Лабораторная работа № 4

Изучение особенностей применение современных специализированных пакетов антивирусных программ и приложений

Цель работы:

Закрепление теоретического материала по изучению действия программ-шпионов.

Изучение способов и правил защиты системы от программ-шпионов.

Приборы и оборудование:

Персональный компьютер

ОС MS Windows 7 (MS Windows 10), MS Office, Браузер Microsoft Internet Explorer (Edge)

Пояснения к работе и задание:

Как работают антивирусные программы

К сожалению, борьба с вирусами -дело весьма сложное, и далеко не каждый программист может правиться с ним самостоятельно. Поэтому практически единственный способ - это использование различных антивирусных программ. Надо четко понимать, что ни одна подобная программа не дает стопроцентной надежности - она может "не узнать" какой-либо вирус или, наоборот, заподозрить его в "добропорядочной программе". Т.к. новые вирусы появляются постоянно, то антивирусные программы следует регулярно обновлять, например, вирусная база AVP сейчас обновлять ежедневно, а антивирус DRWEB примерно раз в три дня.

У большинства антивирусов есть два режима использования - сканер и монитор. В режиме: сканирования тщательно проверяются файлы, расположенные на диске при этом вы можете указать для проверки отдельные файлы, директории или весь винчестер.

Рис. 1. Так выглядит окно системного трея с включенной программой-ревизором Spider

Монитор же является резидентной программой (т.е. он запущен все время, пока включен компьютер) и "на лету'" проверяет запускаемые вами программы и файлы, к которым эти программы обращаются (рис. 1). Как правило, монитор производит менее тщательную проверку, чем сканер, но все же позволяет выловить наиболее распространенные вирусы. к сожалению, у антивирусов есть один минус - они довольно ощутимо замедляют работу компьютера, ведь им надо проанализировать каждый файл, перед тем как разрешить его использование. Именно из-за этих недостатков пользователи очень часто отключают антивирусы.

Разумеется, можно отключить монитор, когда вы работаете со знакомыми программами, но если вы работаете с Интернет или запускаете какие-то новые программы, то лучше перестраховаться. И еще - стоит потратить пару минут и настроить сканер на автоматический запуск, скажем, в пятницу вечером, и проверку всех дисков и файлов. Помимо антивирусов, есть еще один очень полезный тип программ - ревизоры (например, ADinf32). Они отслеживают изменения в файлах, хранящихся на диске. При первом запуске такая программа Просматривает ваши файлы и для каждого из них запоминает контрольную суммы, а при последующих запусках пересчитывает суммы и сравнивает их с хранящимся значением. И, разумеется, выдает предупреждение, если размер какого-то файла изменился (вирус, заражая файл, несколько увеличивает его размер). . .

Использование ревизора требует некоторого терпения, Т.к. сначала у вас уйдет определенное время на его настройку - указание тех директорий и файлов, которые не надо отслеживать. А потом вам придется просматривать списки измененных файлов и решать, вирус это или нет?.. Но это вполне производительная трата времени - совместное использование антивируса и ревизора дает очень высокую степень защиты от вирусов.

Обзор антивирусных программ

Антивирусы - это программы, которые обнаруживают и удаляют вирусы с вашего компьютера. Наиболее представительными, на мой взгляд, являются DrWeb (www.dials.ru), Antiviral Tolkit Pro (AVP) (www.avp.ru), ADInf (Www.dials.ru или www.adinf.com). Эти программы постоянно получают международные сертификаты и считаются одними из лучших.

Кроме того, на упомянутых сайтах можно найти множество полезной информации о вирусах вообще. А главное обновления антивирусных баз.

В деле борьбы с вирусами главное - иметь свежий антивирус. В любом случае существует вероятность заполучить вирус или троянца. Антивирус может его сперва-не найти (если вирус еще неизвестен антивирусной программе). Но после обновления, т.е. получения с сайта производителя антивируса набора свежих антивирусных баз с последними дополнениями существует высокая вероятность, что вирус будет немедленно обнаружен и уничтожен (рис. 2).

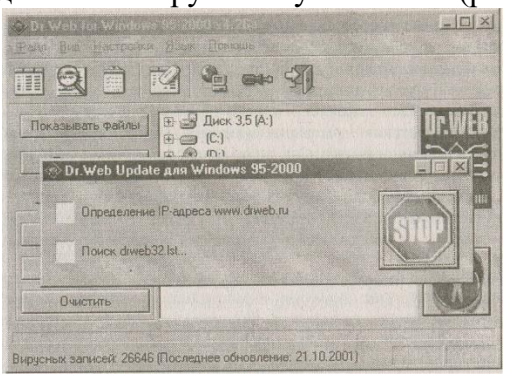

Рис. 2. Так выглядит обновление антивирусных баз для DrWEB

Также важно не запускать неизвестных вам программ. Из-за неуемного любопытства многие люди постоянно скачивают из Интернета различные программы и сразу запускают их или, купив пиратский компакт-диск, запускают программы, не проверив их на наличие вирусов. Если вы хотите работать с подобными программами, то установите антивирусный монитор (который отличается от антивирусного сканера). Когда вы запускаете DrWeb на проверку дисков – это антивирусный сканер. А поставляемый с ним в комплекте Spider - это антивирусный монитор (в комплекте с AVP поставляется monitor). Антивирусный монитор загружается вместе с операционной системой и постоянно проверяет все запускаемые файлы. И если находит вирус, то вам об этом сообщает. А потом, по вашей команде, может вылечить. А если не вылечит, то просто может уничтожить зараженную программу. И эта последовательность действий зависит от особенностей вируса, а также возможностей и установленных опций антивируса.

Понятно, что тотальная проверка файлов несколько замедляет работу, но поверьте, дело того стоит.

Коммерческие антивирусные программы

Теперь мы рассмотрим коммерческие антивирусные программы, которые предлагает нам сегодняшний рынок.

Собственно, наибольшую популярность у отечественных пользователей снискали две компании-производителя антивирусных программ: ЗАО "Лаборатория

Касперского" и ЗАО "ДиалогНаука" (http://www.dlals.ru). Мы рассмотрим их подробно, также уделим внимание лучшим зарубежным антивирусным программам.

Aidstest

Создание Д. Н. Лозинским, в далеком 1988 г., первой версии программы привело к появлению ЗАО "ДиалогНаука". Когда-то Aidstest бьm весьма почитаем, но, похоже, сейчас его время ушло - на смену пришел Doctor Web. Не в пользу Aidstest'a говорит и то, что в нем отсутствуют не DOS-версии *(т.е. все параметры приходится задавать искточительно из командной строки, следовательно, от пользователя требуются специальные знания) Но разработчики не унывают, например, последняя версия продукта уже позволяет удаленно проверять файлы через Интернет! Какие еще функции можно возложить на Aidstest? Программа неплохо сканирует и обезвреживает файловые и загрузочные вирусы, а также их комбинации. Конечно, ввиду своей чрезвычайно низкой требовательности к ресурсам, она идеально подойдет для маломощных или старых машин. Во всех остальных случаях придется обратиться к другим средствам DSAV.*

Doctor Web

Легендарная программа, разработанная И. А. Даниловым в 1994г. и пришедшая на смену морально устаревающему Aidstest'у. Она до сих пор не потеряла своей популярности, кстати, недавно вышла ее новая версия 4.26. Существует в двух вариантах-16-,И 32-битном. Последний факт дает основания предполагать, что Doctor Web будет и в дальнейшем нас радовать качественными обновками.

Последняя версия продукта распознает вполне приличное количество вирусов, поэтому приверженцам "ДиалогНауки" советуем со всей серьезностью относиться к обновлению антивирусного программного обеспечения. С недавнего времени Doctor Web выпускают не только для DOS/Windows, но и для OS/2, Noveil NetWare, Linux и ряда других платформ. Бесплатные и ознакомительные некоммерческие версии некоторых перечисленных продуктов компании можно загрузитъ на http://www.dials.ru/download. Если захотите что-либо купить, на страничке http://www.dials.ru/commerce/shop.htm можно найти список электронных (и не только) магазинов.

AVP

Эта торговая марка известна далеко за пределами России, а последние несколько лет она неизменно фигурирует в тройке лучших антивирусных производителей мира: если верить статистике, ей отдает предпочтение каждый второй пользователь! И это неудивительно - сложно найти обеспечение, равное по надежности программам AVP (AntiViral Toolkit Pro) или "АнтивирусКасперского". Эту истину неоднократно подтверждали множество именитых компьютерных изданий. Линейка AVP состоит из четырех продуктов: Lite и Gold, ориентированных на домашние ПК, Platinum - для малого бизнеса, и "Решение для Корпоративных пользователей" - для крупного.

Lite

Из названия можно сделать вывод о некоторой неполноценности продукта. На самом деле, это не совсем так. Конечно, лучше всего он подойдет для начинающих пользователей, поскольку чрезвычайно прост в обращении. Однако, вместе с тем, он обладает весьма серьезными возможностями борьбы с вирусами, "троянцами", интернет-червями, Java-апплетами, модулями ActiveX и др. Программа позволяет контролировать трафик из сети, электронную почту, дискеты и прочие внешние носители, архивированные файлы многих популярных форматов независимо от того, защищены ли они паролем!

Кстати, ввиду своей простоты, AVP Lite работает только под управлением DOS и "Windows 9x".

Gold

Главное отличие этой версии программы от предыдущей состоит в том, что она поддерживает не только системы на базе DOS/Windows 9x, но и NT/2000. Также AVP Gold содержит встроенные функции управления временем, порядком и параметрами запуска антивируса, регулирования прав доступа к изменению конфигурации. Преимущество, общее для всех продуктов AVP - возможность заказать "противоядие" от ранее неизвестного вируса и, главное, получить его не позже, чем через двое суток!

Чтобы получить демо-версию "Антивируса Касперского" на русском или английском языке (http://www.kaspersky.ru/download.asp), придется предварительно заполнить анкету. Желающим купить нормальную версию продукт советую посетить "On-line магазин" компании по адресу http://www.kaspersky.ru/buyonline.asp .

Ход выполнения лабораторной работы:

1. Изучить приведенный в методическом описании к лабораторной работе материал.
2. Выполнить практическое ознакомление с разделами с применением возможностей лаборатории.
3. Оформить отчет в установленной форме по разделам.
4. Ответить на контрольные вопросы.
5. Представить результаты работы преподавателю.

Контрольные вопросы:

1. Назовите особенности воздействий компьютерных вирусов.
2. Перечислите виды компьютерных вирусов.
3. Назовите особенности работы антивирусных программ.
4. Перечислите виды антивирусных программ.
5. Какие пакеты относятся к коммерческим антивирусным программам?