Тема: Антивирусные программы: классификация, сравнительный анализ

Для удобной и безопасной работы за компьютером необходимо иметь минимальные представления о способах защиты личных данных, следует знать, что такое компьютерные вирусы, и с помощью какого программного обеспечения с ними необходимо бороться.

Компьютерный вирус – это вредоносное программное обеспечение, способное нанести непоправимый ущерб компьютеру и информации, хранящейся на его носителях [4]. Его основной целью является нанесение вреда, хищение информации и многое другое. Определить наличие вируса на компьютере можно по признакам, представленным на рисунке 1.

Наличие одного или нескольких признаков заражения не дают 100 % гарантии, что компьютер заражен вирусом. Эту гарантию дает специальная программа – антивирус. Антивирусное программное обеспечение служит для выявления компьютерных вирусов, их удаления, лечения и профилактики.

Сегодня на рынке представлено огромное разнообразие антивирусных программ. Каждая из них имеет свои достоинства и недостатки, но все антивирусы должны отвечать следующим критериям:

* стабильность и надежность работы;
* регулярное обновление базы данных;
* определение разнообразных типов вирусов;
* умение работать с файлами разнообразных типов;
* осуществление проверки всех новых файлов автоматически;
* возможность восстанавливать зараженные файлы, не стирая их с жесткого диска [3].

Как было сказано ранее, антивирусное программное обеспечение служит для диагностики, лечения и профилактики компьютерных вирусов. Диагностика выявляет вирусы и уведомляет пользователя компьютера. Найдя вирус, антивирусное программное обеспечение может предложить пользователю вылечить инфицированный файл, поместить его в карантин или удалить [4]. Профилактика заключается в том, что антивирусная программа запускается вместе с операционной системой и проверяет на наличие вируса каждую запускаемую программу или файл, т.е. зачищает компьютер постоянно.

На сегодняшний день в мире существует огромное разнообразие компьютерных вирусов. Согласно данным компании Symantes, в 2008 году суммарное количество вирусов превысило 1 миллион экземпляров [5]. Именно для определения того или иного типа вируса у антивирусных программ есть база данных сигнатур, с которой антивирус сверяет сканируемые файлы. И при обнаружении подозрительности оповещает об этом пользователя.

Антивирусные программы имеют три режима проверки на наличие вредоносного программного обеспечения: минимальный, средний (оптимальный), максимальный (параноидальный).

Параноидальный уровень защиты обеспечивает максимальную степень защиты, но обычно при этом потребляет большое количество ресурсов компьютера. Оптимальный уровень обеспечивает достаточный уровень защиты, он рекомендуется для повседневной работы. Минимальный уровень защиты обычно включает в себя проверку по базе данных сигнатур, то есть антивирус выдаёт информацию, только если это действительно 100 % вирус [3].

Компьютерные вирусы опасны как для аппаратной части компьютера, так и для персональных данных. Чтобы защитить их, необходимо установить на компьютер антивирусную программу. Рассмотрим наиболее популярные на 2017 год антивирусные программы (рис. 2):

Антивирус лаборатории Касперского – Internet Security 2017. Самая известная антивирусная программа на территории Российской Федерации. Данный антивирус работает с операционными системами Windows, Mac, а также планшетными и мобильными устройствами на базе Android [2]. Лаборатория Касперского предоставляет антивирусные программы для малого, среднего и крупного бизнеса, которые защищают Интернет-соединения, банковые операции, веб-камеру и имеют функцию родительского контроля. Антивирус предоставляет возможность поиска и установки обновлений программ и удаление неиспользуемых программ, имеется бесплатный тестовый период – 30 дней.

Avast Free Antivirus 2017 – интуитивно понятная и не требующая значительных ресурсов программа для защиты компьютера [6]. Данное антивирусное программное обеспечение распространяется бесплатно, но можно приобрести расширенную или максимальную версии, которые содержат в себе дополнительные функции. Avast совместим с большинством современных операционных систем, а также смартфонов на базе Android и iPhone. Как и Антивирус лаборатории Касперского предоставляет антивирусные программы для бизнеса, защищает Интернет-соединения, банковые и финансовые операции и проверяет безопасность сети Wi-Fi.

360 Total Security. Данный антивирус быстр и прост в использовании, практически с каждым обновлением программы ее арсенал функций возрастает. Данная антивирусная программа совместима с теми же операционными системами, что и ее конкуренты. Этот продукт защищает веб-браузер, сжимает данные в памяти компьютера, проверяет и очищает системный реестр, защищает сеть Wi-Fi от внешних угроз. Для опытных пользователей имеются гибкие настройки приложения, возможность оптимизировать работу системы через антивирус и выбора темы оформления интерфейса на интересующую тематику [1]. Данный антивирус также является бесплатным, но можно купить премиум версию, которая отличается расширенным функционалом.

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, 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 стелсвирусы 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.

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

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 недешево; 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.

Doctor Web

В последнее время стремительно растет популярность другой анти-вирусной программы - Doctor Web. Dr. Web так же, как и Aidstest относится к классу детекторов - докторов, но в отличие от последнего, имеет так называемый «эвристический анализатор» - алгоритм, позволяющий обнаруживать неизвестные вирусы. «Лечебная паутина», как переводится с английского название программы, стала ответом отечественных программистов на нашествие самомодифицирующихся вирусов-мутантов. Последние при размножении модифицируют свое тело так, что не остается ни одной характерной цепочки байт, присутствовавшей в исходной версии вируса. Dr. Web можно назвать антивирусом нового поколения по сравнению с Aidstest и его аналогами.

Программа DoctorWeb предназначена для борьбы с полиморфными вирусами, способна обнаруживать изменения в собственном теле. С помощью мощного аналитического анализатора может распознавать заражение файлов неизвестными вирусами, в том числе в упакованных файлах.

Программой предусматривается возможность проведения эвристического анализа на трех уровнях. При этом исследуются файлы и системные области дисков с целью обнаружения неизвестных вирусов по характерным кодовым последовательностям.

Работа с программой может выполняться в режиме полноэкранного интерфейса с использованием меню и диалоговых окон или в режиме вызова из командной строки. Второй вариант предпочтителен при многократном регулярном использовании программы для контроля дискет. При этом для удобства команду запуска программы DoctorWeb включают в меню пользователя оболочки NortonCommander или в командный файл.

Управление режимами также как и в Aidstest осуществляется с помощью ключей. Пользователь может указать программе, тестировать как весь диск, так и отдельные подкаталоги или группы файлов, либо же отказаться от проверки дисков и тестировать только оперативную память. В свою очередь можно тестировать либо только базовую память, либо, вдобавок, ещё и расширенную (указывается с помощью ключа /H). Как и Aidstest Doctor Web может создавать отчет о работе (ключ /P), загружать знакогенератор Кириллицы (ключ /R), поддерживает работу с программно-аппаратным комплексом Sheriff (ключ /Z).

Но, конечно, главной особенностью «Лечебной паутины» является наличие эвристического анализатора, который подключается ключом /S. Баланса между скоростью и качеством можно добиться, указав ключи, уровень эвристического анализа: 0 - минимальный, 1 - оптимальный, 2 - максимальный; при этом, естественно, скорость уменьшается пропорционально увеличению качества. К тому же Dr. Web позволяет тестировать файлы, вакцинированные CPAV, а также упакованные LZEXE, PKLITE, DIET. Для этого следует указать ключ /U (при этом распаковка файлов будет произведена на текущем устройстве) или /U диск: (где диск: - устройство, на котором будет производиться распаковка), если дискета, с которой запущен Doctor Web защищена от записи. Многие программы упакованы таким способом, хотя пользователь может и не подозревать об этом. Если ключ /U не установлен, то Doctor Web может пропустить вирус, забравшийся в запакованную программу.

Важной функцией является контроль заражения тестируемых файлов резидентным вирусом (ключ /V). При сканировании памяти нет стопроцентной гарантии, что «Лечебная паутина» обнаружит все вирусы, находящиеся там. Так вот, при задании функции /V Dr. Web пытается воспрепятствовать оставшимся резидентным вирусам заразить тестируемые файлы.

Тестирование винчестера Dr. Web-ом занимает на много больше времени, чем Aidstest-ом, поэтому не каждый пользователь может себе позволить тратить столько времени на ежедневную проверку всего жесткого диска. Таким пользователям можно посоветовать более тщательно (с опцией /S2) проверять принесенные извне дискеты. Если информация на дискете находится в архиве (а в последнее время программы и данные переносятся с машины на машину только в таком виде; даже фирмы-производители программного обеспечения, например Borland, пакуют свою продукцию), следует распаковать его в отдельный каталог на жестком диске и сразу же, не откладывая, запустить Dr. Web, задав ему в качестве параметра вместо имени диска полный путь к этому подкаталогу. И все же нужно хотя бы раз в две недели производить полную проверку «винчестера» на вирусы с заданием максимального уровня эвристического анализа.

Так же как и в случае с Aidstest при начальном тестировании не стоит разрешать программе лечить файлы, в которых она обнаружит вирус, так как нельзя исключить, что последовательность байт, принятая в антивирусе за шаблон может встретиться в здоровой программе. Если по завершении тестирования Dr. Web выдаст сообщения о том, что нашел вирусы, нужно запустить его с опцией /P (если эта опция не была указана) для того, чтобы посмотреть, какой файл заражен. После этого нужно скопировать файл на дискету или на электронный диск и попытаться удалить, указав «Лечебной паутине» ключ /F. При неудачном лечении следует поступить так же, как в аналогичной ситуации, описанной выше для программы Aidstes.

Norton Antivirus

В рамках обзора антивирусных программ. Вот уже добрый десяток лет компания Symantec является признанным лидером практически во всех сегментах рынка программного обеспечения, где представлены её программы. Не стали исключением и антивирусные решения. Так Norton Antivirus по-прежнему остаётся продуктом номер один во всём мире по защите компьютера от вирусных атак, и новая версия программы лишь подтвердила сей факт. На ней мы и остановимся более подробно.

С первым и довольно весомым нововведением новоиспеченный пользователь программы сталкивается уже при установке. Так в Norton Antivirus 2004 включен специальный модуль Pre-Install scanner, позволяющий проверить и при необходимости оздоровить компьютер уже на стадии инсталляции. Таким образом, программа без проблем может быть установлена даже на зараженный компьютер. Второе важное новшество - это обновлённая защита программы от несанкционированного копирования. Отныне работу с Norton Antivirus придётся начинать с активации программы.

С помощью NortonAntiVirus можно: проверить на вирусы отдельные файлы, папки или диски; запланировать автоматический поиск вирусов в заданное время; по плану или в любой нужный момент выполнить обновление файлов описания вирусов с помощью функции LiveUpdate.

Сотрудники фирмы Symantec отслеживают сообщения о появлении новых вирусов. После идентификации нового вирусы информация о нем (сигнатура) заносится в файлы описания вирусов. Поэтому данные файлы рекомендуется обновлять не реже, чем раз в месяц.

Во время проверки дисков и файлов (в ручном или запланированном режиме) NortonAntiVirus ищет вирусы по этим сигнатурам. Если обнаружен файл, зараженный одним из этих вирусов, то NortonAntiVirus может устранить заражение автоматически.

Борьбу с вирусами Norton AntiVirus ведет следующим образом.

- Выявляет проникшие в систему известные вирусы и уничтожает их (автозащита).

- Преграждает вирусам путь в систему (автозащита и вакцинация).

- Следит за подозрительными действиями, которые могут означать присутствие неизвестного вируса (автозащита с технологией вирусного датчика).

Перечисленные автоматические функции включены по умолчанию. В зависимости от степени риска в той среде, где используется компьютер, можно усилить или ослабить меры защиты путем настройки различных параметров Norton AntiVirus.

Кроме автоматического поиска вирусов средствами автозащиты, можно в любой момент начать ручной поиск или назначить его выполнение на определенное время.

NortonAntiVirus выдает сигналы тревоги при обнаружении:

- известного или неизвестного вируса;

- вирусоподобного действия (из числа тех, которые обычно совершаются вирусами при распространении или порче файлов);

- изменения вакцинации (когда файл либо не вакцинирован, либо подвергся изменению с момента последней вакцинации).

NortonAntiVirus может исправить большинство зараженных файлов. Однако если исправить файл не удается, его необходимо удалить с диска и затем заменить незараженной копией. Следует хранить оригинальные диски программ в безопасном месте и создавать резервные копии ценных файлов.

При проверке программных файлов NortonAntiVirus просматривает также документы и шаблоны MicrosoftWord и Excel. Хотя эти файлы не являются программными, в них могут легко проникать так называемые макровирусы.

Уничтожение вирусов.

Существует два способа уничтожения вирусов.

- Исправление зараженного файла, загрузочной записи или главной загрузочной записи.

- Удаление зараженного файла с диска и последующая замена его незараженной копией.

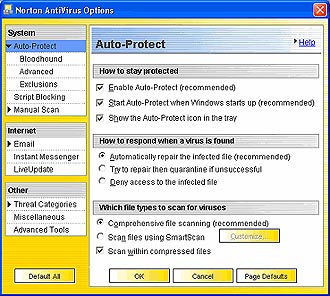


Рисунок 2.1 - Окно NortonAntiVirus

Ну, в остальном, по большому счёту, новая версия антивируса ничем не отличается от своего предшественника. Налицо всё тот же набор стандартных функций:

- автоматическое удаление вирусов, «червей» и различного рода «троянских» программ;

- проверка и обезоруживание входящей и исходящей электронной почты;

- выявление и блокировка вирусов в файлах, вложенных в сообщения службы передачи мгновенных сообщений;

- автоматическая загрузка обновлений системы антивирусной безопасности для защиты от новых угроз; технология Worm Blocking, позволяющая обнаруживать заражение «червями» (такими, как Nimda) в исходящих почтовых сообщениях;

- технологии Script Blocking и Worm Blocking, позволяющие выявить новые угрозы еще до того, как для них будут созданы описания вирусов;

- предусмотрены пошаговые инструкции для установки программы, в том числе, и на зараженные вирусами системы.

Не претерпел изменений и интерфейс программы, который по прежнему остаётся чрезвычайно удобным и, несмотря на свою англоязычность (русской версии я к моменту написания этой статьи, к сожалению, не нашёл), интуитивно понятным даже пользователю новичку.

Поставляется Norton Antivirus 2004 в двух различных вариантах. Для домашних пользователей предусмотрена стандартная версия, которая предлагается разработчиками на сайте по цене $49. Для среднего и малого бизнеса предназначается Norton Antivirus 2004 Professional, который имеет несколько дополнительных возможностей, в частности, поставляется с двумя лицензиями. Стоимость этой версии составляет $69. В заключение хотелось бы отметить, что компания Symantec в очередной раз подтвердила своё лидерство на рынке антивирусных программ, а Norton Antivirus по-прежнему остаётся самым популярным продуктом в этой сфере. Поэтому его смело можно рекомендовать абсолютно всем, для кого имеет значение защита и безопасность собственного компьютера.