расширенный" (частичная настройка устанавливаемых компонентов) и "Эксперт" (полностью настраиваемая установка). Сразу же предлагается указать, используете ли вы прокси-сервер, а также запрашиваются некоторые настройки будущих обновлений. Кроме того, NOD32 заранее интересуется, желаете ли вы использовать "двунаправленную систему своевременного обнаружения" – функция передачи лаборатории Eset подозрительных объектов, найденных на компьютере. Все компоненты защиты при желании будут предложены к установке с подробным описанием поэтапно.

Для защиты системы вниманию пользователя предложены следующие модули:

- Antivirus MONitor (AMON). Сканер, автоматически проверяющий файлы перед их запуском или просмотром;

- NOD32. Сканирование всего компьютера или выбранных разделов. Отличительная особенность – программирование на запуск в часы с наименьшей загрузкой;

- Internet MONitor (IMON). Резидентный сканер, проверяющий Интернет-трафик (HTTP) и входящую почту, полученную по протоколу POP3;

- Email MONitor (EMON). Модуль для работы с почтовыми клиентами, сканирует входящие и исходящие электронные сообщения через интерфейс MAPI (применяется в Microsoft Outlook и Microsoft Exchange);

- Document MONitor (DMON). Основан на использовании запатентованного интерфейса Microsoft API, проверяет документы Microsoft Office.

**Интерфейс и работа**. Пользователи домашних сетей сразу же мысленно сравнят интерфейс NOD32 с популярным сетевым сканером Netlook – антивирус использует схожую структуру доступа к компонентам. Интерфейс NOD32 организован максимально эргономично и эффективно. Основные пункты меню содержат подзаголовки, которые в свою очередь открывают справа от основного окна область работы с выбранным модулем или компонентом. Каждый подпункт (кроме сканера NOD32) предлагает подробнейшую настройку, которая подойдет скорее специалисту или администратору, нежели рядовому пользователю. Тем не менее, при желании разобраться во всех тонкостях модулей NOD32 вам будет предложена справка, наглядно демонстрирующая и объясняющая назначение настроек.

Обновление – одна из сильных сторон NOD32. Первоначально на выбор предложены целых 3 сервера с возможностью последующего добавления адресов. Также поддерживаются локальные обновления с сетевых ресурсов. Присутствует возможность создания дискет или CD с обновлениями. Обновление происходит каждые несколько часов.

Антивирус Касперского Personal.

Антивирус Касперского Personal предназначен для антивирусной защиты персональных компьютеров, работающих под управлением операционных систем Windows 98/ME, 2000/NT/XP, от всех известных видов вирусов, включая потенциально опасное программное обеспечение. Программа осуществляет постоянный контроль всех источников проникновения вирусов - электронной почты, интернета, дискет, компакт-дисков и т.д. Уникальная система эвристического анализа данных эффективно нейтрализует неизвестные вирусы. Можно выделить следующие варианты работы программы (они могут использоваться как отдельно, так и в совокупности):

* Постоянная защита компьютера - проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.
* Проверка компьютера по требованию - проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов. Такую проверку вы можете запускать самостоятельно или настроить ее регулярный автоматический запуск.

Антивирус Касперского Personal теперь не проверяет повторно те объекты, которые были проанализированы во время предыдущей проверки и с тех пор не изменились, не только при постоянной защите, но и при проверке по требованию. Такая организация работы заметно повышает скорость работы программы.

Программа создает надежный барьер на пути проникновения вирусов через электронную почту. Антивирус Касперского Personal автоматически осуществляет проверку и лечение всей входящей и исходящей почтовые корреспонденции по протоколам POP3 и SMTP и эффективно обнаруживает вирусы в почтовых базах.

Программа поддерживает более семисот форматов архивированных и сжатых файлов и обеспечивает автоматическую антивирусную проверку их содержимого, а также удаление вредоносного кода из архивных файлов формата ZIP, CAB, RAR, ARJ, LHA и ICE.

Простота настройки программы осуществляется за счет возможности выбора одного из трех предопределенных уровней***:*** Максимальная защита, Рекомендуемая защита и Максимальная скорость.

Обновления антивирусных баз осуществляется каждый час, при этом обеспечивается их гарантированная доставка при разрыве или смене соединений с интернетом.

В состав Антивируса Касперского включен специальный компонент, обеспечивающий защиту файловой системы компьютера от заражения, - Файловый Антивирус*.* Он запускается при старте операционной системы, постоянно находится в оперативной памяти компьютера и проверяет все открываемые, сохраняемые и запускаемые вами или программами файлы.

По умолчанию Файловый Антивирус проверяет ТОЛЬКО НОВЫЕ или ИЗМЕНЕННЫЕ ФАЙЛЫ, то есть файлы, которые добавились или изменились со времени последнего обращения к ним. Это возможно благодаря применению новых технологий iChecker и iSwift. Для реализации технологий используется таблица контрольных сумм файлов. Процесс проверки файла выполняется по следующему алгоритму:

1. Каждый файл, к которому происходит обращение пользователя или некоторой программы, перехватывается компонентом.
2. Файловый Антивирус проверяет наличие информации о перехваченном файле в базе iChecker и iSwift. Далее возможны следующие действия:
	* Если информации о перехваченном файле в базе нет, он подвергается детальной антивирусной проверке. Контрольная сумма проверенного файла фиксируется в базе.
	* Если информация о файле присутствует в базе, Файловый Антивирус сравнивает текущее состояние файла с его состоянием, зафиксированным в базе на момент предыдущей проверки. При полном совпадении информации файл передается пользователю для работы без проверки. Если файл каким-то образом изменился, он будет детально проверен, и новая информация о нем будет записана в базу.

Процесс проверки включает следующие действия:

1. Файл анализируется на присутствие вирусов. Распознавание вредоносных объектов происходит на основании сигнатур угроз, используемых в работе. Сигнатуры содержат описание всех известных на настоящий момент вредоносных программ, угроз, сетевых атак и способов их обезвреживания.
2. В результате анализа возможны следующие варианты поведения:
	1. Если в файле обнаружен вредоносный код, Файловый Антивирус блокирует файл, помещает его копию в резервное хранилище и пытается обезвредить файл. В результате успешного лечения файл становится доступным для работы, если же лечение произвести не удалось, файл удаляется.
	2. Если в файле обнаружен код, похожий на вредоносный, но стопроцентной гарантии этого нет, файл помещается в специальное хранилище - карантин.
	3. Если в файле не обнаружено вредоносного кода, он сразу же становится доступным для работы.

Помимо обеспечения защиты ваших данных программа обладает дополнительными сервисами, расширяющими возможности работы с Антивирусом Касперского.

В процессе работы программа помещает некоторые объекты в специальные хранилища. Цель, которая при этом преследуется, - обеспечить максимальную защиту данных с минимальными потерями.

* Резервное хранилище содержит копии объектов, которые были изменены или удалены в результате работы Антивируса Касперского. Если какой-либо объект содержал важную для вас информацию, которую не удалось полностью сохранить в процессе антивирусной обработки, вы всегда сможете восстановить объект из его резервной копии.
* Карантин содержит возможно зараженные объекты, которые не удалось обработать с помощью текущей версии сигнатур угроз.

Рекомендуется периодически просматривать списки объектов, возможно некоторые из них уже неактуальны, а некоторые можно восстановить.

Часть сервисов направлена на помощь в работе с программой, например:

* Сервис Служба технической поддержки обеспечивает всестороннюю помощь в работе с Антивирусом Касперского. Эксперты Лаборатории Касперского постарались включить все возможные способы обеспечения поддержки: on-line поддержка, форум вопросов и предложений от пользователей программы и т.д.
* Сервис уведомлений о событиях помогает настраивать оповещение пользователей о важных моментах в работе Антивируса Касперского. Это могут быть как события информационного характера, так и ошибки, которые требуют безотлагательного устранения, и знать о них крайне важно.
* Сервис самозащиты программы и ограничения доступа к работе с ней обеспечивает защиту собственных файлов программы от изменения и повреждения со стороны злоумышленников, запрещает внешнее управление сервисами программы, а также вводит разграничение прав других пользователей вашего компьютера на выполнение некоторых действий с Антивирусом Касперского. Например, изменение уровня защиты может значительно повлиять на безопасность информации на вашем компьютере.
* Сервис управления лицензионными ключами позволяет получать подробную информацию об используемой лицензии, производить активацию вашей копии программы, а также осуществлять управление файлами лицензионных ключей.

Создание диска аварийного восстановления позволит восстановить работоспособность компьютера на уровне, предшествующем заражению. Это особенно полезно в ситуации, когда после повреждения вредоносным кодом системных файлов невозможно произвести загрузку операционной системы компьютера.

Также предоставляется возможность изменять внешний вид Антивируса Касперского и настраивать параметры текущего интерфейса программы.

Антивирусная утилита AVZ.

Антивирусная утилита AVZ является инструментом для исследования и восстановления системы, и предназначена для автоматического или ручного поиска и удаления:

* SpyWare, AdvWare программ и модулей (это одно из основных назначений утилиты);
* Руткитов и вредоносных программ, маскирующих свои процессы
* Сетевых и почтовых червей;
* Троянских программ (включая все их разновидности, в частности Trojan-PSW, Trojan-Downloader, Trojan-Spy) и Backdoor (программ для скрытного удаленного управления компьютером);
* Троянских программ-звонилок (Dialer, Trojan.Dialer, Porn-Dialer);
* Клавиатурных шпионов и прочих программ, которые могут применяться для слежения за пользователем;

Утилита является прямым аналогом программ Trojan Hunter и LavaSoft Ad-aware 6. Первичной задачей программы является удаление AdWare, SpyWare и троянских программ.

Сразу следует отметить, что программы категорий SpyWare, AdWare по определению не являются вирусами или троянскими программами. Они шпионят за пользователем и загружают информацию и программный код на пораженный компьютер в основном из маркетинговых соображений (т.е. передаваемая информация не содержит критических данных – паролей, номеров кредитных карт и т.п., а загружаемая информация является рекламой или обновлениями). Однако очень часто грань между SpyWare и троянской программой достаточно условна и точная классификация затруднительна.

Особенностью программы AVZ является возможность настройки реакции программы на каждую из категорий вредоносных программы – например, можно задать режим уничтожения найденных вирусов и троянских программ, но заблокировать удаление AdWare.

Другой особенностью AVZ являются многочисленные эвристические проверки системы, не основанные на механизме поиска по сигнатурам – это поиск RootKit, клавиатурных шпионов, различных Backdoor по базе типовых портов TCP/UDP. Подобные методы поиска позволяют находить новые разновидности вредоносных программ.

Кроме типового для программ данного класса поиска файлов по сигнатурам в AVZ встроена база с цифровыми подписями десятков тысяч системных файлов. Применение данной базы позволяет уменьшить количество ложных срабатываний эвристики и позволяет решать ряд задач. В частности, в системе поиска файлов есть фильтр для исключения известных файлов из результатов поиска, в диспетчере запущенных процессов и настроек SPI производится цветовое выделение известных процессов, при добавлении файлов в карантин производится блокировка добавления известных AVZ безопасных файлов.

Как показывает практика, очень часто программа типа SpyWare может быть классифицирована как AdWare и наоборот (причины просты – целью шпионажа в большинстве случаев является целевая реклама). Для таких случаев в классификации введена обобщающая категория Spy, которая грубо может трактоваться как AdWare+SpyWare. Термин Spy переводится как «шпион», «тайный агент», «следить», «подглядывать». Этот термин достаточно хорошо подходит к программам подобного класса.

Ограничения программы:

1. Т.к. утилита направлена в первую очередь на борьбу с SpyWare и AdWare модулями, и в настоящий момент она не поддерживает проверку архивов некоторых типов, PE упаковщиков и документов. Для борьбы со SpyWare в этом просто нет надобности. Тем не менее, утилита совершенствуется и появление подобных функций планируется;

2. Утилита не лечит программы, зараженные компьютерными вирусами. Для качественного и корректного лечения зараженной программы необходимы специализированные антивирусы (например, антивирус Касперского, Dr Web и т.п.).

**ГЛАВА 2. СРАВНИТЕЛЬНЫЙ АНАЛИЗ АНТИВИРУСНЫХ ПРОГРАММ**

Для доказательства преимуществ своих продуктов разработчики антивирусов часто используют результаты независимых тестов. Одним из первых тестировать антивирусные продукты начал британский журнал Virus Bulletin, первые тесты, опубликованные на их сайте, относятся к далекому 1998 году. Основу теста составляет коллекция вредоносных программ WildList. Для успешного прохождения теста необходимо выявить все вирусы этой коллекции и продемонстрировать нулевой уровень ложных срабатываний на коллекции "чистых" файлов журнала. Тестирование проводится несколько раз в год на различных операционных системах; успешно прошедшие тест продукты получают награду VB100%. Результаты проведения теста представлены в таблице 1.

Таблица 1. «Результаты тестирования».

|  |  |  |  |
| --- | --- | --- | --- |
|  | Dr Web 4.33 | ЛабораторияКасперского | Eset NOD32 |
| **Количество успешно проведенных тестов VB100% за 2006-2007г** | **4** | **10** | **11** |
| **Общий уровень обнаружения вредоносного программного обеспечения** | **92.40%** | **98.88%** | **94.38%** |
| **Среднее время реакции на новые угроз, часы** | **6-8** | **0-2** | **4-6** |
| **Лечение активного заражения** | **82%** | **71%** | **18%** |
| **Занимаемая оперативная память в обычном режиме работы, кВ** | **8338** | **4500** | **29124** |
| **Время сканирования данных, мин.** | **79** | **28** | **23** |
| **Количество отсканированных данных**  | **133848** | **124914** | **123724** |
| **Усредненная по всем тестам рейтинг антивирусов (чем меньше, тем лучше)** | **7,83** | **2,25** | **4,75** |

По данным таблицы видно, что у одних антивирусов выигрышным оказывается один показатель, у других - другой. При этом естественно, что в своих рекламных материалах разработчики антивирусов делают упор только на те тесты, где их продукты занимают лидирующие позиции. Так, например, Лаборатория Касперского делает акцент на скорости реакции на появление новых угроз, Eset NOD32 - на силе своих эвристических технологий, Dr Web 4.33 описывает свои преимущества в лечении активного заражения.

Но что же делать пользователю, как сделать правильный выбор? Выбирая антивирус для своей системы, нужно убедиться, что он периодически завоевывает награду VB100%. Это гарантирует, что разработчики антивируса постоянно контролируют появление новых опасных вирусов, своевременно обновляют антивирусную базу данных и совершенствуют алгоритмы обнаружения вирусов. Понятно, что решение, которое выберет пользователь, должно быть сбалансированным и по большинству параметров должно входить в число лидеров по результатам

**ЗАКЛЮЧЕНИЕ**

В настоящее время компьютерные вирусы знакомы всем пользователям компьютерных систем. Актуальность проблемы антивирусной защиты объясняется следующими причинами:

лавинообразный рост числа компьютерных вирусов. В настоящее время число известных вирусов превысило за 256 000 (данные за 21 февраля 2007 г.) и продолжает интенсивно расти.

неудовлетворительное состояние антивирусной защиты в существующих корпоративных компьютерных сетях. Сегодня сети российских компаний находятся в постоянном развитии. Однако вместе с этим развитием постоянно растет и число точек проникновения вирусов в корпоративные сети. Как правило, такими точками являются шлюзы и серверы Интернета, серверы файл-приложений, серверы групповой работы и электронной почты, рабочие станции;

в последнее время получили распространение вирусы для мобильных устройств, включая телефоны, и для unix-подобных систем, на которых строятся корпоративные информационные сети.

Хорошая антивирусная программа должна:

Обеспечивать эффективную защиту в режиме реального времени. Резидентная часть (монитор) программы должна постоянно находиться в оперативной памяти вашего компьютера и производить проверку всех файловых операций (при создании, редактировании, копировании файлов, запуске их на исполнение), сообщений электронной почты, данных и программ, получаемых из интернета.

Позволять проверять все содержимое локальных дисков "по требованию", запуская проверку вручную или автоматически по расписанию.

Защищать ваш компьютер даже от неизвестных вирусов: программа должна включать в себя технологии поиска неизвестных вирусов, основанные на принципах эвристического анализа.

Уметь проверять и лечить архивированные файлы.

Давать возможность регулярно (ежедневно!) обновлять антивирусные базы (через Интернет, с дискет или CD - как вам удобнее).

И все-таки остается вопрос: «Какой антивирус выбрать?»

Вскоре после появления персональных компьютеров и начала массового распространения вирусов появилось огромное количество антивирусных программ. Сейчас в России используются главным образом две очень хорошие, проверенные, качественные антивирусные программы: Dr Web и Антивирус Касперского. Каждая из них имеет несколько разновидностей, ориентированных на разные сферы применения: для использования на домашних компьютерах, для малого и среднего бизнеса, для крупных корпоративных клиентов, для защиты локальных сетей, для почтовых, файловых серверов, серверов приложений. Обе эти программы, безусловно, отвечают всем вышеперечисленным требованиям. Замечены за ними обеими и некоторые недостатки, в частности, частенько конфликтуют с некоторыми запускаемыми из-под Windows MSDOS-приложениями.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Безруков Н.Н. Классификация компьютерных вирусов MS-DOS и методы защиты от них/ Н.Н. Безруков. – М.: СП "ICE", 1990
2. Безруков Н.Н. Компьютерные вирусы/ Н.Н. Безруков. - М.: Наука, 1991.
3. Денисов Т.В. Антивирусная защита//Мой Компьютер-№4-1999г.
4. Могилев А.В. Информатика: учебное пособие для студ. пед. вузов / А.В.Могилев Н.И.Пак, Е.К.Хеннер; Под ред. Е.К.Хеннера. – М.: Изд. Центр «Академия», 2000.-816с.