МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ, НАУКИ И ИННОВАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

САМАРКАНДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ВЕТЕРИНАРНОЙ МЕДИЦИНЫ, ЖИВОТНОВОДСТВА И БИОТЕХНОЛОГИЙ

Кафедра Информационных Технологии

Сафарова Лола Ульмасовна

Методическое указание

к выполнению лабораторных работ по дисциплины

“ ИНФОРМАЦИОННО-КОММУНИКАЦИОНЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ И СИСТЕМЫ ”

Применение антивирусных программ.

САМАРКАНД - 2025

Составитель: Сафарова Лола Улмасовна заведующий кафедры Информационных технологий

Лабораторное занятие №5.
Выполнение лабораторных заданий по теме
«Безопасность информации в компьютере.».
Самарканд.

Основной целью данного указания является закрепление студентами полученных теоретических знаний по пройденному дисциплины «**Информационно-коммуникационные технологии в отраслях**» при решении прикладных задач.

Методическое указание предназначено для студентов 1 - курса бакалавриата.

Рассмотрена и рекомендована к публикации на заседании учебно-методического совета Самаркандского государственного университета ветеринарной медицины животноводства и биотехнологий _____ _____ 2025 года протокол № ____

Рецензенты: Доцент кафедры «Информационных технологий » к.э.н Урдушев Х

Профессор кафедры «Информационных технологий» Самаркандского филиала ТУИТ, д.т.н. Примова Х

Содержание

СОДЕРЖАНИЕ

САМАРКАНДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ВЕТЕРИНАРНОЙ МЕДИЦИНЫ, ЖИВОТНОВОДСТВА И БИОТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ

ПАСПОРТ
ЛАБОРАТОРНОГО ЗАНЯТИЯ ПО ДИСЦИПЛИНЕ “ИНФОРМАЦИОННО-КОММУНИКАЦИОНЫЕ ТЕХНОЛОГИИ В ЭКОНОМИКЕ И СИСТЕМЫ”

”

Лабораторная работа № 5

Тема: Безопасность информации в компьютере

Количество часов: 2

Цель: – ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидности вирусов, способы заражения и методы борьбы**.**

- получить представление о понятии «компьютерный вирус»;
- узнать о методах борьбы с вредоносным ПО;

получить первичные навыки работы с антивирусами

Оборудование: персональный компьютер, антивирусная программа.

Литературы

Основные литературы

1. Kenjaboev A.T., Ikramov M.M., Allanazarov A.Sh. Axborot - kommunikatsiya texnologiyalari. – Toshkent: O‘zbekiston faylasuflari milliy jamiyati nashryoti, 2017 yil. – 408 bet.

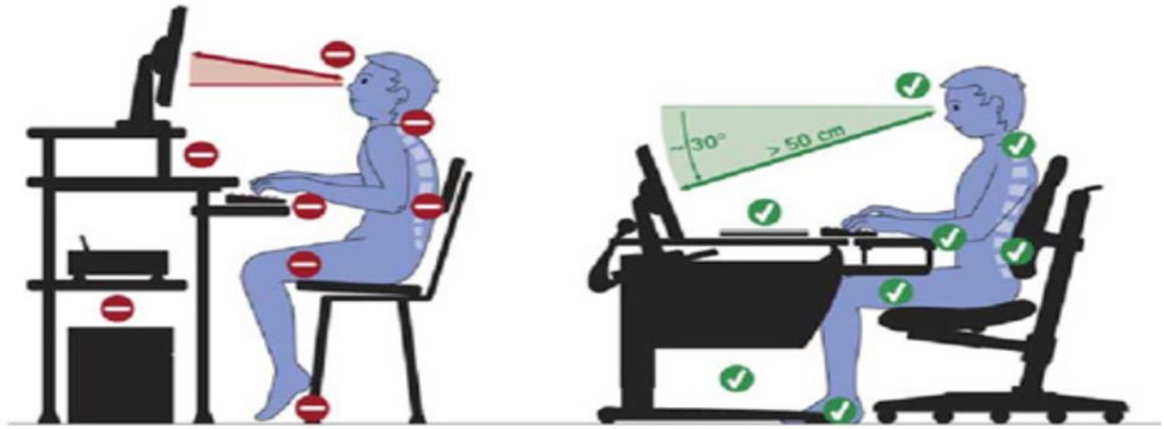
2. Aminov S.M., Muxamadiyev S.I., Rasulov S.Sh. Axborot kommunikatsion texnologiyalar fanidan amaliy va laboratoriya mashg‘ulotlarini bajarish bo‘yicha o‘quv qo‘llanma. –T.:ToshDAU, 2020 yil. – 248 bet.

3. Шыныбеков Д.А., Ускенбаева Р.К. и др. Информационно-коммуникационные технологии. 1-е изд. Учебник. – Алматы: Издание АО «Международный университет информационных технологий» 2017 год. – 559 стр.

4. Misty E. Vermaat, Susan L. Sebok, Steven M. Freund. Jennifer T. Campbel, Mark Frydenberg. Discovering Computers: Tools, Apps, Devices, and the Impact of Technology (textbook). Cengage Learning. 20 Channel Center Street. Boston, MA 02210. USA, 2016 year. – 691 pages.

5. Alexis Leon & Mathews Leon. Fundamentals Of Information Technology. Vikas Publishing House Pvt Limited. ISBN 8182092450, 9788182092457. 2019 year. – 602 pages.

Техника безопасности при работе на компьютере



Ход урока:

• Краткое повторение теоретических понятий;
• Объяснить порядок выполнения лабораторных занятий;
• Распределение лабораторных заданий;
• Выполнение лабораторных работ (в электронном виде) и регистрация(в платформе hemis.otmsamvmi.uz);
• Оценка лабораторной работы.

Заведующий кафедры: Сафарова Л.У

Ход работы

Теоретические сведения.

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа, внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или FAT-таблицу, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющихся в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Типы вредоносного программного обеспечения

Трояны. (Trojan.Win32) - это тип вирусов, называемая троянами, осовая цель которых это вредоносное воздействие по отношению к системе. Это наиболее распространенный тип вредоносных программ. У них нет механизмов создания собственных копий, но в некоторые включают возможность преодоления защиты компьютера. Типичные случаи заражения - это попадание трояна вместе с вирусом или сетевым червем, а также в результате невнимательности пользователя программы злоумышленником. Вот краткий список типов троянов, которые чаще всего можно встретить:

Trojan-SPY - Клавиатурные шпионы.

Trojan-PSW- Похитители паролей.

Backdoor – удаленное управление над ПК..

Trojan-Proxy – Анонимные сервера и прокси для рассылки спама.

Trojan-Cliker – Изменяющий настройки браузера. Трояны, меняющие адреса стартовой страницы, поисковиков и других веб адресов хранящихся в браузере.

Trojan-Dropper – Установщики других вредоносных программ. Трояны, которые позволяют производить скрытую установку других вредоносных программ.

Trojan-Downloader - Загрузчики вредоносных программ.

Черви. (Worm.Win32) – это еще один из видов вредоносных программ, которые распространяются по различным сетям, каналам. Они самостоятельно преодолевают системы защиты, персональных компьютеров, и

автоматизированных систем (серверов). Создают и распространяют свои копии, которые могут в корне отличаться от исходного. Чаще всего сетевой червь в паре с трояном: червь преодолевает системы защиты и внедряет трояна, или же, червь загрузив себя в систему продолжает распространяться, и при этом каждая копия, находящееся в системе, загружает другое вредоносное по с Интернет.

По путям проникновения можно выделить следующие типы червей:

Mail-Worm – из названия можно понять, что это черви распространяющиеся через сообщения электронной почты.

IM-Worm – черви, которые используют Интернет-пейджеры.

P2P-Worm – от peer-to-peer, через файлообменные (торрент) сети.

Net-Worm – это черви, которые для распространения используют протоколы Интернет, в частности TCP/IP. Сюда же входит и локальная сеть.

Проявление наличия вируса в работе на ПЭВМ

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

Некоторые признаки заражения:

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы и т.д.;
- работа на компьютере существенно замедляется;
- некоторые файлы оказываются испорченными и т.д.
- операционная система не загружается;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- значительное увеличение количества файлов на диска;
- существенное уменьшение размера свободной оперативной памяти и т.п.

Некоторые виды вирусов вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, форматируют весь жесткий диск на компьютере. Другие вирусы стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске.

Таким образом, если не предпринимать мер по защите от вируса, то последствия заражения компьютера могут быть очень серьезными.

Разновидности компьютерных вирусов

Вирусы классифицируют по среде обитания и по способу воздействия. По среде обитания вирусы подразделяются на следующие виды:

- файловые вирусы, которые внедряются главным образом в исполняемые файлы, т.е. файлы с расширением exe, com, bat, но могут распространяться и через файлы документов;
- загрузочные, которые внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска;

- макровирусы, которые заражают файлы-документы и шаблоны документов Word и Excel.;
- сетевые, распространяются по компьютерной сети;

По способу воздействия (особенностям алгоритма) вирусы отличаются большим разнообразием. Известны вирусы-паразиты, вирусы-черви, вирусы-невидимки (стелс-вирусы), вирусы-призраки (вирусы-мутанты), компаньон-вирусы, троянские кони и др.

Чаще всего встречаются вирусы, заражающие исполнимые файлы. Некоторые вирусы заражают и файлы, и загрузочные области дисков.

Чтобы предотвратить свое обнаружение, некоторые вирусы применяют довольно хитрые приемы маскировки. Рассмотрим "невидимые" и самомодифицирующиеся вирусы.

"Невидимые" вирусы. Многие **резидентные вирусы** (резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них) (и файловые, и загрузочные) предотвращают свое обнаружение тем, что перехватывают обращения операционной системы к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде. Разумеется, этот эффект наблюдается только на зараженном компьютере - на "чистом" компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить.

Самомодифицирующиеся вирусы. Другой способ, применяемый вирусами для того, чтобы укрыться от обнаружения, - модификация своего тела. Многие вирусы хранят большую часть своего тела в закодированном виде, чтобы с помощью дизассемблеров нельзя было разобраться в механизме их работы. Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры этой кодировки, а кроме того, изменяют и свою стартовую часть, которая служит для раскодировки остальных команд вируса. Таким образом, в теле подобного вируса не имеется ни одной постоянной цепочки байтов, по которой можно было бы идентифицировать вирус. Это, естественно, затрудняет нахождение таких вирусов программами-детекторами.

Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

- Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:
- копирование информации - создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. Такая комбинация называется **сигнатурой**. При ее обнаружении в каком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей "известны".

Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова - в ней могут сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, неизвестные программам-детекторам.

Программы-ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Многие программы-ревизоры являются довольно "интеллектуальными" - они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Понятно, что в нормальной ситуации такие изменения практически никогда не встречаются, поэтому программа-ревизор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они вызваны именно вирусом.

Программы-фильтры, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и

нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые **программы-фильтры** не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны - они позволяют обнаружить многие вирусы на самой ранней стадии.

Программы-вакцины, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Рассмотрим структуру этой обороны.

Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На переднем крае обороны находятся программы-фильтры. Эти программы могут первыми сообщить о работе вируса и предотвратить заражение программ и дисков.

Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры.

Самый глубокий эшелон обороны - это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные. В "стратегическом резерве" находятся архивные копии информации. Это позволяет восстановить информацию при её повреждении.

Итак, одним из основных методов борьбы с вирусами является своевременная профилактика их появления и распространения. Только комплексные профилактические меры защиты обеспечивают защиту от возможной потери информации. В комплекс таких мер входят:

1. Регулярное архивирование информации (создание резервных копий важных файлов и системных областей винчестера).
2. Использование только лицензионных дистрибутивных копий программных продуктов.
3. Систематическая проверка компьютера на наличие вирусов. Компьютер должен быть оснащен эффективным регулярно используемым и постоянно обновляемым пакетом антивирусных программ. Для обеспечения большей безопасности следует применять параллельно несколько антивирусных программ.
4. Осуществление входного контроля нового программного обеспечения, поступивших дискет. При переносе на компьютер

файлов в архивированном виде после распаковки их также необходимо проверять.

5. При работе на других компьютерах всегда нужно защищать свои дискеты от записи в тех случаях, когда на них не планируется запись информации.
6. При поиске вирусов следует использовать заведомо чистую операционную систему, загруженную с дискеты.
7. При работе в сети необходимо использовать антивирусные программы для входного контроля всех файлов, получаемых из компьютерных сетей. Никогда не следует запускать непроверенные файлы, полученные по компьютерным сетям.

Современные технологии антивирусной защиты позволяют защитить от вируса файловые сервера, почтовые сервера и сервера приложений. Например, антивирус Касперского для защиты файловых серверов позволяет обнаружить и нейтрализовать все типы вредоносных программ на файловых серверах и серверах приложений, работающих под управлением ОС Solaris, включая "троянские" программы, Java и ActiveX – апплеты.

В состав антивируса Касперского для защиты файловых серверов входят:

- антивирусный сканер, осуществляющий антивирусную проверку всех доступных файловых систем на наличие вирусов по требованию пользователя. Проверяются в том числе архивированные и сжатые файлы;
- антивирусный демон, являющийся разновидностью антивирусного сканера с оптимизированной процедурой загрузки антивирусных баз в память, осуществляет проверку данных в масштабе реального времени;
- ревизор изменений, Kaspersky Inspector, отслеживает все изменения, происходящие в файловых системах компьютера. Модуль не требует обновлений антивирусной базы: контроль осуществляется на основе снятия контрольных сумм файлов (CRC – сумм) и их последующего сравнения с данными, полученными после изменения файлов.

Комбинированное использование этих модулей позволяет создать антивирусную защиту, наиболее точно отвечающую системным требованиям.

Обнаруженные подозрительные или инфицированные объекты могут быть помещены в предварительно указанную "карантинную" директорию для последующего анализа.

Антивирус Касперского обеспечивает полномасштабную централизованную антивирусную защиту почтовых систем, работающих под управлением ОС Solaris.

Проверке на наличие вирусов подвергаются все элементы электронного письма – тело, прикрепленные файлы (в том числе архивированные и компрессированные), внедренные OLE-объекты, сообщения любого уровня вложенности. Обнаруженные подозрительные или инфицированные объекты могут быть вылечены, удалены, переименованы, или помещены в заранее определенную карантинную директорию для последующего анализа.

Ежедневное обновление базы вирусных сигнатур, автоматически реализуется через Интернет при помощи специально встроенного модуля и обеспечивает высокий уровень детектирования компьютерных вирусов.

Задание 1. Изучение интерфейса

В этом задании изучается интерфейс **Антивируса Касперского**. Фактически, он состоит из четырех окон:

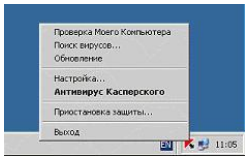
- **Главного окна**, в котором можно управлять задачами и компонентами антивируса. В нем также расположены ссылки на остальные окна
- **Окна настроек**, предназначенного для настройки задач и компонентов
- **Окна статистики и отчетов**, в котором можно получить данные о результатах работы антивируса
- **Окна справочной системы**

В ходе выполнения задания нужно будет поочередно вызвать все четыре окна интерфейса **Антивируса Касперского** и ознакомиться с их внешним видом.

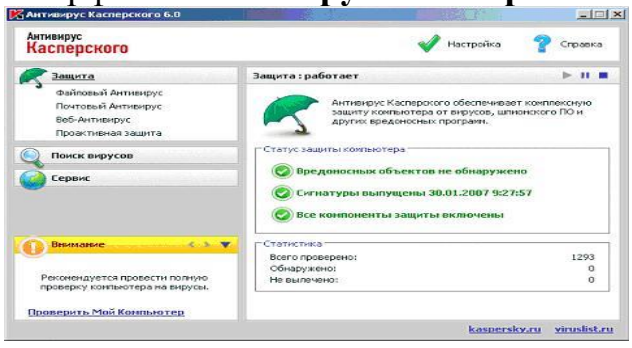
1. О том, что **Антивирус Касперского** в данный момент загружен и работает, символизирует иконка на системной панели в правом нижнем углу экрана. В зависимости от задачи, выполняемой антивирусом, картинка на ней может меняться. В дальнейшем в ходе лабораторных работ во время выполнения разных задач 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**

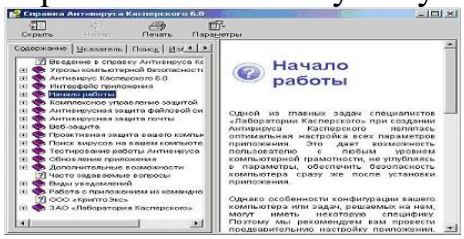


2. В верхней правой части окна размещено две ссылки: **Настройка** и **Справка**. Первая используется для настройки антивируса, вторая - для вывода справочной системы.

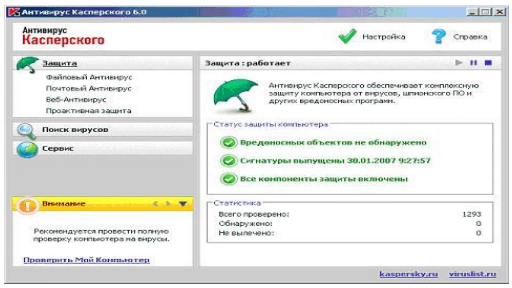
Нажмите ссылку **Справка**

3. Открывшееся окно содержит руководство пользователя **Антивирусом Касперского**. При возникновении каких-либо проблем, в

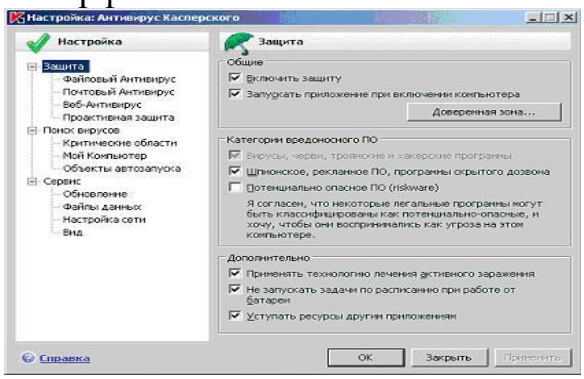
первую очередь всегда нужно обращаться к нему. Ознакомьтесь с содержанием справочной системы в левой панели окна и закрыв его вернитесь к главному окну антивируса



4. В главном окне нажмите ссылку **Настройка**, расположенную слева от **Справка**

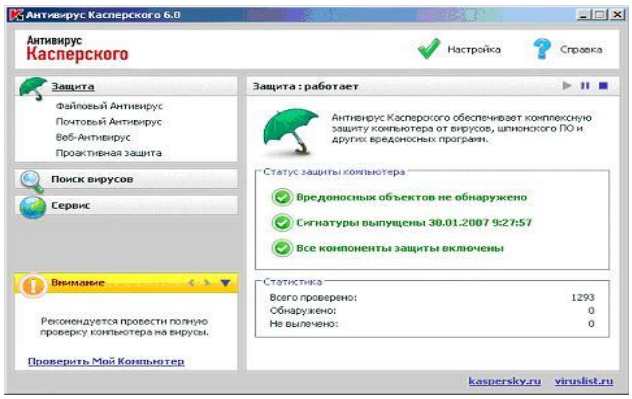


5. Открывшееся окно **Настройка** предназначено для настройки параметров работы антивируса. Изучите окно **Настройка**, пройдя по всем вкладкам. Нажмите **Закрыть** и вернитесь к главному окну интерфейса



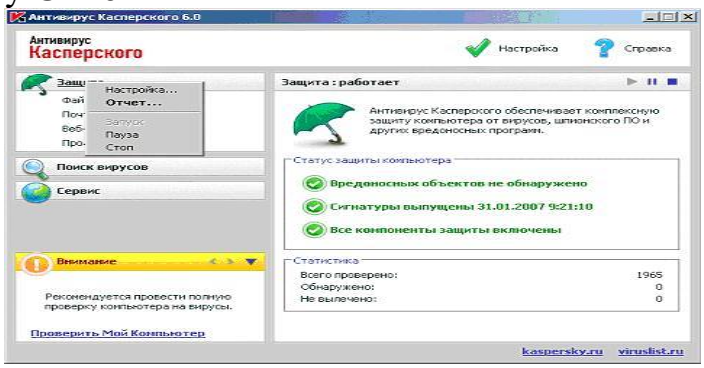
6. Найдите элемент **Защита**, выделенный подчеркиванием (

, в левой части окна) и нажатием на нем правой клавишей мыши выведите контекстное меню

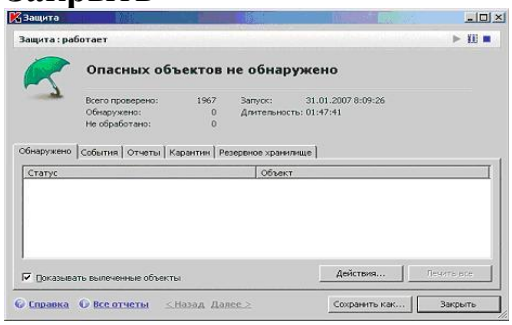


7. Контекстное меню разделено на две зоны: верхняя содержит ссылки **Настройка** (открывает рассмотренное выше окно **Настройка**) и **Отчет**. Нижняя - кнопки управления работой защиты.

Для перехода к последнему из основных, четвертому окну, выберите ссылку **Отчет**

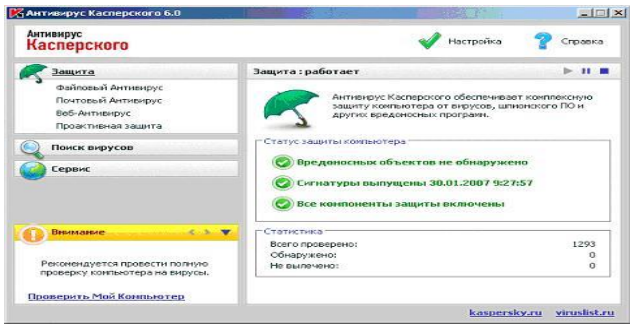


8. Ознакомьтесь с внешним видом этого окна и нажмите **Закрыть**

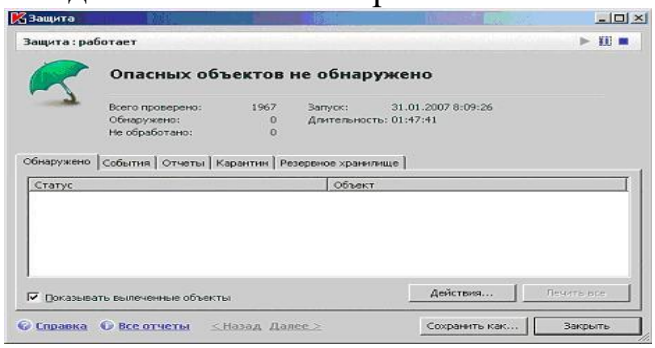


9. В главном окне интерфейса обратите внимание, что весь текст в информационной части окна, разбитый серыми рамками на группы, содержит ссылки. Таким образом, в главном окне представлен только небольшой отчет о неком компоненте антивируса, а по нажатию на него выводится окно с подробной информацией.

Убедитесь в этом, щелкнув левой клавишей мыши по группе **Статистика**.



10. В результате должно открыться то же окно, что в пункте 10. Убедитесь в этом и закройте окно статистики, нажав **Закрыть**



11. Вернитесь к главному окну интерфейса антивируса и закройте его

Задание 2. Структура и настройки

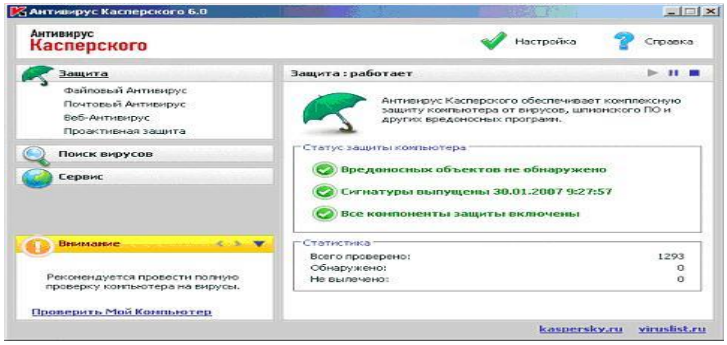
Это задание посвящено изучению **Окна настроек** и на его примере - структуры **Антивируса Касперского**.

Как и любой антивирус для рабочей станции, персональный **Антивирус Касперского** обеспечивает:

- Проверку в режиме реального времени, то есть "на лету" или постоянную защиту. В терминах **Антивируса Касперского** это называется одним словом - "**Защита**". Она в свою очередь делится на защиту файловой системы, почты, проверку просматриваемых веб-страниц и проактивную защиту. Эти элементы называются "компонентами защиты", настраивать и управлять ими можно по отдельности
- Проверку по требованию, в терминах **Антивируса Касперского** - задачи типа "**Поиск вирусов**"
- Средства обновления антивирусных баз, просмотра статистики и отчетов и пр. - все это объединяется термином "**Сервис**"

В задании нужно будет перейти к окну **Настройка** и с помощью расположенного в нем дерева настроек изучить структуру антивируса.

1. Откройте главное окно интерфейса антивируса



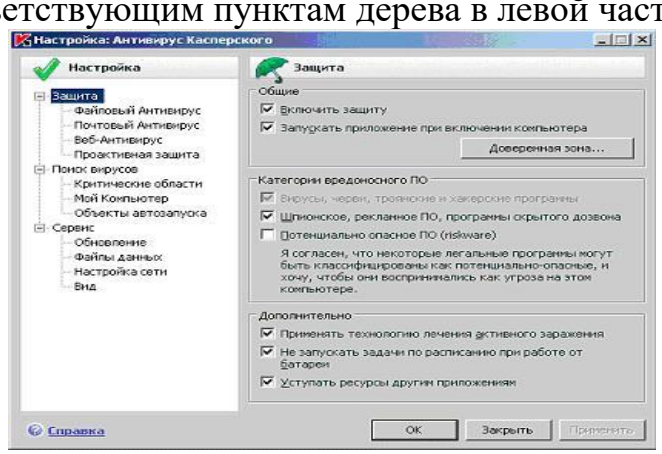
2. Перейдите к окну настроек, нажав ссылку **Настройка** (

)

3. Открывшееся окно **Настройка** разделено вертикально на две части. Слева - дерево настроек, в котором можно выбирать нужный компонент или группу параметров. В правой части выводятся все настройки, относящиеся к выбранному в левой части (в дереве) пункту.

Как видно из структуры дерева, все настройки **Антивируса Касперского** делятся на три большие группы в соответствии с описанными в начале задания функциями: **Защита**, **Поиск вирусов** и **Сервис** (прочитайте об этих группах в **Справке**).

Ознакомьтесь с окном Настройка, поочередно переходя по соответствующим пунктам дерева в левой части окна.

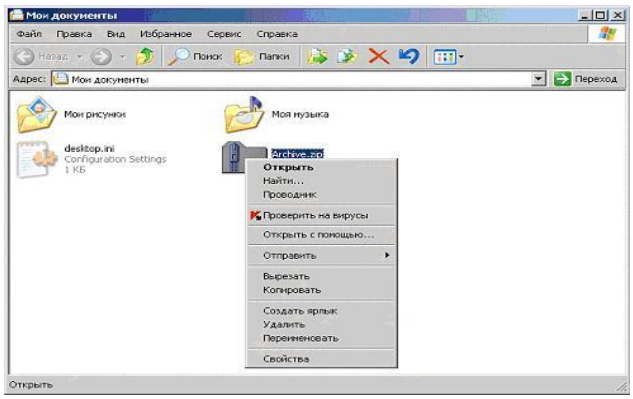


4. Перейдите к группе **Поиск вирусов**. Это - настройки проверки по требованию, то есть по требованию пользователя. Она используется в случае, если необходимо проверить некий объект или группу объектов.

Для запуска проверки по требованию нужно определить две вещи: что проверять и с какими настройками это делать.

Антивирус Касперского позволяет выбрать объекты, которые нужно проверить, двумя путями:

Антивирус встраивается в контекстное меню каждого файла, размещенного на жестком диске (**Проверить на вирусы**). В этом случае производится проверка только выделенного объекта или объектов. При этом используются общие настройки, то есть те, которые выводятся при нажатии пункта **Поиск вирусов**

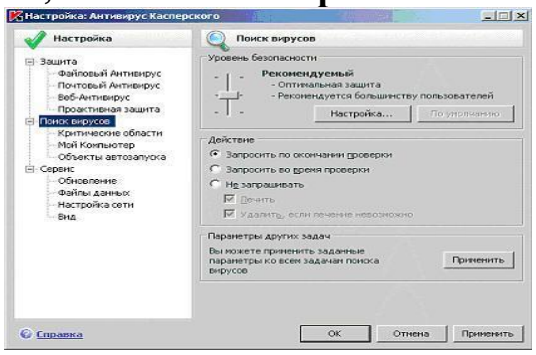


Можно заранее определить папку или группу папок или объектов и сформировать отдельную задачу. Тогда для нее можно задать свои собственные настройки и в дальнейшем запускать эту задачу одним нажатием кнопки. По умолчанию **Антивирус Касперского** создает три такие системные задачи с заранее определенным набором проверяемых объектов: **Проверку критических областей**, **Моего Компьютера** и **Объектов автозапуска**.

Таким образом, настройки группы **Поиск вирусов** соответствуют настройкам задачи, запускаемой из контекстного меню различных объектов. При этом она содержит три подгруппы, соответствующие другим задачам проверки по требованию с заданным набором проверяемых объектов: **Критические области**, **Мой компьютер**, **Объекты автозапуска**.

По мере формирования пользовательских задач проверки по требованию, они будут аналогично добавляться в дерево настроек в группу **Поиск вирусов**.

Ознакомьтесь с доступными для настройки параметрами системных задач проверки по требованию, поочередно выделяя пункты **Критические области**, **Мой компьютер** и **Объекты автозапуска**



5. Перейдите к группе настроек **Сервис**. В ней собраны настройки всех остальных компонентов антивируса. При выделении пункта **Сервис** открываются настройки уведомления пользователя о событиях в жизни антивирусной защиты компьютера (сообщать ли об обнаружении вируса, о приближающемся окончании лицензии, о проблемах с обновлениями и др.), здесь можно настроить защиту паролем и разрешить или запретить внешнее управление приложением.
Группа **Сервис** также включает такие важные подгруппы:

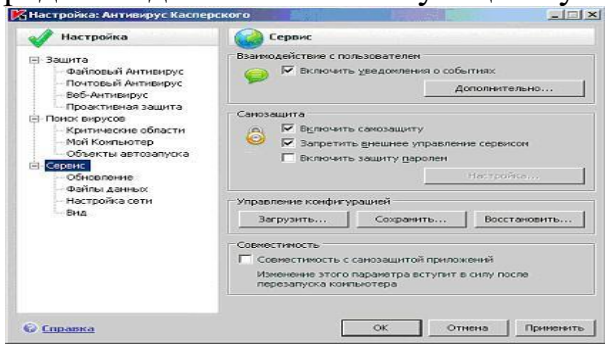
Обновление - это непосредственно настройки обновления антивирусных баз: расписание обновления, какие базы загружать

Файлы данных - тут настраиваются параметры хранения отчетов и прочей статистики. Также тут настраиваются параметры **Резервного хранилища** и **Карантина**.

Настройка сети - тут собраны параметры слежения за сетевыми соединениями, общие для почтового и веб-антивирусов, какие порты контролировать и что делать при обнаружении попытки установить защищенное соединение.

Вид. В этой группе настроек определяются параметры внешнего вида программы: цветовая гамма, использовать ли анимацию значка в системной панели и др.

Изучите доступные настройки группы **Сервис** и ее подгрупп, поочередно выделяя соответствующие пункты в дереве настроек



6. Нажмите **Отмена** и вернитесь в главное окно **Антивируса Касперского**
7. Закройте интерфейс **Антивируса Касперского**

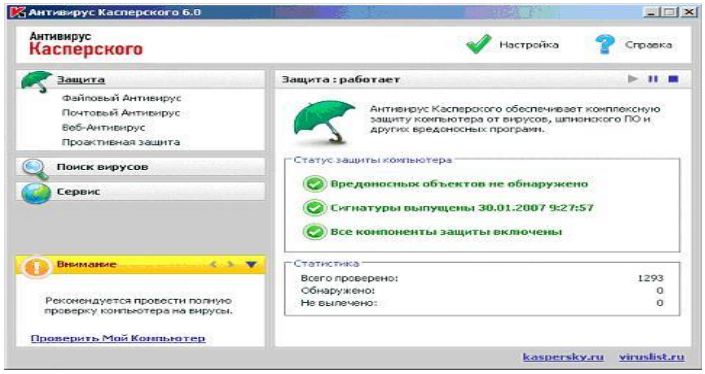
Задание 3. Постоянная защита

Работу с постоянно защитой можно разделить на три части:

- **Настройка** - она выполняется в одноименном окне и была рассмотрена в предыдущем задании
- **Управление** - каждый компонент постоянной защиты можно при необходимости приостановить, а потом запустить. Эти действия выполняются в главном окне интерфейса (элементы управления дополнительно продублированы в окне статистики)
- **Обслуживание**, то есть работу со статистикой. Выполняется в окне статистики

В этом задании нужно изучить последние две задачи: управление компонентами постоянной защиты и работу с отчетами.

1. Откройте главное окно интерфейса **Антивируса Касперского**

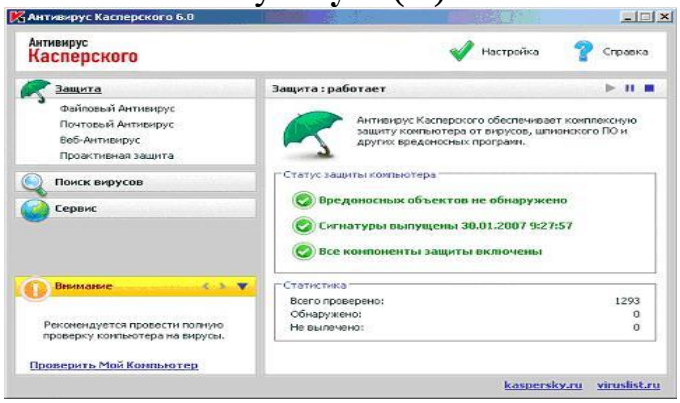


2. Перейдите к разделу **Защита**, выделив одноименный пункт

3. При вызове интерфейса **Антивируса Касперского** через системное меню **Пуск** или щелчком по иконке, по умолчанию выбран пункт **Защита**.

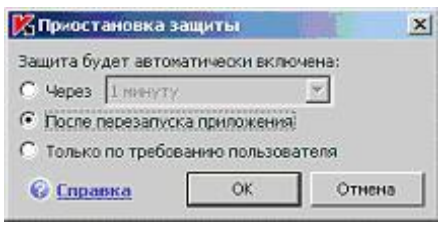
В заголовке этой части видна надпись `Защита:работает`. Это означает, что защита включена и работает. Соответственно, в расположенной справа от нее группе управляющих кнопок (▶ ⏸ ■) элемент **Пуск** (▶) не активен. Остальные два элемента соответствуют паузе (⏸) и остановке[1)] (■) проверки в режиме реального времени.

Нажмите кнопку **Пауза** (⏸)



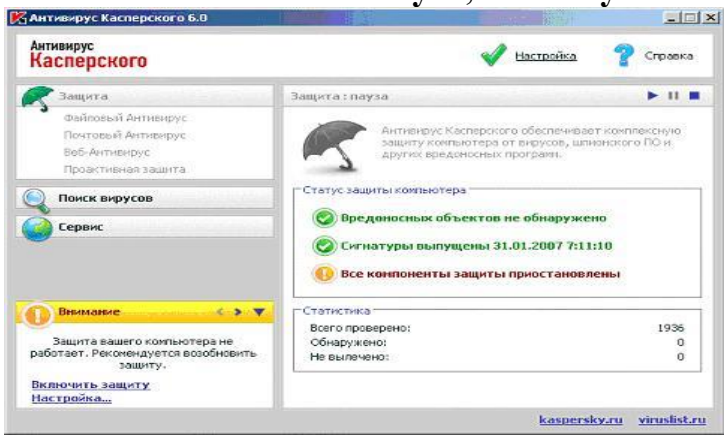
4. В общем случае приостанавливать или останавливать работу защиты не рекомендуется. Однако иногда это может потребоваться - например, при перемещении с диска на диск большого файла, и вы заведомо знаете, что он безопасен. Поэтому при нажатии кнопки **Пауза** появляется окно с предложением выбрать, когда нужно вернуть защиту в строй: через некий промежуток времени, после перезапуска антивируса или это должен сделать сам пользователь вручную, нажав кнопку **Пуск** (▶).

Ознакомьтесь со всеми предлагаемыми сценариями включения защиты и нажмите **ОК**

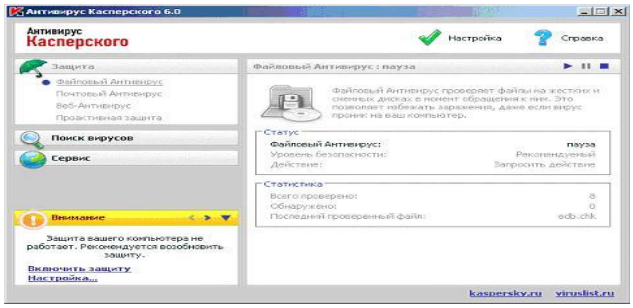


5. Вернувшись к главному окну, проследите за произошедшими изменениями.

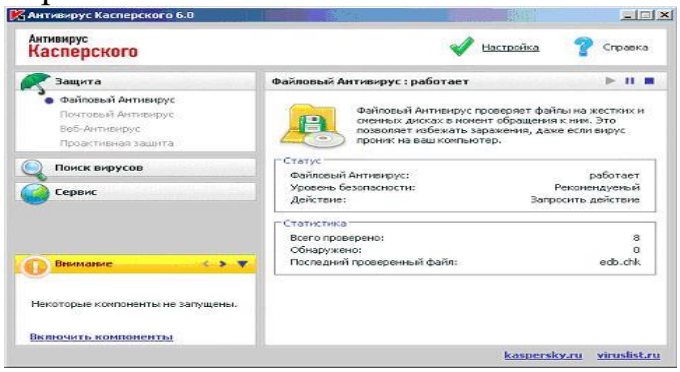
Обратите внимание, что строка со статусом защиты теперь выглядит затемненной, а ее текст гласит, что защита приостановлена (Защита : пауза). При этом также затенена кнопка **Пауза**, а вот **Пуск** стал активным ( ).



6. Перейдите к подразделу **Файловый Антивирус**
7. Изучите представленную в окне информацию. Обратите внимание на группу " **Статус**" в информационной части окна. К ней подается краткая сводка основных настроек, в том числе текущий статус компонента. В данном случае видно, что **Файловый Антивирус** приостановлен ("**Пауза**"). Об этом же символизирует и надпись в заголовке: Файловый Антивирус : пауза



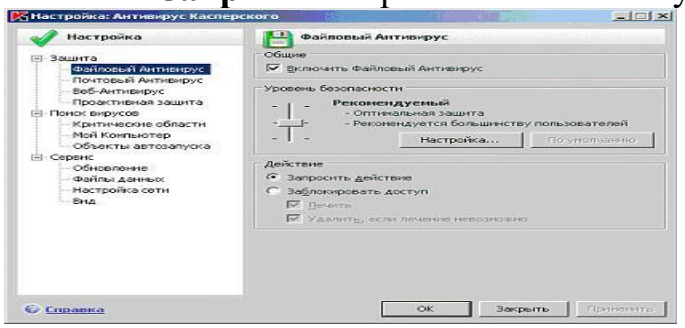
8. Запустите **Файловый Антивирус**, нажав кнопку **Пуск** ( )
9. Проследите за изменениями в интерфейсе окна. Обратите внимание, что произошел запуск только файлового антивируса, все остальные компоненты остались выключенными. Об этом свидетельствует затененность названий подразделов раздела **Защита** в меню левой части окна. При этом общее название **Защита** опять стало черным



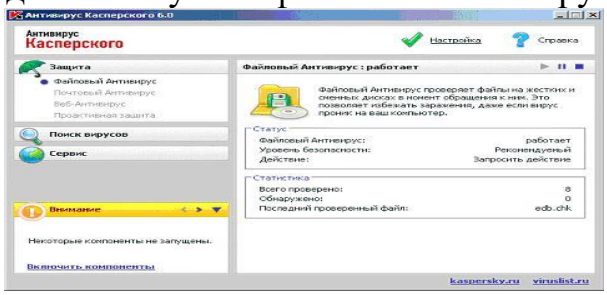
10. Наведите курсор на поле группы настроек " **Статус**" и нажмите левую клавишу мыши

11. Вследствие этого действия откроется изученное в предыдущем задании окно **Настройка**, причем на разделе, посвященном непосредственно файловому антивирусу.

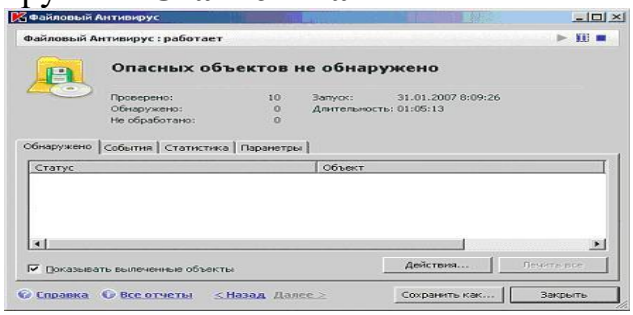
Нажмите **Закрыть** и вернитесь к главному окну интерфейса



12. Обратите внимание на группу "**Статистика**". В ней сказываются основные результаты работы выбранного компонента. В данном случае - файлового антивируса

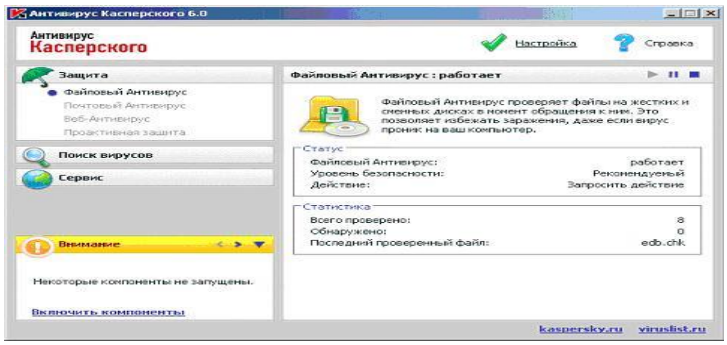


13. Для получения подробного отчета, щелкните по полю группы "**Статистика**"



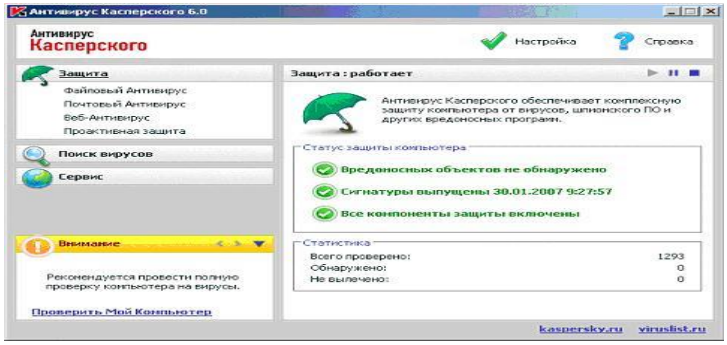
14. Открывшееся окно содержит подробную статистику работы компонента. Просмотрите содержание всех четырех закладок: **Обнаружено**, **События**, **Статистика** и **Параметры**

15. Нажмите кнопку **Закрыть** и вернитесь к главном у окну интерфейса



16. Теперь повторите эти же действия, начиная с пункта 7, только применительно ко всем трем оставшимся компонентам защиты: почтовому антивирусу, веб-антивирусу и проактивной защите.

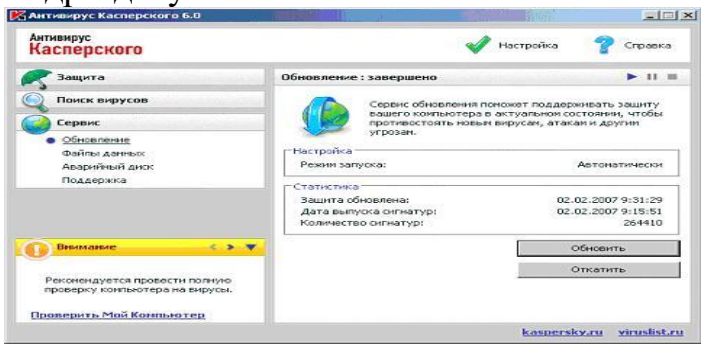
В результате выполнения этого задания все компоненты постоянной защиты должны быть включены



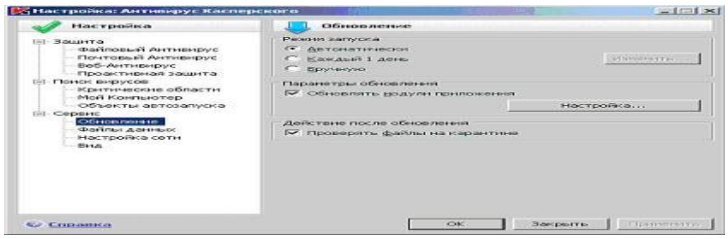
Задание 4. Настройка обновления

В этом задании нужно ознакомиться с настройками по умолчанию для задачи получения обновлений и при необходимости внести в них изменения (в соответствии с использующимися на Вашем компьютере настройками сети).

1. Откройте главное окно интерфейса и перейдите к подразделу **Обновление**



2. Откройте окно настройки, нажав на группу "**Настройка**"
3. Откроется окно **Настройка**, причем сразу на подразделе **Обновление**

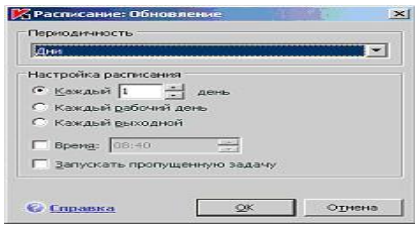


4. Все настройки обновления, размещенные в правой части, разделены на три группы:

Режим запуска - расписание, с которым будет запускаться процедура обновления. Предлагается выбрать один из трех вариантов:

Автоматически. Это означает, что процедура получения новых файлов будет запускаться через промежутки времени, указанные в самих обновлениях. Таким образом, решение о необходимости участить или наоборот, увеличить интервал между загрузками новых обновлений остается за вирусными экспертами **Лаборатории Касперского**. Это - оптимальный сценарий для большинства пользователей, у которых открыт постоянный доступ в Интернет. Поэтому именно его предлагается использовать по умолчанию

Каждый 1 день. Если выбрать этот сценарий, то с помощью расположенной рядом кнопки можно задать подробное расписание (в том числе и раз в час, и каждый определенный день недели), когда должна запускаться процедура обновления. Этот способ рекомендуется использовать если доступ к сети Интернет ограничен и пользователь заранее знает, когда он может выделить несколько минут на загрузку новых баз



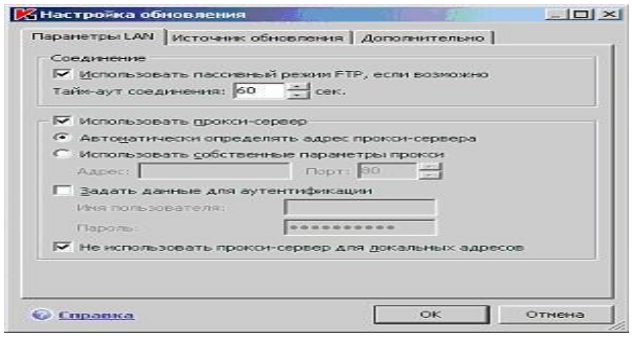
- **Вручную**. Этот режим предназначен для случая, когда обновление необходимо получать без использования всемирной сети - например, передавая файлы по сети или с помощью мобильных носителей. Такой способ может использоваться при очень ограниченном канале связи с Интернет или при его отсутствии

- **Параметры обновления** определяют какие файлы будут загружаться и какие настройки сети нужно при этом использовать.

5. Перейдите к окну настройки сетевых параметров, нажав кнопку **Настройка**

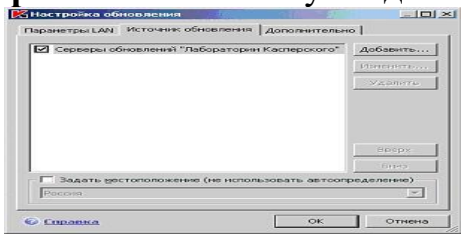
Открывшееся окно **Настройка обновления** содержит три закладки. На первой, **Параметры LAN**, задаются параметры соединения с Интернет. Их

можно узнать у провайдера, администратора компьютерного класса или преподавателя.



6. Перейдите к закладке **Источник обновления**.

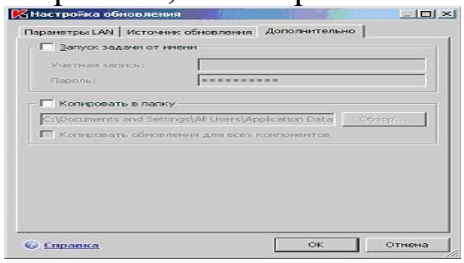
Источник обновления - это еще один важный параметр задачи получения обновлений. По умолчанию обновления загружаются с серверов **Лаборатории Касперского**. Их адреса фиксированы разработчиками программы и изменению не подлежат. Серверам обновлений **Лаборатории Касперского** соответствует одноименный пункт в списке всех источников.



7. Перейдите к закладке **Дополнительно**
8. Ознакомьтесь с представленными на ней полями, обратив внимание на группу **Копировать в папку**.

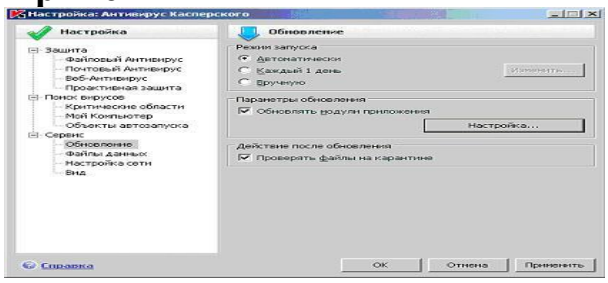
Эта настройка может быть полезна в случае, когда только Ваш компьютер имеет доступ в Интернет, а другие компьютеры сети - нет. В этом случае можно настроить автоматическое копирование файлов обновлений, полученных Вашим антивирусом, в определенный каталог. Тогда эту папку можно будет указать в качестве источника обновлений в настройках остальных компьютеров сети.

Настройка **Запуск от имени** может быть необходима в случае, если учетная запись системы Вашего компьютера не обладает достаточными правами на доступ к источнику обновления, например сетевой папке. В этом случае нужно отметить флаг **Запуск от имени**, узнать у системного администратора сети или преподавателя имя учетной записи, обладающей такими правами, и ее пароль и заполнить одноименные поля



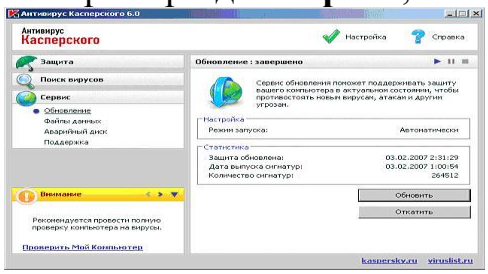
9. Закройте окно настройки обновлений, нажав **ОК**

10. Если параметры Вашей сети совпадают с предложенными по умолчанию, нажмите **Отмена**, если в них были внесены изменения - **Применить**



11. Выберите **Режим запуска Автоматически**, нажмите кнопку **Применить** и **Ок**.

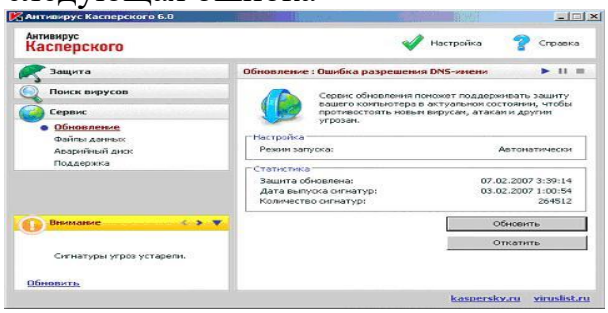
12. В **Главном окне** интерфейса **Антивируса Касперского** выберите раздел **Сервис**, затем подраздел **Обновления**.



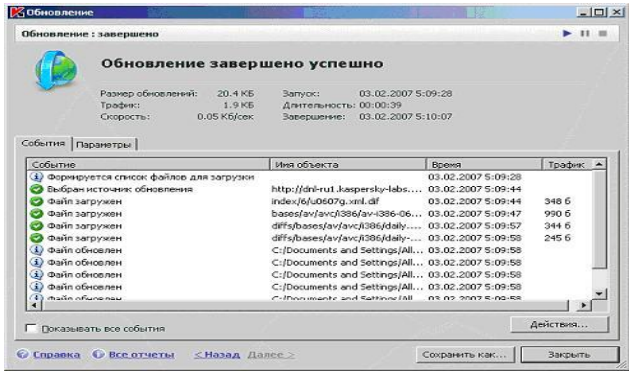
13. Нажмите кнопку 

для запуска процедуры Обновления.

14. Если на вашем компьютере отсутствует подключение к Интернет, и попытка обновления не удалась, то появится примерно следующая ошибка



15. Если подключение к сети Интернет присутствует на вашем компьютере, начнется процесс обновления и по завершению будет выведено сообщение «Обновление завершено успешно»



Вопросы для самоконтроля:

1). Что называется компьютерным вирусом?
2). Что происходит, когда зараженная программа начинает работу?
3). Как может маскироваться вирус?
4). Каковы признаки заражения вирусом?
5). Какие типы компьютерных вирусов выделяются?
6). Каковы особенности самомодифицирующихся вирусов?
7). Какие методы защиты от компьютерных вирусов можно использовать?
8). Как действуют программы-детекторы?
9). Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?
10). Перечислите меры защиты информации от компьютерных вирусов.
11). Какие модули входят в состав антивируса Касперского для защиты файловых систем? Каково назначение этих модулей?