Урок № 52.
Тема урока: «Практическое занятие № 20. Обнаружение вредоносных программ.»

Цель работы: Ознакомиться с различными видами программных средств защиты от вирусов. Получить навыки работы с антивирусной программой Антивирус
Касперского 6.0.

Краткое содержание теоретической части:

1. Антивирусные программы и пакеты

Вскоре после появления первых вирусов были созданы противостоящие им антивирусные средства. Компьютерные вирусы непрерывно совершенствуются. То же происходит и с антивирусными средствами. Сегодня защитные функции уже не возлагаются на единичную антивирусную программу. Пакеты антивирусных программ состоят из нескольких компонентов, каждый из которых решает свою задачу.

Термин «антивирус» носит исторический характер. Как уже упоминалось, антивирусные пакеты предназначены для борьбы со всеми типами враждебных программ.

В частности, механизмы объединения двух программ в один исполняемый файл рассматриваются как средство внедрения троянских программ и вызывают реакцию со стороны антивирусных средств.

1.1 Сканирующие программы

Сканеры просматривают оперативную память компьютера и носители данных (служебные секторы и файловую структуру) в поисках вирусоподобных объектов.

Поиск вирусов основан на сличении фрагментов кода или иных признаков с образцами, характерными для известных вирусов, зарегистрированных в антивирусной базе данных. Современные антивирусные сканеры способны выявить и самошифрующиеся (полиморфные) вирусы.

Кроме розыска вирусов, сканеры выполняют и лечебно-предохранительные функции. Они обычно способны уничтожить вирус и восстановить исходное состояние файла. Файл также можно переименовать, удалить или отправить в «карантин» - специальную папку, исключающую активизацию вируса. При «лечении» зараженных файлов сохраняется опасность их необратимого повреждения, поэтому для ценных файлов принято перед лечением создавать в карантинной папке копию.

Если антивирусная программа не поддерживает работу с карантинной папкой, можно организовать карантин своими руками. Для этого достаточно запаковать подозрительный файл каким-либо архиватором и сохранить архив в надежном месте. Вирус, содержащийся в заархивированном файле, работать не может.

Хорошие антивирусные сканеры обладают и дополнительными функциями: возможностью запуска с гибкого диска, средствами поиска вирусов в архивах, базах данных и запакованных файлах. Полезны также средства интеграции с Проводником Windows. В последнем случае запустить сканирование можно через контекстное меню. Это удобно, если надо проверить отдельный объект (файл или папку).

1.2 Антивирусные мониторы

Мониторами называют средства наблюдения за идущими процессами. Соответственно, антивирусные мониторы - это программы, работающие в фоновом режиме и наблюдающие за файловыми операциями операционной системы (копирование, открытие, запуск и другие). Антивирусный монитор можно считать сканером, работающим в режиме реального времени. Сканер запускается по желанию, например один раз в месяц, а монитор работает всегда. Он включается при загрузке компьютера и следит за всеми операциями.

Между сканерами и мониторами есть большая разница. Цель сканера - обнаружить вирусы, имеющиеся на компьютере. Цель монитора - поймать вирус при попытке проникновения.

Например, на компьютере можно установить несколько сканеров разных производителей. В этом случае сильные стороны одного сканера могут компенсировать слабости другого. Устанавливать несколько мониторов не имеет смысла - они выполняют одни и те же операции в одно и то же время и могут только мешать друг другу. Эффективность и устойчивость работы компьютера почти наверняка упадут.

1.3 Программы-ревизоры

Ревизоры, или инспекторы, встречаются в самых серьезных версиях антивирусных пакетов, рассчитанных на корпоративного или профессионального потребителя.

Основная задача ревизора - контролировать вирусную активность, то есть регистрировать вирусные или вирусоподобные действия. Ревизор способен обнаружить даже неизвестные вирусы, сведения о которых отсутствуют в антивирусной базе данных.

Программа-ревизор отслеживает изменение файлов, хранящихся на дисках, а также служебных записей диска. При первом запуске создается база данных, в которую записываются размеры и контрольные суммы файлов, а также их атрибуты и некоторые другие данные. Для наиболее важных системных файлов этих данных достаточно, чтобы восстановить файл в случае повреждения. Кроме того, ревизор сохраняет дубликаты служебных разделов дисков (главная загрузочная запись, загрузочные записи дисков, содержимое корневого каталога), чтобы и в случае катастрофы пользователь мог добраться до своих файлов.

При последующих запусках (или в фоновом режиме работы) ревизор проверяет эти данные для зарегистрированных файлов. Десятки и сотни файлов создаются и модифицируются на компьютере ежедневно, что ни в коей мере не говорит о

деятельности вирусов. Но некоторые изменения дают основание для подозрений - и о них ревизор сигнализирует. Вот какие изменения считаются подозрительными:

- изменено содержимое файла, а дата создания или последнего изменения файла не изменилась;
- размеры разных файлов изменились одинаково;
- в атрибутах файла появилась некорректная дата или время, что может быть пометкой, сделанной файловым вирусом;
- изменен важный системный файл, внесенный в список файлов, не подлежащих изменению.

Принципы действия программ-ревизоров хорошо известны создателям вирусов.

Поэтому нередко вирус начинает работу с того, что пытается обнаружить и заглушить программу-ревизор, чтобы она не могла сообщить о подозрительной деятельности.

1.4 Средства автоматического обновления антивирусных баз

В основе всех программных продуктов антивирусного пакета лежат антивирусные базы данных. Регулярное появление новых вирусов и их разновидностей требует столь же регулярного обновления этих баз. Разработчики антивирусных средств выкладывают дополнения к базам на своих сайтах ежедневно, так как для некоторых почтовых вирусов возникновение и развитие «эпидемии» происходит буквально за несколько часов. Но частоту обновления своих баз выбирает пользователь - он может избрать ежедневное, еженедельное, ежемесячное или кумулятивное обновление. В последнем случае базы приводятся в актуальное состояние независимо от даты предыдущего обновления.

Кумулятивное обновление можно выполнять вручную, время от времени (не обязательно регулярно) посещая Web-узел разработчика. Но регулярные обновления целесообразно автоматизировать. Для этого в состав пакета обычно входит специальный модуль, способный автоматически связаться с сайтом поставщика антивирусных баз, принять необходимые файлы и обновить действующую базу.

1.5 Комплекты аварийного восстановления

Хорошее антивирусное средство предусматривает возможность того, что его попытаются применить слишком поздно - тогда, когда вирус уже успел начать свою разрушительную деятельность и, возможно, вывести из строя жесткий диск. На такой случай можно создать комплект дисков, с помощью которых можно проверить компьютер на наличие вирусов даже при неработающем жестком диске.

Во многих случаях удается не только установить наличие вируса, но и ликвидировать его последствия, хотя бы самые критичные, препятствующие нормальному запуску.

1.6 Планировщики заданий

Недостаток антивирусной системы состоит в том, что постоянный антивирусный контроль заметно снижает эффективность работы. При нормально организованной работе угроза заражения не столь уж высока, и желательно организовать работу антивирусных средств так, чтобы они не превращались в помеху.

Например, достаточно, если сканер отработает один раз в сутки - утром или вечером. Но, например, мониторы и ревизоры эффективны, только если они работают постоянно, запускаясь вместе с операционной системой. Средства обновления баз данных можно запускать - раз в день или в неделю.

Организовать запуск нужных программ по приемлемому расписанию позволяют специальные программы, планировщики заданий, цель которых – автоматизация рутинных операций. Настроив планировщик один раз, можно навсегда забыть о компьютерных вирусах и доверить борьбу с ними автоматике и поставщику антивирусных средств.

ВЫПОЛНЕНИЕ РАБОТЫ

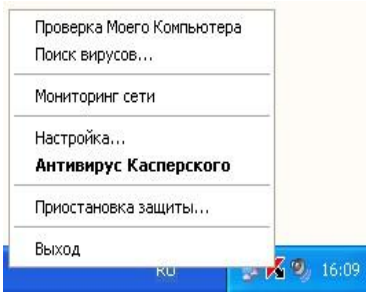
Получение практических навыков работы с Антивирусом Касперского 6.0

Задание № 1

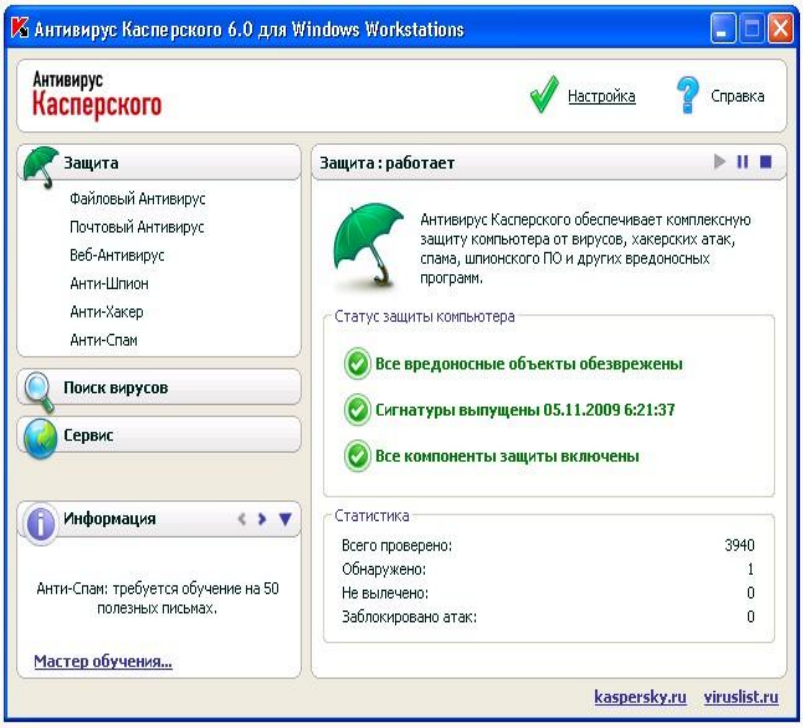
1. Убедитесь в том что, Антивирус Касперского в данный момент загружен и работает, об этом символизирует иконка  на системной панели в правом нижнем углу экрана. В зависимости от задачи, выполняемой антивирусом, картинка на ней может меняться. В дальнейшем в ходе лабораторных работ во время выполнения разных задач всегда обращайте внимание на вид этой иконки.

Дополнительно она служит для быстрого доступа к основным функциям антивируса: двойной щелчок левой клавишей мыши на ней вызывает главное окно интерфейса, а контекстное меню, открываемое щелчком правой клавиши мыши позволяет сразу перейти на нужное окно интерфейса.

Откройте контекстное меню иконки Антивируса Касперского и ознакомьтесь с представленным здесь списком ссылок:



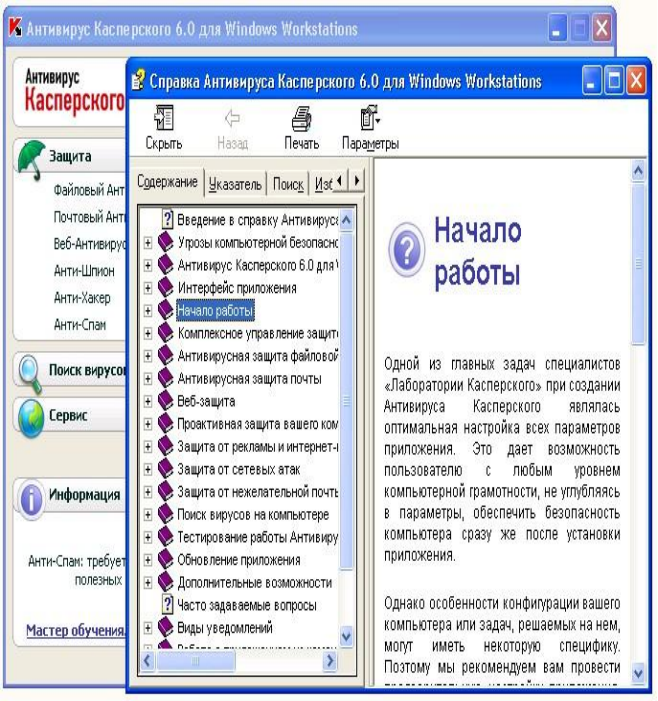
2. С помощью двойного щелчка на иконке откройте главное окно интерфейса Антивируса Касперского



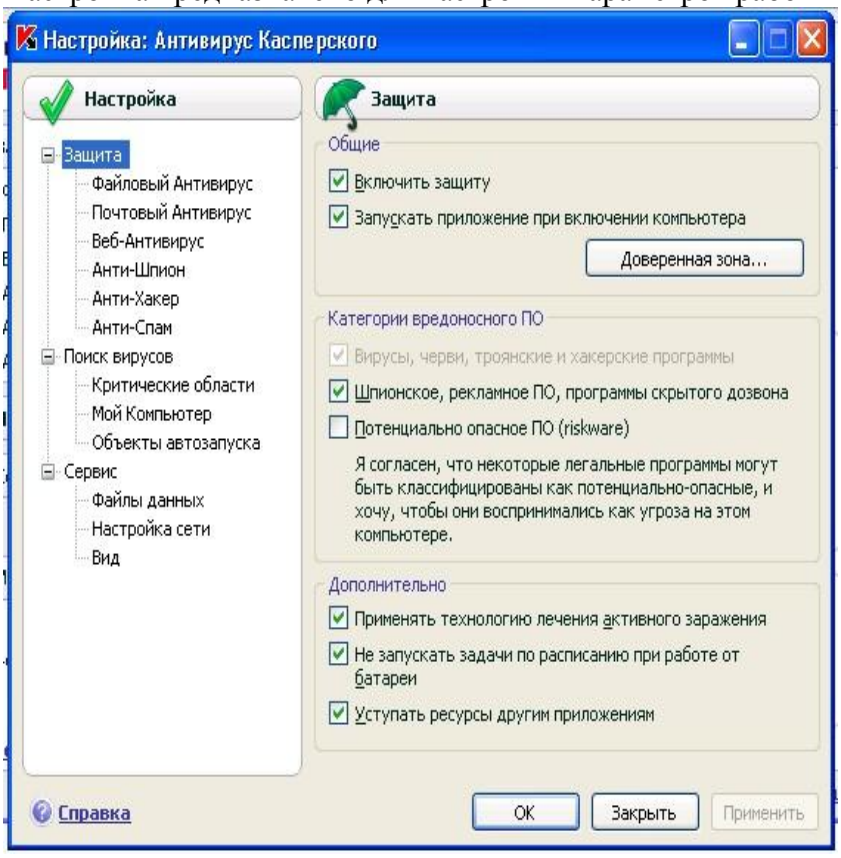
3. В верхней правой части окна размещено две ссылки: Настройка и Справка. Первая используется для настройки антивируса, вторая - для вывода справочной системы.

Нажмите ссылку Справка

Открывшееся окно содержит руководство пользователя Антивирусом Касперского. При возникновении каких-либо проблем, в первую очередь всегда нужно обращаться к нему. Ознакомьтесь с содержанием справочной системы в левой панели окна и закрыв его вернитесь к главному окну антивируса



4. В главном окне нажмите ссылку Настройка, расположенную слева от Справка.
Открывшееся окно Настройка предназначено для настройки параметров работы антивируса.



5. Изучите настройки антивируса. Какие по вашему мнению для эффективной работы антивируса лучше произвести настройки?

По интересующим вопросам обратитесь к разделу Справка.

Сохраните ваши настройки

6. Зайдите в раздел поиска вирусов нажав на кнопку в контекстном меню

Произведите выбор объектов для проверки нажав на кнопку «Добавить» и «Удалить».

Произведите поиск вирусов нажав на кнопку «Поиск вирусов». 7. При окончании поиска изучите файл отчета поиска.

ЗАДАНИЕ САМОКОНТРОЛЯ. (РЕЗУЛЬТАТ ПРИШЛИТЕ МНЕ НА ПОЧТУ)

Подготовьте доклад на тему: «Общие сведения и особенности работы антивирусной программы *[Название антивирусной программы]*». Название антивирусной программы выбрать согласно предложенному списку

Объем доклада 4-5 страницы..

№ п\п	Название антивирусной программы
1	AVG
2	Dr.Web
3	Avira
4	Panda AntiVirus
5	McAfee VirusScan
6	Eset Nod32
7	Microsoft Security Essentials
8	Norton AntiVirus
9	Антивирус Касперского
10	Avast!