# ГЛАВА 4

# АНТИВИРУСНЫЕ ПРОГРАММЫ И ПРОАКТИВНАЯ АНТИВИРУСНАЯ ЗАЩИТА

Рассмотрены наиболее эффективные антивирусные программы, описаны основные компоненты стандартной антивирусной защиты, основные требования к антивирусным программам, основные технические характеристики, классификация и принципы работы антивирусных программ. Приведен краткий обзор наиболее эффективных антивирусных программ, приведены конкретные практические рекомендации пользователя антивирусных программ от разработчиков антивирусного программного обеспечения. Отдельный раздел посвящен относительно новому направлению проактивной антивирусной защиты – функции, возможности, методы применения. Особенности работы с этими защитными средствами продемонстрированы на конкретных примерах (Behavior Control, Component Control, Removeble Media Protection – защита переносных мультимедийных устройств, Soft-protection и др.). здесь же рассмотрены типовые потенциально опасные действия и процедуры пользователей корпоративных информационных сетей. Завершает главу раздел, посвященный описанию первой операционной системы с «кибериммунитетом» – KasperskyOS.

## 4.1. Антивирусные программы

Для защиты от компьютерных вирусов созданы специальные антивирусные программы, которые позволяют обнаруживать и уничтожать вирусы. Современные антивирусные программы представляют собой многофункциональные продукты, сочетающие в себе как превентивные, профилактические средства, так и средства восстановления данных.

***Антивирусная программа (антивирус)*** – это компьютерная программа, которая предназначена для обезвреживания вирусов и различного рода вредоносного ПО, с целью обеспечения сохранности данных и обеспечения надежной работы вычислительных устройств сетей.

Антивирусные программы (**антивирусы**) используют два основных принципа работы.

- Сканирование компьютера и сопоставление уже имеющегося вируса с базой данных на сервере определенного производителя.
- Сканирование и обнаружение программ, которые ведут себя подозрительно и могут по определению являться вредоносными.

### 4.1.1. Стандартные компоненты антивирусной защиты

Перечислим ниже с кратким их описанием, наиболее часто используемые компоненты антивирусный защиты:

*Файловый Антивирус*

Файловая система может содержать вирусы и другие опасные программы. Такие вредоносные программы могут годами храниться в файловой системе пользователя, проникнув однажды со съемного диска или из Интернета, и никак не проявлять себя. Однако стоит только открыть этот зараженный файл, как вирус тут же проявит себя.

Файловый Антивирус – это компонент, контролирующий файловую систему компьютера. Он проверяет все открываемые, запускаемые и сохраняемые файлы на вашем компьютере и всех присоединенных дисках. Каждое обращение к файлу перехватывается приложением, и файл проверяется на присутствие известных вирусов. Дальнейшая работа с файлом возможна только в том случае, если файл не заражен или был успешно вылечен Антивирусом. Если же файл по каким-либо причинам невозможно «вылечить», он будет удален, при этом копия файла будет сохранена в резервном хранилище.

*Почтовый Антивирус*

Электронная почтовая корреспонденция широко используется злоумышленниками для распространения вредоносных программ. Она является одним из основных средств распространения червей, поэтому крайне важно контролировать все почтовые сообщения.

Почтовый Антивирус – это компонент проверки всех входящих и исходящих почтовых сообщений компьютера. Он анализирует электронные письма на присутствие вредоносных программ. Письмо будет доступно адресату только в том случае, если оно не содержит опасных объектов.

*Веб-Антивирус*

Один из путей заражения – различные веб-сайты, поражающие компьютер с помощью скриптов, содержащихся на веб-страницах.

Веб-Антивирус специально разработан для предотвращения подобных ситуаций. Данный компонент перехватывает и блокирует выполнение скрипта, расположенного на веб-сайте, если он представляет угрозу. Строгому контролю также подвергается весь http-трафик.

*Проактивная защита*

С каждым днем вредоносных программ становится все больше, они усложняются, комбинируя в себе несколько видов, методы распространения становятся все более сложными для обнаружения.

Для того чтобы обнаружить новую вредоносную программу еще до того, как она успеет нанести вред, ведущими компаниями мира был разработан специальный компонент – Проактивная защита. Он основан на контроле и анализе поведения всех программ, установленных на вашем компьютере. На основании выполняемых

действий принимается решение: является программа потенциально опасной или нет. Таким образом, ваш компьютер защищен не только от уже известных вирусов, но и от новых, еще не исследованных. Более подробно функции и возможности современных антивирусов проактивной защиты рассмотрим в следующем разделе этой главы.

*Анти-Шпион*

В последнее время широкое распространение получили программы, производящие несанкционированный показ материалов рекламного характера (баннеры, всплывающие окна), программы несанкционированного дозвона на платные интернет-ресурсы, различные средства удаленного администрирования и мониторинга, программы-шутки и т.д.

Анти-Шпион отслеживает подобные действия на вашем компьютере и блокирует их выполнение. Например, компонент блокирует показ баннеров и всплывающих окон, мешающих пользователю при работе с веб-ресурсами, блокирует работу программ, пытающихся осуществить несанкционированный пользователем дозвон, анализирует веб-страницы на предмет фишинг-мошенничества.

*Анти-Хакер*

Для вторжения на ваш компьютер хакеры используют любую возможную «лазейку», будь то открытый порт, передача информации с компьютера на компьютер и т.д.

Анти-Хакер – это компонент, предназначенный для защиты вашего компьютера при работе в Интернете и других сетях. Он контролирует все исходящие и входящие соединения, проверяет порты и пакеты данных.

*Анти-Спам*

Не являясь источником прямой угрозы, нежелательная корреспонденция (спам) увеличивает нагрузку на почтовые серверы, засоряет почтовый ящик пользователя, ведет к потере времени и тем самым наносит значительный финансовый урон.

Компонент Анти-Спам встраивается в установленный на вашем компьютере почтовый клиент и контролирует все поступающие почтовые сообщения на предмет спама. Все письма, содержащие спам, помечаются специальным заголовком. Предусмотрена также возможность настройки Анти-Спама на обработку спама (автоматическое удаление, помещение в специальную папку и т.д.).

Домашние ПК не так часто подвергаются вирусным атакам. Обычно разработчики антивирусного программного обеспечения для домашних компьютеров делают акцент на такие компоненты:

- антивирус;
- файрволл;
- антируткит;
- антиспам.

Что же касается ***рабочих станций***, то тут ситуация немного посложнее, поскольку большинство структур работают с серверами. Соответственно, тут и уровень безопасности должен быть выше. Поэтому администраторы используют соответствующие «серверные» антивирусы и клиентские приложения для них.

Сегодня существует большое количество различных корпораций, которые занимаются разработкой все более и более новых антивирусов и накоплением баз данных к ним.

***Антивирусы*** защищают компьютер от вирусов и других вредоносных программ, например червей и программных троянов. ***Антивирусные программы*** нужно регулярно обновлять в Интернете. Для получения обновлений надо подписаться на услугу обновления антивирусных баз производителя антивирусной программы. Перед каждым подключением к сети Интернет необходимо запускать антивирусную программу!

***Основные задачи антивирусов*:**

- сканирование файлов и программ в режиме реального времени;
- сканирование компьютера по требованию;
- сканирование интернет-трафика;
- сканирование электронной почты;
- защита от атак враждебных веб-узлов;
- восстановление поврежденных файлов (лечение).

### *4.1.2. Основные требования к антивирусным программам*

Поскольку количество и разнообразие типов вирусов периодически увеличивается и чтобы их быстро и эффективно обнаружить, антивирусная программа должна соответствовать ряду важных требований:

***Стабильность и надежность работы.*** Этот параметр является определяющим – даже самый лучший антивирус окажется совершенно бесполезным, если он не сможет нормально функционировать на вашем компьютере, если в результате какого-либо сбоя в работе программы процесс проверки компьютера не пройдет до конца. Тогда всегда есть вероятность того, что какие-то зараженные файлы остались программой незамеченными.

***Размеры вирусной базы программы*** (количество вирусов, которые автоматически выявляются программой). С учетом постоянного появления все новых вирусов база данных должна регулярно обновляться (расширяться) – что толку от программы, не видящей новых вирусов. Сюда же следует отнести и возможность программы определять разнообразные типы вирусов, и умение работать с файлами различных типов (архивы, документы). Важным также является наличие резидентного монитора, осуществляющего проверку всех новых файлов автоматически, по мере их записи на диск.

***Скорость работы программы и наличие дополнительных возможностей.*** К дополнительным возможностям относится, например**,** тип алгоритмов определения даже неизвестных программе вирусов (эвристическое сканирование). Сюда же следует отнести возможность восстанавливать зараженные файлы, не стирая их с жесткого диска, а только удалив из них вирусы. Немаловажным является также процент ложных срабатываний программы (ошибочное определение вируса в «чистом» файле).

***Многоплатформенность*** (наличие версий программы под различные операционные системы). Конечно, если антивирус используется только дома, на одном компьютере, то этот параметр не имеет большого значения, но антивирус для крупной

организации (предприятия) просто обязан поддерживать все распространенные операционные системы. Кроме того, при работе в сети немаловажным является наличие серверных функций, предназначенных для административной работы, а также возможность работы с различными видами серверов.

### *4.1.3.Основные характеристики антивирусных программ*

Антивирусные программы делятся на: программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры, программы-вакцины.

***Программы-детекторы*** обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные.

***Универсальные детекторы*** в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов.

***Специализированные детекторы*** выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они не способны обнаруживать все известные вирусы.

Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

***Программы-доктора*** (фаги) не только находят зараженные вирусами файлы, но и «лечат» их, т.е. 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***, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий.

***Программы-ревизоры*** относятся к наиболее надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран видеомонитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

Современные программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить «законные» изменения (модификации) версии проверяемой программы от изменений, внесенных вирусом.

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

- попытки коррекции файлов с расширениями COM и EXE;
- изменение атрибутов файлов;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение н предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования (до размножения). Однако они не «лечат» файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги. К практическим недостаткам программ-сторожей можно отнести их «назойливость» (например, они постоянно выдают предупреждение о любой попытке копирования исполняемого файла), а также возможные конфликты с другим программным обеспечением.

***Вакцины*** (иммунизаторы) – это резидентные программы, предотвращающие заражение файлов. Обычно 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 последнее время программы-вакцины имеют ограниченное применение.

Существенным недостатком таких программ являются их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

### *4.1.4. Классификация и принципы работы антивирусных программ*

Самыми популярными антивирусными программами являются антивирусные сканеры (другие названия: доктора, фаги, полифаги). Следом за ними по эффективности и популярности следуют CRC-сканеры (ревизор, checksumer, integrity checker). Часто оба метода объединяются в одну универсальную антивирусную программу, что значительно повышает ее мощность. Применяются также различного типа мониторы (фильтры, блокировщики) и иммунизаторы (детекторы).

***Сканеры.*** Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Сканеры также можно разделить на две категории – «универсальные» и «специализированные». Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макровирусов. Специализированные сканеры, рассчитанные только на макровирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel. Сканеры также делятся на «резидентные», производящие сканирование «на лету», и «нерезидентные», обеспечивающие проверку системы только по запросу.

***CRC-сканеры.*** Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов.

Эти CRC-суммы затем сохраняются в базе данных антивируса. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был несанкционированно изменен или заражен вирусом.

***Мониторы.*** Антивирусные мониторы – это резидентные программы, перехватывающие «вирусоопасные» ситуации и сообщающие об этом пользователю. К «вирусоопасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в загрузочные сектора дисков, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты их размножения.

***Иммунизаторы.*** Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса. Первые обычно записываются в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение. Недостаток у таких иммунизаторов всего один, но он летален: абсолютная неспособность сообщить о заражении стелс-вирусом. Поэтому такие иммунизаторы, как и мониторы, практически не используются в настоящее время.

### *4.1.5. Краткий обзор антивирусных программ*

При выборе антивирусной программы пользователю необходимо учитывать не только задекларированный разработчиком процент обнаружения вирусов, но и способность обнаруживать новые вирусы, общее количество вирусов в антивирусной базе, частоту ее обновления, наличие дополнительных функций (опций).

Сегодня хороший антивирус должен уметь распознавать не менее 25 000 вирусов, независимо от того, где они или уже прекратили свое существование или еще только находятся в лабораториях и не распространяются. Например, реально можно встретить 200–300 вирусов, а опасность представляют только несколько десятков из них.

Ниже из множества антивирусных программ рассмотрим только ряд наиболее известных из них.

***Norton AntiVirus 4.0 и 5.0*** (производитель: «Symantec»).

Один из наиболее известных и популярных антивирусов. Процент распознавания вирусов очень высокий (близок к 100%). В программе используется оригинальный алгоритм, который позволяет распознавать даже новые, пока неизвестные вирусы.

Состоит из одного модуля, который постоянно находится в памяти компьютера и осуществляет такие задачи, как мониторинг памяти и сканирование файлов на диске. Доступ к элементам управления и настройкам программы выполняется с помощью соответствующих «закладок» и «кнопок».

Автозащита должна быть постоянно включенной, работать в фоновом режиме, не прерывая работу ПК.

Автозащита этой антивирусной программы автоматически:

– обнаруживает и защищает ПК от всех типов вирусов, включая макровирусы, вирусы загрузочных секторов, вирусы резидента памяти и троянских коней, червей и других вредоносных вирусов;

– защищает компьютер от вирусов, которые передаются через сеть Интернет, проверяя все файлы, которые загружаются из Интернета.

В интерфейсе программы Norton AntiVirus имеется специальная функция LiveUpdate, позволяющая «щелчком» на одной-единственной кнопке обновлять через Web как программу, так и набор сигнатур вирусов. Мастер по борьбе с вирусами выдает подробную информацию об обнаруженном вирусе, а также предоставляет пользователю возможность выбора: удалять вирус либо в автоматическом режиме, либо более осмотрительно, посредством пошаговой процедуры, которая позволяет увидеть каждое из выполняемых в процессе удаления действий.

Антивирусные базы обновляются очень часто (иногда обновления появляются несколько раз в неделю). Имеется резидентный монитор. Некоторым недостатком данной программы является сложность настройки.

***Dr Solomon's AntiVirus*** (производитель: «Dr Solomon's Software»).

Считается одним из самых лучших антивирусов (Евгений Касперский как-то сказал, что это единственный конкурент его AVP). Обнаруживает практически 100% известных и новых вирусов. Большое количество функций, сканер, монитор, эвристика и все, что необходимо, чтобы успешно противостоять вирусам.

***McAfee VirusScan*** (производитель: «McAfee Associates»).

Это один из наиболее известных антивирусных пакетов, хорошо удаляет вирусы. Небольшой недостаток – хуже, чем у других пакетов, обстоят дела с обнаружением новых разновидностей файловых вирусов. Он быстро устанавливается с использованием настроек по умолчанию, но его можно настроить и по собственному усмотрению. Вы можете сканировать все файлы или только программные, распространять или не распространять процедуру сканирования на сжатые файлы. Имеет много функций для работы с сетью Интернет.

***Dr.Web*** (производитель: «Диалог Наука»).

Популярный отечественный антивирус. Хорошо распознает вирусы, но в его базе их пока меньше, чем у других антивирусных программ. Программа Dr. Web относится к классу антивирусных программных средств, называемых «*полифагами*». Она предназначена для поиска и обезвреживания файловых, загрузочных и файлово-загрузочных вирусов. Существенной особенностью Dr. Web, которая выделяет его среди других программ-полифагов, является использование оригинального эвристического анализатора наряду с традиционным методом обнаружения вирусов по их сигнатурам (определенной последовательности байтов в теле программы, которая однозначно идентифицирует конкретный вирус). Большинство существующих в настоящее время программ-полифагов используют только метод обнаружения вирусов по сигнатурам.

Тем самым возможности таких программ по обнаружению вирусов ограничены строго определенным набором, который известен только автору программы. Однако использование эвристического анализатора позволяет выявлять также вирусы, сигнатура которых неизвестна автору программы. Алгоритмы, используемые в Dr.Web, позволяют выявлять все известные в настоящее время типы вирусов.

Программы семейства Dr.Web выполняют поиск и удаление известных им вирусов из памяти и с дисков компьютера, а также осуществляют эвристический

анализ файлов и системных областей дисков компьютера. Эвристический анализ позволяет с высокой степенью вероятности обнаруживать новые, ранее неизвестные, компьютерные вирусы.

В комплект программ для Windows 95–XP входит полифаг Dr.Web и резидентный сторож SpIDer Guard. Программа-полифаг обнаруживает и удаляет фиксированный набор известных вирусов в памяти, файлах и системных областях дисков компьютера.

Резидентный сторож (называемый также монитором), находясь в памяти компьютера, постоянно контролирует вирусоподобные ситуации, производимые различными программами с диском и памятью.

Начиная с версии 4.20, в комплект программ для Windows обязательно входит Планировщик Dr. WEB, позволяющий производить запуск антивирусных программ и проверку устройств хранения информации, а также осуществлять обновление вирусных баз и компонентов программы по графику, задаваемому пользователем.

***Antiviral Toolkit Pro – ATP*** (производитель: «Лаборатория Касперского»).

Этот антивирус признан во всем мире как один из самых надежных. Несмотря на простоту в использовании, он обладает всем необходимым арсеналом для борьбы с вирусами. Эвристический механизм, избыточное сканирование, сканирование архивов и упакованных файлов – это далеко не полный перечень его возможностей.

Лаборатория Касперского внимательно следит за появлением новых вирусов и своевременно выпускает обновления антивирусных баз. Имеется резидентный монитор для контроля за исполняемыми файлами.

***Антивирус Касперского 7.0.*** Это классическая защита компьютера от вирусов, троянских и шпионских программ, а также от любого другого вредоносного ПО.

Основные функции:

Три степени защиты от известных и новых интернет-угроз:

1) проверка по базам сигнатур;
2) эвристический анализатор;
3) поведенческий блокиратор:
   - защита от вирусов, троянских программ и червей;
   - защита от шпионского (spyware) и рекламного (adware) ПО;
   - Проверка файлов, почты и интернет-трафика в режиме реального времени;
   - защита от вирусов при работе с ICQ и другими IM-клиентами;
   - защита от всех типов клавиатурных шпионов;
   - обнаружение всех видов руткитов;
   - автоматическое обновление баз.

***AVAST!***

Антивирусная программа Avast! v. home edition 4.7 русифицирована и имеет удобный интерфейс, содержит резидентный монитор, сканер, средства автоматического обновление баз и т.д. Защита Avast основана на резидентных провайдерах, которые являются специальными модулями для защиты таких подсистем, как файловая система, электронная почта и т.д. К резидентным провайдерам Avast! относятся: Outlook/Exchange, Web-экран, мгновенные сообщения, стандартный экран, сетевой экран, экран P2P, электронная почта.

Название изначально расшифровывалось как Nemocnica na Okraji Disku («Больница на краю диска»).

***NOD32*** – это комплексное антивирусное решение для защиты в реальном времени от широкого круга угроз. Eset NOD32 обеспечивает защиту от вирусов, а также от других угроз, включая троянские программы, черви, spyware, adware, phishing-атаки. В решении Eset NOD32 используется патентованная технология, которая предназначена для выявления новых возникающих угроз в реальном времени путем анализа выполняемых программ на наличие вредоносного кода, что позволяет предупреждать действия авторов вредоносных программ.

Наравне с базами вирусов NOD32 использует эвристические методы. Считается, что среди других ведущих антивирусных пакетов NOD32 отличается малым использованием системных ресурсов.

**Основные достоинства:**

– **незначительное влияние на системные ресурсы** NOD32 экономит ресурсы жесткого диска и оперативной памяти, оставляя их для критических приложений;

– **простота управления.** Обновления программы и вирусной базы данных выполняются автоматически в фоновом режиме.

### *4.1.6. Полезные практические рекомендации пользователям от разработчиков антивирусного программного обеспечения*

Распространение вирусов по электронной почте можно было бы предотвратить недорогими и эффективными средствами без установки антивирусных программ, если бы были устранены дефекты программ электронной почты, которые сводятся к выполнению без ведома и разрешения пользователя исполняемого кода, содержащегося в письмах.

- Обучение пользователей может стать эффективным дополнением к антивирусному программному обеспечению. Простое обучение пользователей правилам безопасного использования компьютера (например, не загружать и не запускать на выполнение неизвестные программы из Интернета) снизило бы вероятность распространения вирусов и избавило бы от надобности пользоваться многими антивирусными программами.
- Пользователи компьютеров не должны все время работать с правами администратора. Если бы они пользовались режимом доступа обычного пользователя, то некоторые разновидности вирусов не смогли бы распространяться (или, по крайней мере, ущерб от действия вирусов был бы меньше). Это одна из причин, по которым вирусы в Unix-подобных системах относительно редкое явление.
- Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы необнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. К несчастью, во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

- Постоянное появление новых вирусов дает разработчикам антивирусного программного обеспечения хорошую финансовую перспективу.
- Некоторые антивирусные программы могут значительно понизить быстродействие. Пользователи могут запретить антивирусную защиту, чтобы предотвратить потерю быстродействия, в свою очередь, увеличивая риск заражения вирусами. Для максимальной защищенности антивирусное программное обеспечение должно быть подключено всегда, несмотря на потерю быстродействия. Некоторые антивирусные программы не очень сильно влияют на быстродействие.
- Иногда приходится отключать антивирусную защиту при установке обновлений программ, таких, например, как **Windows Service Packs**. Антивирусная программа, работающая во время установки обновлений, может стать причиной неправильной установки модификаций или полной отмене установки модификаций. Перед обновлением **Windows 98**, **Windows 98 Second Edition** или **Windows ME** на **Windows XP (Home или Professional)**, лучше отключить защиту от вирусов, в противном случае процесс обновления может завершиться неудачей.
- Некоторые антивирусные программы на самом деле могут являться шпионским ПО, которое под них маскируется. Лучше несколько раз проверить, что антивирусная программа, которую вы загружаете, действительно является таковой. Еще лучше использовать ПО известных производителей и загружать дистрибутивы только с сайта разработчика.
- Некоторые из продуктов используют несколько ядер для поиска и удаления вирусов и spyware. Например, в разработке NuWave Software, используется 4 ядра (два для поисков вирусов и два для поиска spyware).

Антивирусные программы принято разделять на **чистые антивирусы** и **антивирусы двойного назначения**. Чистые антивирусы отличаются наличием антивирусного ядра, которое выполняет функцию сканирования по образцам. Принципиальным в этом случае является то, что возможно лечение, если известен вирус. Чистые антивирусы, в свою очередь, по типу доступа к файлам подразделяются на две категории: осуществляющие контроль по доступу (on access) или по требованию пользователя (on demand). Обычно on access-продукты называют **мониторами**, а on demand-продукты – **сканерами**. Кроме того, антивирусные программы, так же как и вирусы, можно разделить в зависимости от платформы, внутри которой данный антивирус работает. В этом смысле наряду с Windows или Linux к платформам могут быть отнесены Microsoft Exchange Server, Microsoft Office, Lotus Notes.

Программы двойного назначения – это программы, используемые как в антивирусах, так и в ПО, которое антивирусом не является. Разновидностью программ двойного назначения являются **поведенческие блокираторы**, которые анализируют поведение других программ и при обнаружении подозрительных действий блокируют их.

При выборе антивирусной программы необходимо учитывать не только процент обнаружения вирусов, но и способность обнаруживать новые вирусы, количество вирусов в антивирусной базе, частоту ее обновления, наличие дополнительных функций.