АГЕНТСТВО ПО УПРАВЛЕНИЮ ГОСУДАРСТВЕННЫМИ УЧРЕЖДЕНИЯМИ ПЕРМСКОГО КРАЯ

ГОУ СПО «ПЕРМСКИЙ РАДИОТЕХНИЧЕСКИЙ КОЛЛЕДЖ

им А. С. ПОПОВА»

Письменная экзаменационная работа

На тему

Защита персонального компьютера, выбор антивируса и брандмауэра

Выполнил: Кудрявцев С.В.

Группа:рв-07-05

Профессия :Радио механик по обслуживанию

и ремонту вычислительной техники

Пермь.2009г

Содержание

# Введение

# 1 Защита персонального компьютера

# 2 Выбор антивируса

# 2.1 Классификация вредоносного ПО

# 2.2 Классификация антивирусных программ

# 2.3 NOD32

# 2.4 Doctor Web

# 2.4 Avira AntiVir Personal

# 2.5 Kaspersky Antivirus

# 2.6 Тест антивирусов

# 3 Выбор брандмауэра

# 3.1 Брандмауэр Windows

# 3.2 Tools Firewall Plus

# 3.3 Comodo Firewall Pro 3.0.25.378

# 3.4 Ashampoo Firewall

# 3.5 Тест брандмауэров

# 4 Заключение

# Список используемых источников

# Введение

Защита информации в компьютерных системах - слагаемые успеха. Прогресс подарил человечеству великое множество достижений, но тот же прогресс породил и массу проблем. Человеческий разум, разрешая одни проблемы, непременно сталкивается при этом с другими, новыми, и этот процесс обречен на бесконечность в своей последовательности. Хотя, если уж быть точным, новые проблемы - это всего лишь обновленная форма старых. Вечная проблема - защита информации. На различных этапах своего развития человечество решало эту проблему с присущей для данной эпохи характерностью. Изобретение компьютера и дальнейшее бурное развитие информационных технологий во второй половине 20 века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества. Главная тенденция, характеризующая развитие современных информационных технологий - рост числа компьютерных преступлений и связанных с ними хищений конфиденциальной и иной информации, а также материальных потерь. По результатам одного исследования, посвященного вопросам компьютерных преступлений, около 58% опрошенных пострадали от компьютерных взломов за последние 12 месяцев. Примерно 18 % опрошенных из этого числа заявляют, что потеряли более миллиона долларов в ходе нападений, более 66 процентов потерпели убытки в размере 50 тыс. долларов. Свыше 22% атак были нацелены на промышленные секреты или документы, представляющие интерес прежде всего для конкурентов. Сегодня, наверное, никто не сможет с уверенностью назвать точную цифру суммарных потерь от компьютерных преступлений, связанных с несанкционированных доступом к информации. Это объясняется, прежде всего, нежеланием пострадавших компаний обнародовать информацию о своих потерях, а также тем, что не всегда потери от хищения информации можно точно оценить в денежном эквиваленте. Причин активизации компьютерных преступлений и связанных с ними финансовых потерь достаточно много, существенными из них являются: переход от традиционной "бумажной" технологии хранения и передачи сведений на электронную и недостаточное при этом развитие технологии защиты информации в таких технологиях; объединение вычислительных систем, создание глобальных сетей и расширение доступа к информационным ресурсам; увеличение сложности программных средств и связанное с этим уменьшение числа их надежности и увеличением уязвимостей.

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

Все чаще в средствах массовой информации появляются сообщения о различного рода пиратских проделках компьютерных хулиганов, о появлении все более совершенных, саморазмножающихся программ. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

# 1 Защита персонального компьютера

Особенности защиты персональных компьютеров (ПК) обусловлены спецификой их использования. Как правило, ПК пользуется ограниченное число пользователей. ПК могут работать как в автономном режиме, так и в составе локальных сетей (сопряженными с другими ПК) и могут быть подключены к удаленному ПК или локальной сети с помощью модема по телефонной линии.

Стандартность архитектурных принципов построения, оборудования и программного обеспечения персональных компьютеров, высокая мобильность программного обеспечения и ряд других признаков определяют сравнительно легкий доступ профессионала к информации, находящейся в ПК. Если персональным компьютером пользуется группа пользователей, то может возникнуть необходимость в ограничении доступа к информации различных потребителей.

Несанкционированным доступом (НСД) к информации ПК будем называть незапланированное ознакомление, обработку, копирование, применение различных вирусов, в том числе разрушающих программные продукты, а также модификацию или уничтожение информации в нарушение установленных правил разграничения доступа. В защите информации ПК от НСД можно выделить три основных направления:

- первое ориентируется на недопущение нарушителя к вычислительной среде и основывается на специальных технических средствах опознавания пользователя;

- второе связано с защитой вычислительной среды и основывается на создании специального программного обеспечения по защите информации;

- третье направление связано с использованием специальных средств защиты информации ПК от несанкционированного доступа.

Возможность использования персональных компьютеров в локальных сетях (при сопряжении их с другими ПК) или применение модемов для обмена информацией по телефонным проводам предъявляет более жесткие требования к программному обеспечению по защите информации ПК. Потребители ПК в различных организациях для обмена информацией все шире используют электронную почту, которая без дополнительных средств защиты может стать достоянием посторонних лиц. Самой надежной защитой от несанкционированного доступа к передаваемой информации и программным продуктам ПК является применение различных методов шифрования (криптографических методов защиты информации).

Для защиты персональных компьютеров используются различные программные методы, которые значительно расширяют возможности по обеспечению безопасности хранящейся информации. Среди стандартных защитных средств персонального компьютера наибольшее распространение получили:

-средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;

-применение различных методов шифрования, не зависящих от контекста информации;

-средства защиты от копирования коммерческих программных продуктов;

- защита от компьютерных вирусов и создание архивов.

- использование специальных программ

- резервное копирование информации.

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

Что угрожает информационной безопасности? Есть несколько факторов: действия, осуществляемые авторизованными пользователями; «электронные» методы воздействия, осуществляемые хакерами; спам; «естественные» угрозы. Но более подробно в работе рассматривается такая угроза как компьютерные вирусы.

Борьбой с компьютерными вирусами профессионально занимаются сотни или тысячи специалистов в десятках, а может быть, сотнях компаний. Казалось бы, тема эта не настолько сложна и актуальна, чтобы быть объектом такого пристального внимания. Однако это не так. Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. Несмотря на огромные усилия конкурирующих между собой антивирусных фирм, убытки, приносимые компьютерными вирусами, не падают и достигают астрономических величин в сотни миллионов долларов ежегодно. Эти оценки явно занижены, поскольку известно становится лишь о части подобных инцидентов.

При этом следует иметь в виду, что антивирусные программы и «железо» не дают полной гарантии защиты от вирусов. Случается так, что пользователи и профессионалы-программисты часто не имеют даже навыков «самообороны», а их представления о вирусе порой являются настолько поверхностными, что лучше бы их представлений и не было.

#

# 2 Выбор антивируса

Тема безопасности в Интернете, несмотря на многообещающие заявления разработчиков современных операционных систем, в последние годы ничуть не утратила своей актуальности. Сегодня мы являемся свидетелями (а порой - и жертвами) бесконечных вирусных эпидемий, с завидным постоянством вспыхивающих на просторах Всемирной Сети, немалые убытки от которых несут не только крупные компании, для которых даже несколько часов простоя оборачиваются многомиллионными потерями, но и мы с вами - обыкновенные пользователи. Ведь среди компьютерных вирусов встречаются не только сравнительно безобидные программки, весь вред от которых сводится к захламлению дискового пространства, но и весьма "зловредные" утилиты, способные уничтожить данные на жестком диске или воровать пароли и другую конфиденциальную информацию. Впрочем, ничуть не меньшие убытки, чем потеря данных, приносит и панический страх пользователей перед самой возможностью заражения, выливающийся в настоящую вирусную истерию. В настоящее время существует большой выбор антивирусных пакетов от разных производителей, однако наибольшей популярностью среди них (по крайней мере, в нашей стране) пользуются известные "гранды" антивирусной отрасли, такие, как "Антивирус Касперского", Dr.Web, NOD32 или Norton Antivirus. Все они имеют огромные армии, как поклонников, так и противников, ведущих нескончаемую "религиозную" войну и друг с другом, и со всем остальным миром.

##

## 2.1 Классификация вредоносного ПО

* Вирусы и черви

Подобные вредоносные программы обладают способностью к несанкционированному пользователем саморазмножению в компьютерах или компьютерных сетях, при этом полученные копии также обладают этой возможностью.

К вирусам и червям не относятся:

троянские программы, распространяющие свои копии по сети и заражающие удалённые машины по команде «хозяина» вредоносной программы (целый ряд представителей Backdoor);

прочие троянские программы, создающие свои многочисленные копии в системе или даже «цепляющиеся» к каким-либо файлам, уже присутствующим в системе. Отличие от вирусов и червей состоит в невозможности дальнейшего самовоспроизведения копий.

Основным признаком, по которому различают типы (поведения) вирусов и червей, является способ их распространения, т.е. как вредоносная программа передает свою копию по локальным или сетевым ресурсам.

* Троянские программы

Эти вредоносные программы созданы для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители данной категории не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения.

Основным признаком, по которому различают типы троянских программ, являются их несанкционированные пользователем действия — те, которые они производят на заражённом компьютере.

* Вредоносные утилиты

Вредоносные программы, разработанные для автоматизации создания других вирусов, червей или троянских программ, организации DoS-атак на удаленные сервера, взлома других компьютеров и т.п. В отличие от вирусов, червей и троянских программ, представители данной категории не представляют угрозы компьютеру, на котором исполняются.

Основным признаком, по которому различают вредоносные утилиты, являются совершаемые ими действия.

## 2.2 Классификация антивирусных программ

Антивирусы можно классифицировать по пяти основным группам: фильтры, детекторы, ревизоры, доктора и вакцинаторы.

Антивирусы-фильтры (сторожа) - это резидентные программы, которые оповещают пользователя обо всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях (например, о попытках изменить установки CMOS). При этом выводится запрос о разрешении или запрещении данного действия. Принцип работы этих программ основан на перехвате соответствующих векторов прерываний. К преимуществу программ этого класса по сравнению с программами-детекторами можно отнести универсальность по отношению, как к известным, так и неизвестным вирусам, тогда как детекторы пишутся под конкретные, известные на данный момент программисту виды. Это особенно актуально сейчас, когда появилось множество вирусов-мутантов, не имеющих постоянного кода. Однако, программы-фильтры не могут отслеживать вирусы, обращающиеся непосредственно к BIOS, а также BOOT-вирусы, активизирующиеся еще до запуска антивируса, в начальной стадии загрузки DOS. К недостаткам также можно отнести частую выдачу запросов на осуществление какой-либо операции: ответы на вопросы отнимают у пользователя много времени и действуют ему на нервы. При установке некоторых антивирусов-фильтров могут возникать конфликты с другими резидентными программами, использующими те же прерывания, которые просто перестают работать.

Наибольшее распространение в нашей стране получили программы-детекторы, а вернее программы, объединяющие в себе детектор и доктор. Наиболее известные представители этого класса -Aidstest, Doctor Web, MicroSoft AntiVirus далее будут рассмотрены подробнее. Антивирусы-детекторы рассчитаны на конкретные вирусы и основаны на сравнении последовательности кодов содержащихся в теле вируса с кодами проверяемых программ.

Такие программы нужно регулярно обновлять, так как они быстро устаревают и не могут обнаруживать новые виды вирусов. Ревизоры - программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохранённой ранее в одном из файлов данных ревизора. При этом проверяется состояние BOOT-сектора, таблицы FAT, а также длина файлов, их время создания, атри-буты, контрольная сумма. Анализируя сообщения программы-ревизора, пользователь может решить, чем вызваны изменения: вирусом или нет. При выдаче такого рода сообщений не следует предаваться панике, так как причиной изменений, например, длины программы может быть вовсе и не вирус. Самые изощренные антивирусы - вакцинаторы. Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной. Таким образом, вирус не может заразить эту программу. Вакцины могут быть пассивные и активные.

Пассивная вакцина представляет собой пакетную программу, которая за один вызов обрабатывает специальным образом файл или все файла на диске либо в каталоге. Обычно при такой обработке проставляется признак, который вирус использует для того, чтобы отличить зараженные программы от незараженных. Например, некоторые вирусы дописывают в конец зараженных файлов определенную строку. Если искусственно дописать в конец всех программ эту строку, то такие программы не будут заражаться вирусом, поскольку он будет считать, что они уже заражены.Обработанная таким образом программа является вакцинированной против данного вируса, при чем операция вакцинации является обратимой: когда опасность заражения будет ликвидирована, строку можно из файла удалить. Другие вирусы проставляют в поле даты заражаемых программ значение секунд, равное 62(MS-DOS допускает запись такого явно нереального значения).

Вакцина может проставить этот признак у всех выполняемых программ, которые тем самым будут защищены от заражения данным типом вируса. В этом случае вакцинирование является необратимым в том смысле, что восстановить первоначальное значение секунд не удастся, хотя они, конечно, могут быть сброшены.

Активные вакцины являются резидентными программами, действие которых основано на имитации присутствия вируса в оперативной памяти. Поэтому они обычно применяются против резидентных вирусов. Если такая вакцина находится в памяти, то, когда при запуске зараженной программы вирус проверяет, находится ли уже в оперативной памяти его копия, вакцина имитирует наличие копии. В этом случае вирус просто передает управление программе - хозяину и его инсталляция не происходит. Простейшие вакцины представляют собой выделенный и слегка модифицированный (лишенный способности к размножению) вирус. Поэтому они могут быть оперативно изготовлены - быстрей, чем доктора. Боле сложные вакцины (поливакцины) имитируют наличие в оперативной памяти нескольких вирусов.

Конечно, приведенный список не исчерпывает всего многообразия антивирусных программ, хотя и охватывает основные их разновидности. Каждая из антивирусных программ подобна узкому специалисту в определенной области, поэтому оптимальной тактикой является комплексное применение нескольких типов антивирусных средств.

## 2.3 NOD32

Антивирус, выпускаемый словацкой фирмой Eset. Возник в конце 1998 года. Большинство обновлений программных продуктов за последний год было связано с решением проблемы совместимости ПО с Windows Vista. И антивирус ESET NOD32 здесь не исключение - в своей третьей версии он стал полностью совместимым с Vista. В основе программы лежит фирменная технология ThreatSense, обеспечивающая защиту файловой системы в режиме реального времени; проверку файлов, выполняемых при запуске системы; защиту электронной почты и доступа в интернет; а также сканирование дисков, папок и отдельных файлов компьютера по требованию. Кроме того, NOD32 может похвастать полным "джентльменским набором" современного антивируса: продвинутой системой проактивной защиты, базирующейся на алгоритмах эвристического анализа; ручным или автоматическим обновлением вирусных баз; возможностью запаролить и, тем самым, защитить программу от вирусов, нацеленных на разрушение антивирусной защиты; планировщиком задач.

Как и Антивирус Касперского, NOD32 не отличается особой толерантностью и не желает находиться в одной системе вместе с другими подобными программами.

Главное окно антивируса ESET NOD32 вопросов ни у кого не вызовет: интерфейс прост и незамысловат, все на русском языке. Все команды выполнены в виде интуитивно понятных гиперссылок. Интерфейс предусматривает два режима: обычный и расширенный. В обычном режиме отображения малоподготовленный пользователь получает доступ лишь к основным, наиболее простым в использовании функциям администрирования системы защиты. Тогда как в расширенном режиме, который больше подходит для опытных пользователей, становится доступна настройка всех параметров защиты и служебных утилит.

##

## 2.4 Doctor Web

Антивирусная технология Dr.Web разрабатывается с 1992 и принадлежит компании «Доктор Веб».

Dr.Web для Windows обеспечивает защиту компьютера пользователя от всевозможных червей, вирусов (в том числе и полиморфных), троянов, макровирусов, spyware и adware, руткитов, программ-дозвонщиков, а также хакерских утилит и вредоносных скриптов. Проверка файлов в ручном режиме осуществляется с помощью антивирусного сканера Dr.Web Сканер, для проверки файлов "на лету" и предотвращения заражения системы в режиме реального времени служит антивирусный сторож (монитор) SpIDer Guard, а сообщения, поступающие через протоколы POP3, SMTP, IMAP и NNTP, проверяет почтовый монитор SpIDer Mail. Сканер для Windows имеет GUI- и консольную версии, кроме того, в дистрибутив программы входит и отдельная утилита для работы в среде DOS.

К дополнительным инструментам программы, повышающим эффективность ее использования, относится модуль автоматического обновления (обеспечивающий обновление как антивирусных баз, так и самих модулей антивируса до нескольких раз в час) и планировщик заданий.

Интерфейс сканера Dr.Web чересчур простой, (для современного коммерческого продукта) и совсем не дружелюбный - в этом отношении антивирус явно уступает всем остальным программам обзора. Серьезные неудобства создает отсутствие в программе единого центра, откуда возможна настройка и управление всеми модулями антивируса.

При установке Dr.Web честно предупреждает, что не собирается уживаться с другими антивирусными приложениями и просит удалить их из компьютера.

##

## 2.4 Avira AntiVir Personal

Бесплатный антивирус для "домашнего" (т.е. индивидуального и некоммерческого) использования - AntiVir Personal - обеспечивает защиту локальной системы от всевозможных вирусов, троянских коней, червей, а также от программ-"дозвонщиков", шуток (далеко не всегда безобидных), клавиатурных шпионов, руткитов и фишинга. По своему функционалу AntiVir мало уступает многим платным антивирусам и обеспечивает:

резидентную защиту от вирусов при загрузке файлов; просмотр и восстановление файлов, поврежденных макровирусами; защиту против любых (в том числе и заранее неизвестных) загрузочных и макровирусов; возможность работы по расписанию; автоматическое обновление программы и антивирусных баз через интернет (правда, не столь оперативное, как у других "конкурсантов"). Наряду с бесплатным Avira AntiVir Personal существует и несколько более "продвинутая" коммерческая версия Avira AntiVir Premium, способная, помимо всего вышеперечисленного, еще и защищать компьютер от spyware- и adware-программ, проверять почту на наличие вирусов, а также создавать "спасательные" CD-диски.

Хотя интерфейс AntiVir на английском языке, разобраться в его возможностях под силу даже новичку. Все функции программы логично объединены несколькими вкладками в главном окне программы. По количеству настроек AntiVir заметно уступает остальным рассмотренным в обзоре программам.

##

## 2.5 Kaspersky Antivirus

Самый популярный в России и крупнейший в Европе производитель систем защиты от вирусов, спама и хакерских атак. Компания входит в пятерку ведущих мировых производителей программных решений для обеспечения информационной безопасности.

«Антивирус Касперского», ориентирован, в первую очередь, на новичков и всех тех, кому нужна надежная защита от вирусов, отвечающая принципу "поставил и забыл". Собственно программа состоит из четырех функциональных модулей: файлового антивируса (проверяет файлы в момент обращения к ним), почтового антивируса (проверяет входящие и исходящие письма), веб-антивируса (проверяет просматриваемые веб-страницы) и проактивной защиты (контролирует подозрительные действия различных приложений). Она обеспечивает не только защиту от традиционных вирусов, червей и троянских коней, но и от таких "напастей", как рекламные и шпионские программы (adware и spyware), "пейджерные" и почтовые вирусы, клавиатурные шпионы и руткиты.

Понятно, что абсолютной защиты от вирусов не существует, и определенная вероятность заражения системы присутствует всегда. Так вот, для того, что бы проникший тем или иным способом в систему вирус не имел возможности вывести из строя сам антивирус, предусмотрена возможность самозащиты программы при помощи пароля. Кроме того, усовершенствованный механизм проактивной защиты от еще не известных вирусов обеспечивает, помимо выдачи традиционных предупреждений о каких-либо подозрительных действиях исследуемых объектов, еще и возможность отката всех действий приложения, которая позволяет свести к минимуму воздействие вредоносной программы на систему.

Кроме того, ее производительность (не в последнюю очередь - благодаря бережному отношению к системным ресурсам) существенно возросла, поэтому изрядно замусоленный тезис о "жуткой тормознутости Каспера" можно смело сдавать в архив. Так, на более или менее современном компьютере даже при активном сканировании файлов диска можно спокойно работать с достаточно "тяжелыми" приложениями, особенно если правильно настроить антивирусный монитор.

Все версии Антивируса Касперского традиционно отличаются простым, но, вместе с тем, очень функциональным и удобным интерфейсом, объединяющим все необходимые утилиты в одном окне; так что разобраться с программой не составит труда даже начинающему пользователю. На основном экране отображаются режимы защиты (включена, приостановлена, остановлена), статус защиты с гиперссылками на соответствующие отчеты, текущая статистика, важные напоминания, а также раскрывающиеся меню: защита, поиск вирусов отчеты и файлы данных, активация и поддержка.

То же самое можно отметить и в части настроек - организация по двухуровневому принципу позволяет не слишком сведущему пользователю с помощью примитивных "ползунков" выставить оптимальный, на его взгляд, уровень защиты системы (выбрав один из трех уровней), не вникая особо в тонкости антивирусной защиты. Впрочем, настройки программы по умолчанию достаточно разумны и не требуют особой коррекции. Хотя "продвинутые" пользователи и специалисты имеют возможность буквально в считанные минуты установить необходимые параметры защиты - богатству настроек Антивируса Касперского может позавидовать любая другая программа.

Заключительными штрихами в портрете завершенного антивирусного продукта является хорошо отлаженная система автоматического обновления антивирусных баз, практически без каких-либо задержек реагирующая на появление новых разновидностей "компьютерной заразы", и традиционная для продуктов Лаборатории Касперского возможность создания диска аварийного восстановления системы.

##

## 2.6 Тест антивирусов

Суть его проста: в каждом тестируемом антивирусе запускалась задача сканирования по требованию каталога, содержащего коллекцию вирусов. Кроме количества обнаруженных вирусов, оценивается еще и время сканирования архива, а также объем системных ресурсов.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Антивирус | Количество опасных объектов | Обнаружено опасных объектов | Эффективность обнаружения % | Время сканирования, с |
| Kaspersky | 3732 | 3680 | 66 | 115 |
| NOD32 | 3732 | 3627 | 41 | 82 |
| Dr.Web | 3732 | 3617 | 40 | 15 |
| Avira | 3732 | 3703 | 80 | 25 |

Первый, и самый главный вывод из результатов теста - ни один из самых современных антивирусов, несмотря на весьма почтенный возраст большинства вирусов в тестовом наборе, не смог показать 100% результата. Второй, ничуть не менее поразительный вывод - оглушительный провал антивируса Dr.Web. И третье - безоговорочная победа бесплатного антивируса AntiVir Personal над всеми коммерческими программами. Среди которых наиболее привлекательно смотрится Антивирус Касперского, по числу обнаруженных вирусов занимающий второе место после лидера.

Бесплатная программа AntiVir Personal, лидирующая по самому главному критерию эффективности антивирусов - количеству выявленных вирусов, несмотря на не самую лучшую функциональность и отсутствие русского интерфейса, вполне может стать хорошим выбором для домашнего использования. Более того, скромные требования к системным ресурсам делают ее оптимальным выбором для достаточно "слабых" машин.

Для решения более серьезных задач хорошим выбором могут стать коммерческие "Антивирус Касперского" или NOD32 с их многочисленными настройками и богатыми функциональными возможностями вполне способные обеспечить пользователю комплексную защиту системы.

#

# 3 Выбор брандмауэра

Число киберпреступлений растет с каждым годом. Опросы показывают, что уже сейчас их жертвы исчисляются миллионами. Во многих случаях неприятностей можно было бы избежать, если бы на компьютере был установлен хороший брандмауэр. Но какую программу можно считать таковой? Чтобы ответить на этот вопрос, производятся некие тесты, подвергающие брандмауэры всевозможным атакам.

Сразу стоит отметить, что, если профессиональные хакеры будут целенаправленно атаковать именно ваш компьютер, брандмауэр может и не спасти. Но отбросить атаки умников из локальной сети или автоматические взломы, производимые вирусами, он вполне способен.

Идеальный персональный брандмауэр должен выполнять шесть функций:

* Блокировка внешних атак. В идеале брандмауэр должен блокировать все известные типы атак, включая сканирование портов, IP-спуффинг, DoS и DDoS, подбор паролей и пр.
* Блокировка утечки информации. Даже если вредоносный код проник в компьютер (не обязательно через сеть, а, например, в виде вируса на купленном пиратском CD), брандмауэр должен предотвратить утечку информации, заблокировав вирусу выход в сеть.
* Контроль приложений Неизбежное наличие открытых дверей (то есть открытых портов) является одним из самых скользких мест в блокировке утечки информации, а один из самых надежных способов воспрепятствовать проникновению вирусов через эти двери — контроль приложений, запрашивающих разрешение на доступ. Кроме банальной проверки по имени файла, весьма желательна проверка аутентичности приложения.
* Поддержка зональной защиты Работа в локальной сети часто подразумевает практически полное доверие к локальному контенту. Это открывает уникальные возможности по использованию новейших (и, как правило, потенциально опасных) технологий. В то же время уровень доверия к Интернет-контенту значительно ниже, а значит, необходим дифференцируемый подход к анализу опасности того или иного содержания.
* Протоколирование и предупреждение Брандмауэр должен собирать строго необходимый объем информации. Избыток (равно как и недостаток) сведений недопустим. Возможность настройки файлов регистрации и указания причин для привлечения внимания пользователя приветствуются.
* Максимально прозрачная работа Эффективность и применяемость системы часто обратно пропорциональны сложности ее настройки, администрирования и сопровождения. Несмотря на традиционный скепсис в отношении «мастеров» (wizards) по настройке и прочих буржуйских штучек, даже опытные администраторы не пренебрегают ими просто в целях экономии времени.

##

## 3.1 Брандмауэр Windows

Брандмауэр (сетевой экран) можно представить в виде стены или фильтра, стоящего на страже локальной сети или вашего компьютера. Впервые брандмауэр появился в Windows XP после внедрения второго служебного пакета обновлений (Service Pack 2). Этот брандмауэр был несовершенным и оставлял открытыми абсолютно все порты вашего компьютера.

Брандмауэр проверяет каждое соединение между внешней сетью, такой как Интернет, и внутренней сетью, после чего или разрешает, или запрещает его.

##

## 3.2 Tools Firewall Plus

Бесплатный, простой в использовании, но эффективный персональный брандмауэр для Windows, защищающий информацию, хранящуюся на вашем компьютере, от несанкционированного доступа из локальных сетей или Интернета. Контролируя работу различных приложений, Firewall Plus пресекает попытки троянов, бэкдоров, клавиатурных шпионов и прочих вредоносных программ нанести ущерб компьютеру и похитить вашу конфиденциальную информацию.

Передовая технология PC Tools Firewall Plus была специально разработана таким образом, чтобы программой могли пользоваться не только специалисты, но и рядовые пользователи. Мощная защита от атак и вредоносных программ активируется по умолчанию. Все, что вам нужно сделать - это инсталлировать программу, и ваш компьютер немедленно окажется под постоянной защитой. Опытные пользователи могут также создавать свои собственные усложненные правила фильтрации пакетов, включая поддержку IPv6, чтобы настроить сетевую защиту по своему усмотрению.

Основные преимущества программы:

защищает ваш компьютер, когда вы работаете, ищете что-либо в Интернете или играете.

автоматическая защита, настраиваемая без каких-либо проблем,

простота использования - программа предназначена как для опытных, так и для начинающих пользователей.

возможность создания дополнительных правил для повышения уровня защиты ПК от распространенных видов атак.

## 3.3 Comodo Firewall Pro 3.0.25.378

Бесплатный брандмауэр Firewall Pro, произведённый американской компанией Comodo Group. Программа, поддерживает операционные системы Windows Vista, 64-битовые версии Windows XP и Windows Server 2003, но больше не поддерживает Windows 2000.

Третья версия была перенесена на новую архитектуру A-VSMART, благодаря которой, по утверждению разработчиков, уровень защиты значительно вырастет. Сделано это будет за счёт усиления надзора за трафиком, мониторинга процессов, а также программа сможет ограничивать доступ к критическим системным объектам. Настройки стали гибче, также появилась возможность создать сложную иерархию правил благодаря группе сконфигурированных политик. Улучшили разработчики и журнал – появились фильтры, благодаря которым в журнал теперь будут попадать те записи об активности брандмауэра, которые нужны именно вам. Также разработчики не оставили без внимания интерфейс программы, ставший более удобным и простым для пользователей. В принципе, учитывая все эти факторы и то, что Firewall Pro распространяется бесплатно, можно сказать, что это лучший брандмауэр для домашних пользователей.

## 3.4 Ashampoo Firewall

Бесплатный, простой и удобный персональный брандмауэр для операционных систем Windows. Встроенный модуль Configuration Assistant для легкой установки и настроики программы под свои нужды и потребности. Режим работы "Easy Mode" предназначен для людей, обладающих небольшими техническими навыками в защите ПК, но также имеется "Expert Mode" для профессионалов, предпочитающих собственноручно настраивать программу.

Имея большое количество дополнительных инструментов, Ashampoo Firewall потребляет совсем немного системных ресурсов и занимает немного места в памяти компьютера. Ashampoo FireWall осуществляет постоянный мониторинг сетевой активности, как исходящих, так и входящих соединений, имеется режим самообучения "Learning Mode", возможность настраивать правила работы ПК, кнопка моментальной блокировки всех соединений и т.д. Имеется русский интерфейс.

##

## 3.5 Тест брандмауэров

Брандмауэру необходимо контролировать входящий и исходящий сетевой трафик. Тесты строятся на тех же методах, которые трояны и другое вредоносное ПО используют для связи с хакерскими серверами.

В тесте участвуют 4 брандмауэра, это Ashampoo FireWall, Comodo Firewall Pro, PC Tools Firewall Plus и брандмауэр Windows.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Продукт | Comodo Firewall Pro | PC Tools Firewall Plus | Брандмауэр Windows | Ashampoo Firewall |
| Номер версии | 3.0.25 | 4.0.0.40 | - | 1.2 |
| Разработчик | Comodo | PC Tools | Microsoft | Ashampoo |
| Сайт | www.comodo.com | www.pctools.com | www.microsoft.ru | www.ashampoo.com |
| Цена | бесплатно | бесплатно | бесплатно | бесплатно |
| Общая оценка, баллов | 86 | 53 | 52 | 46 |
| Тесты на безопасность (утечка сканирование портов) и оценка безопасности (0–10) | 95% пройдено, безопасность: 10 | 6% пройдено, безопасность: 1 | 5% пройдено, безопасность: 1 | 5% пройдено, безопасность: 1 |
| Защита DoS атак | + | + | + | + |
| Блокирование сканеров портов | + | + | + | + |
| Имеющиеся уровни безопасности | 2 | 1 | 1 | 1 |
| Протоколирование (лог) | + с функцией архивирования | + с функцией архивирования | + | + |
| Автоматические правила | + | + | + | - |
| Автоматические обновления | + | + | + через обновления Windows | + |
| Выслеживание злоумышленника | - | - | - | - |
| Разблокирование отдельных портов | + | + | + | - |
| Разблокирование отдельных программ | + | + | + | + |
| Распознавание LAN | + | - | + | - |
| Предупреждения | детальная информация, но рассчитана на экспертов | подробный отчет по всем важным параметрам | информации мало, подробности отсутствуют | подробный отчет по всем важным параметрам |
| Подсказки | подробная справка, всегда с учетом контекста | руководство начального уровня, в остальном никаких подсказок | подробная справка на сайте разработчика | немногочисленные поясняющие тексты в самой программе |
| Ассистенты | - | - | - | - |
| Расход оперативной памяти, Мбайт | 5,4 | 18,5 | 35,5 | 21,3 |
| Занимаемое место на жестком диске, Мбайт | 57,6 | 18,3 | в составе Windows | 13 |
| Интерфейс | плохо структурирован, мало поясняющих текстов | хорошо структурирован, с поясняющими текстами | упрощенный стиль, поясняющие тексты отсутствуют | хорошо структурирован, с поясняющими текстами |
| Язык интерфейса | английский | русский | русский | русский |

Результат шокирует: собственный брандмауэр Windows совсем не контролирует исходящий трафик, а его конкуренты PC Tools и Ashampoo выявляют не более 6% атак. Достойно смотрится только победитель Comodo Firewall Pro - 95%. Чтобы брандмауэр работал эффективно, необходимы адекватные правила безопасности. Если они слишком строгие, ни одна программа не сможет выйти в Интернет, если же слишком мягкие - любой вредитель с легкостью проникнет на компьютер. Проблема заключается в сложности настройки: когда речь заходит о номерах портов, IP-диапазонах и типах протоколов, у большинства пользователей попросту опускаются руки. Поэтому в идеале брандмауэры должны задавать правила сами или хотя бы предлагать готовые варианты настроек. По этому показателю все участники теста оказались на высоте: все они регулярно обновляются. Хороший брандмауэр должен не только гарантировать надежную защиту, но и расходовать как можно меньше системных ресурсов. Выяснилось, чтонаиболее расточителен Ashampoo - 50 Мбайт. По сравнению с ним победитель теста расходует всего-то ничего - 5 Мбайт оперативной памяти.

#

# 4 Заключение

Подводя итог, хотелось бы подчеркнуть, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях. В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности.

Несмотря на широкую распространенность антивирусных программ, вирусы продолжают «плодиться». Чтобы справиться с ними, необходимо создавать более универсальные и качественно-новые антивирусные программы, которые будут включать в себя все положительные качества своих предшественников. К сожалению, на данный момент нет такой антивирусной программы, которая гарантировала бы защиту от всех разновидностей вирусов на 100%, но некоторые фирмы, например AntiVir на сегодняшний день достигли неплохих результатов.

Что же касается брандмауэров, то по результатам многочисленных тестов лучшим из них был Comodo Firewall Pro.

Защищенность компьютера в свою очередь зависит от грамотности самого пользователя, и лишь при применении всех видов защит можно достигнуть высокого уровня безопасности компьютера, и соответственно, информации.

# Список используемых источников

1. Компьютерный электронный журнал. www.izcity.com
2. Бесплатная защита//chip. – 2008 - № 11 – стр. 124-127