# Вирусы и антивирусное программное обеспечение

# Введение

Для моей курсовой работы по информатике я выбрала тему ”вирусы и антивирусное программное обеспечение ”. Потому что, будучи «чайником» мне пришлось ни раз бороться с вирусами на своем ПК. Эта тема до боли близка мне- ей я и хочу посвятить свою работу.

Компьютерные вирусы. Что это такое и как с этим бороться? На эту тему уже написаны десятки книг и сотни статей, 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. Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека - в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

Как и в случае обычной простуды, компьютер, атакованный вирусом, начинает проявлять болезненные симптомы. Заражение человека вирусом приводит к замедлению реакции, изменению веса, общей слабости, болевым ощущениям, частичной или полной амнезии и даже смерти. При инфицировании вирусом компьютеры проявляют аналогичные симптомы: замедленное выполнение программ по сравнению с обычным, необъяснимые изменения в размере файлов, необычные и частые сообщения об ошибках, потеря или изменения данных и полный крах системы. Некоторые относительно безвредные компьютерные вирусы тиражируются, но не делают ничего ужасного. Эти вирусы могут, выдавать на экран ошибочное сообщение. Однако в некоторых случаях вирус, атаковавший, скажем, больничную систему жизнеобеспечения и выдавший некорректное сообщение, может иметь фатальные последствия. Кроме того, вирусы способны нанести серьезный ущерб системе, например стереть всю информацию с жесткого диска.

# Что такое вирус?

Один из известных ”докторов” Д.Н Лозинский дал определение вируса на примере клерка.

Представим себе аккуратного клерка, который приходит на работу к себе в контору и каждый день обнаруживает у себя на столе стопку листов бумаги со списком заданий, которые он должен выполнить за рабочий день. Клерк берет верхний лист, читает указания начальства, пунктуально их выполняет, выбрасывает «отработанный» лист в мусорное ведро и переходит к следующему листу. Предположим, что некий злоумышленник тайком прокрадывается в контору и подкладывает в стопку бумаг лист, на котором написано следующее:«Переписать этот лист два раза и положить копии в стопку заданий соседей» Что сделает клерк? Дважды перепишет лист, положит его соседям на стол, уничтожит оригинал и перейдет к выполнению второго листа из стопки, т.е. продолжит выполнять свою настоящую работу. Что сделают соседи, являясь такими же аккуратными клерками, обнаружив новое задание? То же, что и первый: перепишут его по два раза и раздадут другим клеркам. Итого, в конторе бродят уже четыре копии первоначального документа, которые и дальше будут копироваться и раздаваться на другие столы.

Примерно так же работает и компьютерный вирус, только стопками бумаг-указаний являются программы, а клерком - компьютер. Так же как и клерк, компьютер аккуратно выполняет все команды программы (листы заданий), начиная с первой. Если же первая команда звучит как «скопируй меня в две другие программы», то компьютер так и сделает, и команда-вирус попадает в две другие программы. Когда компьютер перейдет к выполнению других «зараженных» программ, вирус тем же способом будет расходиться все дальше и дальше по всему компьютеру.

В приведенном выше примере про клерка и его контору лист-вирус не проверяет, заражена очередная папка заданий или нет. В этом случае к концу рабочего дня контора будет завалена такими копиями, а клерки только и будут что переписывать один и тот же текст и раздавать его соседям - ведь первый клерк сделает две копии, очередные жертвы вируса - уже четыре, затем 8, 16, 32, 64 и т.д., т.е. количество копий каждый раз будет увеличиваться в два раза.

Если клерк на переписывание одного листа тратит 30 секунд и еще 30 секунд на раздачу копий, то через час по конторе будет «бродить» более 1.000.000.000.000.000.000 копий вируса! Скорее всего, конечно же, не хватит бумаги, и распространение вируса будет остановлено по столь банальной причине.

Как это ни смешно (хотя участникам этого инцидента было совсем не смешно), именно такой случай произошел в 1988 году в Америке - несколько глобальных сетей передачи информации оказались переполненными копиями сетевого вируса (вирус Морриса), который рассылал себя от компьютера к компьютеру. Поэтому «правильные» вирусы делают так: Переписать этот лист два раза и положить копии в стопку заданий соседей, если у них еще нет этого листа».

Проблема решена - «перенаселения» нет, но каждая стопка содержит по копии вируса, при этом клерки еще успевают справляться и с обычной работой.

«А как же уничтожение данных?» - спросите Вы. Все очень просто - достаточно дописать на лист примерно следующее:

«1. Переписать этот лист два раза и положить копии в стопку заданий соседей, если у них еще нет этого листа.  
2. Посмотреть на календарь - если сегодня пятница, попавшая на 13-е число, выкинуть все документы в мусорную корзину»

Примерно это и выполняет хорошо известный вирус «Jerusalem» (другое название - «Time»).

Кстати, на примере клерка очень хорошо видно, почему в большинстве случаев нельзя точно определить, откуда в компьютере появился вирус. Все клерки имеют одинаковые (с точностью до почерка) КОПИИ, но оригинал-то с почерком злоумышленника уже давно в корзине.

Компьютерные вирусы – это программы, которые умеют воспроизводить себя в нескольких экземплярах, возможно, приписываясь к другим программам, и, возможно, совершать некоторые побочные действия. Это определение дается, скорее, на интуитивном уровне, поскольку строгого определения компьютерного вируса пока не существует.

Первой из причин, не позволяющих дать точное определение вирусу, является невозможность однозначно выделить отличительные признаки, которые соответствовали бы только вирусам.

Второй же трудностью, возникающей при формулировке определения компьютерного вируса, является то, что данное определение должно быть привязано к конкретной операционной системе, в которой этот вирус распространяется. Например, теоретически могут существовать операционные системы, в которых наличие вируса просто невозможно. Таким примером может служить система, где запрещено создавать и изменять области выполняемого кода, т.е. запрещено изменять объекты, которые либо уже выполняются, либо могут выполняться системой при каких-либо условиях.

Поэтому представляется возможным сформулировать только обязательное условие для того, чтобы некоторая последовательность выполняемого кода являлась вирусом.

Обязательным свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

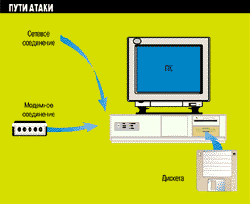
Следует отметить, что это условие не является достаточным (т.е. окончательным), поскольку на пример, операционная система MS-DOS удовлетворяет данному свойству, но вирусом не является.

Вот почему точного определения вируса до сих пор нет, и вряд ли оно появится в обозримом будущем. Следовательно, нет точно определенного закона, по которому «хорошие» файлы можно отличить от «вирусов». Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

# Откуда же берутся компьютерные вирусы?

Напоминаю, что в отличие от биологических вирусов компьютерные вирусы создаются человеком. Авторы вирусов своими "произведениями" приносят массу вреда пользователям компьютеров. Они могут вызвать сбои в работе компьютеров или даже полную потерю данных на жестком диске.

Вирус может проникнуть в систему одним из нескольких возможных путей: дискета, CD-ROM производителя ПО, сетевой интерфейс или модемное соединение, глобальная сеть Internet при получении электронной почты (рисунок 1) .



**Рисунок 1.**

Вирусы проникают в компьютер с дискет, через модемы и по сетевым соединениям.

Исторически дискета - это наиболее распространенный носитель вирусов, главным образом из-за того, что они использовались для переноса информации с одного компьютера на другой.

Заразить дискету гораздо проще. На нее вирус может попасть, если вы просто вставили дискету в дисковод зараженного компьютера и, например, прочитали ее оглавление.

Ситуация здесь та же, что и с вирусом СПИДа - чем больше число партнеров, с которыми вы обмениваетесь программами (дискетами), тем выше вероятность заражения.

Однако этим пути проникновения вирусов в систему далеко не исчерпываются.

У той простоты, с которой Интернет позволяет обмениваться информацией, есть и обратная сторона: из-за нее Интернет стал благоприятной средой для распространения компьютерных вирусов и других вредоносных программ. Конечно, далеко не каждая программа или документ, скаченные из Интернета или присланные Вам по электронной почте, содержат в себе вирусы. Дорожащие репутацией операторы досок объявлений и системные операторы интерактивных служб производят сканирование новых файлов на наличие вирусов, прежде чем сделать их доступными публике, однако никогда нельзя быть уверенным, что полученные файлы проверены. Каждому, кто работает в Интернете, совершенно необходима хорошая антивирусная защита.

Но в первую очередь, это касается тенденции приобретения вирусами функции распространения по электронной почте. Согласно статистике службы технической поддержки "Лаборатории Касперского", около 85% всех зарегистрированных случаев заражения были вызваны проникновением вирусов именно при помощи этого источника. Таким образом, по сравнению с 1999 г., рост числа подобных инцидентов составил около 70%.

В этой связи "Лаборатория Касперского" еще раз отмечает важность установки надежной системы антивирусной защиты для электронной почты.

Переключение внимания создателей вирусов на электронную почту вполне закономерно. Как показывает практика, больше всего вредоносных программ создается для тех операционных систем, приложений, технологий передачи данных, которые имеют наибольшую популярность. Сегодня электронная почта является де-факто стандартом как делового, так и неформального общения. Сотни миллионов людей по всему миру не представляют нормального бизнеса без этого способа коммуникации с партнерами. Это и предопределило ориентацию создателей вирусов на электронную почту.

# Признаки появления вирусов.

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;
* невозможность загрузки операционной системы;
* 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.

# Немного истории

Поговорим о новейшей истории: «Brain», «Vienna», «Cascade» и далее. Те, кто начал работать на IBM-PC аж в середине 80-х, еще не забыли повальную эпидемию этих вирусов в 1987-89 годах. Буквы сыпались на экранах, а толпы пользователей неслись к специалистам по ремонту дисплеев (сейчас все наоборот: винчестер сдох от старости, а валят на неизвестный передовой науке вирус). Затем компьютер заиграл чужеземный гимн «Yankee Doodle», но чинить динамики уже никто не бросился - очень быстро разобрались, что это - вирус, да не один, а целый десяток.

Так вирусы начали заражать файлы. Вирус «Brain» и скачущий по экрану шарик вируса «Pingpong» ознаменовали победу вируса и над Boot-сектором. Все это очень не нравилось пользователям IBM-PC, и - появились противоядия. Одним из первых антивирусов был отечественный ANTI-KOT: это легендарный Олег Котик выпустил в свет первые версии своей программы, которая уничтожала целых 4 (четыре) вируса (американский SCAN появился у нас в стране несколько позднее). К сожалению, ANTI-KOT определяет вирус «Time» («Иерусалимский») по комбинации «MsDos» в конце файла, а некоторые другие антивирусы эти самые буквы аккуратно прицепляют ко всем файлам с расширением COM или EXE.

Следует обратить внимание на то, что истории завоевания вирусами России и Запада различаются между собой. Первым вирусом, стремительно распространившимся на Западе был загрузочный вирус «Brain», и только потом появились файловые вирусы «Vienna» и «Cascade». В России же наоборот, сначала появились файловые вирусы, а годом позже - загрузочные.

Время шло, вирусы плодились. Все они были чем-то похожи друг на друга, лезли в память, цеплялись к файлам и секторам, периодически убивали файлы, дискеты и винчестеры. Одним из первых «откровений» стал вирус «Frodo.4096» - один из первых из известных файловых вирусов-невидимок (стелс). Этот вирус перехватывал INT 21h и, при обращении через DOS к зараженным файлам, изменял информацию таким образом, что файл появлялся перед пользователем в незараженном виде. Но это была только надстройка вируса над MS-DOS. Не прошло и года, как электронные тараканы полезли внутрь ядра DOS (вирус-невидимка «Beast.512»). Идея невидимости продолжала приносить свой плоды и далее: летом 1991 года пронесся, кося компьютеры как бубонная чума, вирус «Dir­\_П».

Но бороться с невидимками было довольно просто: почистил RAM - и будь спокоен, ищи гада и лечи его на здоровье. Но больше хлопот доставляли самошифрующиеся вирусы, которые иногда встречались в очередных поступлениях в коллекции. Ведь для их идентификации и удаления приходилось писать специальные подпрограммы, отлаживать их. Но на это никто тогда не обращал внимания, пока... Пока не появились вирусы нового поколения, те, которые носят название полиморфик-вирусы. Эти вирусы используют другой подход к невидимости: они шифруются (в большинстве случаев), а в расшифровщике используют команды, которые могут не повторяться при заражении различных файлов.

# Классификация вирусов

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

* среде обитания
* способу заражения среды обитания
* воздействию
* особенностям алгоритма

В зависимости от **среды обитания** вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, т. е. В файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord). Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

**По способу заражения вирусы** делятся на резидентные и нерезидентные. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

**По степени воздействия** вирусы можно разделить на следующие виды:

* **неопасные**, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах
* **опасные** вирусы, которые могут привести к различным нарушениям в работе компьютера
* **очень опасные**, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

### По особенностям алгоритмов выделяют следующие группы вирусов:

1. **"Компаньоны - спутники"** - вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE файлов файлы спутники, имеющие то же самое имя, но с расширением .Com или Bat. Вирус записывается в Com или Bat-файл и никак не изменяет EXE-файл. При активации такого файла операционная система первым обнаружит и выполнит Bat-файл или COM-файл, т.е. вирус, который затем уже запустит и EXE-файл.
2. **"Черви - репликаторы"** - вирусы, которые распространяются в компьютерной сети и, так же как и компаньон вирусы, не изменяют файлы или сектора на дисках. Они проникают в память компьютера из сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают файлы, но могут вообще не обращаться к ресурсам компьютеров (кроме оперативной памяти).
3. **"Паразитические"** - все вирусы, которые при распространении своих копий изменяют содержимое дисковых секторов или файлов. В эту группу относятся вирусы, которые не являются "червями" и "спутниками".
4. **"Студенческие"** - крайне примитивные вирусы, часто нерезидентные и содержащие большое число ошибок, именно по этой причине они могут быть любой степени опасности, если их быстро не удалить из компьютера.
5. **"Стелс невидимки"** вирусы, представляющие собой совершенные программы, которые перехватывают обращения операционной системы к пораженным файлам или секторам дисков и "подставляют" вместо себя незараженные участки информации. Такие вирусы используют оригинальные алгоритмы, позволяющие "обманывать" резидентные АВП.
6. **"Полиморфик - призраки -  мутанты"** вирусы (само шифрующиеся) достаточно трудно обнаруживаемые вирусы, не имеющие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик вируса не имеют ни одного совпадения.
7. **"Троянские кони"** -  вирусы, которые могут маскироваться под полезную программу и выполнять разрушительные действия при каждой активации. Они могут размножаться без внедрения в другие файлы, а более совершенные из них, активируются при определенных ситуациях или событиях в ЭВМ или сети.
8. **"Макро"** вирусы этого семейства используют возможности макроязыков в системах обработки данных (текстовые редакторы, электронные таблицы и т.д.). В настоящее время наиболее распространены макро вирусы заражающие документы редакторов Microsoft Word, Excel, Access.

# Антивирусные программы.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными. Различают следующие виды антивирусных программ:

* программы-детекторы;
* программы-доктора или фаги;
* программы-ревизоры;
* программы-фильтры;
* программы-вакцины или иммунизаторы.

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

Программы-доктора или фаги, а также программы-вакцины 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. Наиболее известные из них: AVP, Aidstest, Scan, Norton AntiVirus, Doctor Web.

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

Программы-ревизоры относятся к самым 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 монитора. 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. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная в России программа Adinf.

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

1. попытки коррекции файлов с расширениями COM, EXE;
2. изменение атрибутов файла;
3. прямая запись на диск по абсолютному адресу;
4. запись в загрузочные сектора диска;
5. загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и 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.

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

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

Главным оружием в борьбе с вирусами являются антивирусные программы. Они позволяют не только обнаружить вирусы, в том числе вирусы, использующие различные методы маскировки, но и удалить их из компьютера. Последняя операция может быть достаточно сложной и занять некоторое время.

Существует несколько основополагающих методов поиска вирусов, которые применяются антивирусными программами. Наиболее традиционным методом поиска вирусов является сканирование.

Оно заключается в поиске сигнатур, выделенных из ранее обнаруженных вирусов. Антивирусные программы-сканеры, способные удалить обнаруженные вирусы, обычно называются полифагами.

Недостатком простых сканеров является их неспособность обнаружить полиморфные вирусы, полностью меняющие свой код. Для этого необходимо использовать более сложные алгоритмы поиска, включающие эвристический анализ проверяемых программ.

Кроме того, сканеры могут обнаружить только уже известные и предварительно изученные вирусы, для которых была определена сигнатура. Поэтому программы-сканеры не защитят ваш компьютер от проникновения новых вирусов, которых, кстати, появляется по несколько штук в день. Как результат, сканеры устаревают уже в момент выхода новой версии.

# Антивирусная программа AntiViral Toolkit Pro

AVP имеет удобный пользовательский интерфейс, большое количество настроек, выбираемых пользователем, а также одну из самых больших в мире антивирусных баз, что гарантирует надежную защиту от огромного числа самых разнообразных вирусов.

В ходе работы AVP сканирует следующие области:

Оперативную память.

Файлы, включая архивные и упакованные.

Системные сектора, содержащие Master Boot Record, загрузочный сектор (Boot-сектор) и таблицу разбиения диска (Partition Table).

AntiViral Toolkit Pro имеет ряд особенностей, характеризующих его работу:

* детектирование и удаление огромного числа самых разнообразных вирусов, в том числе полиморфных или самошифрующихся вирусов;стелс-вирусов или вирусов-невидимок;макро вирусов, заражающих документы Word и таблицы Excel;
* сканирование внутри упакованных файлов (модуль Unpacking Engine);
* сканирование внутри архивных файлов (модуль Extracting Engine);
* сканирование объектов на гибких, локальных, сетевых и CD-ROM дисках;
* эвристический модуль Code Analyzer, необходимый для детектирования НЕИЗВЕСТНЫХ вирусов;
* поиск в режиме избыточного сканирования;
* проверка объектов на наличие в них изменений;

“AVP Monitor” – резидентный модуль, находящийся постоянно в оперативной памяти компьютера и отслеживающий все файловые операции в системе. Позволяет обнаружить и удалить вирус до момента реального заражения системы в целом;

* удобный пользовательский интерфейс;
* создание, сохранение и загрузка большого количества различных настроек;
* механизм проверки целостности антивирусной системы;
* мощная система помощи;

AVP Центр Управления – программа-оболочка, позволяющая организовать эффективную антивирусную защиту на ПК.

Опишем некоторые из них.

###### AVP Monitor.

AVP Monitor представляет собой резидентную антивирусную программу, которая постоянно находится в оперативной памяти и контролирует операции обращения к файлам и секторам. Прежде чем разрешить доступ к объекту, AVP Monitor проверяет его на наличие вируса. Таким образом, он позволяет обнаружить и удалить вирус до момента реального заражения системы.

Главное окно AVP Monitor содержит 5 вкладок: "Общие", "Объекты", "Действия", "Настройки", "Статистика". Перемещаясь по вкладкам и выбирая нужные опции, Вы можете изменять настройки программы.

Чтобы все произведенные Вами действия по выбору опций вступили в силу, нужно нажать кнопку "Применить"(в этом случае окно AVP Monitor останется открытым) или кнопку "OK"(в этом случае окно свернется в иконку) которые находятся в нижней части окна.

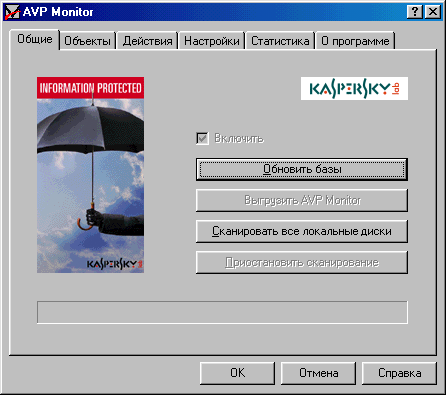
##### 

##### Вкладка "Общие".

В верхней части вкладки "Общие" содержится различная информация о программе (номер версии, дата последнего обновления и количество известных программе вирусов, регистрационная информация, информация о разработчиках). Нажав кнопку "Техническая поддержка", Вы получите информацию о каналах, по которым осуществляется техническая поддержка для легальных пользователей программы.

В нижней части вкладки находится флажок "Включить", с помощью которого можно включать или выключать монитор.

Кнопка "Выгрузить AVP Monitor" позволяет завершить работу программы.

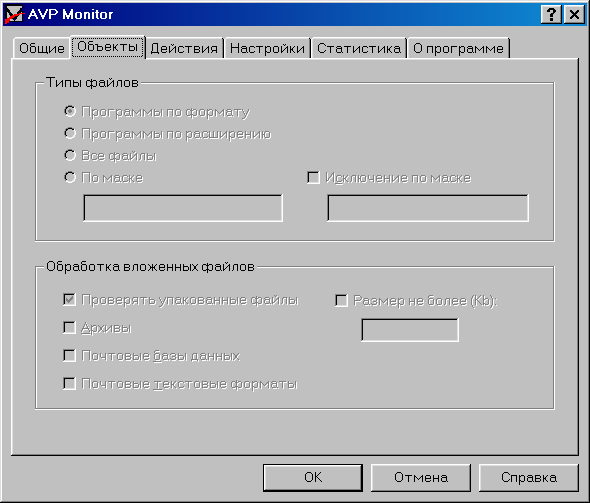


##### Вкладка "Объекты".

Эта вкладка позволяет выбирать типы файлов, которые будут проверяться.

Вы можете выбрать один из типов файлов:

* Программы по формату - проверять на наличие вируса только программы, т.е. объекты, имеющие внутренний формат выполняемых файлов, а также все файлы, имеющие расширения: .BAT, .COM, .EXE, .OV\*, .SYS, .BIN, .PRG, .VxD, .DLL, .OLE.;
* Программы по расширению - проверять все выполняемые файлы, имеющие расширения: \*.BAT, \*.COM, \*.EXE, \*.OV\*, \*.SYS, и т.д.
* Все файлы - проверять все файлы, независимо от их внутреннего формата;
* По маске - проверять файлы по маскам, задаваемым пользователем. Маски нужно вписывать в поле ввода через запятую. Например: \*.EXE, \*.COM, \*.DOC.



##### Вкладка "Действия".

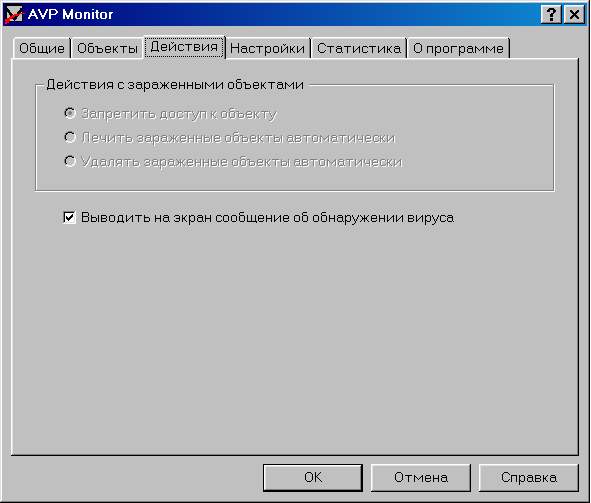
Вкладка "Действия" позволяет задавать действия AVP Monitor при обнаружении зараженного объекта. Вы можете выбрать одно из следующих действий:

* + - Запрашивать пользователя о действии - если Вы выберите эту опцию, то

при каждой попытке обращения к зараженному объекту будет появляться синий экран, содержащий информацию об этом зараженном объекте, имя вируса и запрос на лечение объекта: "Попытаться удалить вирус?" Нажмите клавишу <Y> если Вы хотите вылечить объект, или клавишу <N> в противном случае;

при каждой попытке обращения к подозрительному объекту (если включена опция "Предупреждения" во вкладке "Настройки") или объекту, содержащему измененный или поврежденный вирус (если включена опция "Анализатор кода" во вкладке "Настройки") будет появляться синий экран, содержащий информацию об этом объекте, имя вируса (или тип вируса) и запрос: "Запретить доступ к объекту?" Нажмите клавишу <Y> если Вы хотите запретить доступ, или клавишу <N> в противном случае;

* + - Лечить зараженные объекты автоматически - лечение зараженных объектов будет производиться автоматически, т.е. без какого-либо запроса;
    - Удалять зараженные объекты автоматически - все зараженные объекты будут автоматически удаляться при обращении к ним. Если выбрать эту опцию, появится предупреждающее сообщение: "Вы действительно хотите удалить ВСЕ зараженные объекты?" Нажмите кнопку "Да" для подтверждения действия, или кнопку "Нет" для возврата в главное окно AVP Monitor;
    - Запретить доступ к объекту - доступ к зараженным объектам будет запрещен.

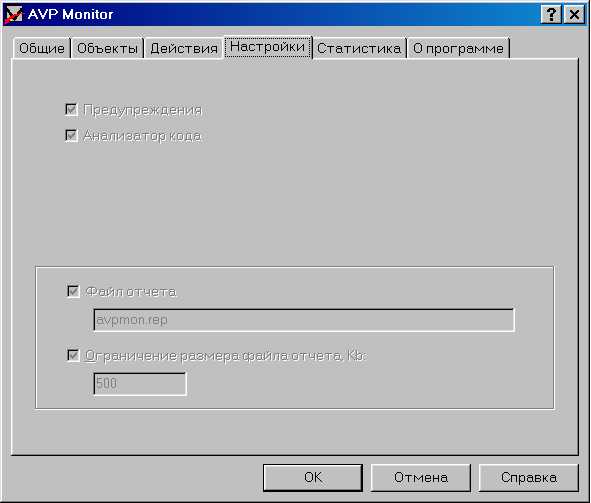


##### 

##### Вкладка "Настройки".

Эта вкладка предоставляет возможность подключения дополнительных механизмов поиска вирусов, а также возможность создания файла отчета. Вы можете поставить следующие флажки:

* **Предупреждения** - включить добавочный механизм проверки. При этом будет выводиться предупреждающее сообщение, если сканируемый файл или сектор содержит измененный или поврежденный вирус, а также, если в памяти компьютера обнаружена подозрительная последовательность машинных инструкций;
* **Анализатор кода** - включить эвристический механизм "Code Analyzer", позволяющий обнаруживать новые, еще не известные программе вирусы;
* **Файл отчета** - создать файл отчета, в который будет заноситься информация об обнаруженных зараженных объектах. В поле ввода рядом с флажком нужно указать имя файла отчета (по умолчанию "Avpm\_rep.txt ");
* **Ограничение размера, Kb**: - ограничить размер файла отчета числом Килобайт, указанных в соответствующем поле ввода (по умолчанию - 500 Kb).



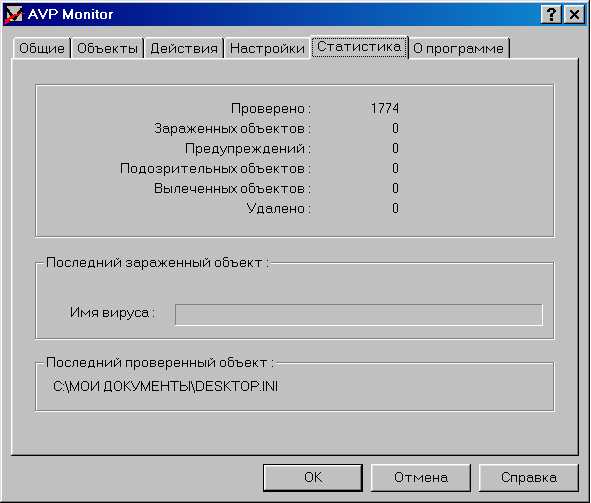
##### Вкладка «Статистика».

В этой вкладке отображается (и динамически обновляется) информация о количестве:

* проверенных объектов;
* инфицированных объектов;
* предупреждений;
* подозрений на вирус;
* вылеченных объектов;
* удаленных объектов;

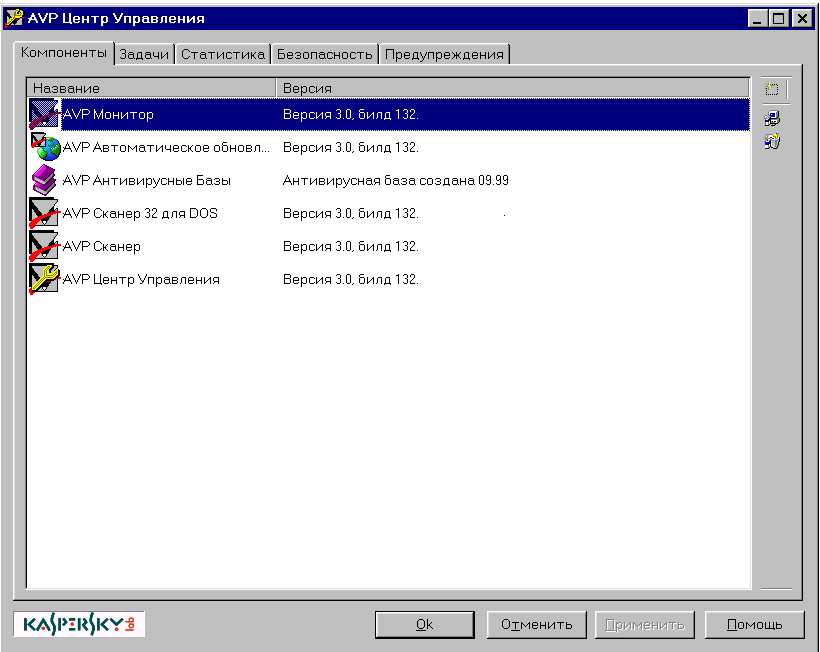
а также следующая информация:

* Последний зараженный объект: - имя последнего зараженного объекта (с указанием пути);
* Имя последнего вируса: название последнего найденного вируса.
* Последний проверенный объект: - имя последнего проверенного объекта (с указанием пути);



###### Программа AVP Центр Управления.

Программа AVP Центр Управления входит в состав пакета антивирусных программ AntiViral Toolkit Pro и выполняет функции управляющей оболочки. Она предназначена для организации установки и обновления компонент пакета, формирования расписания для автоматического запуска задач, а также контроля результатов их выполнения.



Возможность получения сводной информации о составе установленных компонент и их версиях облегчает общение пользователя со службой технической поддержки "Лаборатории Касперского" и позволяет своевременно принять решение о необходимости обновления. Использование функции автоматического обновления обеспечивает регулярную загрузку актуальных версий компонент и пополнение базы данных информацией о новых вирусах.

С помощью программы AVP Центр Управления Вы можете планировать запуск антивирусных программ, входящих в состав пакета. Тем самым повышается эффективность работы и, в то же время, сохраняется высокая защищенность системы от вирусов.

Возможность автоматического запуска внешних программ позволяет использовать AVP Центр Управления и в качестве традиционного планировщика задач. При этом в большинстве случаев исчезает необходимость в использовании других средств автоматического запуска, что ведет к экономии ресурсов компьютера. Кроме того, обеспечивается точная взаимная синхронизация задач, связанных с антивирусной защитой системы и прочими задачами, что позволяет избежать конфликтов между ними.

AVP Центр Управления – это программная оболочка, предназначенная для запуска различных задач (приложений). С помощью этой программы Вы можете запускать приложения как вручную, так и автоматически по расписанию. В качестве задач выступают другие модули пакета антивирусных программ: AVP Сканер, AVP Монитор и Обновление AVP.

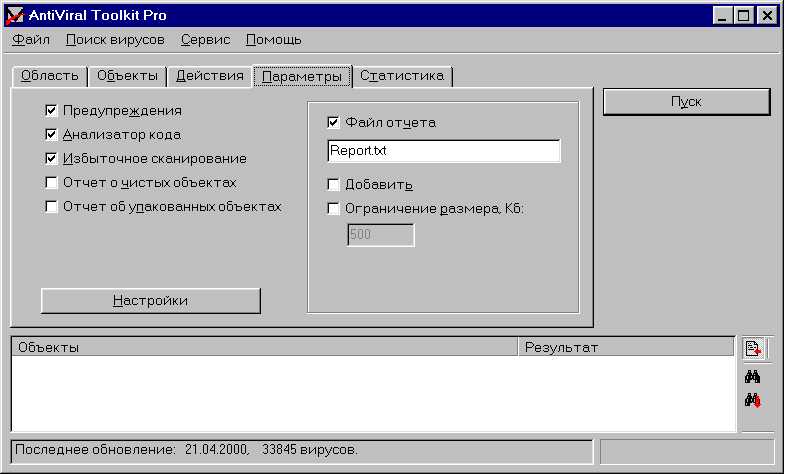
###### 

###### AVP сканер

###### Избыточное сканирование

Избыточное сканирование - это механизм полного сканирования содержимого исследуемых файлов вместо стандартной обработки только “точек входа” (т.е. тех мест, где начинается обработка программ системой).

Этот режим рекомендуется использовать, когда вирус не обнаружен, но в работе системы продолжаются “странные” проявления (частые “самостоятельные” перезагрузки, замедление работы некоторых программ и др.). В остальных случаях использование этого режима не рекомендуется, так как процесс сканирования замедляется в несколько раз и увеличивается вероятность ложных срабатываний при сканировании незараженных файлов.



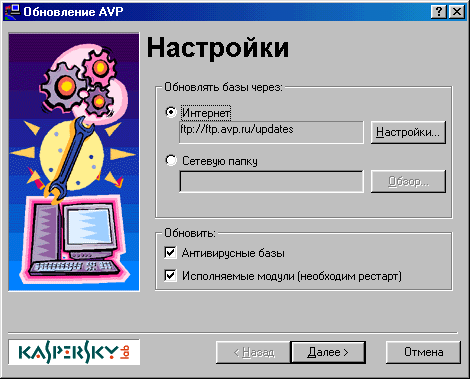
###### Программа Обновление AVP.

Программа Обновление AVP входит в состав пакета антивирусных программ AntiViral Toolkit Pro и предназначена для автоматизированного обновления базы данных, в которой хранится информация о вирусах, а также программных компонент пакета.

Обновление может осуществляться через Internet с использованием постоянного или Dial Up подключения, либо по локальной сети.

В условиях крупной корпоративной локальной сети затраты времени и трафик Internet могут быть существенно сокращены за счет организации централизованного обновления. При этом каждый пользователь избавляется от необходимости самостоятельно загружать файлы обновления через Internet – эта задача возлагается на сетевого администратора, который помещает их в специально отведенный каталог на жестком диске одного из компьютеров локальной сети (например, файлового сервера). В таком случае следует настроить программу Обновление AVP для обновления через локальную сеть.

Для регулярного автоматического обновления удобно организовать запуск программы Обновление AVP по расписанию средствами программы AVP Центр Управления. Для этого необходимо создать и настроить задачу управления автоматическим обновлением.



# Краткая характеристика некоторых антивирусов

### Dr Solomon's AntiVirus Toolkit

Достоинства: в целом самые лучшие результаты обнаружения и устранения вирусов.

Недостатки**:** весьма недешев; обновленные версии доступны только на дискетах, распространяемых по подписке.

Звание "Лучший выбор" получил Dr Solomon's AntiVirus Toolkit, несмотря на высокую цену - 85 долл. Нашелся только один программный продукт - VirusScan фирмы McAfee, который в наших тестах устранил больше "диких" вирусов, чем Dr Solomon's Toolkit. Благодаря толковому интерфейсу на экран по вашему распоряжению выводится любая нужная вам антивирусная функция, наряду с полной экранной энциклопедией всех известных вирусов и вызываемых ими последствий. Бродячие охотники за вирусами наверняка оценят также входящую в пакет загрузочную дискету Magic Bullet ("Волшебная пуля"), которая позволяет быстро найти и уничтожить вирус в любой системе.

Недостатком данного пакета является невозможность сетевой загрузки новых данных о вирусах; число же обновленных версий ограничено четырьмя в год.

Компания сообщила нам о том, что скоро она станет продавать Toolkit только в наборе для пяти пользователей ценою в 349 долл. Однако с середины марта компания вывела на рынок новую, упрощенную версию, которая называется Dr Solomon's AntiVirus и стоит 50 долл. Насколько можно судить по бета-версии, которую мы видели, этот новый пакет не в состоянии сканировать сетевые дисководы, но он сохраняет все те возможности, благодаря которым Toolkit столь удобен для персонального употребления, включая энциклопедию вирусов и дискету Magic Bullet (переименованную в SOS). Пользоваться интерфейсом стало проще, появилась возможность получения обновленных версий в режиме оперативного доступа, а стоимость ежемесячного обновления - 30 долл. в год. Мы еще не тестировали эту новую версию, но в ней использованы те же программные средства обнаружения вирусов, что и в Toolkit, так что она должна работать столь же хорошо.

http://www.drsolomon.com/

### F-Prot Professional

Достоинства:почти безупречное обнаружение вирусов; широкие возможности настройки; способность при обнаружении вируса посылать сигнал тревоги по электронной почте.

Недостатки:необходимость пароля и переустановки программы для обновления версий; весьма посредственные способности удаления вирусов.

Цена немалая - 99 долл., однако предлагаемая за эти деньги F-Prot Professional представляет собой действенную и эффективную антивирусную утилиту, напичканную возможностями, которые понравятся администраторам локальных сетей. Если, однако, ваша система с установленной на ней Windows 95 работает вне сети и вы нуждаетесь всего лишь в ненавязчивой антивирусной защите, то предусмотренные в F-Prot Professional всякие локально-сетевые наращения могут быть для вас излишеством. Кроме того, вы, возможно, захотите иметь пакет, лучше удаляющий вирусы: F-Prot Professional обнаружила 99% использованных в нашем тесте вирусов, поражающих файлы, но лишь 78% из них смогла уничтожить.

Набор базовых функций F-Prot Professional сравним с аналогичными наборами других рассмотренных пакетов. В дополнение к этому F-Prot Professional, подобно пакетам ThunderByte и McAfee VirusScan, допускает расширенные возможности контроля за тем, какие именно диски, папки или файлы должны быть включены в регулярное сканирование или исключены из него. Это позволяет сэкономить время, игнорируя файлы, которые вы просканировали ранее и которые, как вам известно, не были изменены. F-Prot Professional - единственный из протестированных нами пакетов, который при обнаружении вируса посылает по локальной сети электронное письмо с сигналом тревоги, он даже способен переслать администратору сети зараженный файл.

Главным недостатком F-Prot Professional является способ обновления файла с сигнатурами вирусов. Хотя обновленные файлы доступны в Web, вам приходится сперва узнать у фирмы пароль: только воспользовавшись им, вы сможете переустанавливать программу для включения в нее обновленного файла - дополнительные операции, не требуемые ни одним из протестированных пакетов.

http://www.commandcom.com/.

### IBM AntiVirus v. 2.5

Достоинства: достаточно хорошая способность к обнаружению вирусов; наличие в одной упаковке версий для работы с разными операционными системами.

Недостатки:консервативный способ дезинфекции негативно отражается на способности программы удалять вирусы.

Согласно документации в IBM AntiVirus заложена самая передовая технология, позволяющая распознавать новые типы вирусов. Этот пакет ценой в 49 долл. неплохо справился с использованными в нашем тесте "дикими" вирусами, заражающими файлы, однако в силу ряда проблем, связанных с этой программой, рекомендовать его было бы нелегко.

IBM AntiVirus - это единственная из протестированных нами программ, которая не удаляет файловый вирус в том случае, если она не уверена в том, что это можно сделать, не повредив зараженный файл. Соответственно, если программа находит вирус, который она не может удалить без ущерба для файла, единственное, что вам остается, это удалить зараженный файл; при этом предполагается, что вы можете вновь установить его с исходного диска или резервной копии. В результате IBM AntiVirus оказалась в состоянии спасти только 32% файлов, зараженных "дикими" вирусами. Однако, подобно большинству других программ, IBM AntiVirus удалила 100% вирусов, поражающих загрузочный сектор.

Помимо ограниченной способности к удалению вирусов, у данной программы имеются и другие обескураживающие свойства. Например, при первой установке она создает аварийную загрузочную дискету, но единственный способ создать еще одну - вернуться назад и воспользоваться установочными дискетами. В других программах соответствующий процесс реализуется проще.

Достоинством программы является то, что файлы, необходимые для ее обновления, доступны на Web-сервере IBM, и главный экран программы предлагает удобное меню для их установки. Если на вашем компьютере несколько операционных систем, то эта программа для вас - она поставляется с версиями для Windows 95, Windows 3.1, DOS и OS/2 в одном весьма недорогом пакете (версия для Windows NT включена в издание программы для предпринимателей - Eneterprise Edition).

http://www.av.ibm.com/.

### McAfee VirusScan for Windows 95

Достоинства: наивысшая оценка за удаление вирусов; работает с разными операционными системами; самая недорогая программа.

Недостатки: самая низкая оценка за обнаружение вирусов; поддержка и гарантированное обновление оплачиваются дополнительно.

McAfee VirusScan - один из наиболее известных антивирусных пакетов. По результатам нашего теста Norton AntiVirus фирмы Symantec отловил все 13 macro-вирусов, тогда как McAfee VirusScan один упустил - это был относительно редкий вирус Imposter. Еще важнее то, что у VirusScan хуже, чем у любого другого пакета, обстоят дела с обнаружением "диких" разновидностей файловых вирусов. Программа смогла обнаружить лишь 93% таких вирусов. Из всех протестированных программ худший показатель только у ближайшего родственника программы - версии VirusScan для Windows NT (92%).

Если бы его эффективность была выше, VirusScan был бы привлекательным пакетом. Он легко и 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.

VirusScan является также единственной из рассмотренных нами программ, которая всего лишь за 45 долл. включает версии для всех основных операционных систем - Windows 95, 3.x и NT, DOS и OS/2.

Зато вам придется платить за поддержку программы. Обновленные версии базы данных свободно доступны в Web, но, согласно Web-странице McAfee, работа этих обновлений не гарантируется без подписки на план технической поддержки компании. Зарегистрированные пользователи получают одно бесплатное обновление программы в течение первых трех месяцев ее эксплуатации. После этого контракт на техническое обслуживание за 49 долл. в год дает вам право на свободное получение неограниченного количества обновленных версий программы и списков сигнатур вирусов, а также на круглосуточные телефонные консультации.

http://www.mcafee.com/.

### Norton AntiVirus 2.0 for Windows 95

Достоинства: стопроцентное обнаружение вирусов в нашем тесте; великолепный интерфейс; автоматическое обновление.

Недостатки: удаляет только 77% "диких" вирусов.

Стоящая 70 долл. программа Norton AntiVirus 2.0 компании Symantec - один из наименее удачных пакетов с точки зрения удаления вирусов; ее результат - 77%. Она, однако, вошла в число всего лишь четырех из девяти протестированных программ, сумевших обнаружить каждый отдельно взятый "дикий" вирус. В целом это быстрый, надежный и простой в обращении инструмент, который начинающие пользователи могут установить на свой компьютер с тем, чтобы больше о нем не заботиться, а опытные пользователи могут настроить нужным для себя образом.

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

Управление всеми основными функциями - заказ на сканирование конкретных дисков, каталогов или файлов, включение и отключение резидентного сканирования - для удобства вынесено непосредственно на главный экран. И всего лишь на расстоянии пары щелчков мыши находятся более продвинутые функции - такие, как обнаружение изменений в размере файла, автоматическое сканирование и выдача отчета.

http://www.symantec.com/.

### ThunderByte AntiVirus Utilities

Достоинства:достаточно хорошая способность к обнаружению файловых вирусов; исключительное удобство сканирования.

Недостатки: предпоследний результат по удалению вирусов из числа протестированных программ; для новичков процедура удаления слишком сложна.

На первый взгляд кажется, что программа ThunderByte AntiVirus Utilities (100 долл.) предлагает тот же набор инструментов, что и программы-конкуренты, включая простые в установке обновленные наборы сигнатур вирусов, которые можно загружать из Web. При более внимательном рассмотрении, однако, обнаруживается, что этот пакет включает ряд весьма продвинутых функций, тогда как некоторых других функций в нем нет.

Устроенный наподобие Проводника в Windows 95 интерфейс ThunderByte содержит ряд удобных дополнительных возможностей, которых вы не найдете в большинстве пакетов. Вы можете распространять или не рапространять сканирование на конкретные диски, папки или файлы. Вы даже можете (что очень удобно) осуществить сканирование конкретных файлов, папок или дисков на лету, просто щелкнув на них правой кнопкой мыши в Проводнике или на Рабочем столе. Но в то же время в ThunderByte отсутствуют некоторые свойства, необходимые любой антивирусной программе. Наиболее вопиющей является неспособность ThunderByte удалять вирусы из загрузочного сектора, хотя программа и обнаружила в нашем тесте все 100% таких вирусов. Она также не смогла просканировать сжатые файлы, а это означает, что вирус в архивированном файле мог остаться незамеченным.

Реализованная в ThunderByte сверхосмотрительная процедура удаления вирусов чрезвычайно полезна для корпоративного использования на многих ПК (при этом забота об удалении вирусов может быть оставлена системным администраторам), но она, скорее всего, разочарует новичков или не слишком профессиональных пользователей. Для удаления файловых вирусов (кроме macro-вирусов) следует сперва создать дискету, содержащую отдельную DOS-утилиту под названием TBCLEAN, и вставить ее в дисковод вашего компьютера перед его включением. Загрузка с дискеты уменьшает шансы на то, что вирус будет активен в памяти во время сканирования, поскольку при этом не осуществляется доступ к инфицированным загрузочному сектору и файлам. (Прилагаемое к программе краткое руководство не описывает эту важнейшую процедуру.)

http://www.thunderbyte.com/.

# Рецепты самозащиты

Не баюкайте себя историями об иррациональных вирусных атаках. Наилучшая оборона - первым делом удостовериться в том, что вирусы не могут подобраться к вашему ПК.

* Проверяйте общие дискеты.
* Устанавливайте защиту от записи на дискеты.
* Не запускайте загруженные файлы сразу.
* Регулярно создавайте резервные копии.
* Запирайте ваш ПК.
* Регулярно обновляйте вашу антивирусную программу.

# Результаты тестирования антивирусных программ

|  |  |  |  |
| --- | --- | --- | --- |
| Антивирусная программа | Платформа | Обнаружено "диких" файловых вирусов, % | Устранено "диких" файловых вирусов, % |
| Dr Solomon's AntiVirus Toolkit | Windows 95 | 100 | 89 |
| F-Prot Professional | Windows 95 | 99 | 78 |
| IBM AntiVirus v.2.5 | Windows 95 | 96 | 32 |
| McAfee VirusScan | Windows 95 | 93 | 90 |
| Norton AntiVirus 2.0 | Windows 95 | 100 | 77 |
| ThunderByte AntiVirus Utilities | Windows 95 | 95 | 60 |
| TouchStone PC-Cillin II | Windows 95 | 100 | 80 |
| McAfee VirusScan | Windows NT | 92 | 59 |
| Norton AntiVirus 2.0 | Windows NT | 100 | 76 |

# Заключение

В заключении хочу сказать, что вирусы –это серьезная проблема , к которой нужно подходить осторожно и рассудительно.

Известны случаи, когда вирусы блокировали работу организаций и предприятий. Более того, несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели человека - в одном из госпиталей Нидерландов пациент получил летальную дозу морфия по той причине, что компьютер был заражен вирусом и выдавал неверную информацию.

Для избежания появления вирусов на вашем ПК используйте средства защиты.

При этом следует иметь в виду, что антивирусные программы и «железо» не дают полной гарантии защиты от вирусов. Примерно так же плохо обстоят дела на другой стороне тандема «человек-компьютер». Как пользователи, так 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.

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.

P.S. огромное спасибо Евгению Касперскому

# Приложение 1

##### В ожидании вирусов для мобильных телефонов

Все началось с обнаружения 6 июня в Испании Интернет-червя Timofonica. Данный червь не имел особых отличительных черт за исключением того, что он отсылал бессмысленные SMS-сообщения владельцам мобильных телефонов сети MoviStar. Это обстоятельство обусловило распространение слуха о появлении первого вируса, способного заражать непосредственно мобильные телефоны. К счастью, реальность была менее сурова, поскольку кроме посылки SMS-сообщений Timofonica более никакого отношения к телефонам не имел.

Двумя месяцами позже была обнаружена утилита под названием HSE, которая имела способность рассылать SMS-сообщения любого содержания на мобильные телефоны ряда немецких сотовых сетей. В отличие от 'Timofonica', эту программу нельзя отнести ни к разряду вирусов, ни Интернет-червей. По сути дела, это просто вредоносная программа, которая может использоваться для совершения несанкционированных действий в отношении владельцев мобильных телефонов.

Наконец, 30 августа мир снова облетела новость о появлении "мобильного" вируса, на этот раз обнаруженного норвежской компанией Web2Wap AS.Как выяснилось позже, норвежские специалисты лишь открыли брешь в системе защиты некоторых моделей телефонных аппаратов Nokia, которая позволяла блокировать клавиатуру телефона при посылке на него SMS-сообщения определенного содержания. Однако никакого отношения к вирусам это событие не имеет.

Важно подчеркнуть, что сама проблема вирусов для мобильных телефонов пока что не может считаться актуальной. Это обусловлено тем, что современные телефоны не имеют необходимых аппаратных возможностей для существования вирусов. Напомним, что для этого требуется выполнение следующих условий: возможность создавать, модифицировать и обмениваться исполняемыми программными объектами для данного конкретного оборудования, популярность оборудования и достаточно низкий уровень защиты.

Однако, появление настоящих "мобильных" вирусов - это вопрос ближайшего будущего. Стандарт MID (Mobile Information Device) на базе языка программирования Java (JavaT 2 Platform Micro Edition - J2ME), представленный 19 августа компанией Sun и рядом ее партнеров, по сути дела открывает зеленый свет разработке вредоносных программ.

# Приложение 2

Вы стараетесь не загружаться с дискет и допускаете до вашего компьютера только программное обеспечение из надежных источников. И вам пока что удавалось уберечь ваш компьютер от вирусной инфекции, так что вы должны быть в безопасности, правда? Не обязательно. Для того чтобы вычислить коэффициент угрожающей вам опасности, пройдите следующий маленький тест.

**1.** Вы запускаете антивирусную программу:

а) всякий раз при включении компьютера,

б) только при загрузке новых файлов,

в) только когда вас заставляет это делать администратор сети,

г) под дулом пистолета.

**2. Вы последний раз обновляли прилагающуюся к вашей антивирусной программе базу данных c сигнатурами вирусов:**

а) в прошлом месяце,

б) в прошлом году,

в) где-то в 90-х,

г) при Брежневе.

**3. Вы иногда позволяете своим коллегам:**

а) наблюдать картинки вашего защищенного паролем хранителя экрана,

б) копировать данные на ваш компьютер и с вашего компьютера с использованием дискет,

в) копировать файлы на ваш жесткий диск и с вашего жесткого диска по сети,

г) пользоваться вашим компьютером в ваше отсутствие.

**4. Вы иногда запускаете программы, найденные:**

а) на CD-ROM или дискете, только что проверенных на наличие вируса,

б) в America Online или любой другой коммерческой телекоммуникационной службе,

в) в Web, Usenet или на частной электронной доске объявлений,

г) на дискете, которую дал вам ваш двоюродный брат Иван.

**5. Вы недавно любовались:**

а) эротикой, извлеченной из Internet,

б) файлом Excel, полученным в качестве приложения к сообщению электронной почты,

в) документом Word на рекламном CD-ROM Microsoft,

г) зрелищем того, как ваш ребенок загружает ПК, вставляя дискету в дисковод A.

#### Ваш результат:

За каждый ответ **а** начислите себе **0** очков.

За каждый ответ **б** начислите себе **1** очко.

За каждый ответ **в** начислите себе **2** очка.

За каждый ответ **г** начислите себе **3** очка.

**12-15**Ваш компьютер находится в опасной зоне. Выключите его из сети и перечитайте эту статью.

**8-11**   
Вы, вероятно, считаете, что "Укротитель вирса Эбола" - это просто хлесткая фраза?

**4-7**Вы считаете себя счастливчиком?

**0-3**Расслабьтесь - вирусы вам не угрожают.

Список использованных источников:

1. Справка Adif ;
2. «Мир ПК» ;
3. «Интеркомпьютер»;
4. «Компьютер Пресс»;
5. «Хакер»;
6. http://dizet.com ;
7. http://www.idg-universe.ru ;
8. http://www.viruslist.com ;
9. http://www.wedbusiness.ru
10. http://www.mcafee.ru ;