МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания
по выполнению практических работ по дисциплине
«ПРОГРАММИРОВАНИЕ АЛГОРИТМОВ ЗАЩИТЫ ИНФОРМАЦИИ»
для студентов специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Ставрополь
2026

СОДЕРЖАНИЕ

Практическое занятие №1

Модели угроз безопасности ПО.

Цель работы: получение практических навыков по выявлению вредоносных программ на локальном компьютере под управлением Microsoft Windows .

Теоретическая часть

Изучение настроек браузера

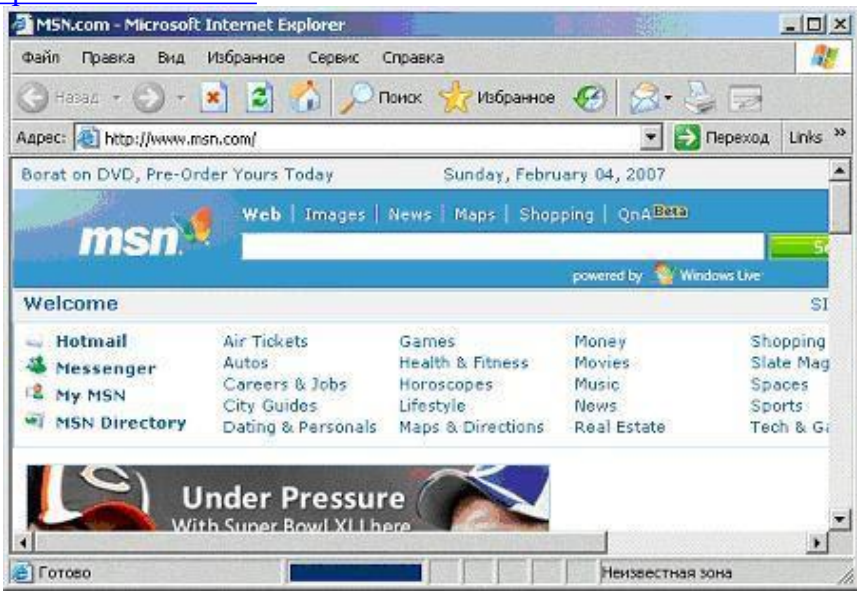
Вирусные проявления бывают явными, косвенными и скрытыми. Если первые обычно видны невооруженным глазом, то косвенные и тем более скрытые требуют от пользователя проявления изрядной доли интуиции. Они часто не мешают работе, и для их обнаружения требуется знать, где и что нужно искать.

Явные проявления обычно выражаются в неожиданно появляющихся рекламных сообщениях и баннерах - обычно это следствие проникновения на компьютер рекламной утилиты. Поскольку их главная цель - это привлечь внимание пользователя к рекламируемой услуге или товару, то им сложно оставаться незаметными. Также, явные проявления могут вызывать ряд троянских программ, например утилиты несанкционированного дозвона к платным сервисам.

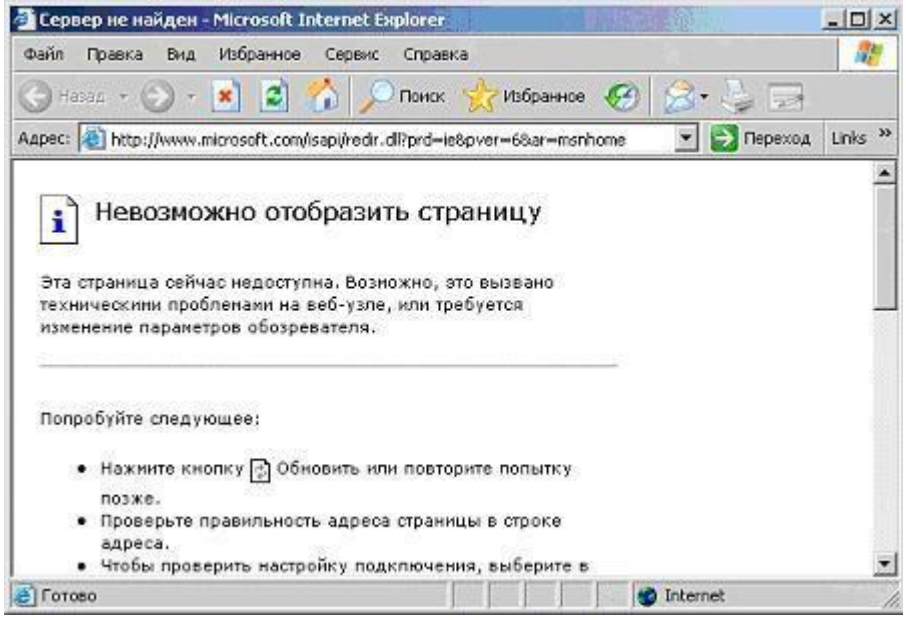
В этом задании предлагается исследовать явные проявления вирусной активности на примере несанкционированного изменения настроек браузера. Этот механизм иногда используется для того, чтобы вынудить пользователей зайти на определенный сайт, часто порнографического содержания. Для этого меняется адрес домашней страницы, то есть адрес сайта, который автоматически загружается при каждом открытии браузера.

1. Откройте браузер Internet Explorer, воспользовавшись одноименным ярлыком на рабочем столе или в системном меню Пуск / Программы

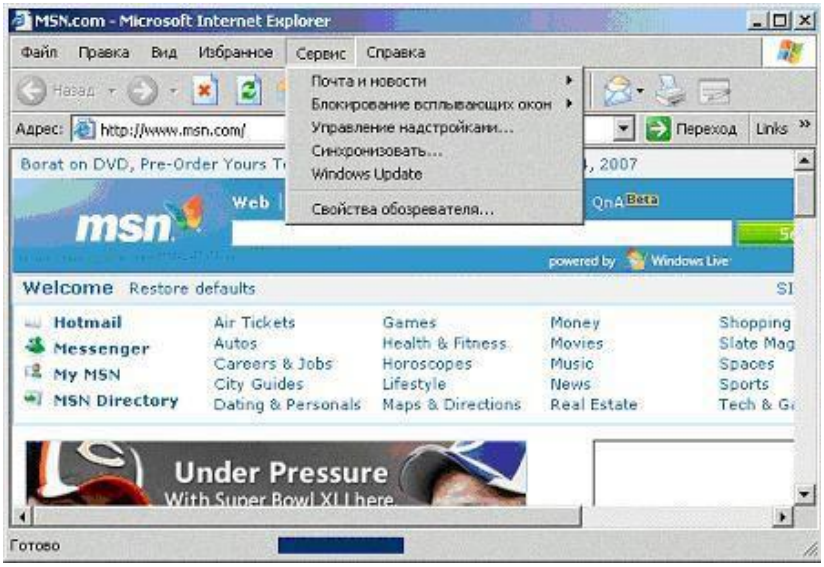
2. Если у Вас открыт и настроен доступ в Интернет и после установки операционной системы стартовая страница изменена не была, должна открыться страница по умолчанию - http://www.msn.com



Если доступ в Интернет не настроен, то выведется соответствующее уведомление:

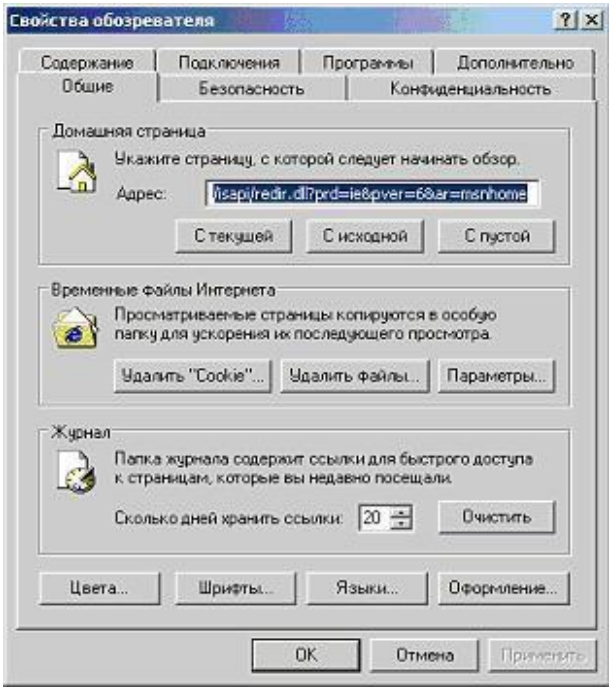


3. Проверьте значение параметра, отвечающего за стартовую страницу. Для этого нужно воспользоваться меню Сервис. Откройте его и выберите пункт Свойства обозревателя

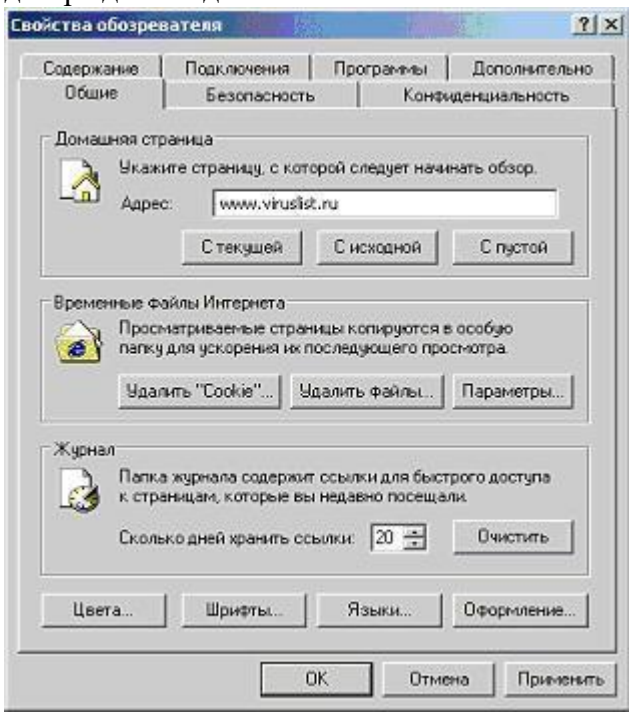


4. Адрес стартовой страницы указан в первом же поле открывшегося окна Свойства обозревателя, на закладке Общие. Значение этого поля совпадает с тем адресом, который был автоматически задан при открытии браузера.

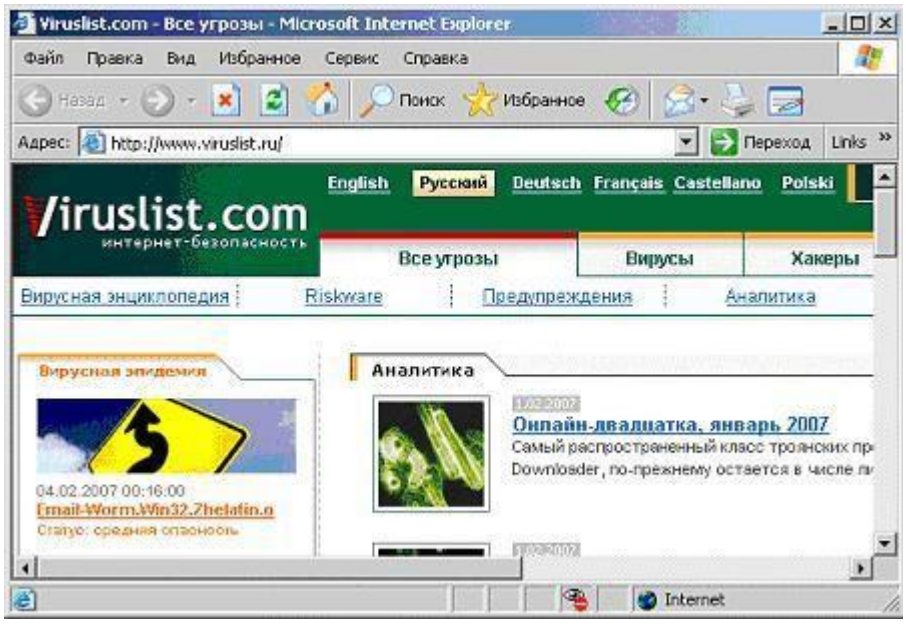
Измените это поле, введя адрес www.viruslist.ru



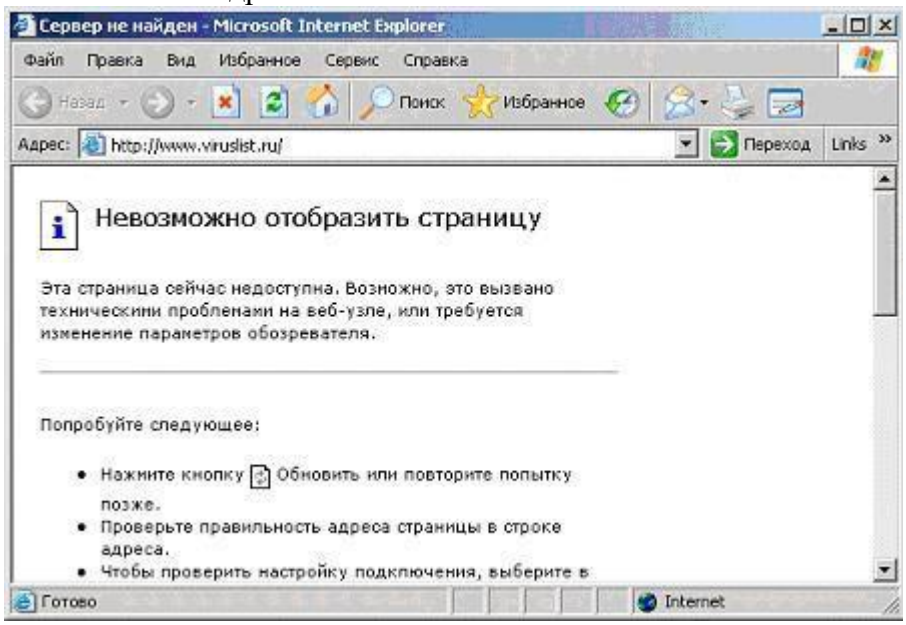
5. Далее для подтверждения сделанных изменений нажмите ОК



6. Закройте и снова откройте браузер
7. Убедитесь, что теперь первым делом была загружена страница www.viruslist.ru



В случае, если на Вашем компьютере доступ в Интернет не настроен, об этом можно догадаться по значению в поле Адрес:



Таким образом, если Ваш браузер начал самостоятельно загружать постороннийсайт, в первую очередь нужно изучить настройки браузера: какой адрес выставлен в поле домашней страницы.

Ряд вредоносных программ ограничиваются изменением этого параметра и для устранения последствий заражения нужно лишь исправить адрес домашней страницы. Однако это может быть только частью вредоносной нагрузки. Поэтому если Вы обнаружили несанкционированное изменение адреса домашней страницы, следует немедленно установить антивирусное программное обеспечение и проверить весь жесткий диск на наличие вирусов.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows XP и программными продуктами: MS Word, Adobe Reader, и браузер Internet Explorer

Указания по технике безопасности: к выполнению практических занятий

допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Что такое вредоносная программа (вирус)?
2. Перечислите основные типы вредоносных программ (вирусов) и опишите принципы их вредоносного действия в компьютерной среде.
3. Какие три вида проявления вредоносных программ вам известны? Приведите примеры.
4. Дайте определение «подозрительный процесс». **Список литературы, рекомендуемый к использованию по данной теме:**

1. Методы и средства инженерно-технической защиты информации Электронный ресурс: Учебное пособие / В. И. Аверченков [и др.]. - Брянск: Брянский государственный технический университет, 2012. - 207 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 5-89838-357-3.

2. Проскурин, В. Г. Защита программ и данных: учеб. пособие для вузов / В. Г. Проскурин. - М.: Академия, 2012. - 208 с. - (Высшее профессиональное образование. Бакалавриат). - Гриф: Доп. УМО. - Библиогр.: с. 195-196. - ISBN 978-5-7695-9288-1.

Практическое занятие №2

Решение задачи доказательства правильности программы для алгоритма дискретного экспоненцирования

Подозрительные процессы.

Цель работы: получение практических навыков по выявлению вредоносных программ на локальном компьютере под управлением Microsoft Windows .

Теоретическая часть

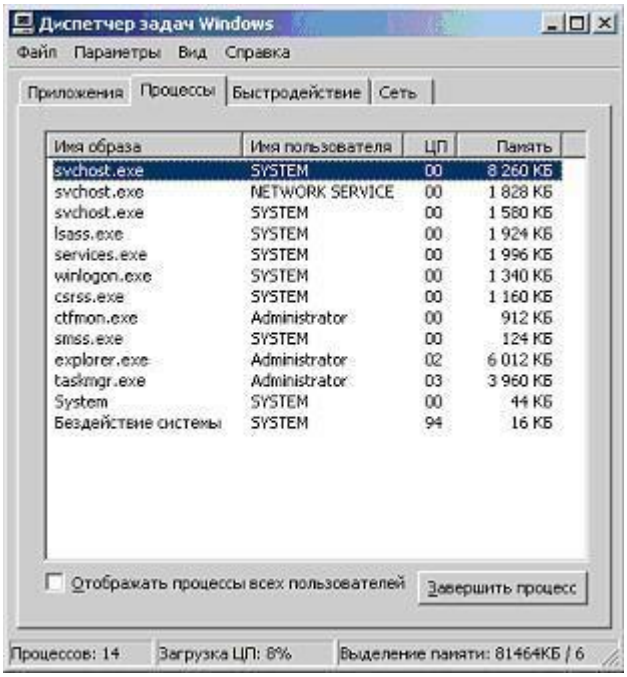
Подозрительные процессы

Одним из основных проявлений вредоносных программ является наличие в списке запущенных процессов подозрительных программ. Исследуя этот список и особенно сравнивая его с перечнем процессов, которые были запущены на компьютере сразу после установки системы, то есть до начала работы, можно сделать достаточно достоверные выводы об инфицировании. Это часто помогает при обнаружении вредоносных программ, имеющих лишь только скрытые или косвенные проявления.

Однако необходимо четко понимать и уметь отличать легальные процессы (например, системные или запущенные программы) от подозрительных. В этом задании необходимо ознакомиться с основным методом исследования запущенных процессов, а именно получить навыки работы с Диспетчером задач Windows, и изучить стандартный их набор.

Диспетчер задач Windows - это стандартная утилита, входящая в любую версию Microsoft Windows. С ее помощью можно в режиме реального времени отслеживать выполняющиеся приложения и запущенные процессы, оценивать загруженность системных ресурсов компьютера и использование сети.

1. Перейдите к Диспетчеру задач Windows, нажав одновременно клавиши Ctrl+Alt+Delete.



Открывшееся окно содержит четыре закладки, отвечающие четырем видам активности, которые отслеживает Диспетчер: приложения, процессы, быстродействие (использование системных ресурсов) и Сеть. По умолчанию у Вас должна открыться вторая закладка, Приложения.

2. Перейдите на вкладку Процессы и внимательно изучите представленный в окне список процессов. Если на компьютере не запущены никакие пользовательские программы, он должен содержать только служебные процессы операционной системы.

Внимание! Эти процессы необходимы системе для стабильной работы

Название процесса	Описание	Возможность завершения
CSRSS.EXE.	Сокращение от «Client/Server Run – Time Subsystem».Процесс отвечает за окна консоли, за создание и удаление потоков, а также частично за работу 16-битной среды MS-DOC. Он относится кподсистеме Win32 пользовательского режима (WIN32.SYS же относится к ядру Kernel) и долженвсегда выполняться.	-
EXPLORER.EXE.	Пользовательская среда, содержащая такие компоненты, как Панель задач, Рабочий стол и томуподобное. Его практически всегда можно закрывать и снова открывать без каких-либо последствий.	+
INTERNAT.EXE	Загружает различные выбранные пользователем языки ввода, показывает на панели задач значок «RL», который позволяет переключатьязыки ввода. С помощью панели управления возможно без использования данного процесса безовсяких проблем переключать раскладку клавиатуры.	+
LSASS.EXE	Этот локальный сервер авторизации отвечаетза IP-директивы безопасности (Интернет- протоколы) и загружает драйвер безопасности. Он запускает процесс, отвечающий за авторизацию пользователей. При успешной авторизации пользователя приложение создает и присваивает ему специальный протокол. Все запущенные далее процессы используют этот протокол.	-
MSTASK.EXE	Отвечает за службу планирования Schedule, которая предназначена для запуска различных приложений в определенное пользователем время.	-
SMSS.EXE	Диспетчер сеансов запускает высокоуровневые подсистемы и сервисы. Процесс отвечает за различные действия, например запуск Winlogon- и Win32-процессов, а также за операции с системными переменными. Когда Smss определяем, что Winlogon или Csrss закрыты, он автоматически выключает систему.	-
SPOOLSV.EXE	Обеспечивает создание очереди на печать, временно сохраняя документы и факсы в памяти.	-
SVCHOST.EXE	Этот всеобъемлющий процесс служит хостомдля других процессов, запускаемых с помощью DLL. Поэтому иногда работают одновременно несколько Svchost. С помощью команды «tlist - s» можно вывести на экран все процессы,использующие Svchost.	-

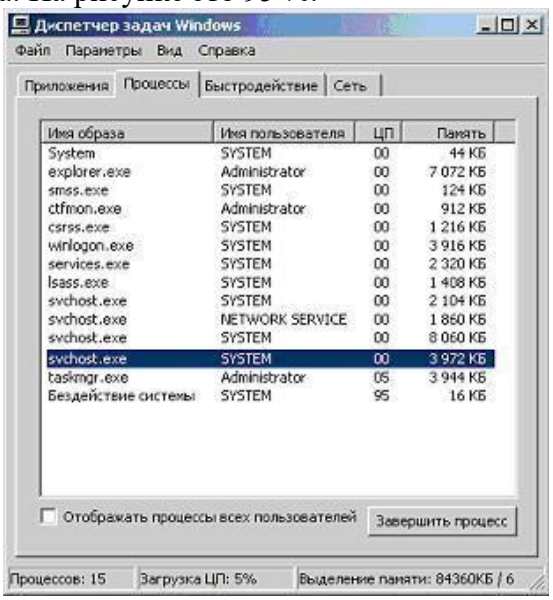
SERVICES .EXE	Процесс управления системными службами. Запуск, окончание, а также все остальные действиясо службами происходят через него.	-
SYSTEM	Этот процесс выполняет все потоки ядра	-

	Kernel.	
SYSTEMIDLE PROCESS	Этот процесс выполняется на любом компьютере. Нужен он, правда, всего лишь для мониторинга процессорных ресурсов, неиспользуемых другими программами.	-
TASKMGR.EXE	Процесс диспетчера задач, закрывать который крайне не рекомендуется.	+
WINLOGON.EXE	Отвечает за управление процессами авторизации пользователей. Он активен, только когда пользователь нажимает «Ctrl+Alt+Del».	-
WINMGTM.EXE	Основной компонент клиентской службы Windows. Процесс запускается одновременно с первыми клиентскими приложениями и выполняется при любом запросе служб. В XP он запускается как клиент процесса Svchost.	-

В данной работе мы рассматриваем ОС Microsoft Windows XP, в Microsoft Windows Vista, количество процессов, необходимых для стабильной работы ОС гораздо больше.

3. Для каждого процесса выводятся его параметры: имя образа (может не совпадать с именем запускаемого файла), имя пользователя, от чьего имени был запущен процесс, загрузка этим процессом процессора и объем занимаемой им оперативной памяти.

4. Поскольку в данный момент не должна быть запущена ни одна пользовательская программа, процессор должен быть свободен. Следовательно, "Бездействие системы" должно оказаться внизу списка с достаточно большим процентом "использования" процессора. На рисунке это 95 %.

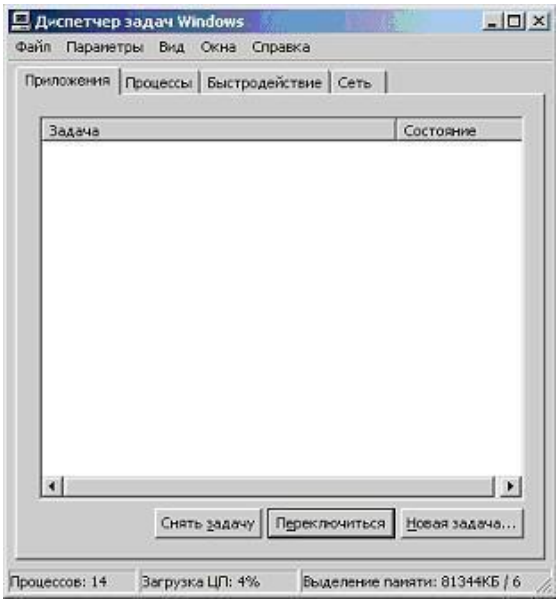


В ряде случаев может потребоваться вручную завершить некий процесс. Это можно сделать с помощью кнопки Завершить процесс.

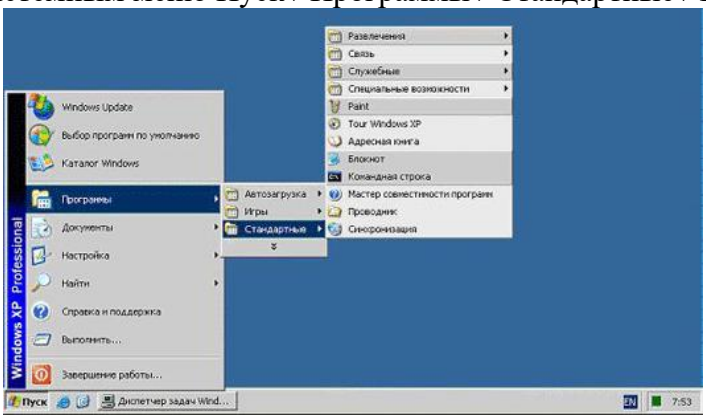
Например, Вы обнаружили подозрительный процесс, на сайте вирусной энциклопедии www.viruslist.ru прочитали, что он однозначно принадлежит вирусу или троянской программе, но антивирусной программы на компьютере нет. Тогда нужно закрыть все работающие приложения и с помощью Диспетчера задач вручную завершить этот процесс. Чтобы исключить появление его снова настоятельно рекомендуется как можно быстрее установить полноценное антивирусное приложение и сразу же запустить проверку всего жесткого диска на наличие вирусов.

5. Выпишите все запущенный процессы на лист бумаги или в текстовый файл и перейдите к закладке Приложения

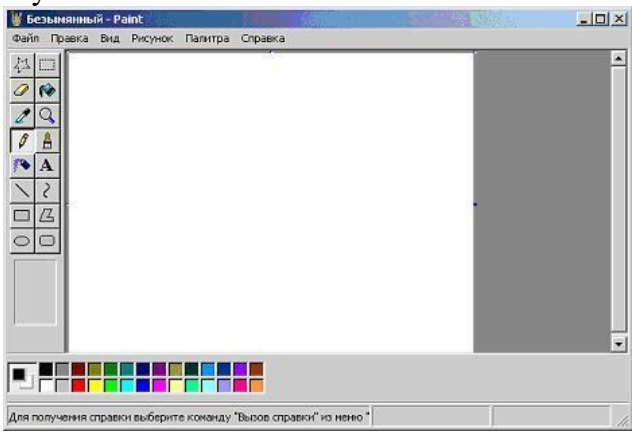
6. Поскольку в данный момент не запущено ни одно приложение, список запущенных приложений пуст



7. Не закрывая окна Диспетчера задач Windows, откройте программу Paint. Для этого воспользуйтесь системным меню Пуск / Программы / Стандартные / Paint



8. Дождитесь запуска Paint

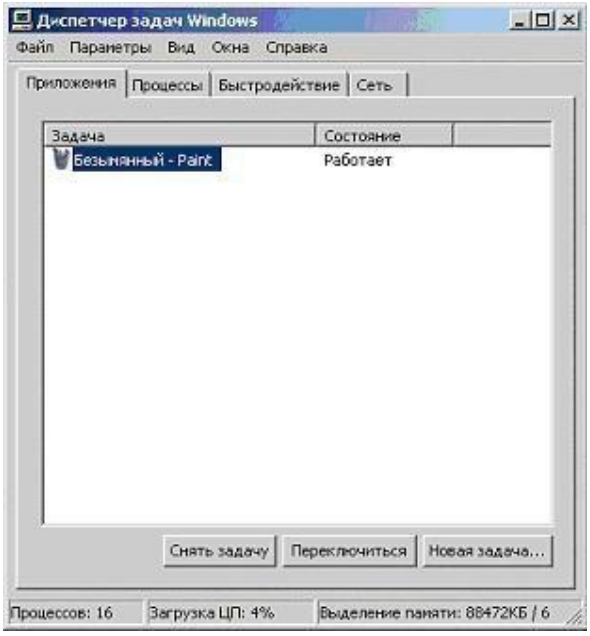


9. Не закрывая приложение Paint, вернитесь к окну Диспетчера задач Windows и проследите за изменениями на закладке Приложения

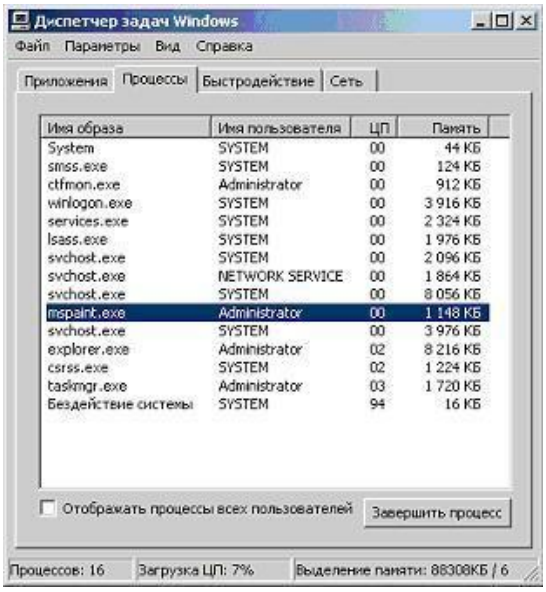
10. Список запущенных приложений должен содержать строку, соответствующею Paint. Поскольку она сейчас работает, это же записано в строке Состояние.

Иногда случается так, что программа вызывает ошибку - тогда в ее состоянии будет написано "Не отвечает". Если некое ранее бесперебойно работающее приложение начало часто без видимых причин переходить в состояние "Не отвечает", это может быть косвенным признаком заражения.

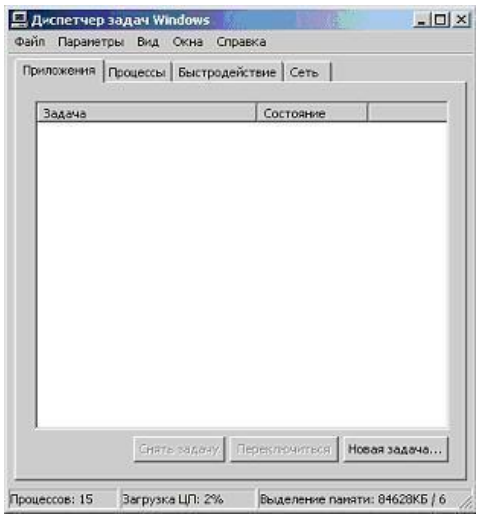
Тогда первое, что можно сделать - это воспользоваться кнопкой Снять задачу и начать поиски причин. Если программа по прежнему не завершила работу, перейдите на вкладку Процессы, найдите в списке процессов нужный Вам процесс и воспользуйтесь кнопкой Завершить процесс.



11. Перейдите к закладке Процессы
12. Сравните список запущенных сейчас процессов с перечнем, составленным на шаге 5 этого задания. Найдите отличие

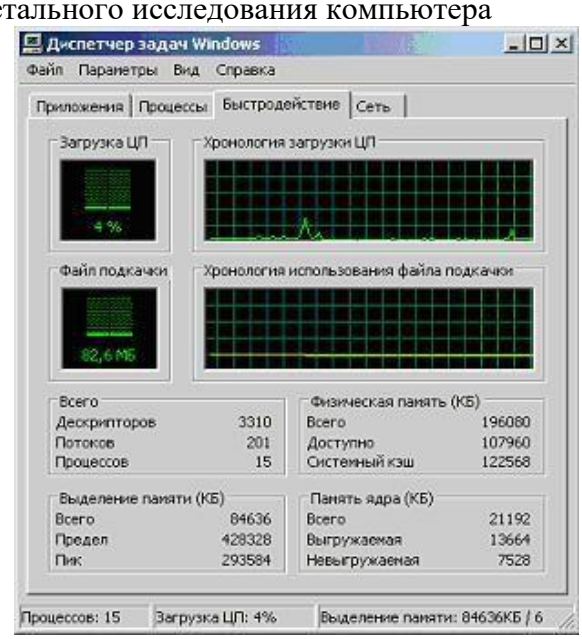


13. Убедитесь, что программе Paint соответствует процесс mspaint.exe. Для этого найдите его в списке запущенных процессов, не закрывая и не сворачивая окно Диспетчера задач Windows, вернитесь в окне Paint и закройте его
14. Проследите, что из списка запущенных процессов пропал mspaint.exe
15. Вернитесь к закладке Приложения и убедитесь, что она снова пуста



16. Перейдите к закладке Быстродействие

17. Внимательно изучите расположенные тут графики. Любые всплески на них должны по времени соответствовать неким действиям, например запуску требовательной к ресурсам программы. Если ничего похожего сознательно не производилось, это может быть причиной для более детального исследования компьютера



18. Закройте окно Диспетчера задач Windows. **Оборудование и материалы:** для выполнения данного практического занятия

необходим компьютер с установленной операционной системой Windows XP и программными продуктами: MS Word, Adobe Reader, и браузер Internet Explorer.

Указания по технике безопасности: к выполнению практических занятий

допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее

Отчет должен содержать титульный лист с темой лабораторной работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Перечислите признаки присутствия на компьютере вирусов.
2. Какие признаки присутствия вируса может выдать браузер?
3. Какие настройки браузера Internet Explorer могут быть несанкционированно изменены вирусной программой?
4. Какие действия необходимо провести при обнаружении подозрительных процессов с помощью Диспетчера задач?

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.
2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.
3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.
4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.
5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.
6. Групер Ш. Электронные ключи с энергонезависимой памятью //КомпьютерПресс.-1993.-N8.-С.60-62.
7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.
8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.
9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьютерПресс.-1993.-N7.-С.49-52.
10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер-Пресс.-1991.-N10.-С.19-24.
11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.
12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

Практическое занятие №3

Синхронные и асинхронные конфиденциальные вычисления

Цель работы: получение практических навыков по выявлению вредоносных программ на локальном компьютере под управлением Microsoft Windows .

Теоретическая часть

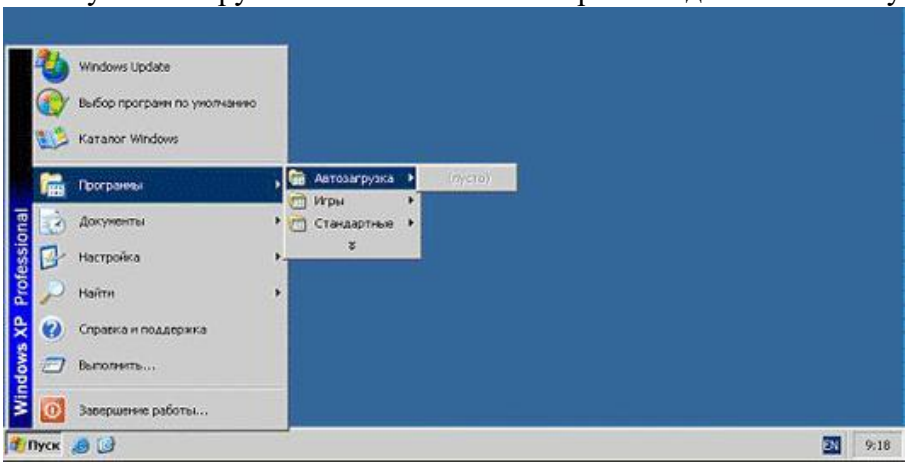
Элементы автозапуска

Для того, чтобы прикладная программа начала выполняться, ее нужно запустить. Следовательно, и вирус нуждается в том, чтобы его запустили. Для этого можно

использовать два сценария: либо сделать так, чтобы пользователь сам его запустил (либо по незнанию, либо с использованием обманных методов), либо внедриться в конфигурационные файлы и запускать одновременно с другой, полезной программой. Оптимальным с точки зрения вируса вариантом служит запуск одновременно с операционной системой - в этом случае запуск практически гарантирован.

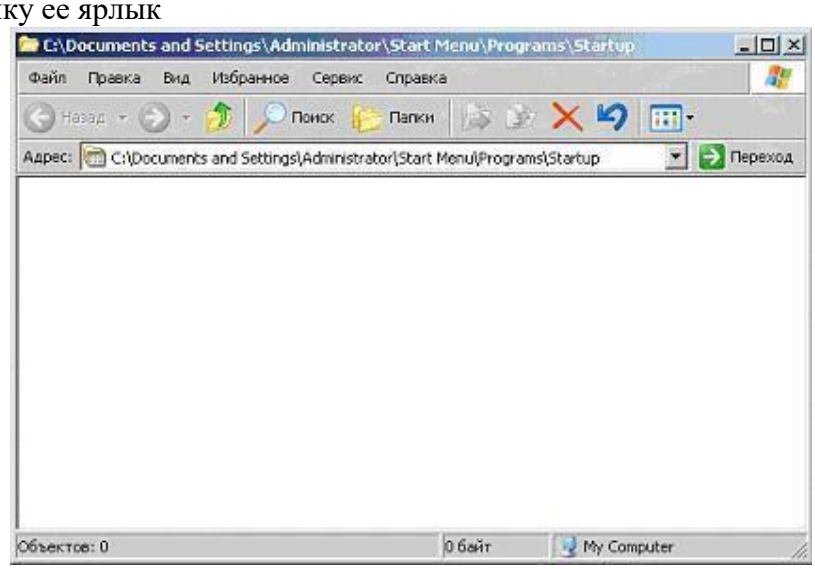
1. Самый простой способ добавить какую-либо программу в автозагрузку - это поместить ее ярлык в раздел Автозагрузка системного меню Пуск / Программы. По умолчанию, сразу после установки операционной системы этот раздел пуст, поскольку ни одной прикладной программы еще не установлено.

Проверьте папку Автозагрузка на Вашем компьютере. Она должна быть пустой

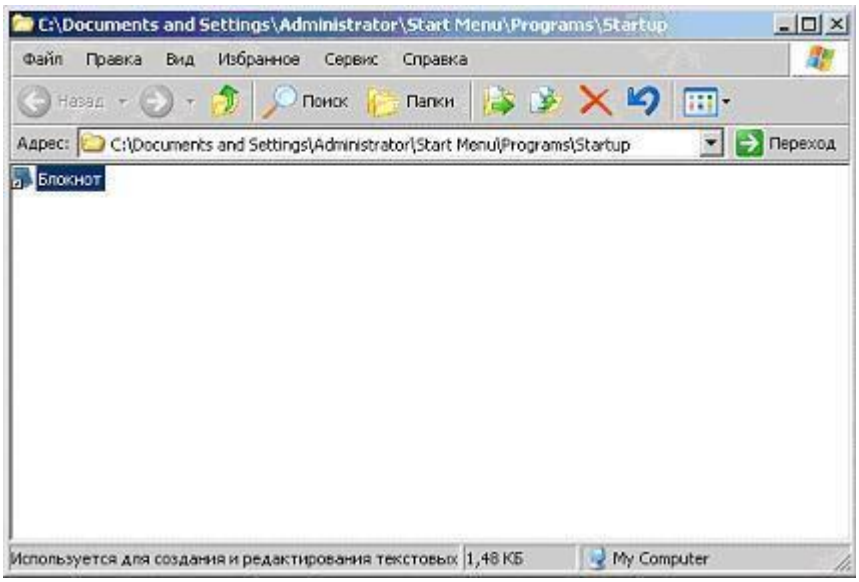


2. Добавьте в список автозагрузки свою программу (создайте ярлык на любую программу, например Калькулятор или Блокнот и поместите его в группу Автозагрузка). Для этого дважды щелкните левой клавишей мыши по названию группы Автозагрузка

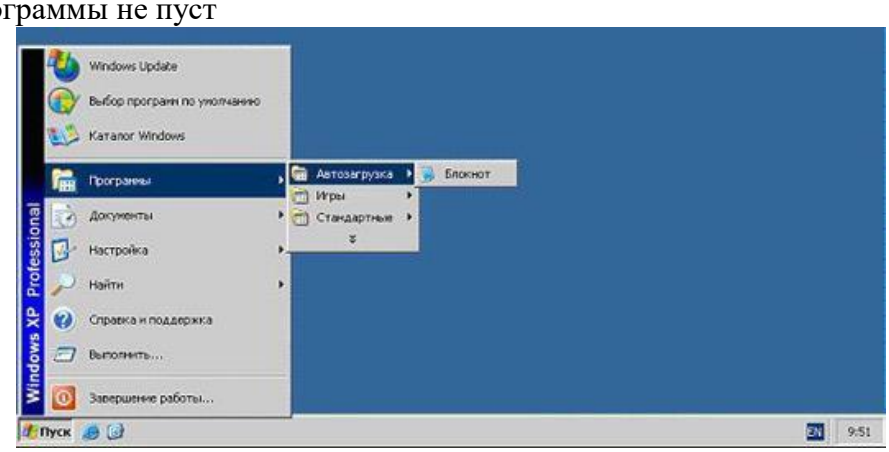
3. В результате должно открыться соответствующее окно папки автозагрузки. Обратите внимание на полный адрес открывшейся папки. Все что нужно сделать, чтобы некая программа запускалась автоматически при старте операционной системы - это поместить в эту папку ее ярлык



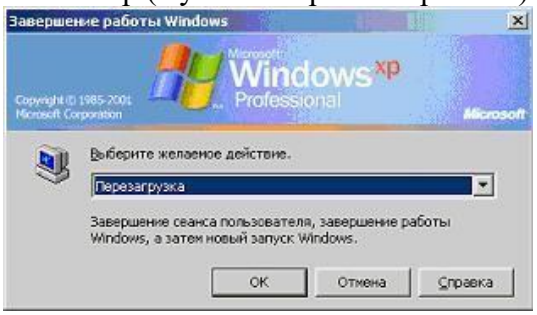
4. В результате этих действий в окне должна появиться копия ярлыка Блокнота



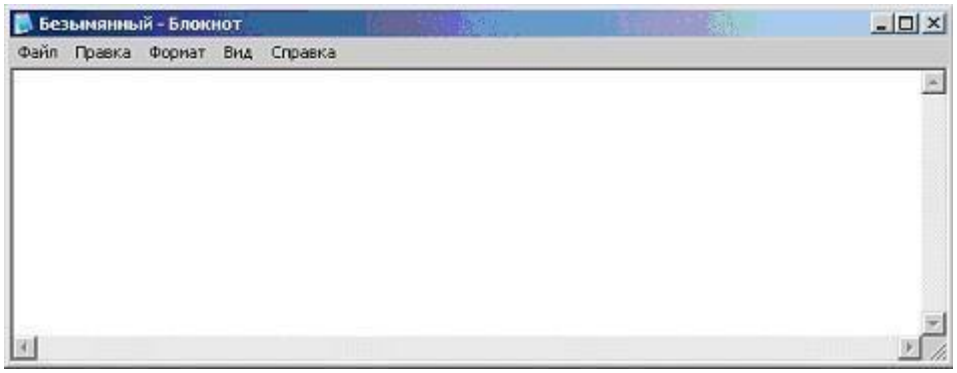
5. Закройте окно и убедитесь, что теперь раздел Автозагрузка в системном меню Пуск / Программы не пуст



6. Перезагрузите компьютер (Пуск / Завершение работы)



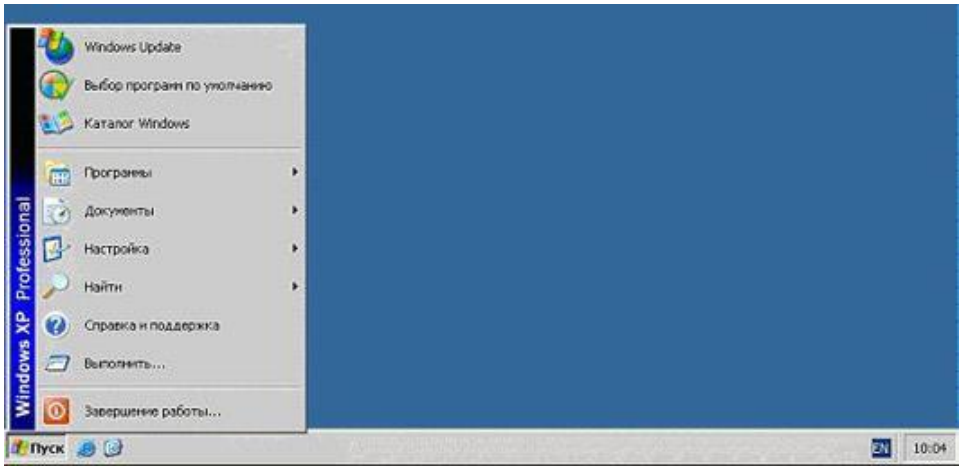
7. Убедитесь, что по завершению загрузки автоматически запустилась программа Блокнот



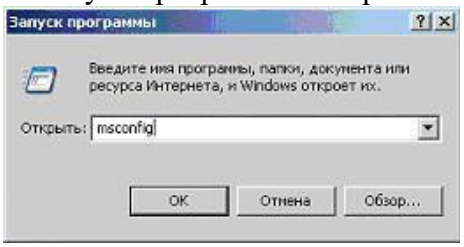
8. При обследовании компьютера нужно помнить, что отсутствие подозрительных ярлыков в разделе Автозагрузка системного меню Пуск / Программы не гарантирует, что ни одно приложение не запускается автоматически. Технически для автозапуска нужно добавить соответствующую запись в системный реестр операционной системы.

Несмотря на то, что реестр Windows очень большой, существует оболочка, позволяющая с ним работать напрямую. Но делать это рекомендуется только в крайнем случае. Для большинства ситуаций, связанных с автозапуском, достаточно использовать системную утилиту Настройка системы .

Запустите ее. Для этого откройте системное меню Пуск и перейдите к пункту Выполнить

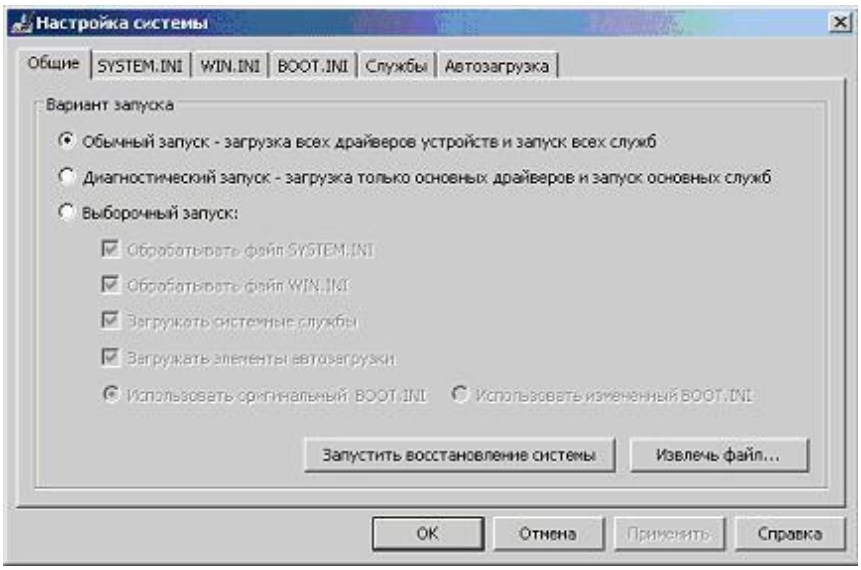


9. В открывшемся окне Запуск программы наберите msconfig и нажмите ОК



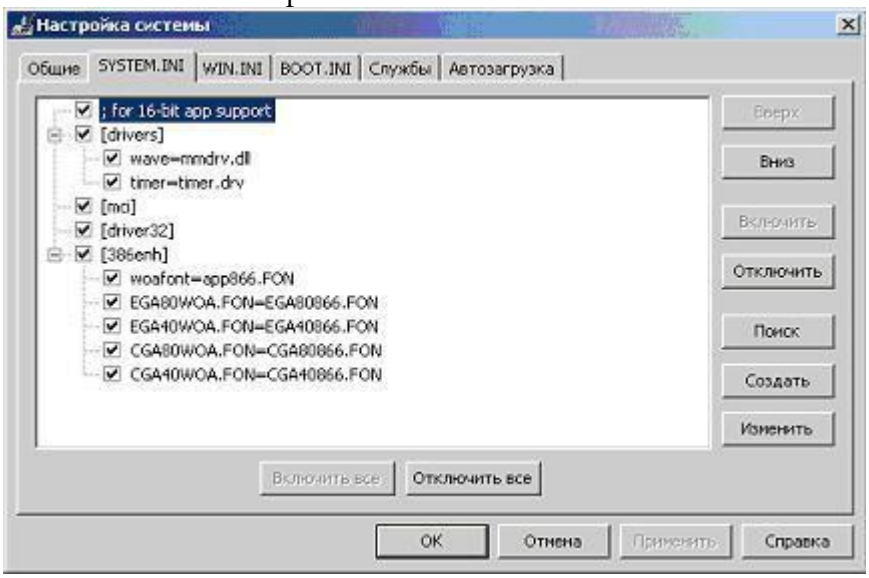
10. Ознакомьтесь с внешним видом окна утилиты Настройка системы.

На первой закладке, Общие, можно выбрать вариант запуска операционнойсистемы. По умолчанию отмечен Обычный запуск. Он обеспечивает максимальную функциональность системы. Остальные два варианта запуска предназначены для диагностики

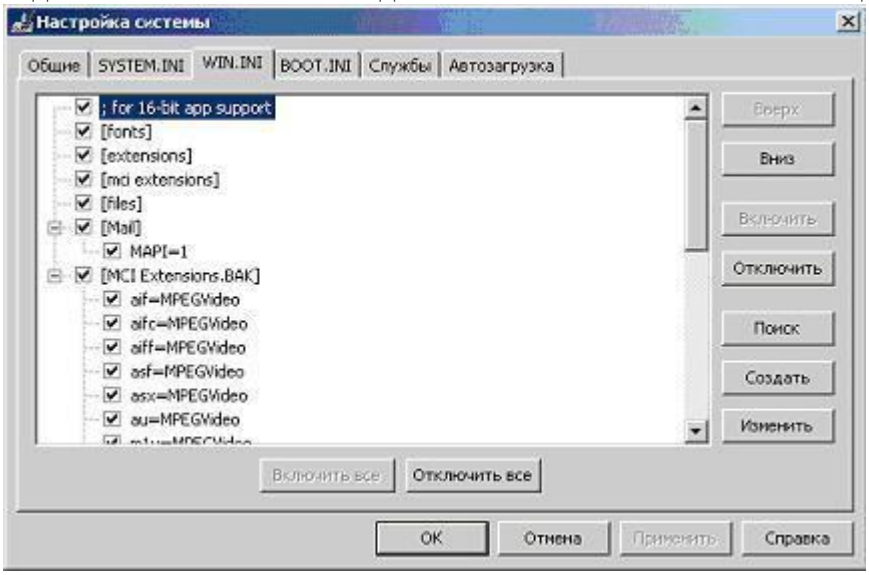


Второй режим, Диагностический запуск, рекомендуется использовать также при подтвердившемся вирусном инциденте - если компьютер уже заражен, сразу установить антивирус в ряде случаев нельзя, например, если вирус сознательно блокирует запуск ряда антивирусных программ. Тогда, если нет возможности удалить или хотя бы временно обезвредить вирус вручную, рекомендует запустить операционную систему в безопасном режиме, инсталлировать антивирус и сразу же проверить весь жесткий диск на наличие вирусов.

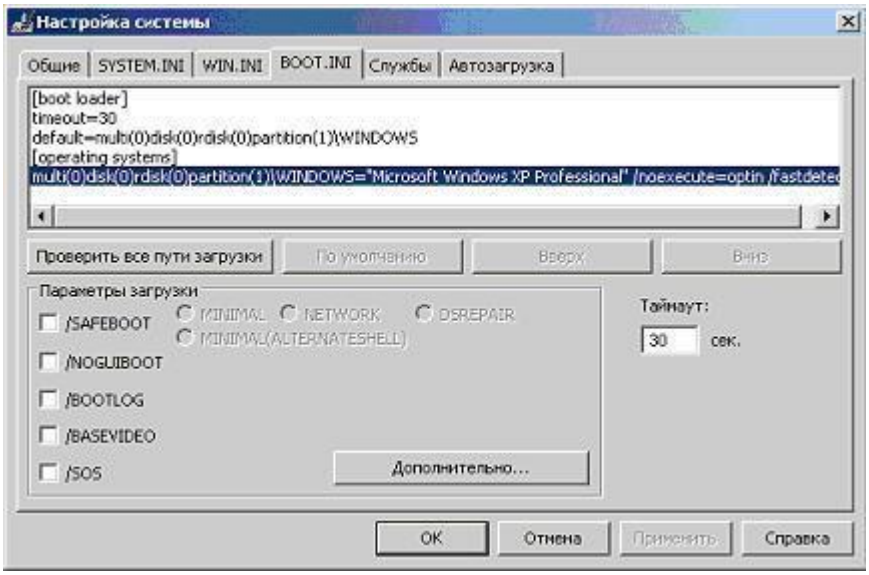
11. Ознакомьтесь со списком запускаемых драйверов и других параметров операционной системы, перейдя к закладке SYSTEM.INI . Тут отображаются все ссылки, указанные в одноименном системном файле



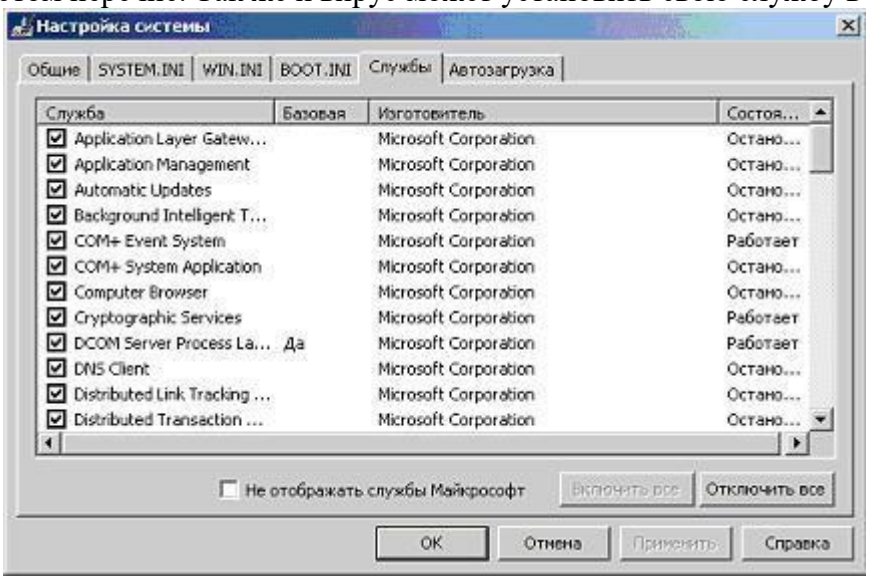
12. Перейдите к аналогичной закладке WIN.INI и ознакомьтесь с ее содержимым



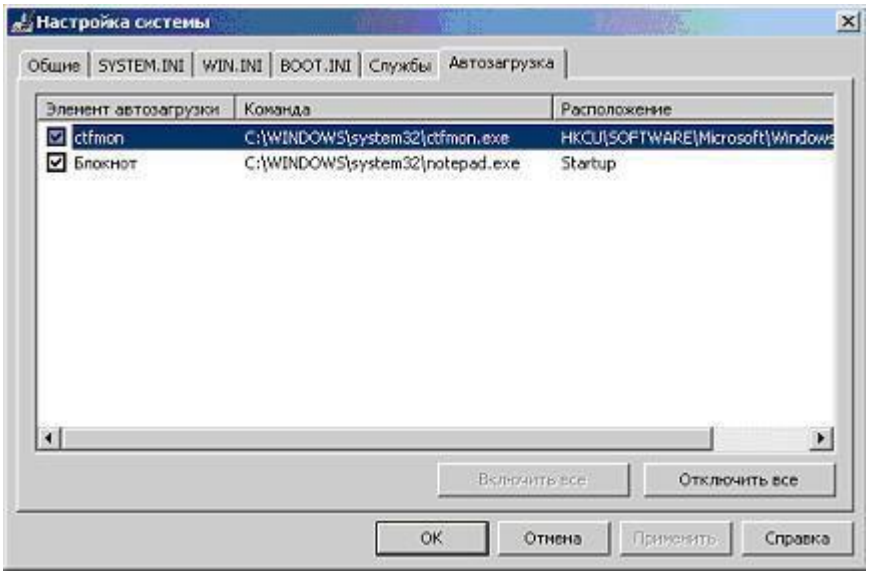
13. Следующая закладка, BOOT.INI, также отображает данные из одноименного файла. Как и предыдущие две, она также содержит системную информацию. Изменять ее можно только обладая соответствующими знаниями!



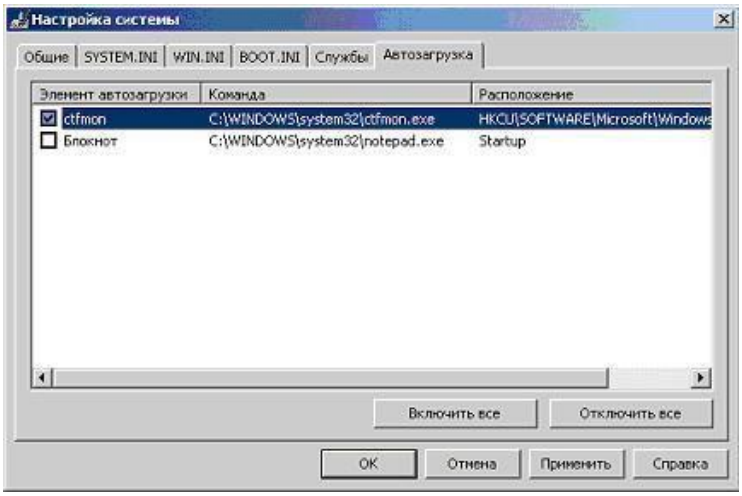
14. Перейдите на закладку Службы. Здесь представлен список всех служб, установленных в системе. Каждая служба представляет собой некое приложение, работающее в фоновом режиме. Например, антивирусный комплекс, обеспечивающий постоянную защиту, также встраивает свою службу, следовательно, она должна присутствовать в этом перечне. Так же и вирус может установить свою службу в системе.



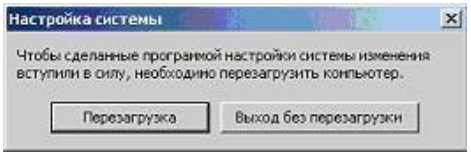
15. Перейдите к последней закладке, Автозагрузка, и убедитесь, что в списке приложений, автоматически запускаемых при загрузке системы, есть Блокнот.



16. Отключите автоматическую загрузку Блокнота, очистив флаг в столбце Элемент автозагрузки и нажмите ОК



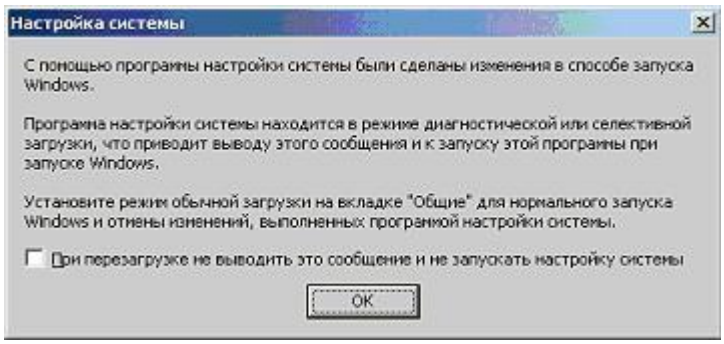
17. В открывшемся окне согласитесь провести перезагрузку, выбрав Перезагрузка



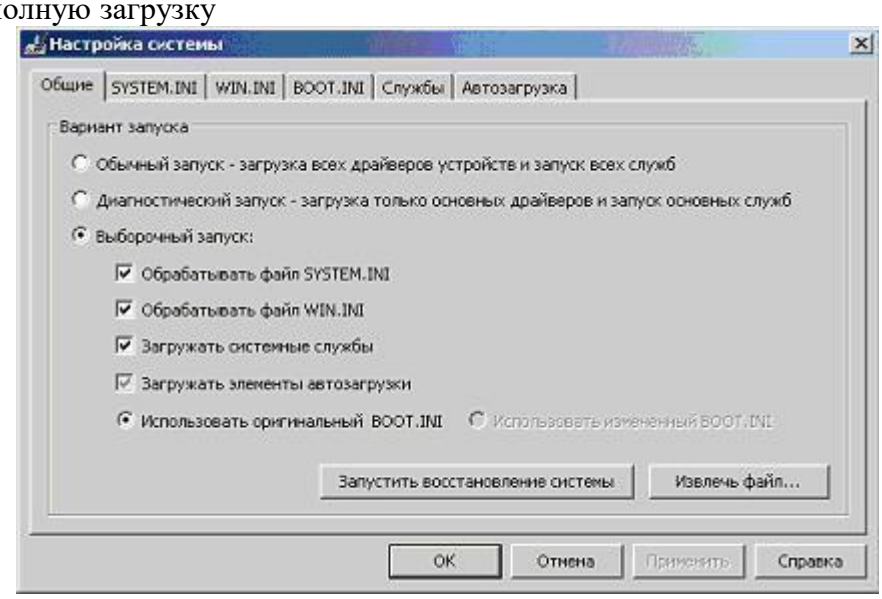
18. Дождитесь окончания перезагрузки

19. Поскольку Вы внесли изменения фактически вручную изменения в параметры автозагрузки (отключив запуск Блокнота), система выведет соответствующее уведомление.

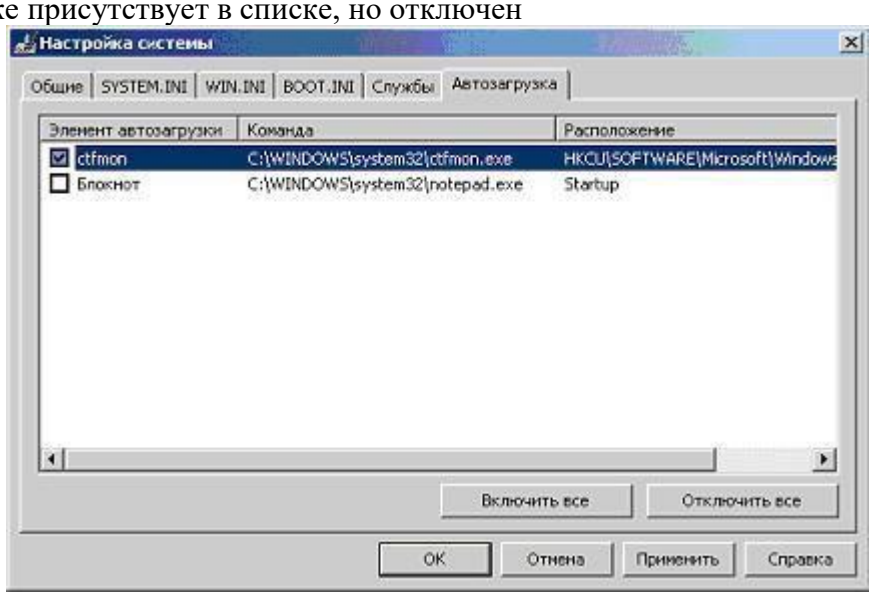
Внимательно прочитайте текст и нажмите ОК



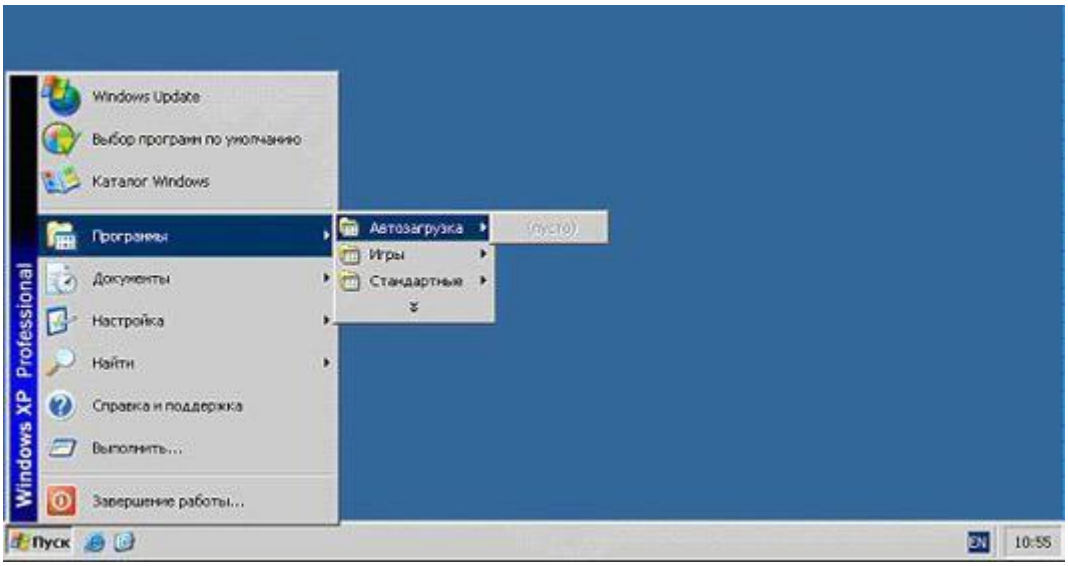
20. Это приведет к открытию окна Настройка системы. Обратите внимание, что теперь используется не обычный запуск, а выборочный. При этом полностью обрабатываются все элементы файлов SYSTEM.INI, WIN.INI и BOOT.INI, загружаются все службы (поскольку мы их не трогали), но флаг Загружать элементы автозагрузки затенен. Это означает неполную загрузку



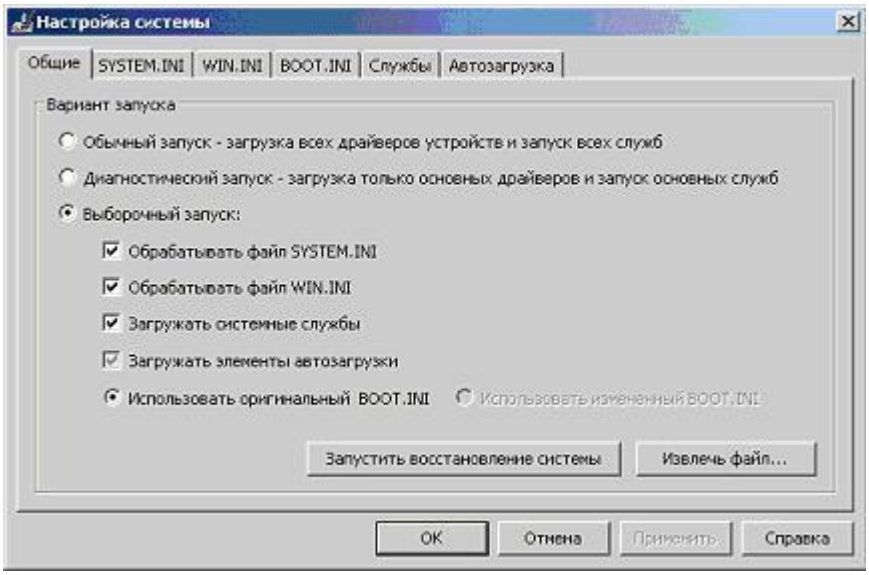
21. Перейдите к закладке Автозагрузка и убедитесь, что ее вид не изменился - Блокнот все так же присутствует в списке, но отключен



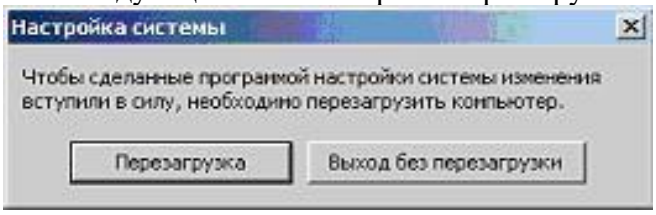
22. Не закрывая окна Настройка системы проверьте, что Блокнот автоматически не запустился и раздел Пуск / Программы / Автозагрузка теперь пуст



23. Вернитесь к закладке Общие окна Настройка системы и выберите сценарий Обычный запуск

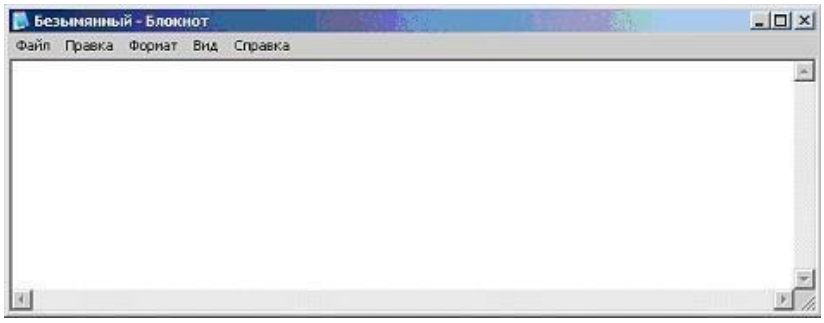


24. Нажмите ОК и в следующем окне выберите Перезагрузка

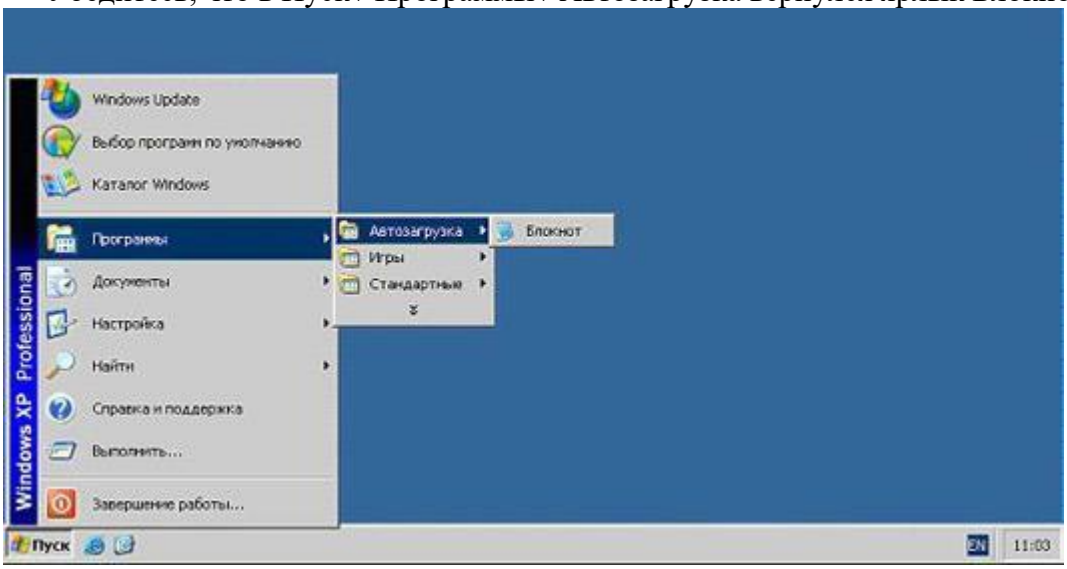


25. Дождитесь окончания перезагрузки, войдите в систему под своей учетной записью и убедитесь, что сообщение о выборочном запуске (как было в пункте 19) не появляется

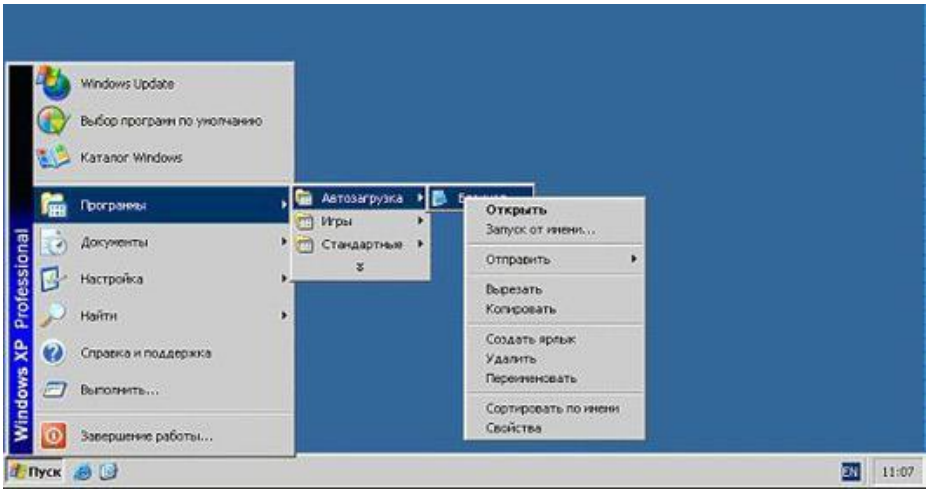
26. Однако поскольку флаг, снятый шаге 23, при переключении в режим Обычный запуск вернулся (Обычный запуск предполагает загрузку всех зарегистрированных компонентов), приложение Блокнот снова автоматически запускается по завершении перезагрузки операционной системы



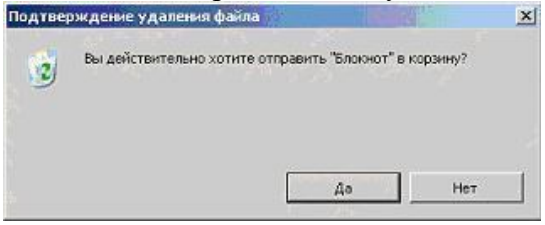
27. Убедитесь, что в Пуск / Программы / Автозагрузка вернулся ярлык Блокнота



28. Удалите его, вызвав контекстное меню (щелчок правой клавишей мыши) и выбрав Удалить



29. Для подтверждения своих намерений в следующем окне нажмите Да



30. Теперь автозагрузка чиста. Убедитесь в этом, выполнив перезагрузку и войдя в систему под своей учетной записью

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows XP и

программными продуктами: MS Word, Adobe Reader, и браузер Internet Explorer.

Указания по технике безопасности: к выполнению практических занятий

допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Для чего служит утилита Настройка системы? Объясните назначение каждой закладки.
2. Что нужно делать, если вы поймали компьютерный вирус?
3. Перечислите правила защиты от заражения компьютера вредоносными программами

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.
2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.
3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.
4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.
5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.
6. Групер Ш. Электронные ключи с энергонезависимой памятью // КомпьютерПресс.-1993.-N8.-С.60-62.
7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.
8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.
9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьютерПресс.-1993.-N7.-С.49-52.
10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер-Пресс.-1991.-N10.-С.19-24.
11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.
12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ.

Практическое занятие №4

Метод создания самотестирующейся расчетной программы с эффективным тестирующим модулем

Цель работы: Получение практических навыков по работе с Командной строкой и по выявлению вредоносных программ на локальном компьютере под управлением Microsoft Windows XP с помощью командной строки.

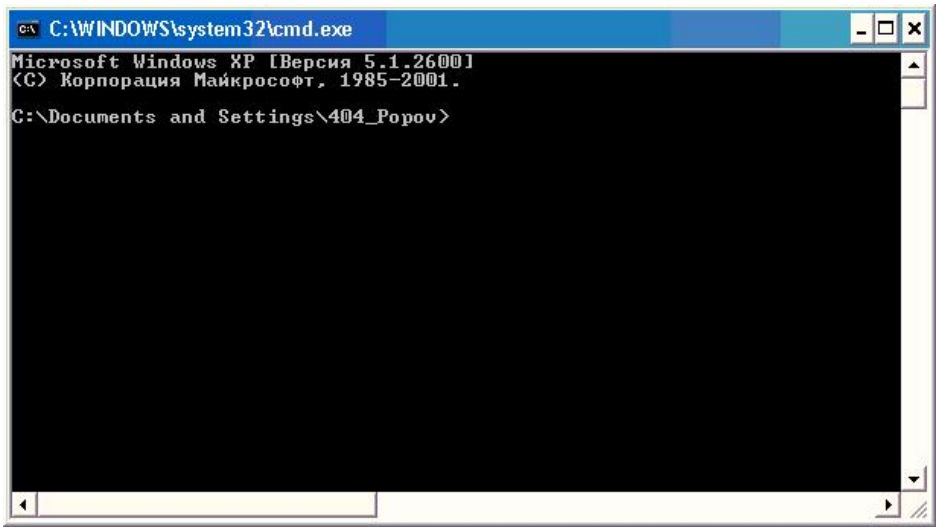
Теоретическая часть

Работа с Командной строкой

В операционной системе Windows, как и в других операционных системах, интерактивные (набираемые с клавиатуры и сразу же выполняемые) команды выполняются с помощью так называемого командного интерпретатора, иначе называемого командным процессором или оболочкой командной строки (command shell). Командный интерпретатор или оболочка командной строки — это программа, которая, находясь в оперативной памяти, считывает набираемые вами команды и обрабатывает их. В Windows 9x, как и в MS-DOS, командный интерпретатор по умолчанию был представлен исполняемым файлом command.com. Начиная с версии Windows NT, в операционной системе реализован интерпретатор команд Cmd.exe, обладающий гораздо более мощными возможностями.

В Windows NT/2000/XP файл Cmd.exe, как и другие исполняемые файлы, соответствующие внешним командам операционной системы, находятся в каталоге %SystemRoot% \SYSTEM32 (значением переменной среды %SystemRoot% является системный каталог Windows, обычно C:\Windows или C:\WinNT).

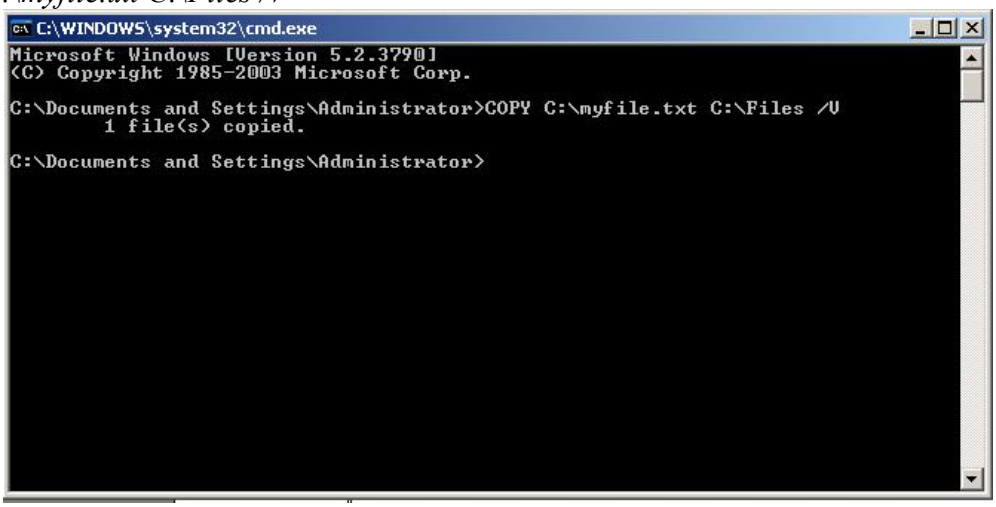
1.Для запуска командного интерпретатора (открытия нового сеанса Командной строки) можно выбрать пункт Пуск / Выполнить, ввести имя файла Cmd.exe и нажать кнопку OK. В результате откроется новое окно, в котором можно запускать команды и видеть результат их работы.



Некоторые команды распознаются и выполняются непосредственно самим командным интерпретатором — такие команды называются внутренними (например, *copy* или *dir*) Другие команды операционной системы представляют собой отдельные программы, расположенные по умолчанию в том же каталоге, что и Cmd.exe, которые Windows загружает и выполняет аналогично другим программам. Такие команды называются внешними (например, more или *xcopy*).

2. Для того, чтобы выполнить команду, вы после приглашения командной строки (например, *C:*) вводите имя этой команды (регистр не важен), ее параметры и ключи (если они необходимы) и нажимаете клавишу <Enter>. Создайте на диске C файл myfile.txt и папку Files. В Командной строке наберите

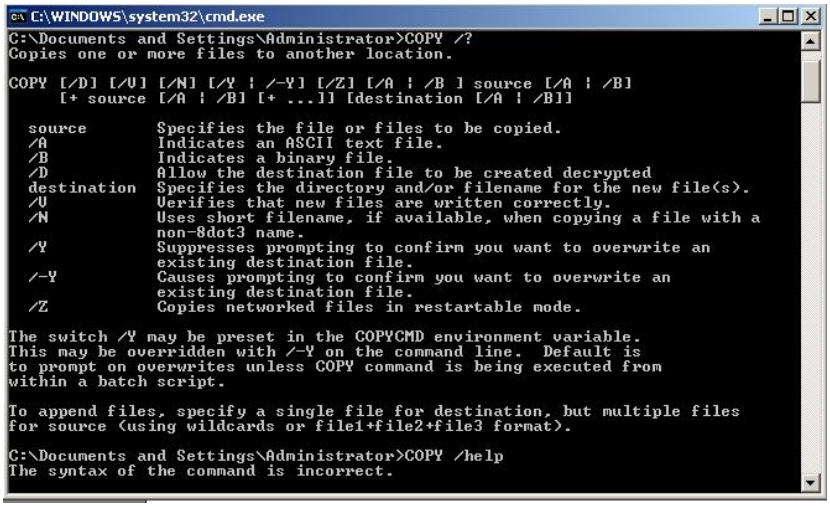
copy C:\myfile.txt C:\Files /V



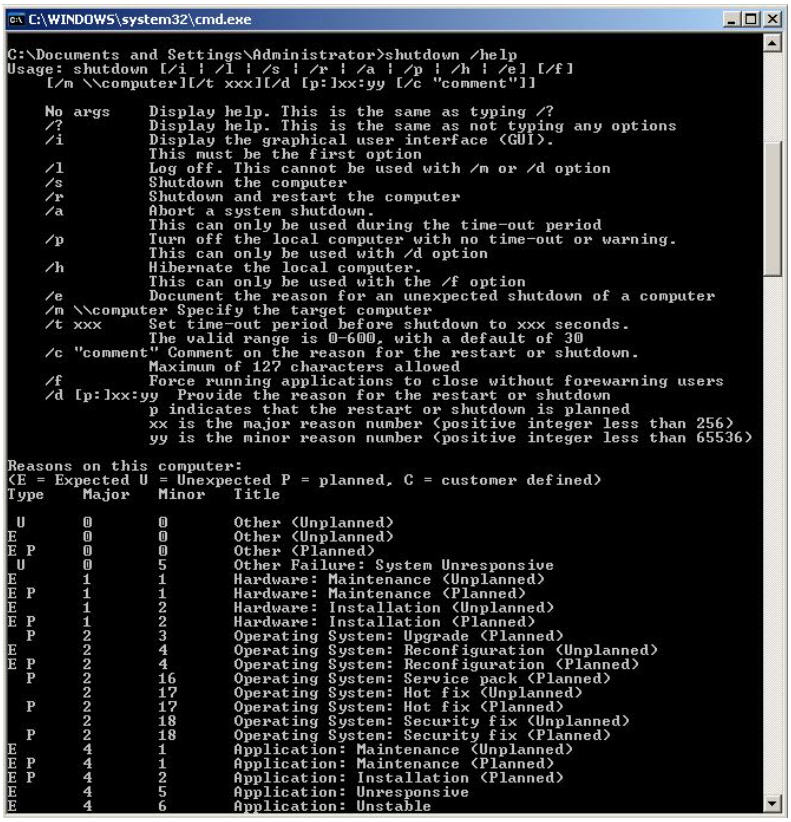
Имя команды здесь — *copy*, параметры — *C:\myfile.txt* и *C:\Files*, а ключом является */V*. Отметим, что в некоторых командах ключи могут начинаться не с символа */*, а с символа – (минус), например, *-V*.

3. Многие команды Windows имеют большое количество дополнительных параметров и ключей, запомнить которые зачастую бывает трудно. Большинство команд снабжено встроенной справкой, в которой кратко описываются назначение и синтаксис данной команды. Получить доступ к такой справке можно путем ввода команды с ключом */?* или */help*. В командной строке наберите

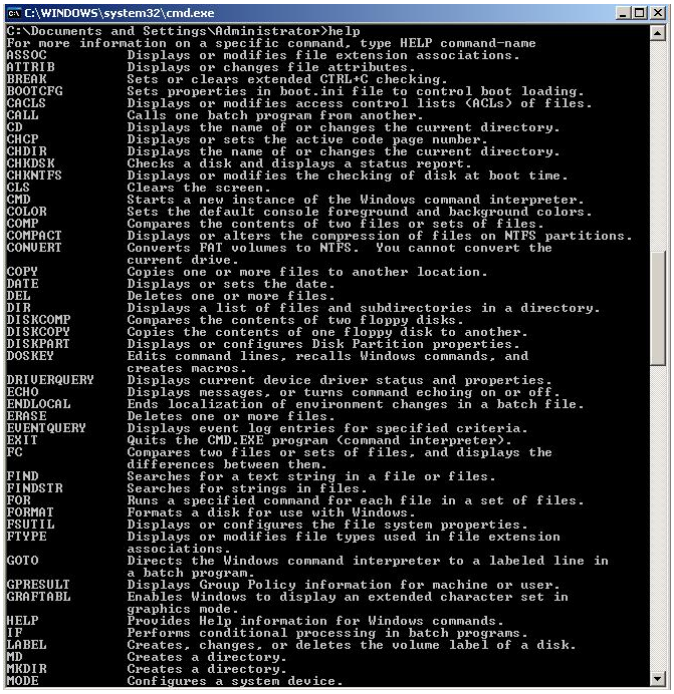
copy /?



shutdown /help



help

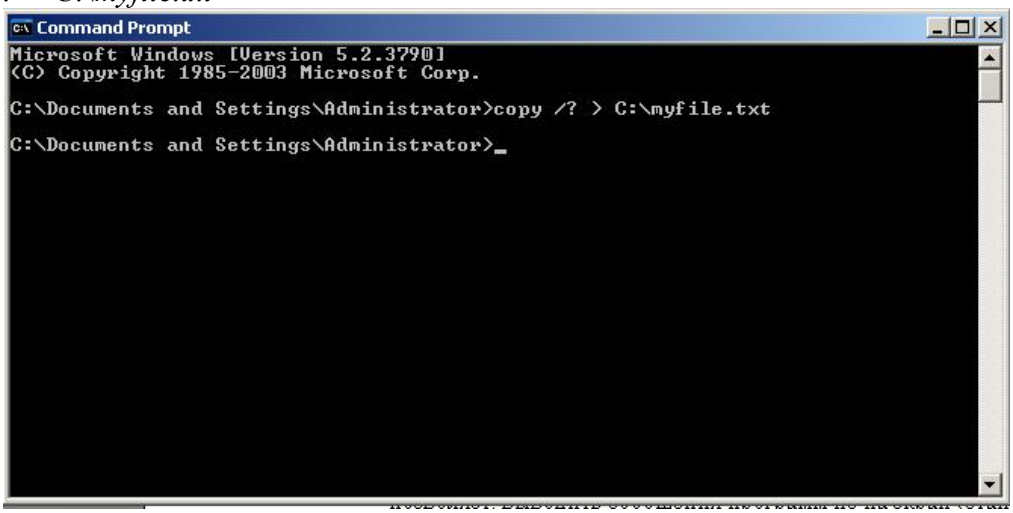


Последняя команда выводит список основных команд Командной строки

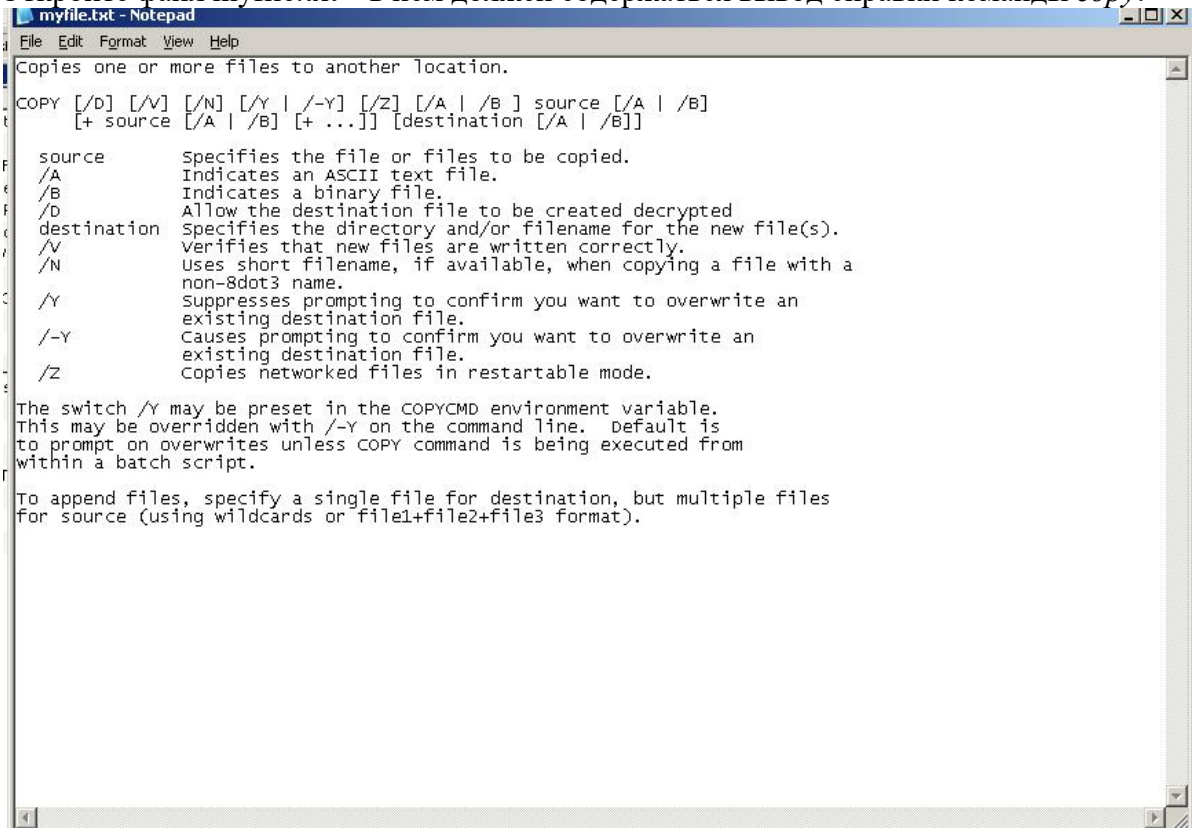
4. С помощью переназначения устройств ввода/вывода одна программа может направить свой вывод на вход другой или перехватить вывод другой программы, используя его в качестве своих входных данных. Таким образом, имеется возможность передавать информацию от процесса к процессу при минимальных программных издержках. Практически это означает, что для программ, которые используют стандартные входные и выходные устройства, операционная система позволяет: выводить сообщения программ не на экран (стандартный выходной поток), а в файл или на принтер (перенаправление вывода), читать входные данные не с клавиатуры (стандартный входной поток), а из

заранее подготовленного файла (перенаправление ввода), передавать сообщения, выводимые одной программой, в качестве входных данных для другой программы. В Командной строке наберите

copy /? > C:\myfile.txt

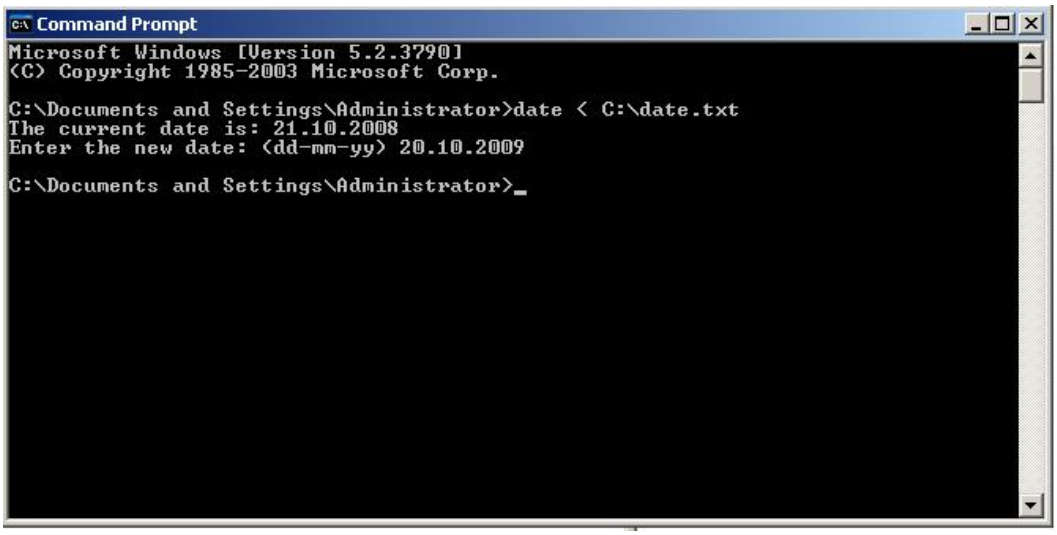


Откройте файл myfile.txt – в нем должен содержаться вывод справки команды *copy*.

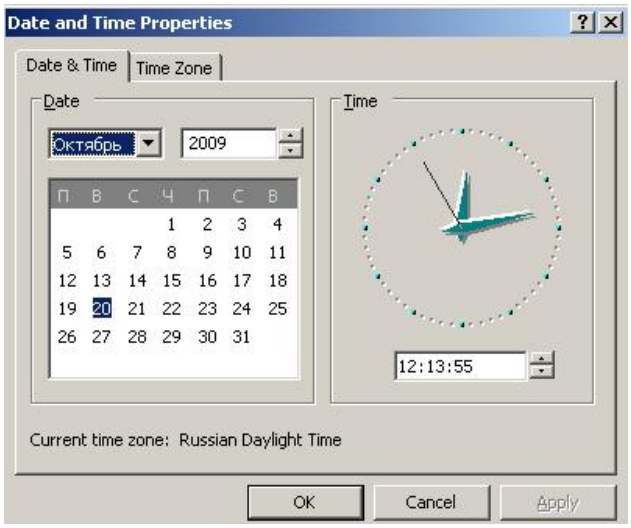


5. С помощью символа < можно прочитать входные данные для заданной команды не с клавиатуры, а из определенного (заранее подготовленного) файла. На диске С создайте файл date.txt и напишите в нем 20.10.2009. В Командной строке наберите

Date < C:\date.txt

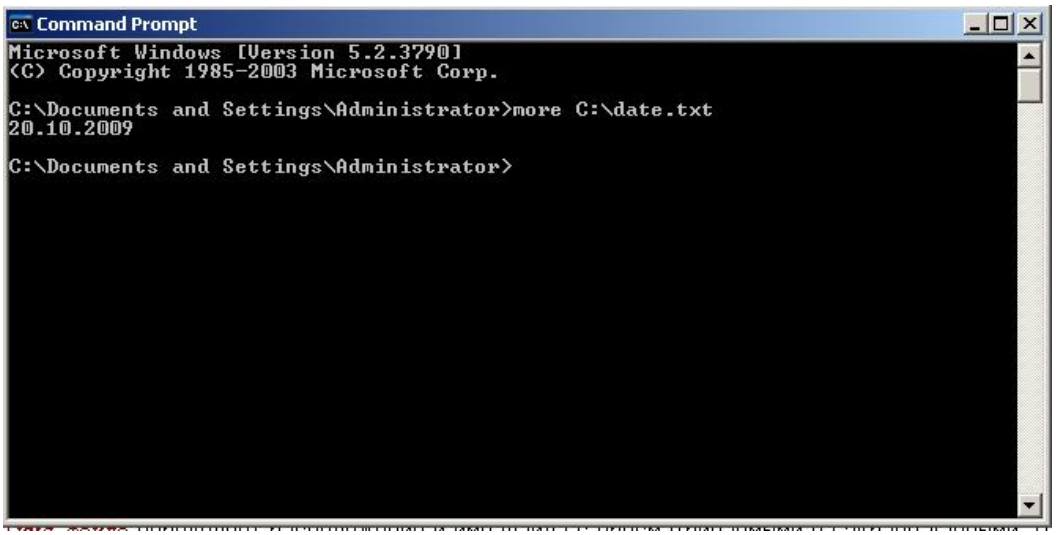


Проверьте дату на вашем компьютере, она должна измениться на 20.10.2009



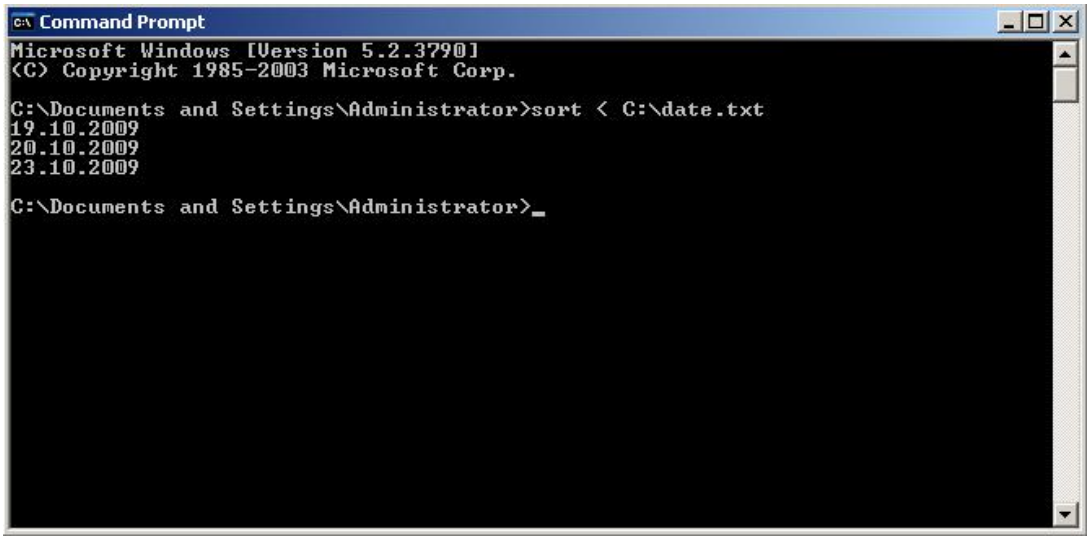
6. Одной из наиболее часто использующихся команд, для работы, с которой применяется перенаправление ввода/вывода и конвейеризация, является *more*. Эта команда считывает стандартный ввод из конвейера или перенаправленного файла и выводит информацию частями, размер каждой из которых не больше размера экрана. Используется *more* обычно для просмотра длинных файлов. В Командной строке наберите

More C:\date.txt

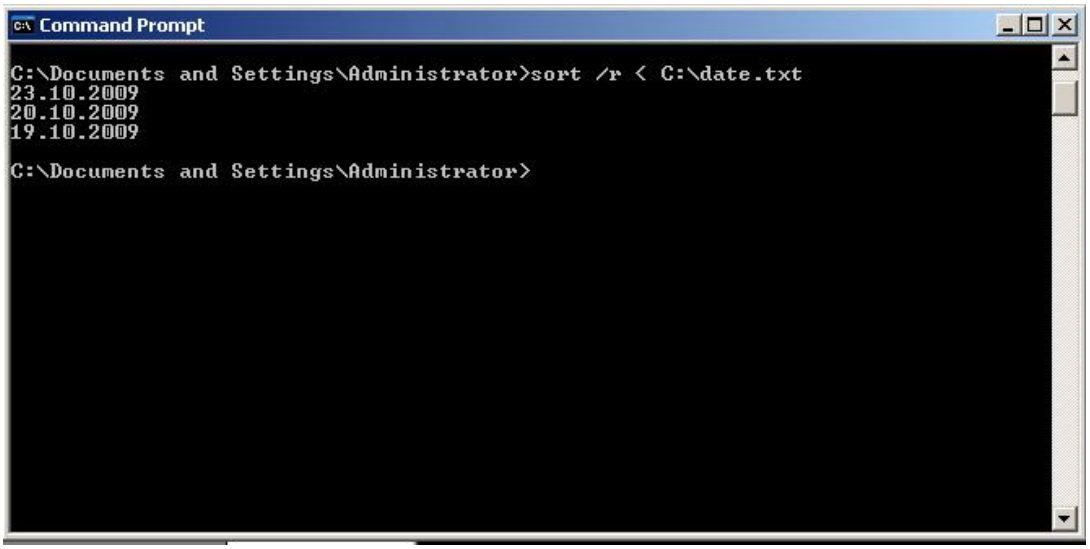


7. Другой распространенной командой, использующей перенаправление ввода/вывода и конвейеризацию, является *sort*. Эта команда работает как фильтр: она считывает символы в заданном столбце, упорядочивает их в возрастающем или убывающем порядке и выводит отсортированную информацию в файл, на экран или другое устройство. В командной строке наберите

sort < C:\date.txt



sort /r < C:\date.txt



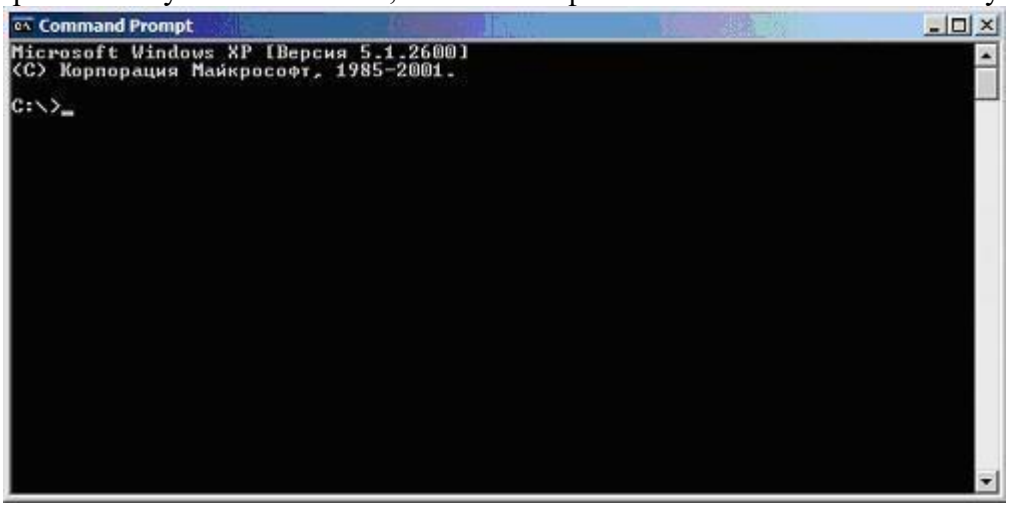
По умолчанию сортировка выполняется в порядке возрастания. Ключ */R* позволяет изменить порядок сортировки на обратный (от Z к A и затем от 9 до 0).

Сетевая активность

Неожиданно возросшая сетевая активность может служить ярким свидетельством работы на компьютере подозрительной программы, производящей несанкционированную рассылку писем, связывающейся со своим автором и передающей ему конфиденциальную информацию или просто загружающую свои дополнительные модули или атакующей соседние компьютеры. Но при этом нужно не забывать, что ряд вполне легальных приложений также имеют свойство иногда связываться с сайтом фирмы-производителя, например для проверки наличия обновлений или более новых версий. Поэтому, прежде чем отключать сеть и выдергивать сетевой шнур, увидев необычно яркое мигание лампочки на сетевой карте, необходимо уметь определять какие программы и приложения вызвали эту подозрительную активность.

Изучить и проанализировать сетевую активность можно с помощью встроенных в операционную систему инструментов или же воспользовавшись специальными отдельно устанавливаемыми приложениями. Это можно сделать при помощи Диспетчера задач Windows, но он показывает только самую общую информацию. Для получения более подробных данных нужно воспользоваться утилитой *netstat*, которая выводит на экран мгновенную статистику сетевых соединений.

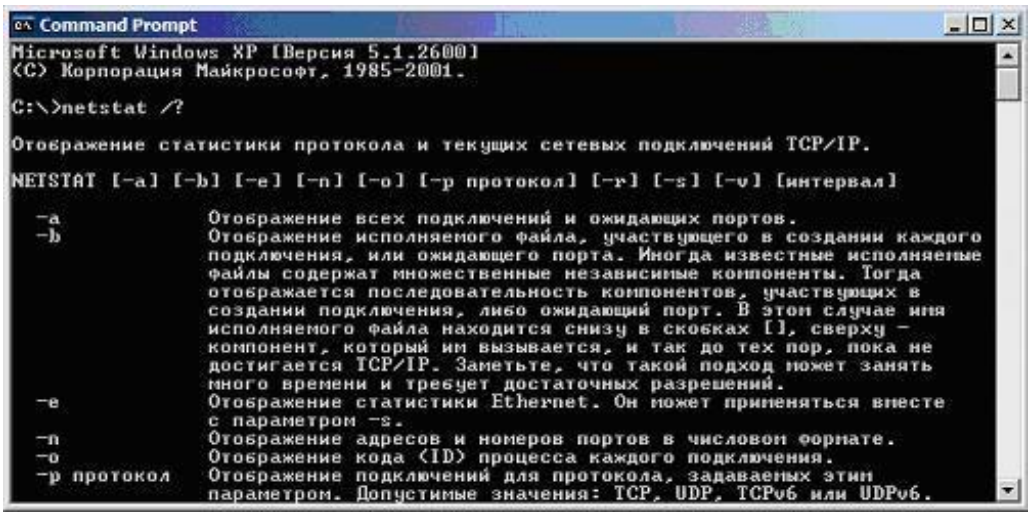
1. Воспользуйтесь системным меню Пуск / Программы / Стандартные / Командная строка или Пуск / Выполнить, ввести имя файла Cmd.exe и нажать кнопку OK



2. В Командной мтроке наберите

netstat /?

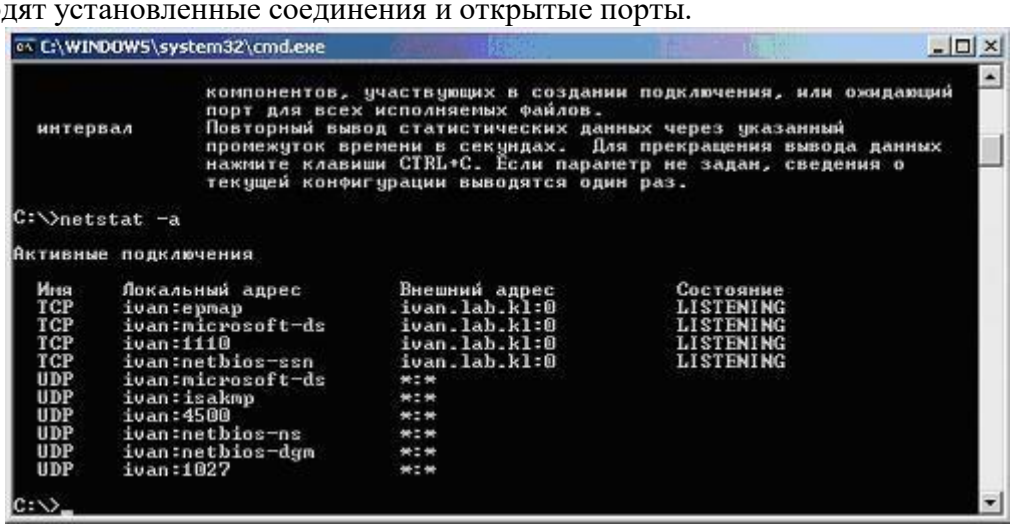
3. Прочитайте описание утилиты *netstat*. Убедитесь, что для вывода самой полной информации нужно использовать ключ *-a*



4. В Командной строке наберите

netstat -a

5. Результатом выполнения команды является список активных подключений, в который входят установленные соединения и открытые порты.



TCP-порты обозначаются строкой “TCP” в колонке Имя. Открытые TCP-порты обозначаются строкой "LISTENING" в колонке состояние. Часть портов связана с системными службами Windows и отображается не по номеру, а по названию - epmap, microsoft-ds, netbios-ssn. Порты, не относящиеся к стандартным службам, отображаются по номерам.

UDP-порты обозначаются строкой "UDP" в колонке Имя. Они не могут находиться в разных состояниях, поэтому специальная пометка "LISTENING" в их отношении не используется. Как и TCP-порты они могут отображаться по именам или по номерам.

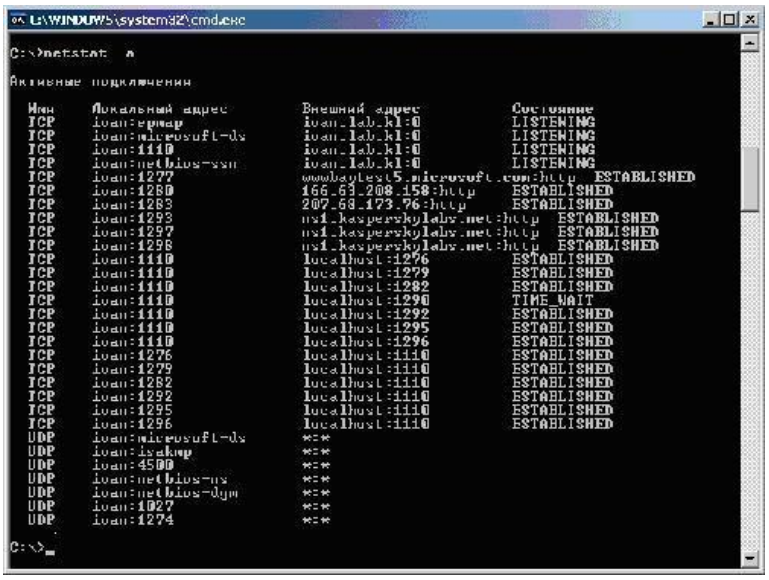
Порты, используемые вредоносными программами, чаще всего являются нестандартными и поэтому отображаются согласно их номерам. Впрочем, могут встречаться троянские программы, использующие для маскировки стандартные для других приложений порты, например 80, 21, 443 - порты, используемые на файловых и веб-серверах.

6. Команда *netstat*, в отличие от Диспетчера задач Windows, не работает в режиме реального времени, а отображает мгновенную статистику. Следовательно, для просмотра активности соединений, скажем, через минуту, нужно заново выполнить команду. В Командной строке наберите

netstat -a

и посмотрите не изменения

7. Исследуйте полученную статистику



8. Закройте окно командной строки. В Командной строке наберите *Exit*

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows XP и программными продуктами: MS Word, Adobe Reader.

Указания по технике безопасности: к выполнению практических занятий

допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Что такое командный интерпретатор или оболочка командной строки?
2. Как запустить командную строку?
3. Какие команды называются внутренними, а какими внешними?
4. Что необходимо сделать, чтобы выполнить команду?
5. Как можно получить справку о команде?
6. Как прочитать входные данные для заданной команды не с клавиатуры, а из определенного файла?
7. Что такое сетевая активность? Назовите ее особенности.
8. Как можно изучить и проанализировать сетевую активность?
9. Для чего нужна команда netstat?

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/

2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.

3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.

4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.

5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.

6. Групер Ш. Электронные ключи с энергонезависимой памятью //КомпьютерПресс.-1993.-N8.-С.60-62.

7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.

8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.

9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьютерПресс.-1993.-N7.-С.49-52.

10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер-Пресс.-1991.-N10.-С.19-24.

11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.

12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

Практическое занятие №5

Сведение защиты программ к забывающему моделированию на RAM-машине

Цель работы: Эта лабораторная работа позволяет освоить процесс установки и первичной настройки Антивируса Касперского на локальный компьютер.

Теоретическая часть

Системные требования

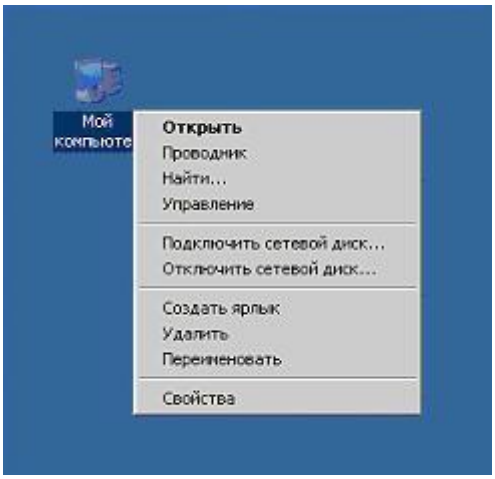
При создании любого приложения программисты дают гарантию, что их продукт будет работать на технике с определенными характеристиками. Это требования к программному обеспечению. Бывают также требования к аппаратному обеспечению - в этом случае постулируется необходимость наличия на компьютере некоторого минимального объема оперативной памяти (если ее меньше, то программа будет очень медленно работать или же не запустится вовсе), свободного пространства на диске (для размещения всех необходимых в работе приложения файлов), тактовой частоты процессора, от которой зависит производительность компьютера и другое.

В случае антивирусных программ часто выдвигается дополнительное требование отсутствия на компьютере другого антивирусного средства, совместная работа с которым может вызвать конфликты (при установке любой антивирусной программы, установщик выводит предупреждение: если на компьютере установлено другое антивирусное программное обеспечение, могут возникнуть конфликтные ситуации).

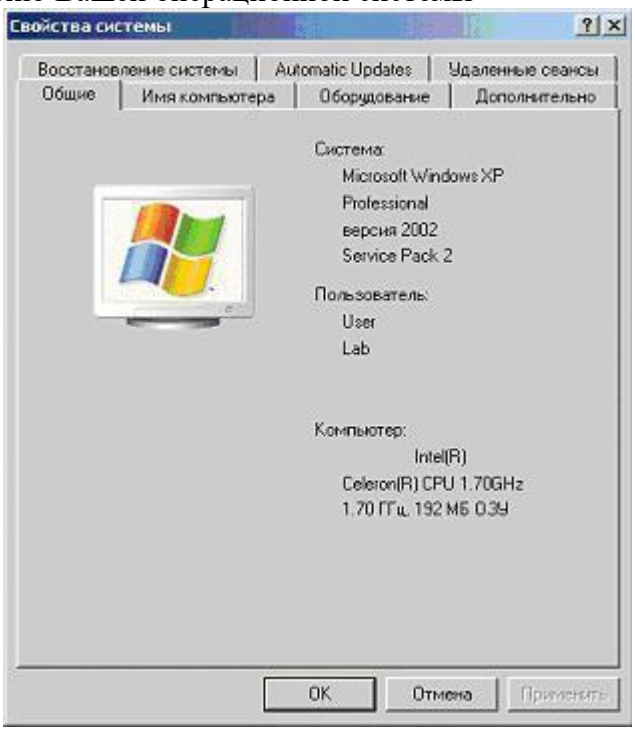
Системные требования обычно приводятся в сопровождающем дистрибутив текстовом файле и/или в документации к продукту. Также всегда с ними можно ознакомиться на сайте компании-производителя.

В этом задании нужно сравнить системные требования Антивируса Касперского с конфигурацией Вашего компьютера и убедиться, что установка этого приложения возможна.

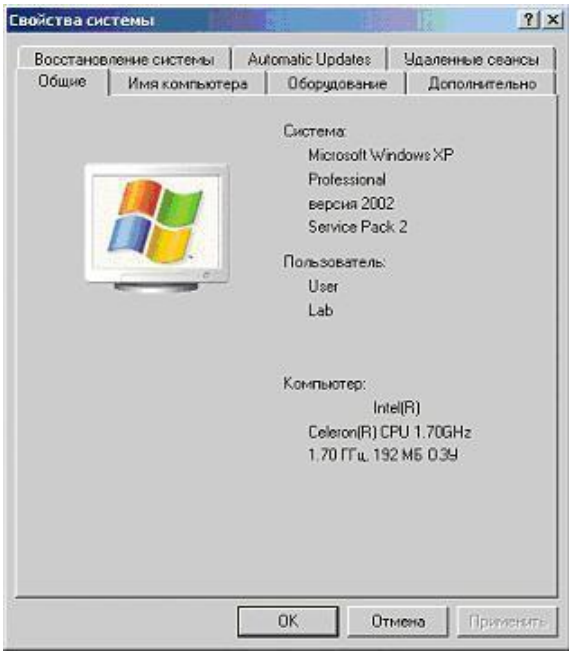
1. Узнайте версию операционной системы, в которой Вы работаете. Для этого найдите иконку Мой компьютер, выведите ее контекстное меню (щелкнув на ней правой кнопкой мыши) и выберите пункт Свойства



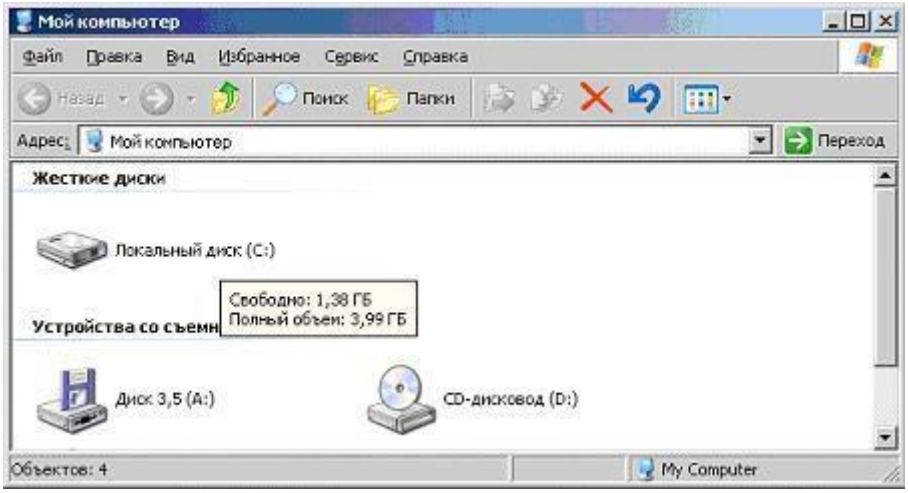
2. Открывшееся окно Свойства системы содержит основные сведения о компьютере и установленной на нем операционной системе. На первой закладке, Общие, представлена сводная информация, в том числе название и версия операционной системы. На картинке это Microsoft Windows XP Professional с установленным Service Pack 2. Запомните название и версию Вашей операционной системы



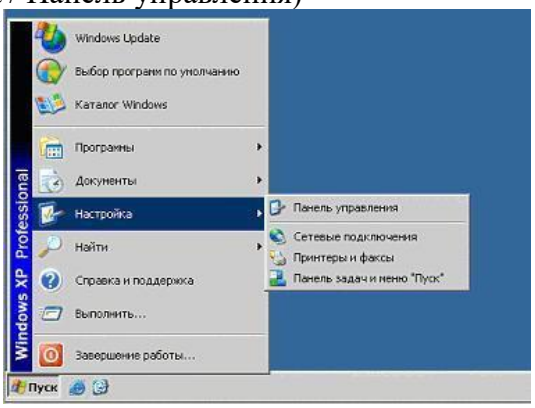
3. Антивирусу Касперского может быть установлен на операционную систему "Microsoft Windows XP Home Edition или XP Professional (Service Pack 1 или выше)". Далее необходимо убедиться, что конфигурация системы позволяет установить Антивирус Касперского. Для этого вернитесь к окну Свойства системы и убедитесь, что установленная операционная система соответствует требованиям Антивируса Касперского.



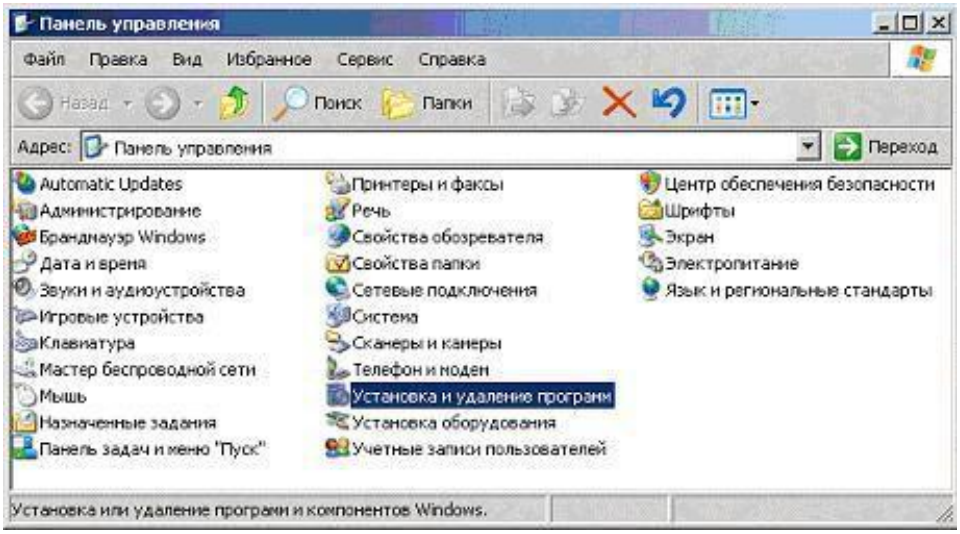
4. Проверьте наличие свободного места на диске. Для этого откройте папку Мой компьютер и задержите на пару секунд курсор мыши над иконкой системного диска. В появившемся сообщении будет указан объем свободного пространства на нем и общий объем диска



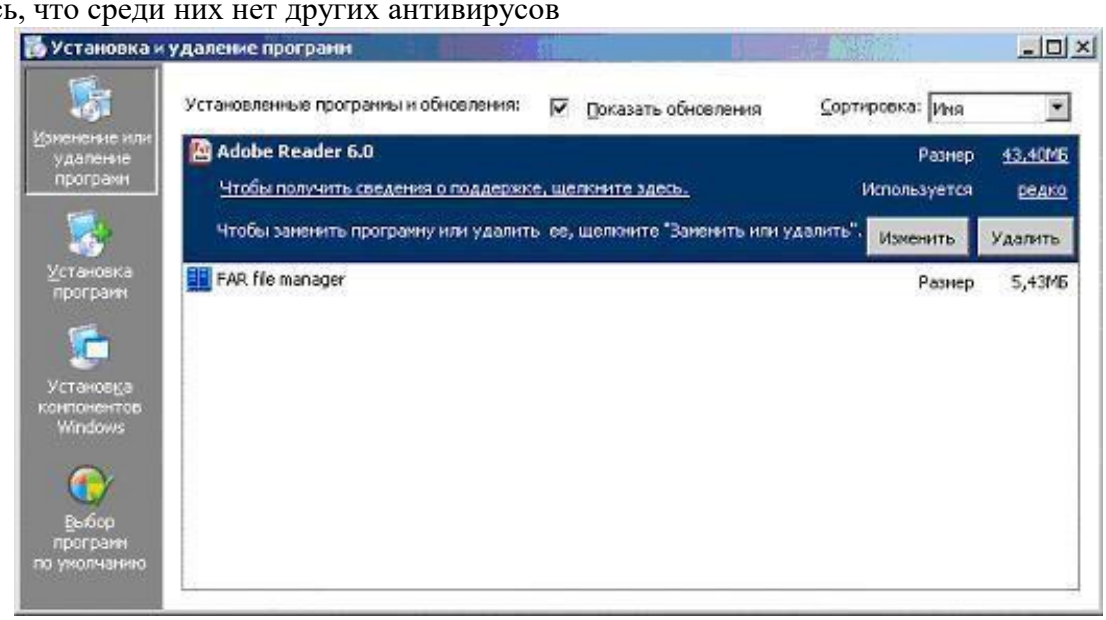
5. Далее необходимо ознакомиться со списком установленных на компьютер программ и убедиться, что среди них нет других антивирусов. Для этого вызовите Панель управления (Пуск / Настройка / Панель управления)



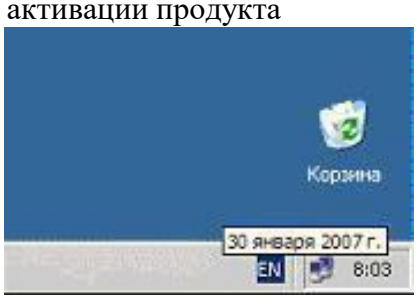
6. В Панели управления найдите элемент Установка и удаление программ и откройте его



7. Ознакомьтесь со списком установленных на компьютере программ и убедитесь, что среди них нет других антивирусов



8. Обратите внимание на системную дату, установленную на Вашем компьютере. Для этого задержите на паку секунд курсор мышки над системным временем в правом нижнем углу экрана. Системная дата должна соответствовать реальной дате, это будет необходимо для корректной активации продукта



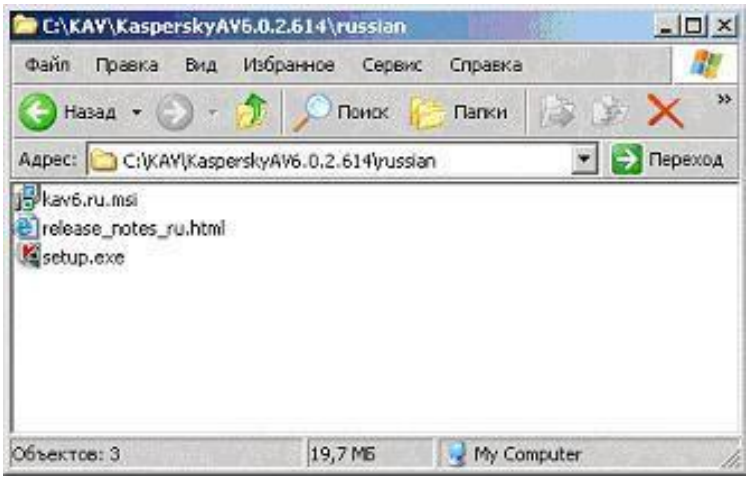
На этом подготовительный этап окончен и можно переходить непосредственно к установке.

Установка

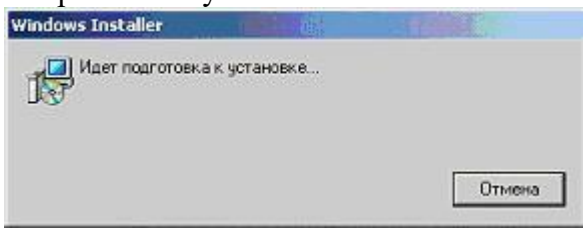
Большинство современных приложений перед запуском необходимо установить. Стандартная процедура установки включает в себя копирование необходимых в работе программы файлов на диск (в нужное место) и регистрацию в реестре операционной системы. Иногда для завершения установки требуется перезагрузка компьютера.

Для успешной установки Антивируса Касперского требуется дистрибутив и лицензионный ключ (файл с расширением .key, содержащий данные, удостоверяющие легальность приобретенного продукта) либо код активации. Эти файлы обычно записываются на CD и передаются пользователю при покупке. В случае приобретения в Интернет-магазине, дистрибутив можно либо загрузить с сайта Лаборатории Касперского, либо заказать отправку почтой или курьером на CD, лицензионный ключ высылается по e-mail. Если Вы имеете код активации, то Антивирус Касперского можно активировать с помощью него, после установки.

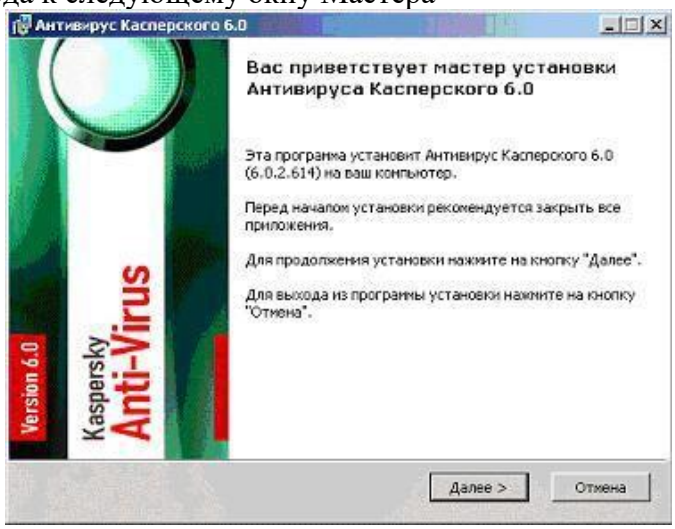
1. Откройте папку с дистрибутивом Антивируса Касперского. Ее расположение можно узнать у преподавателя



2. Найдите файл setup.exe и запустите его

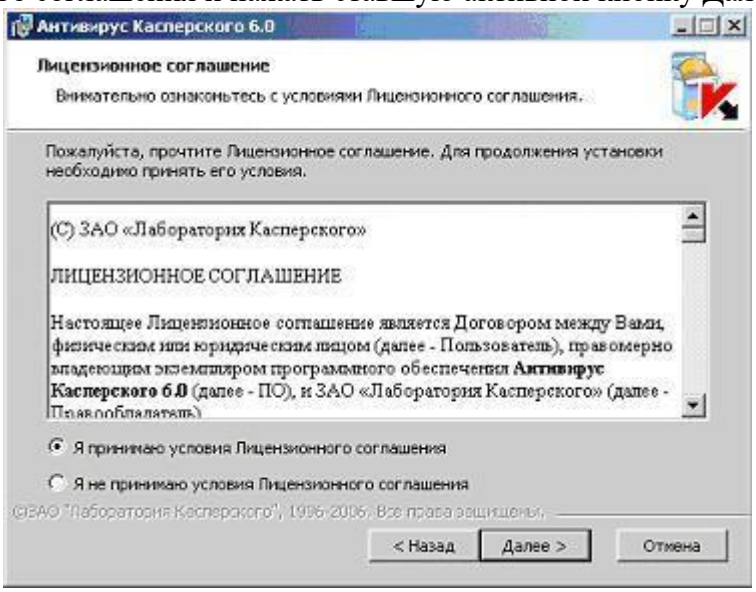


3. Если система удовлетворяет всем необходимым Антивирусу Касперского требованиям, запустится Мастер установки. В первом окне он поприветствует Вас и сообщит, что собирается сделать. Внимательно прочтите предложенный текст, выполните указание закрыть все сторонние открытые приложения (если таковые имеются) и нажмите кнопку Далее для перехода к следующему окну Мастера

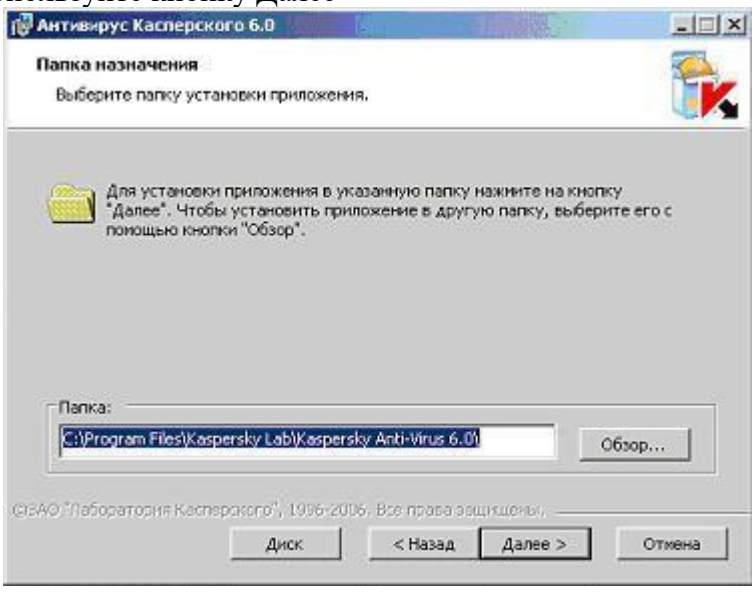


4. На втором шаге Мастера необходимо ознакомиться с Лицензионным соглашением между Вами и Лабораторией Касперского, производителем Антивируса

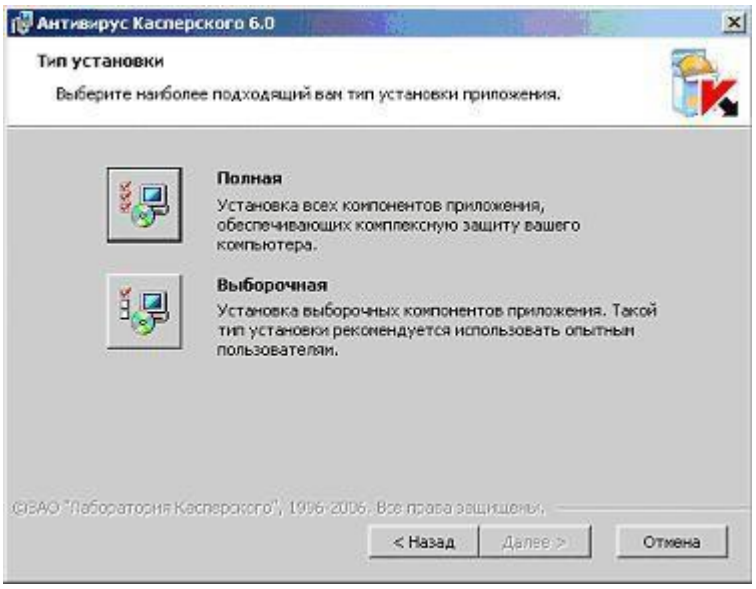
Касперского. В нем описаны все права и обязанности обоих сторон, в том числе ответственность за нарушение авторских прав и самостоятельное изготовление копий антивируса. Внимательно прочтите его. Установку можно продолжить только согласившись со всеми положениями, для этого нужно отметить пункт Я принимаю условия Лицензионного соглашения и нажать ставшую активной кнопку Далее



5. На следующем шаге нужно определить директорию, куда будут скопированы основные системные файлы антивируса. По умолчанию предлагается использовать C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus. Если она по каким-то причинам не подходит (например, у вас заканчивается место на диске C), с помощью кнопки Обзор всегда можно выбрать другую. Для продолжения установки и перехода к следующему окну тут и в дальнейшем используйте кнопку Далее



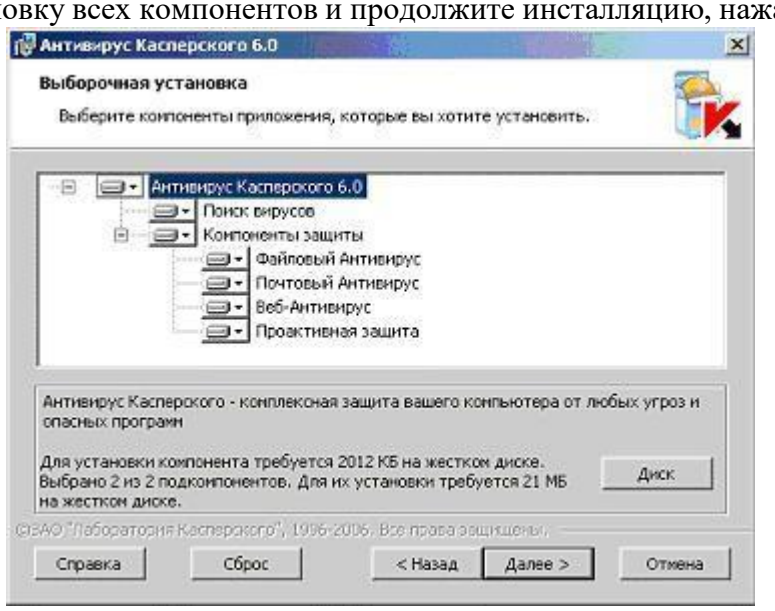
6. Далее нужно выбрать тип установки: полную или выборочную. Полная означает установку всех компонентов Антивируса Касперского, а выборочная позволяет некоторые из них отключить. Выберите Выборочную, нажав на квадратную кнопку слева от описания этого типа установки



7. Как и было обещано, в следующем окне можно указать, какие компоненты Антивируса Касперского необходимо установить, а какие пропустить. На рисунке изображен вид этого окна по умолчанию, соответствующий полной установке. Будет ли установлен тот или иной компонент символизирует иконка слева от него: - устанавливать, нет.

Тут же можно получить краткое описание каждого компонента - для этого необходимо выделить (щелкнуть правой кнопкой мыши) интересующий компонент и внизу окна появится нужная информация. На рисунке выделен Антивирус Касперского, следовательно внизу показано описание самой программы.

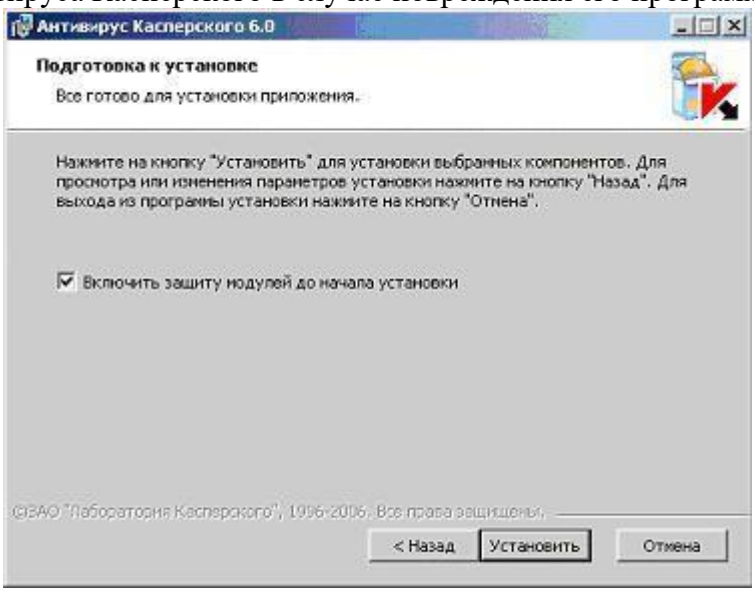
Оставьте установку всех компонентов и продолжите инсталляцию, нажав Далее



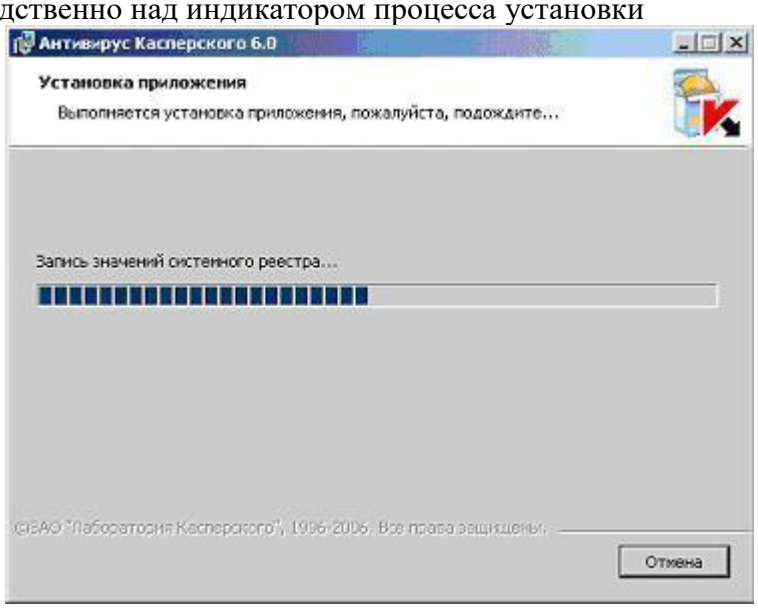
8. Далее Мастер проверяет наличие на компьютере других антивирусных программ, полный список которых можно найти в файле release_notes.txt в разделе "Установка". Если такие найдутся, то пользователю будет выведено соответствующее уведомление с предложением их удалить. Но в нашем случае компьютер чист и этот этап в интерфейсе никак не отображается

9. На следующем этапе нужно подтвердить намерение установить программу, нажав Установить. После этого начнется непосредственное копирование файлов и регистрация программы в реестре, и вернуться к предыдущим окнам Мастера установки будет невозможно.

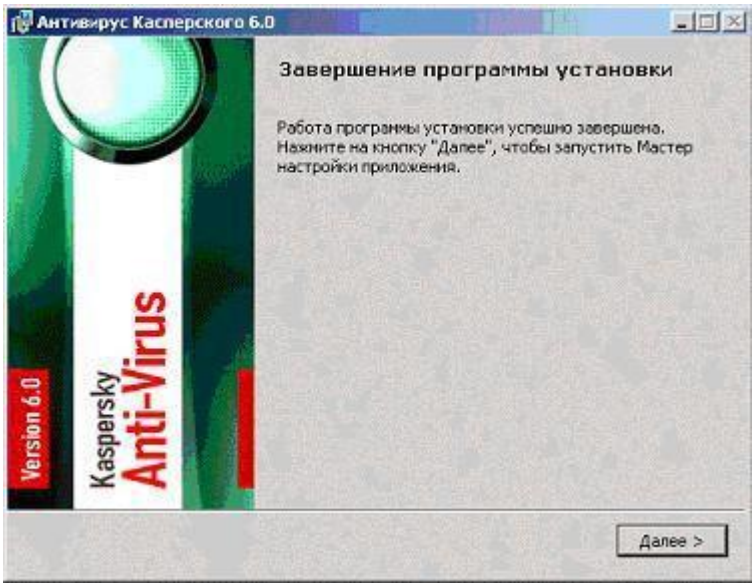
Расположенный в центре окна флаг Включить защиту модулей до начала установки рекомендуется оставить включенным. Но в дальнейшем, при повторной инсталляции этой же версии Антивируса Касперского его следует очищать. Он отвечает за сохранность сделанных во время установки настроек, они могут потребоваться в дальнейшем для восстановления Антивируса Касперского в случае повреждения его программных модулей



10. Нажмите кнопку Установить и проследите за действиями Мастера. Они описываются непосредственно над индикатором процесса установки



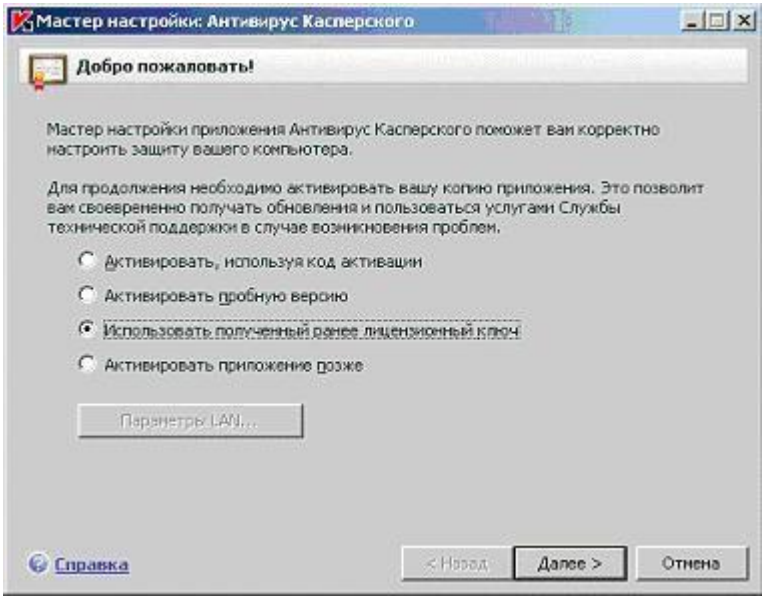
11. По окончании инсталляции Мастер установки выводит информационное окно. Вам необходимо ознакомится с расположенным в нем текстом и запустить Мастер настройки приложения. Для этого нажмите Далее



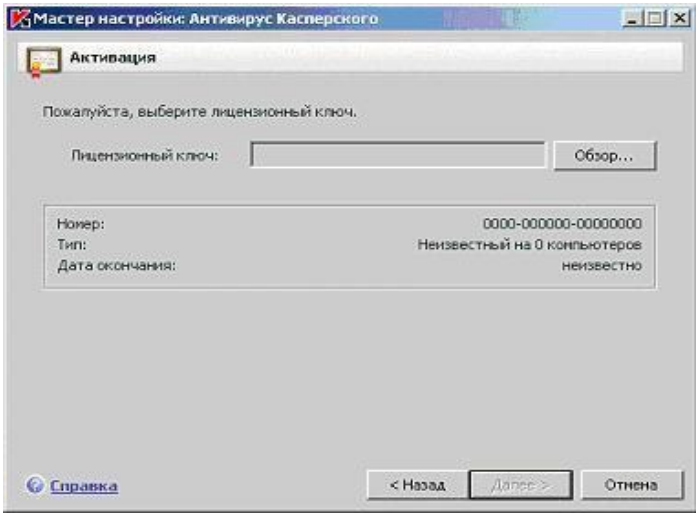
12. На первом этапе настройки нужно активировать приложение. Это можно сделать одним из четырех предложенных вариантов:

- Используя код активации, коммерческий или пробный. Такой код может быть выдан при покупке через Интернет, в этом случае активация происходит также через Интернет;
- Активировать, используя полученный ранее ключевой файл (именно этот способ будет использован в этой лабораторной работе);
- Активировать позже - если ключевого файла нет, то можно установить антивирус в пробном режиме (программа будет работать 30 дней и будет не доступно обновление антивирусных баз , следовательно, надежную защиту получить не получится).

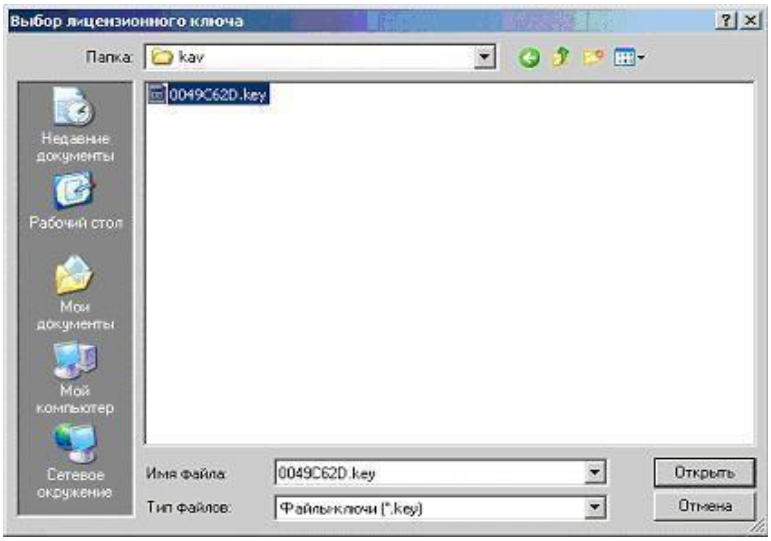
Выберите вариант Использовать полученный ранее лицензионный ключ и нажмите Далее



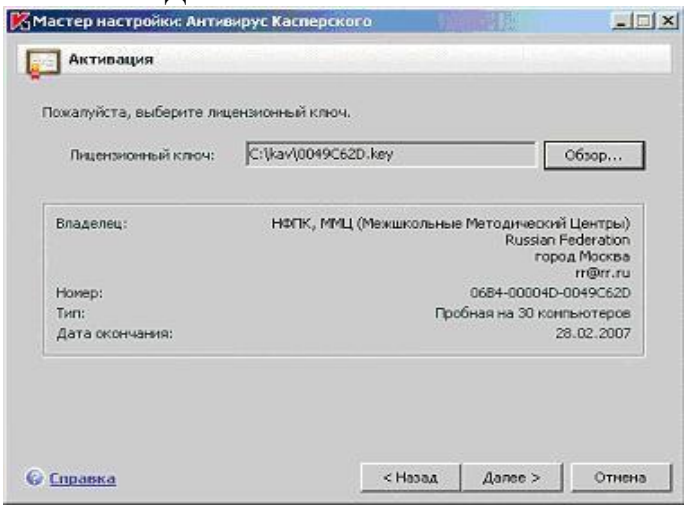
13. В следующем окне нужно указать путь к лицензионному файлу. Для этого нажмите кнопку Обзор



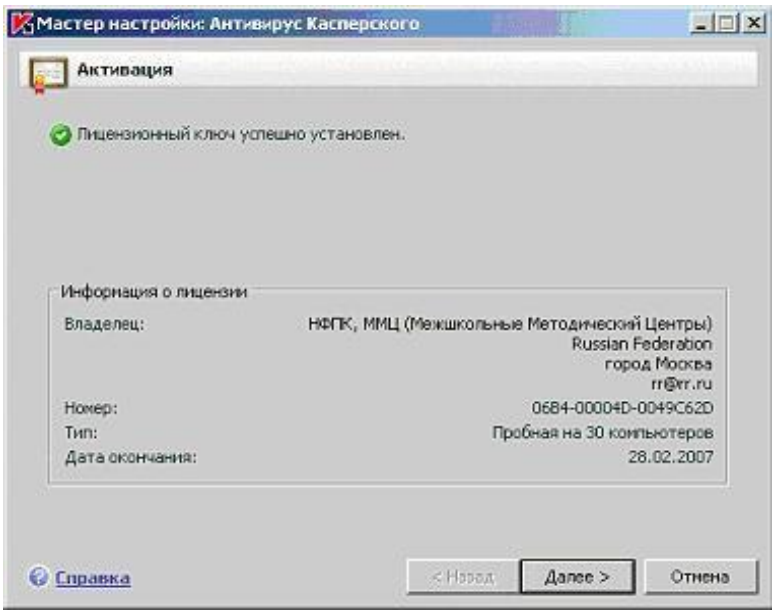
14. Перейдите к указанной преподавателем папке с ключевым файлом, выделите его и нажмите Открыть



15. После открытия выбранного файла, в окне Мастера появится информация о нем. Ознакомьтесь с ней и нажмите Далее

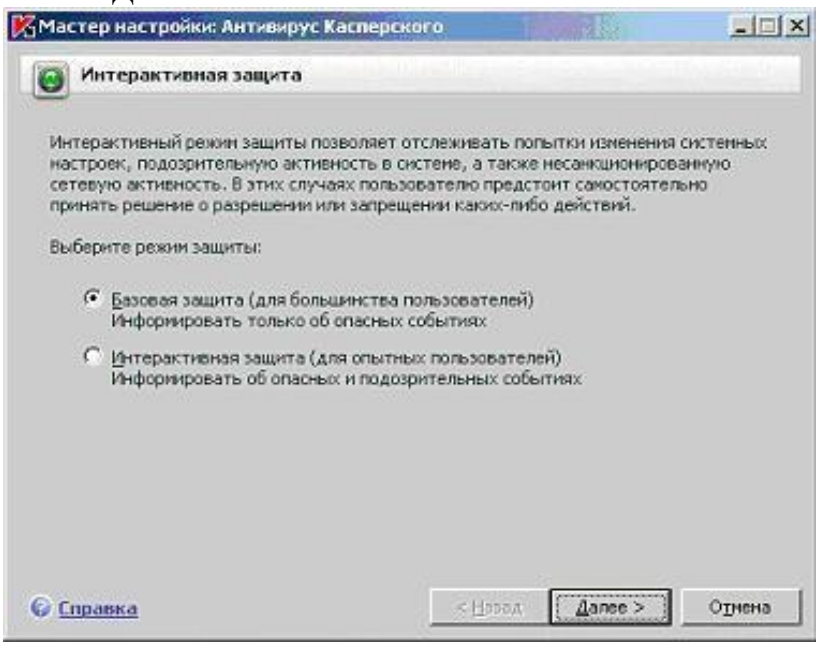


16. На этапе перехода к следующему окну проводится проверка открытого лицензионного ключа. Если он действителен, то происходит его активация. Для продолжения настройки нажмите Далее

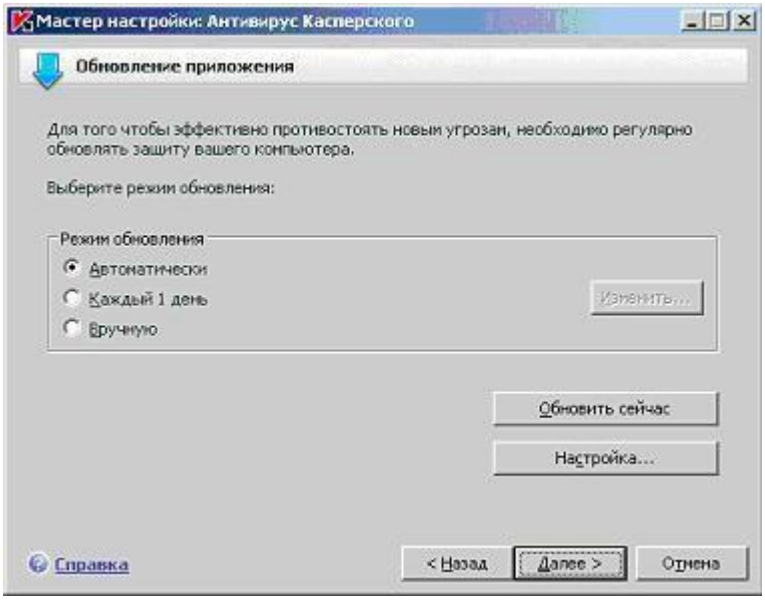


17. После активации начинается этап первоначальной настройки антивируса. Мастер установки предлагает настроить только основные параметры работы приложения и все сделанные в ходе инсталляции настройки впоследствии можно будет легко изменить с помощью графического интерфейса.

Первое окно предлагает выбрать режим интерактивной защиты. Прочитайте описание различий между этими двумя режимами, оставьте выбранную по умолчанию Базовую защиту и нажмите Далее



18. Далее предлагается определить режим обновления, по умолчанию выбран пункт Автоматически. Он подходит для большинства пользователей. Однако нужно знать, что в общем случае настроить и обновить антивирусные баз можно уже прямо в ходе установки (для этого предназначены кнопки Настройка и Обновить сейчас и меню выбора режима обновления)

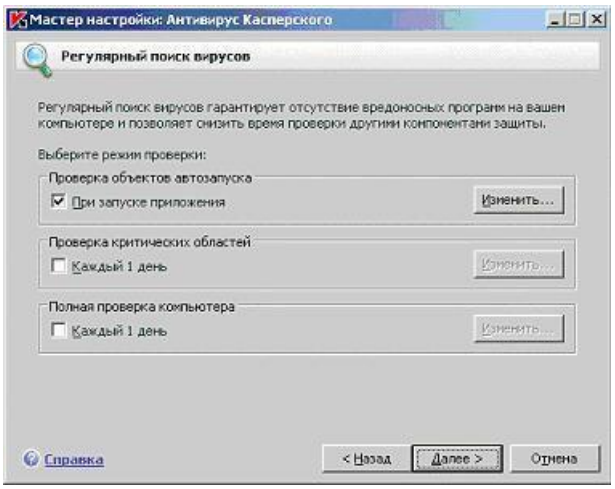


19. В следующем окне можно задать настройки и расписание запуска проверки на наличие вирусов объектов автозапуска, критических областей и полной проверки компьютера.

Для большинства пользователей рекомендуется настроить проверку объектов автозапуска (как наиболее часто поражаемой области компьютера) при каждой перезагрузке Антивируса Касперского. Это обычно соответствует каждой перезагрузке компьютера.

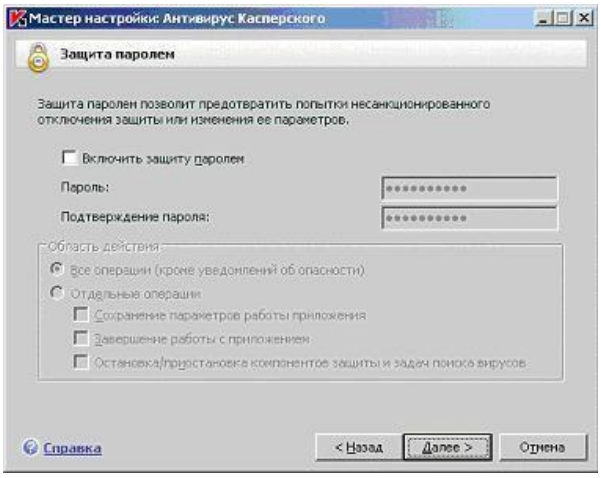
Под проверкой критических областей подразумевается поиск вирусов в важных системных областях. По умолчанию это системная память, объекты автозапуска, загрузочные секторы дисков и папки C:\Windows и C:\Windows\system32.

В этой лабораторной работе оставьте отмеченным только флаг проверки объектов автозапуска и нажмите Далее



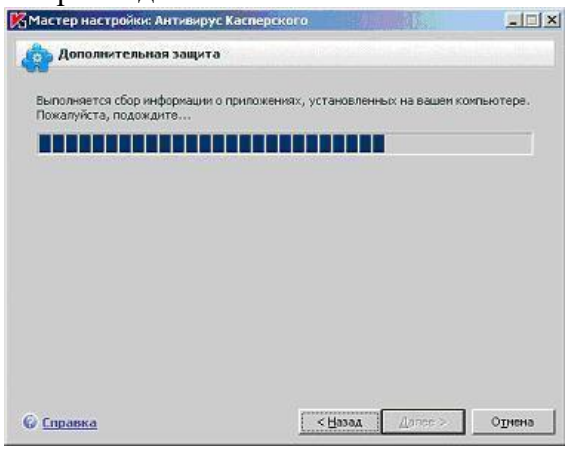
20. Антивирус Касперского позволяет поставить защиту паролем на ряд операций: изменения настроек, выгрузки антивируса или остановки работы компонентов и задач поиска вирусов. Если такая защита установлена, то при попытке совершить защищенную операцию будет предложено ввести пароль. Это может быть полезно, если компьютер используется несколькими пользователями и кому-то из них нельзя доверять.

В этой лабораторной работе устанавливать пароли не нужно, поэтому оставьте флаг Включить защиту паролем пустым и нажмите Далее



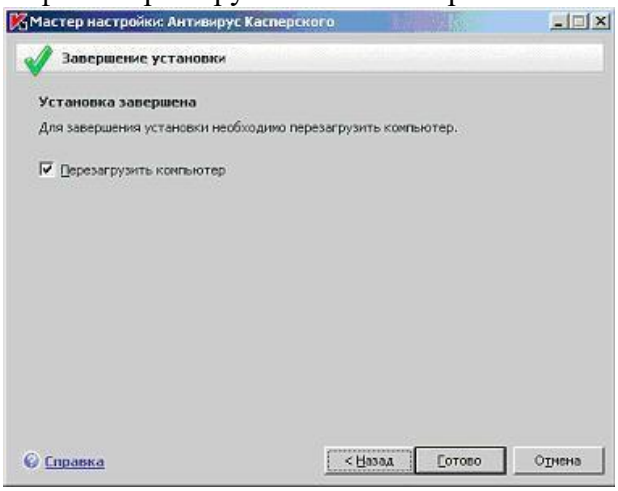
21. На последнем этапе Мастер настройки проводит анализ Вашей системы и собирает данные об установленных программах. В дальнейшем эта информация пригодится для контроля целостности приложений, дополнительного компонента антивирусной защиты.

Дождитесь окончания сбора сведений о системе



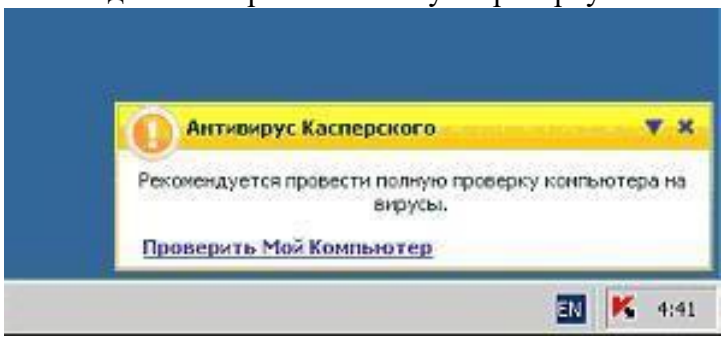
22. Следующее окно информирует, что установка завершена, но требует перезагрузки. Без перезагрузки установка Антивируса Касперского не может считаться завершенной. Поэтому убирать отметку с флага Перезагрузить компьютер можно только в исключительных случаях. В данном случае это не требуется.

Оставьте отмеченным флаг Перезагрузить компьютер и нажмите Готово



23. Дождитесь завершения перезагрузки компьютера и войдите в систему под своей учетной записью

24. Обратите внимание, что после перезагрузки в правом нижнем углу экрана появилось сообщение о необходимости провести полную проверку компьютера на вирусы.



Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, антивирус Касперского.

Указания по технике безопасности: к выполнению практических занятий допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Что такое системные требования для установки программного продукта?
2. На что нужно обратить внимание перед установкой Антивируса Касперского?
3. Что необходимо для успешной установки Антивируса Касперского?
4. Как происходит установка Антивируса Касперского?
5. Как произвести настройку Антивируса Касперского?
6. Как активировать Антивирус Касперского?

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.

2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.

3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.

4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.

5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.

терПресс.-1993.-N8.-С.60-62.

7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.

8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.

9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьютерПресс.-1993.-N7.-С.49-52.

10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер-Пресс.-1991.-N10.-С.19-24.

11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.

12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

Практическое занятие №6

Применение инкрементальных алгоритмов для защиты от вирусов

Цель работы: Эта лабораторная работа посвящена изучению интерфейса Антивируса Касперского, отвечающему за взаимодействие с пользователем.

Теоретическая часть

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 •

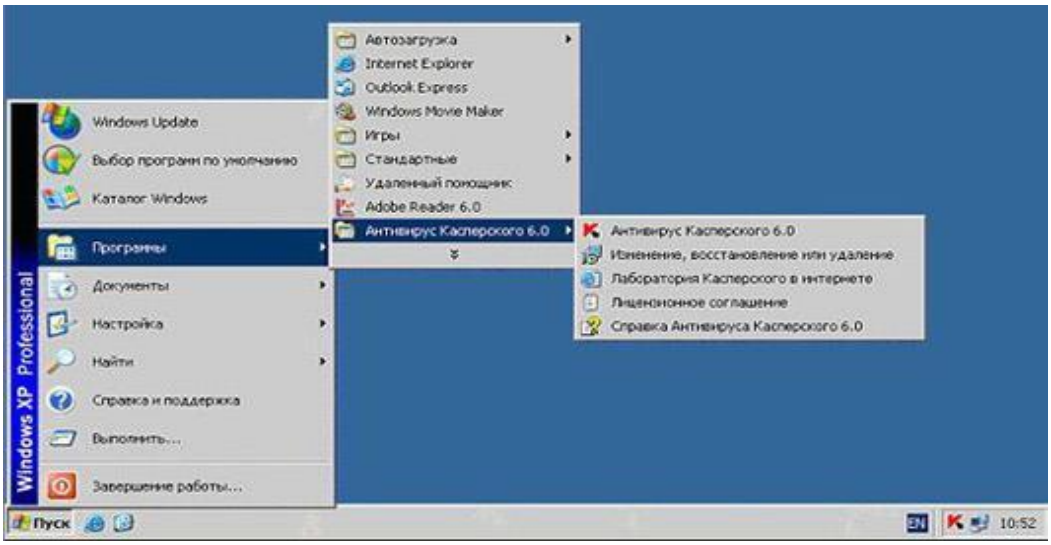
Окна статистики и отчетов, в котором можно получить данные о результатах работы антивируса

- Окна справочной системы

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

1. После успешного завершения процесса установки Антивируса Касперского в системном меню Пуск / Программы появляется новая группа - Антивирус Касперского. В ней содержится пять ярлыков, название каждого отражает смысл, например Антивирус Касперского открывает главное окно интерфейса Антивируса Касперского.

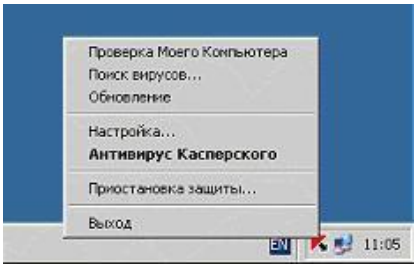
Откройте меню Пуск / Программы / Антивирус Касперского и ознакомьтесь с его содержимым



2. 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

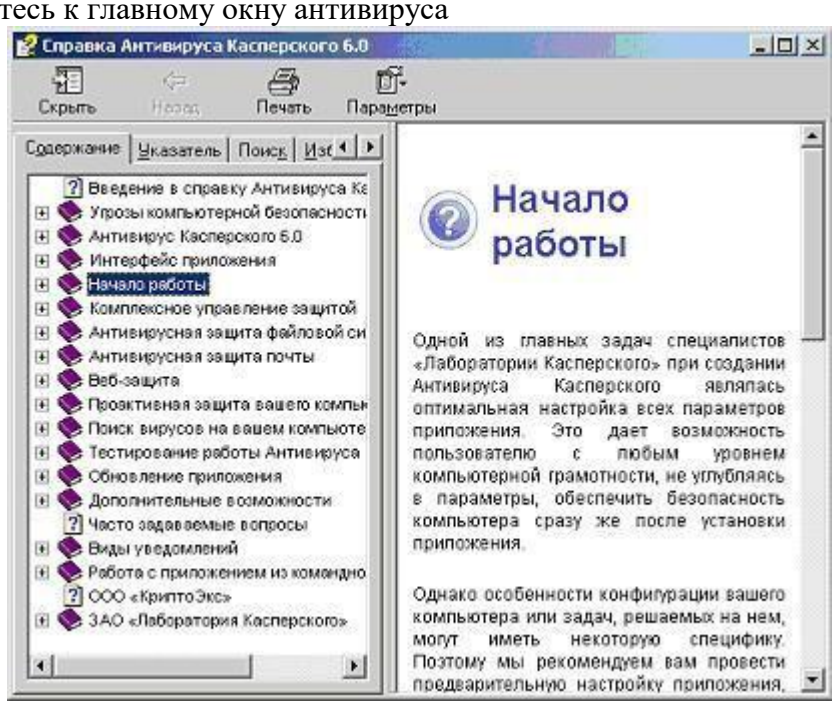


3. С помощью двойного щелчка на иконке откройте главное окно интерфейса Антивируса Касперского

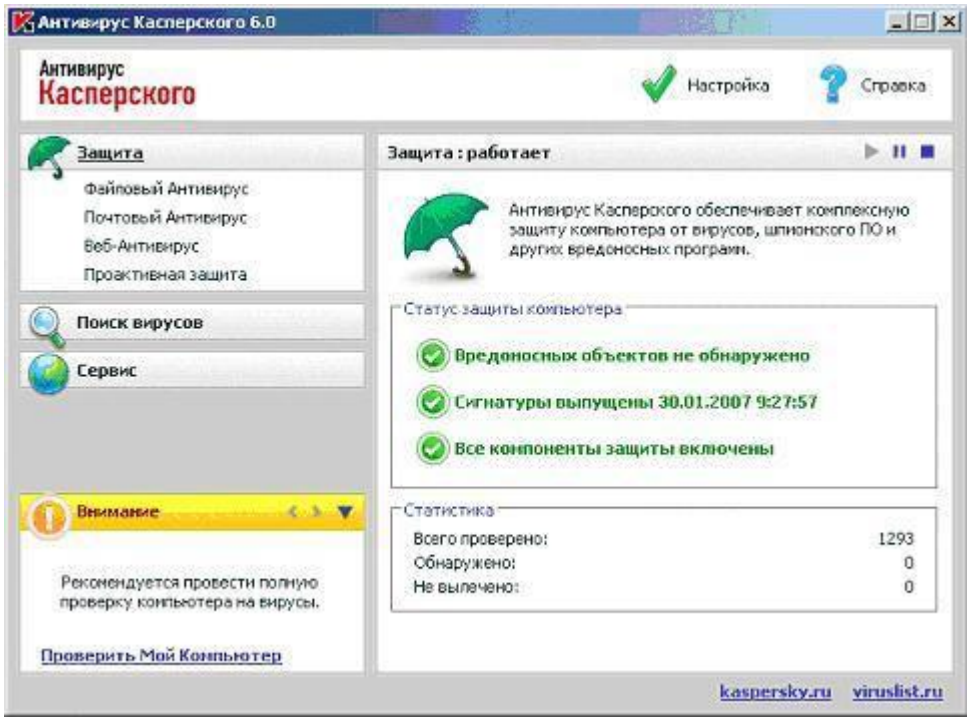
4. В верхней правой части окна размещено две ссылки: Настройка и Справка. Первая используется для настройки антивируса, вторая - для вывода справочной системы.

Нажмите ссылку Справка

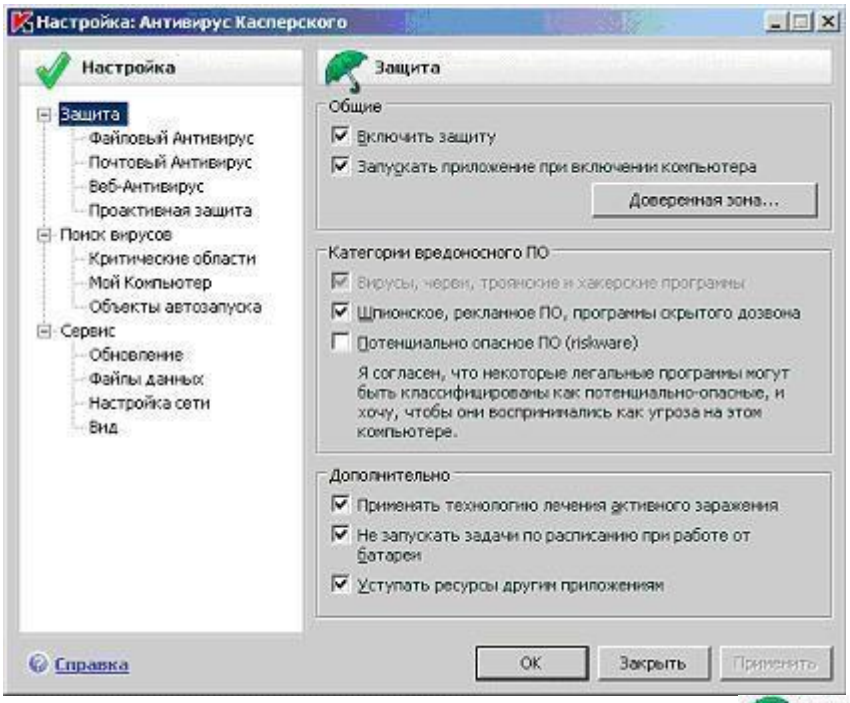
5. Открывшееся окно содержит руководство пользователя Антивирусом Касперского. При возникновении каких-либо проблем, в первую очередь всегда нужно обращаться к нему. Ознакомьтесь с содержанием справочной системы в левой панели окна и закрыв его вернитесь к главному окну антивируса



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

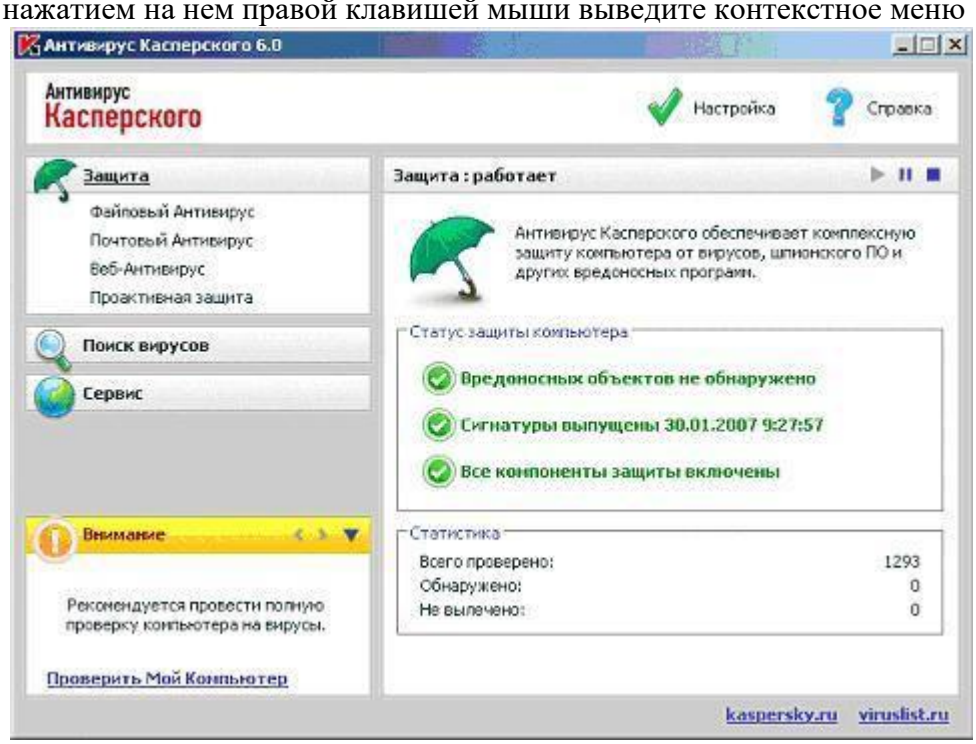


7. Открывшееся окно Настройка предназначено для настройки параметров работы антивируса. Изучите окно Настройка, пройдя по всем вкладкам. Нажмите Закрыть и вернитесь к главному окну интерфейса



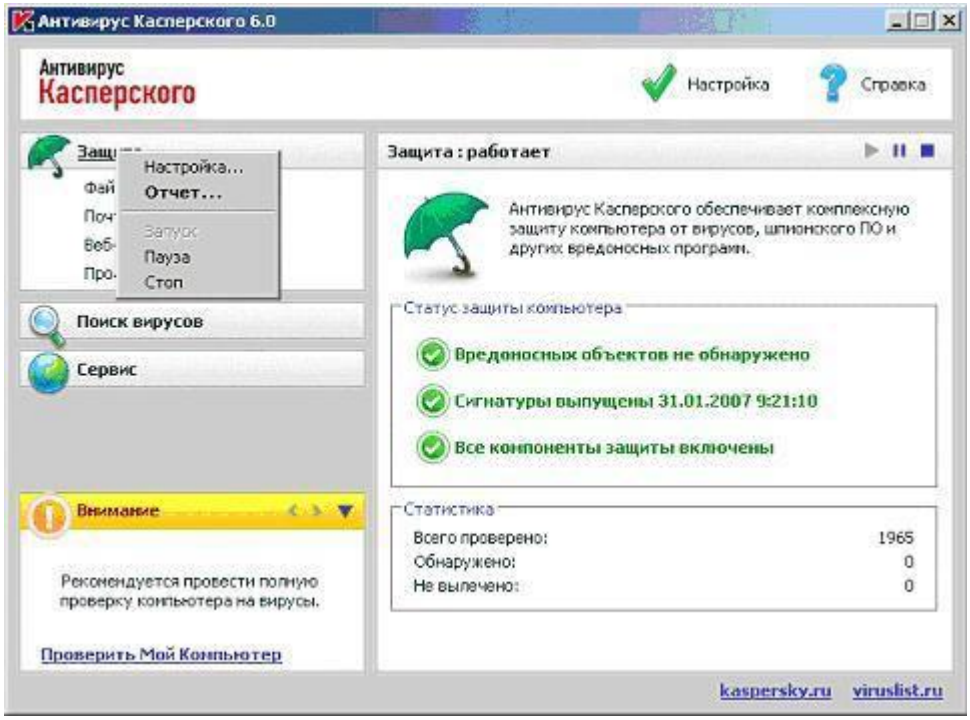
8. Найдите элемент Защита, выделенный подчеркиванием (

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

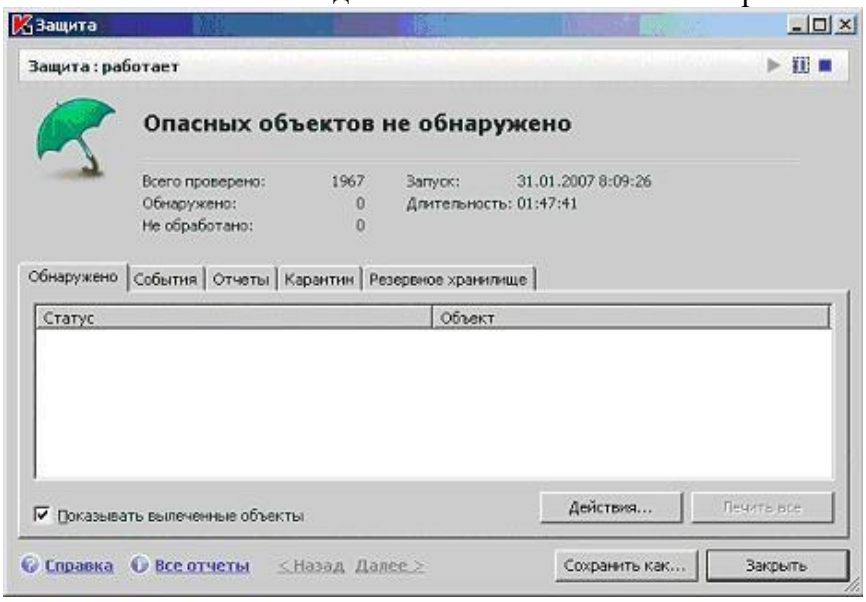


9. Контекстное меню разделено на две зоны: верхняя содержит ссылки Настройка (открывает рассмотренное выше окно Настройка) и Отчет. Нижняя - кнопки управления работой защиты.

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

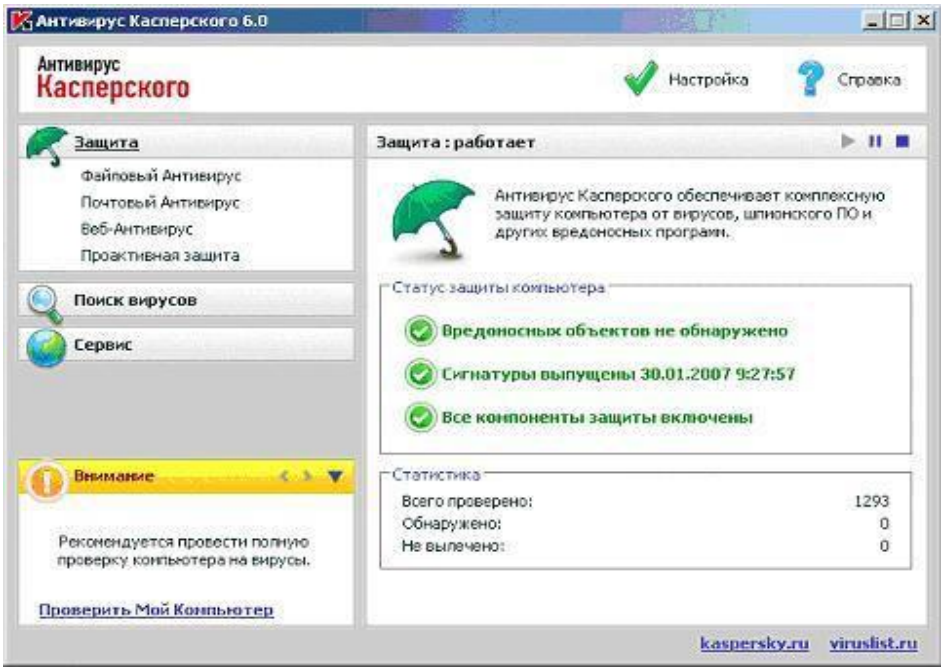


10. Ознакомьтесь с внешним видом этого окна и нажмите Закрыть

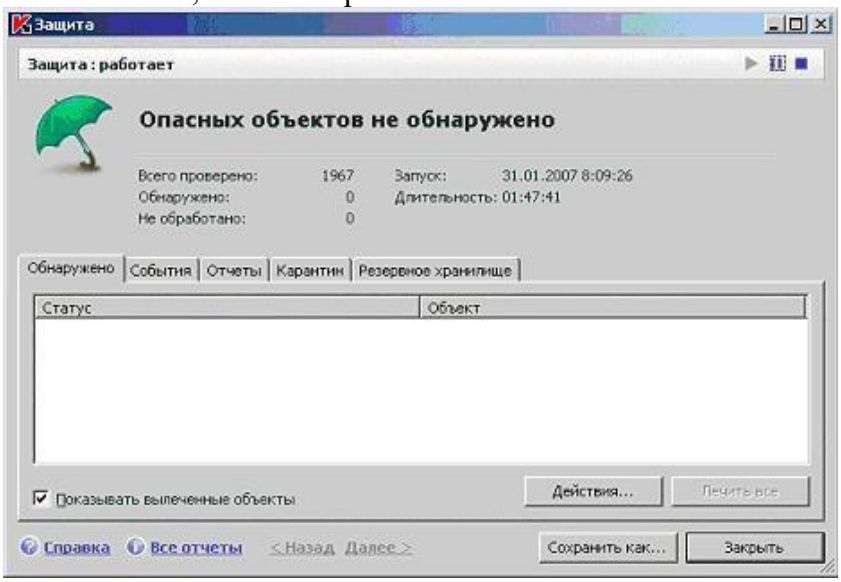


11. В главном окне интерфейса обратите внимание, что весь текст в информационной части окна, разбитый серыми рамками на группы, содержит ссылки. Таким образом, в главном окне представлен только небольшой отчет о неком компоненте антивируса, а по нажатию на него выводится окно с подробной информацией.

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



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



13. Вернитесь к главному окну интерфейса антивируса и закройте его

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".

Оборудование и материалы: для выполнения данного практического занятия

необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, антивирус Касперского.

Указания по технике безопасности: к выполнению практических занятий

допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Из каких четырёх окон состоит интерфейс Антивируса Касперского?
2. Как понять, что антивирус работает?
3. Что обеспечивает Антивирус Касперского?
4. Как приостановить работу Антивируса Касперского? **Список литературы, рекомендуемый к использованию по данной теме:**

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.

2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.

3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.

4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.

5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.

6. Групер Ш. Электронные ключи с энергонезависимой памятью // КомпьютерПресс.-1993.-N8.-С.60-62.

7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.

8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.

9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьютерПресс.-1993.-N7.-С.49-52.

10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер-Пресс.-1991.-N10.-С.19-24.

11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.

12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ.

Практическое занятие №7

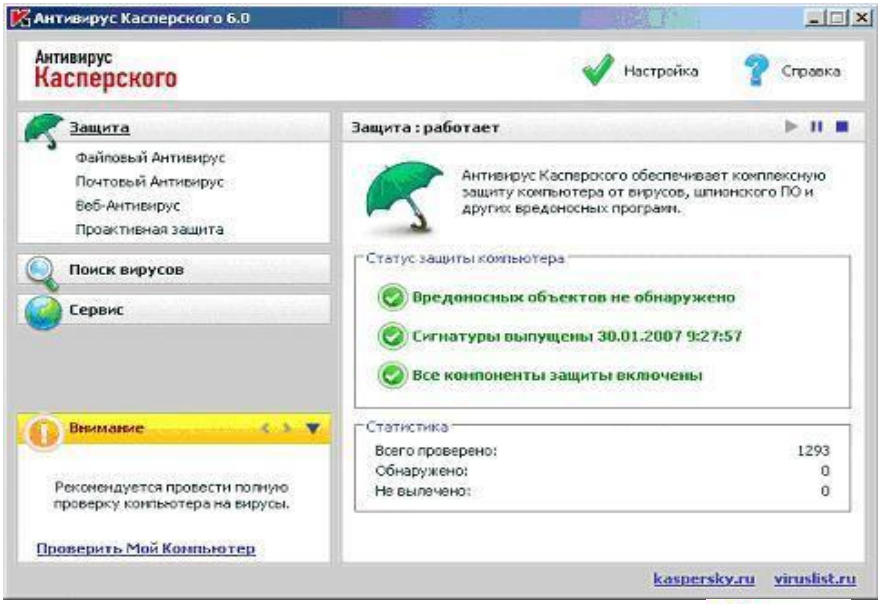
Метод расчета вероятности наличия РПС на этапе испытаний ПО

Цель работы: Эта лабораторная работа посвящена изучению интерфейса Антивируса Касперского, отвечающему за взаимодействие с пользователем.

Теоретическая часть

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

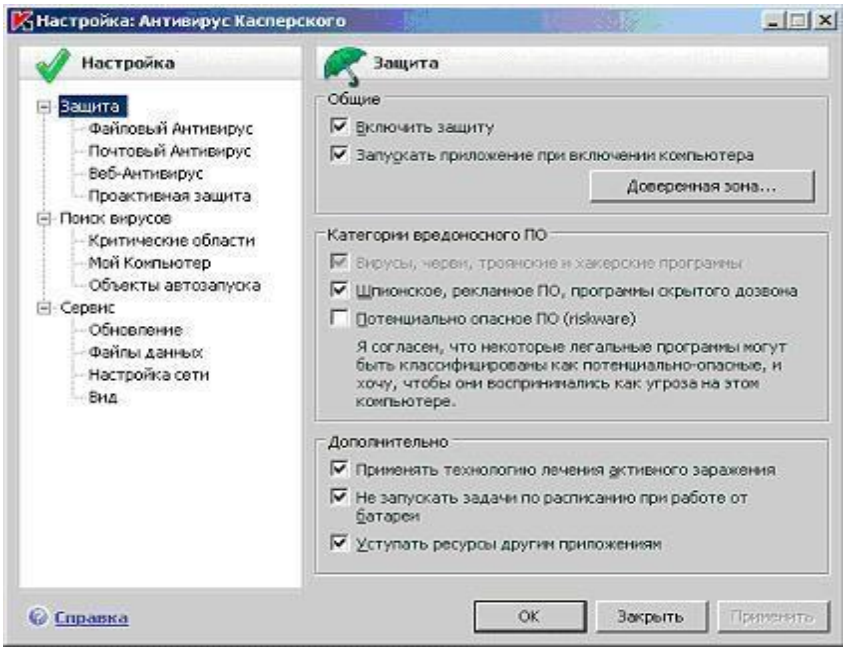


2. Перейдите к окну настроек, нажав ссылку Настройка ()

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.

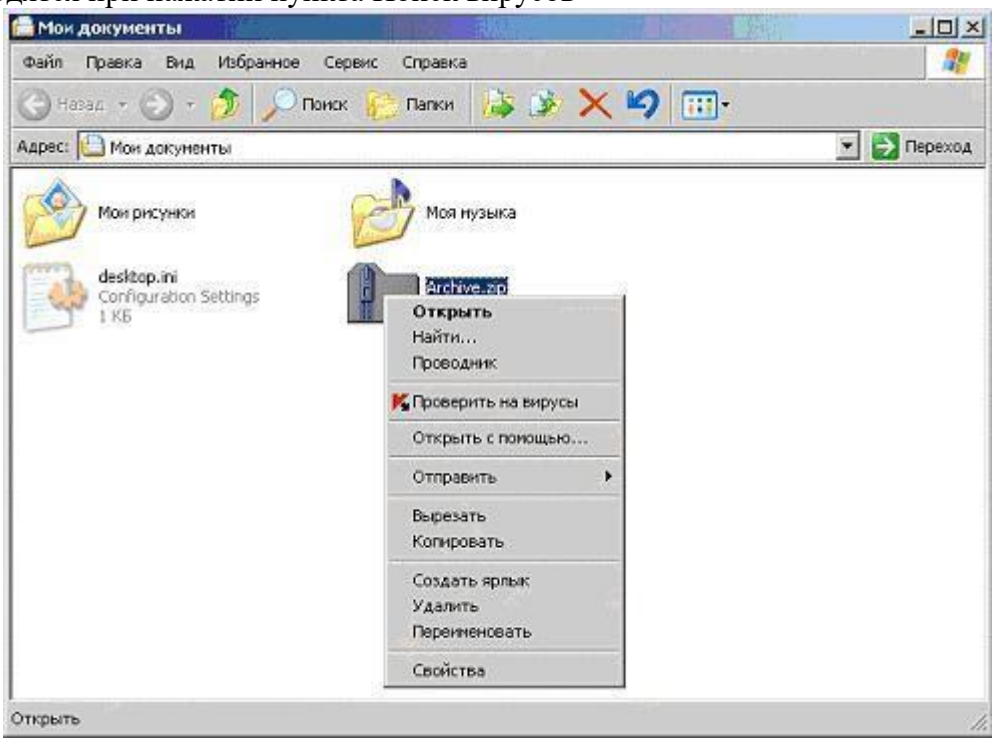


4. Перейдите к группе Поиск вирусов. Это - настройки проверки по требованию, то есть по требованию пользователя. Она используется в случае, если необходимо проверить некий объект или группу объектов.

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



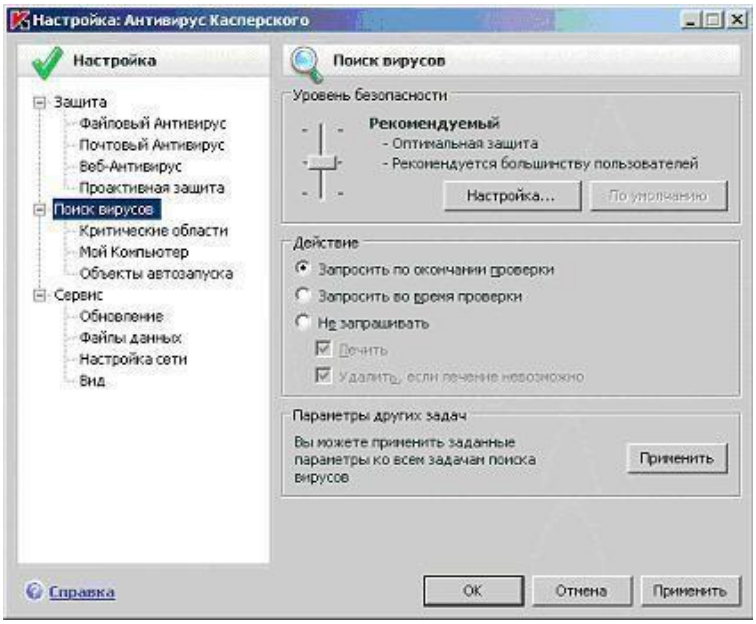
Можно заранее определить папку или группу папок или объектов и сформировать отдельную задачу. Тогда для нее можно задать свои собственные настройки и в дальнейшем запускать эту задачу одним нажатием кнопки. По умолчанию Антивирус

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 окончаниилицензии, 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:

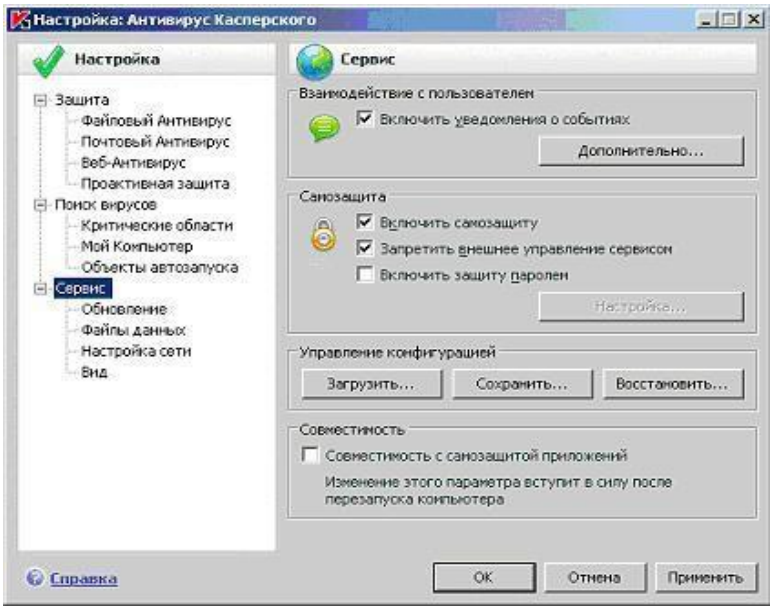
Обновление - это непосредственно настройки обновления антивирусных баз: расписание обновления, какие базы загружать

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

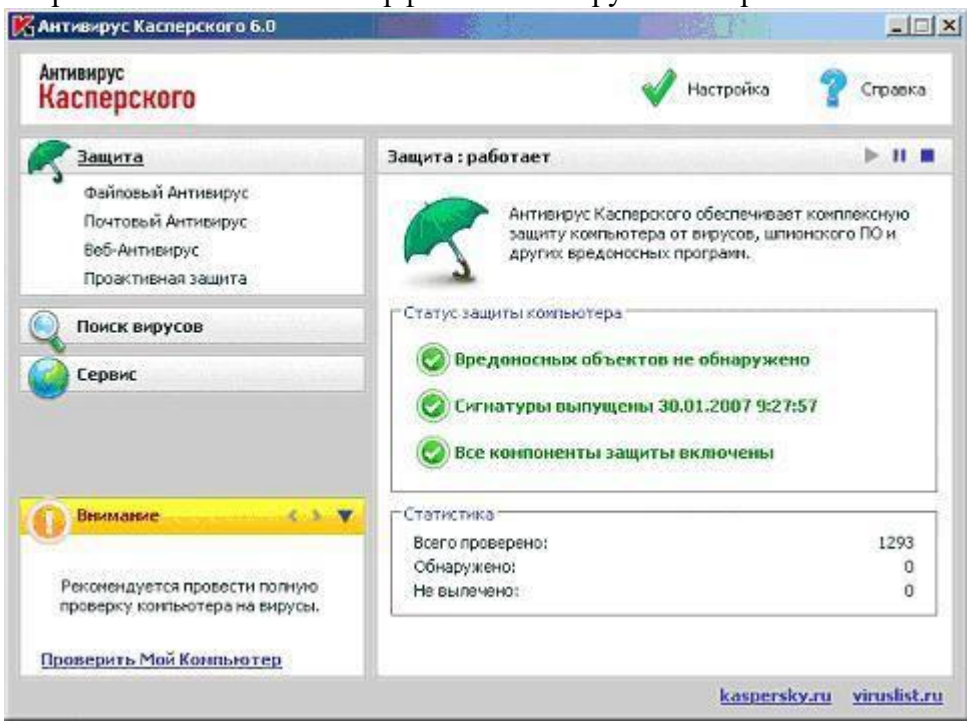
Постоянная защита

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

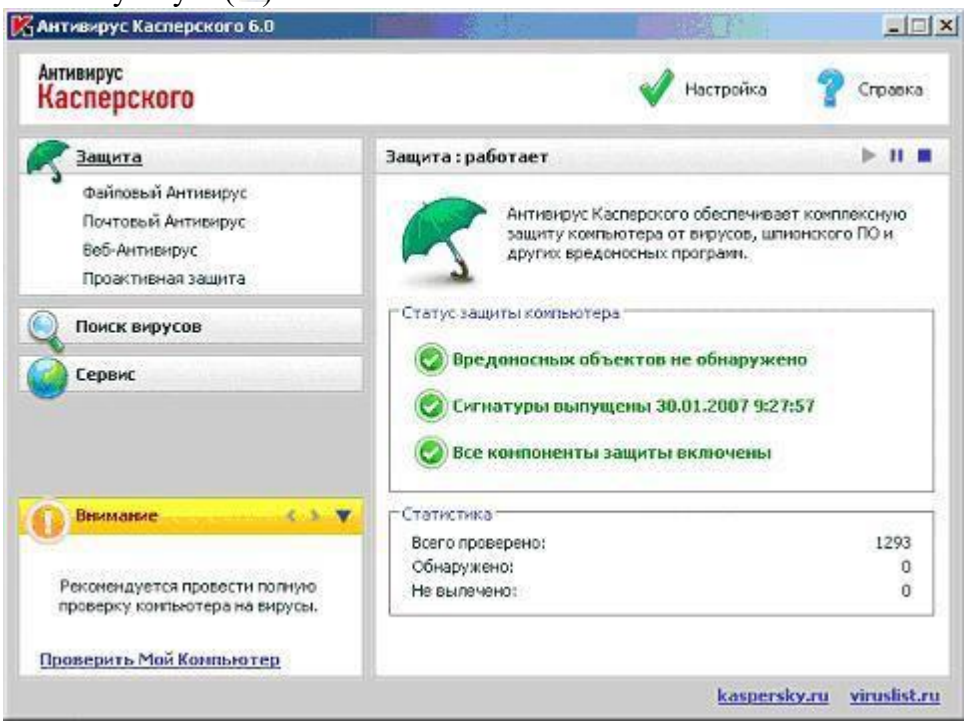


2. Перейдите к разделу Защита, выделив одноименный пункт

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

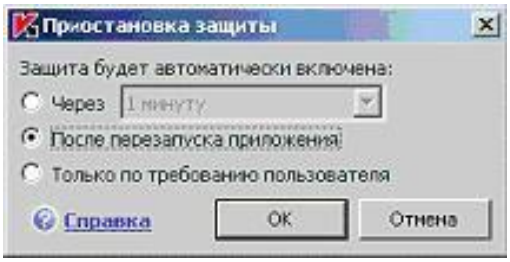
В заголовке этой части видна надпись Защита : работает . Это означает, что защита включена и работает. Соответственно, в расположенной справа от нее группе управляющих кнопок (▶ ⏸ ■) элемент Пуск (▶) не активен. Остальные два элемента соответствуют паузе (⏸) и остановке[1] (■) проверки в режиме реального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

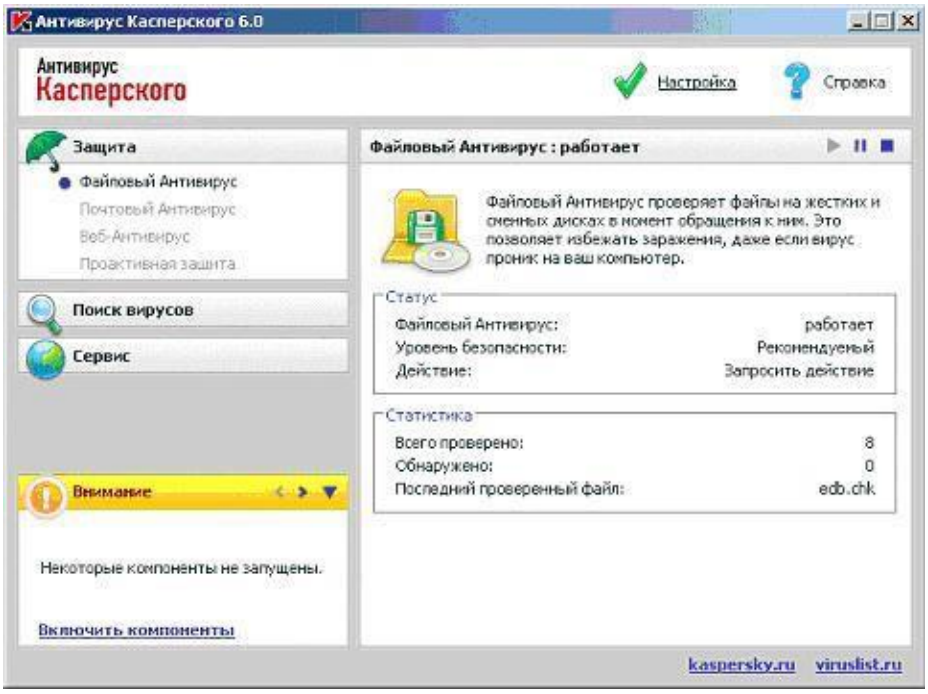
Обратите внимание, что строка со статусом защиты теперь выглядит затемненной, а ее текст гласит, что защита приостановлена (Защита : пауза). При этом также затенена кнопка Пауза, а вот Пуск стал активным (▶ ⏸ ■).

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:

8. Запустите Файловый Антивирус, нажав кнопку Пуск ( )

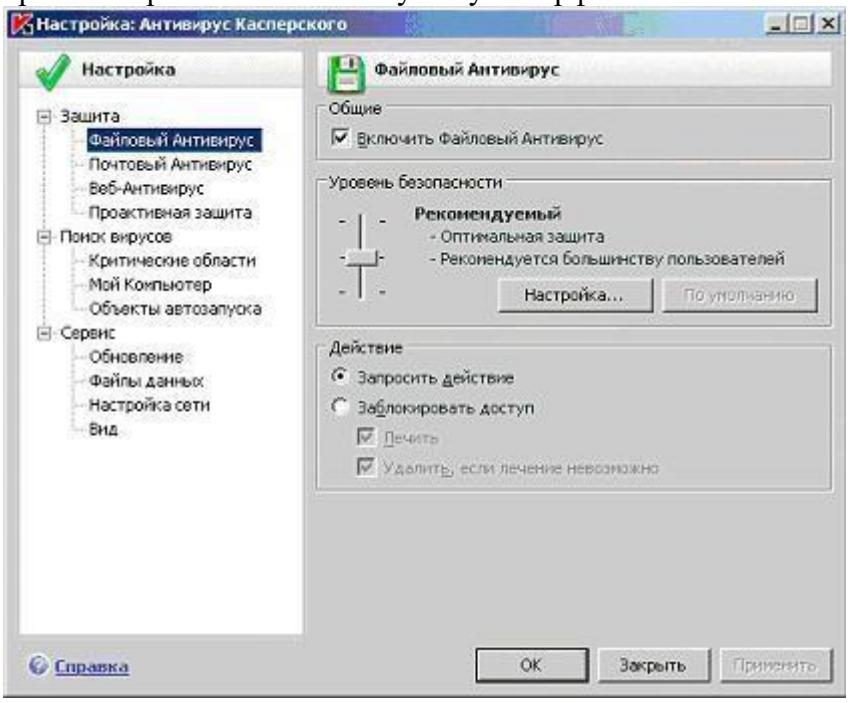
9. Проследите за изменениями в интерфейсе окна. Обратите внимание, что произошел запуск только файлового антивируса, все остальные компоненты остались выключенными. Об этом свидетельствует затененность названий подразделов раздела Защита в меню левой части окна. При этом общее название Защита опять стало черным



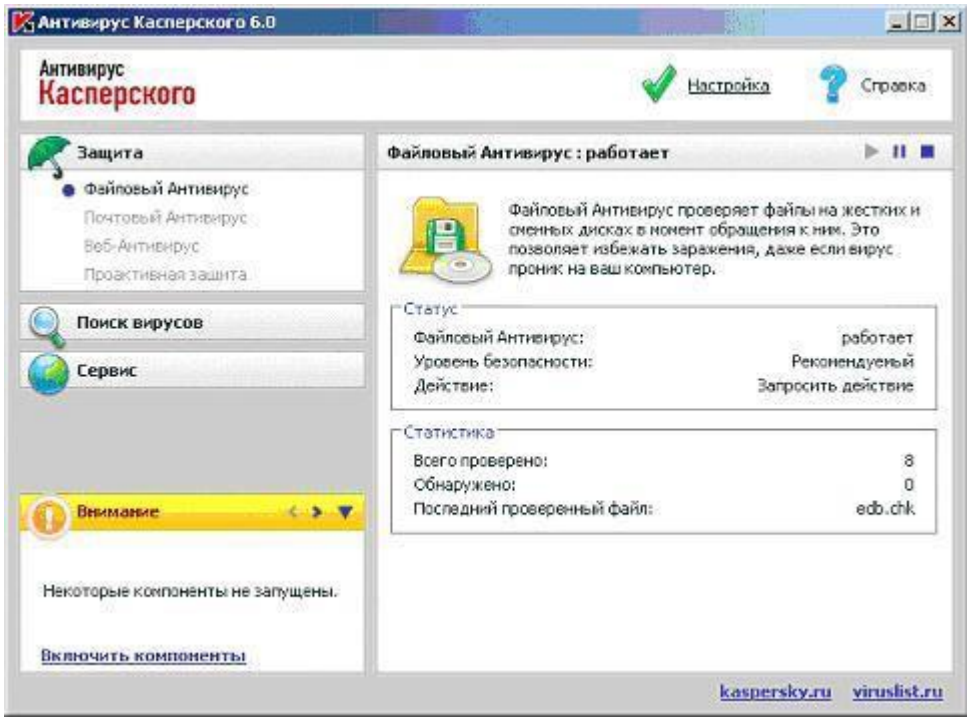
10. Наведите курсор на поле группы настроек " Статус" и нажмите левую клавишу мыши

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

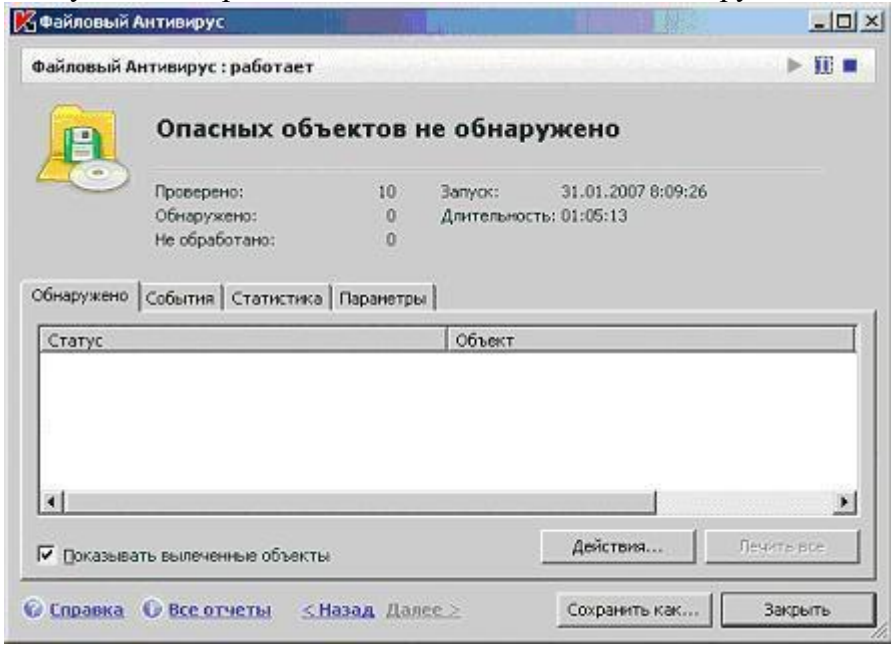
Нажмите Закрыть и вернитесь к главному окну интерфейса



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

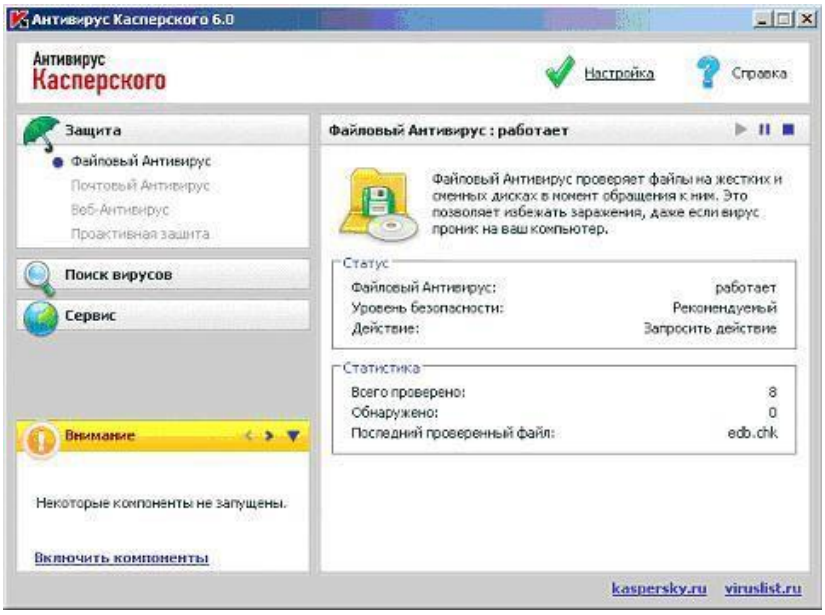


13. Для получения подробного отчета, щелкните по полю группы "Статистика"



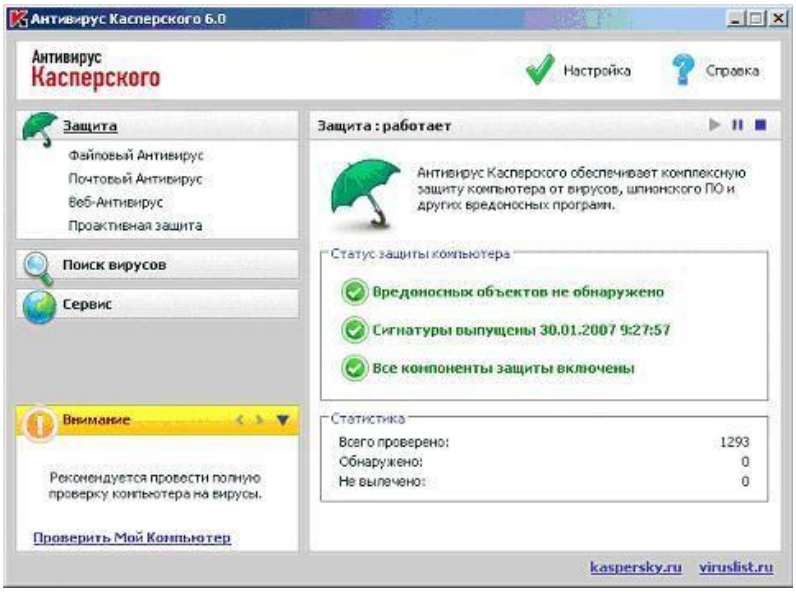
14. Открывшееся окно содержит подробную статистику работы компонента. Просмотрите содержание всех четырех закладок: Обнаружено, События, Статистика и Параметры

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.

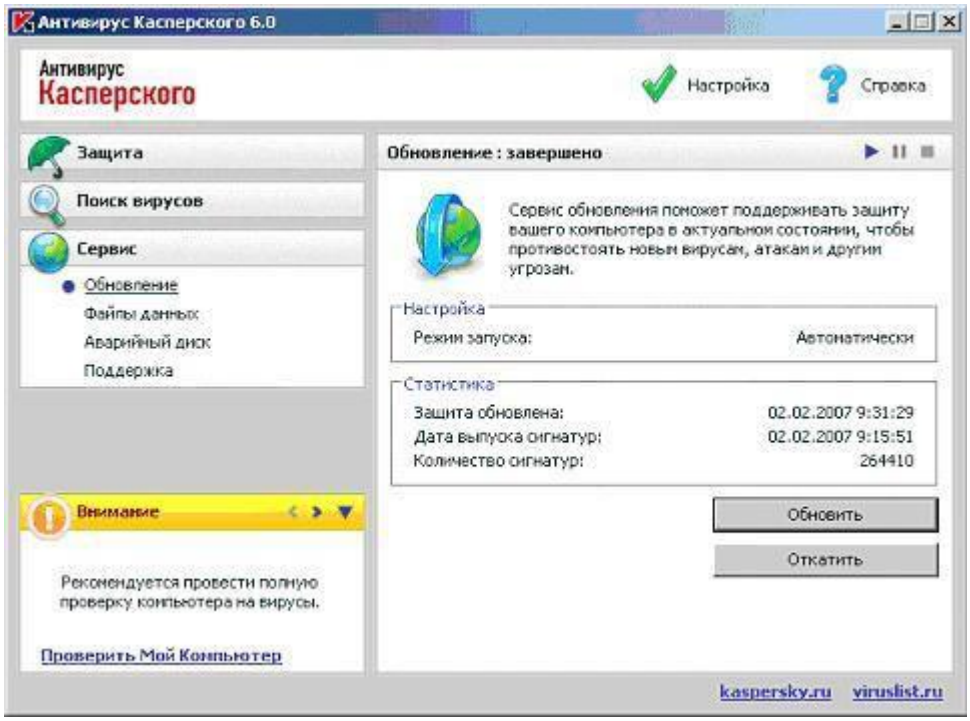
В результате выполнения этого задания все компоненты постоянной защиты должны быть включены



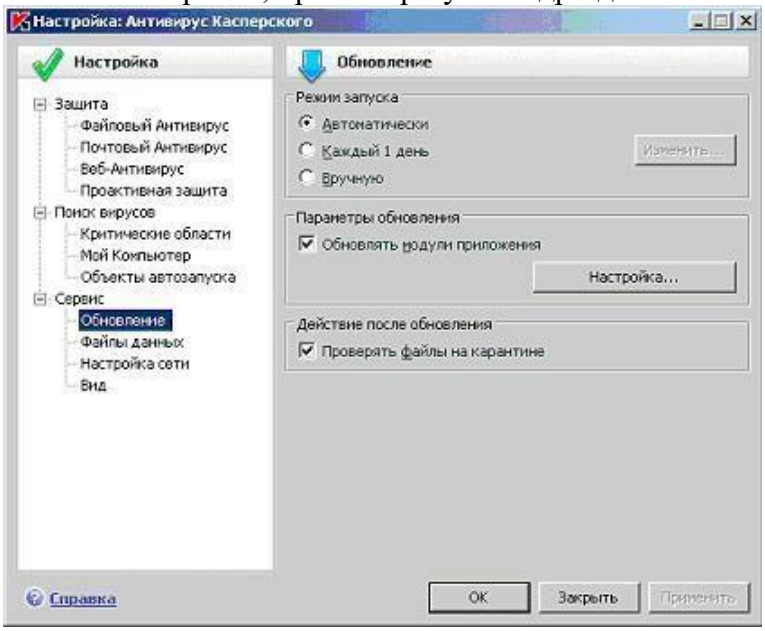
Настройка обновления

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



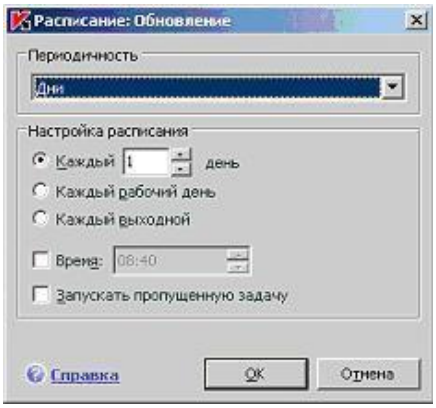
2. Откройте окно настройки, нажав на группу "Настройка"
3. Откроется окно Настройка, причем сразу на подразделе Обновление



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 ЛабораторииКасперского. 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,

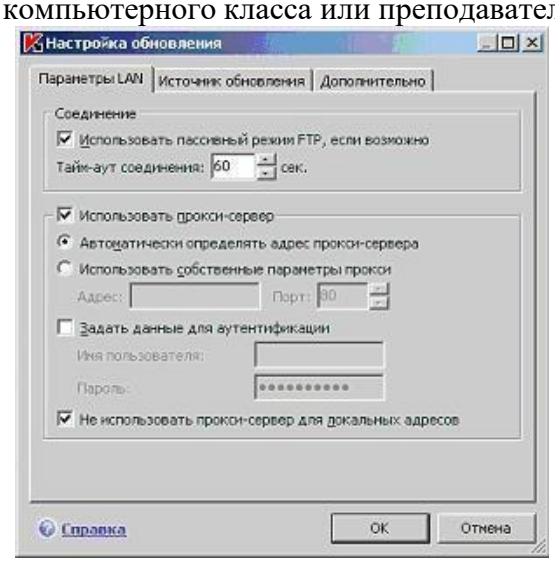
и каждый определенный день недели), когда должна запускаться процедура обновления. Этот способ рекомендуется использовать если доступ к сети Интернет ограничен и пользователь заранее знает, когда он может выделить несколько минут на загрузку новых баз



- 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.

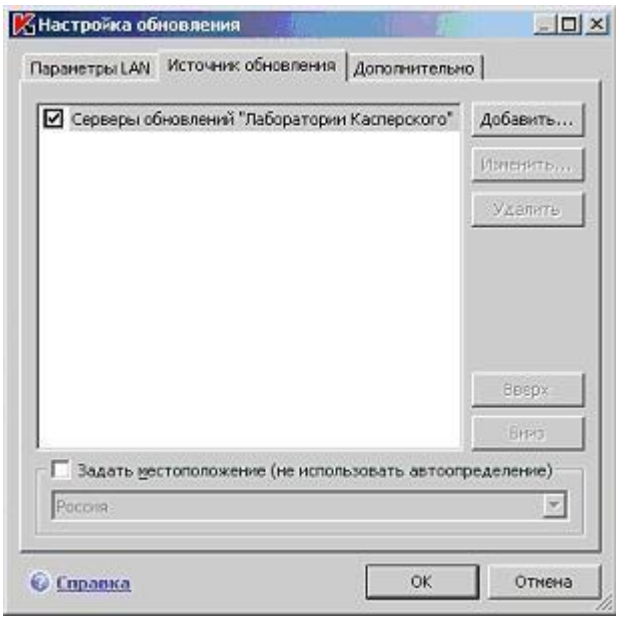
5. Перейдите к окну настройки сетевых параметров, нажав кнопку Настройка

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.

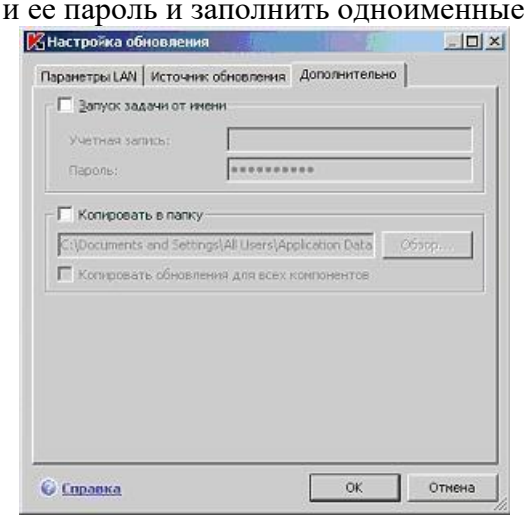


7. Перейдите к закладке Дополнительно

8. Ознакомьтесь с представленными на ней полями, обратив внимание на группу Копировать в папку.

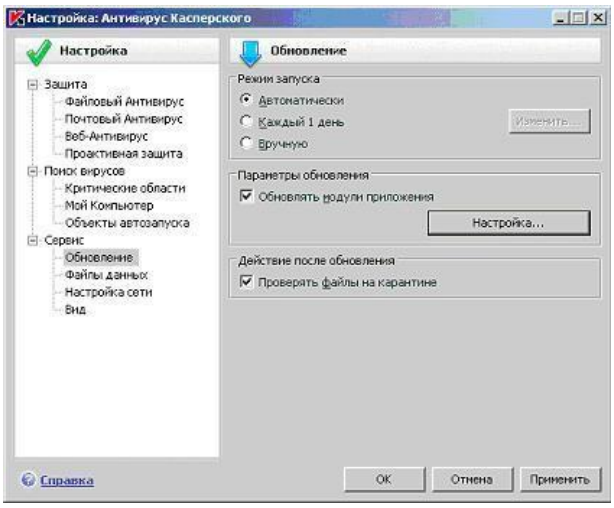
Эта настройка может быть полезна в случае, когда только Ваш компьютер имеет доступ в Интернет, а другие компьютеры сети - нет. В этом случае можно настроить автоматическое копирование файлов обновлений, полученных Вашим антивирусом, в определенный каталог. Тогда эту папку можно будет указать в качестве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



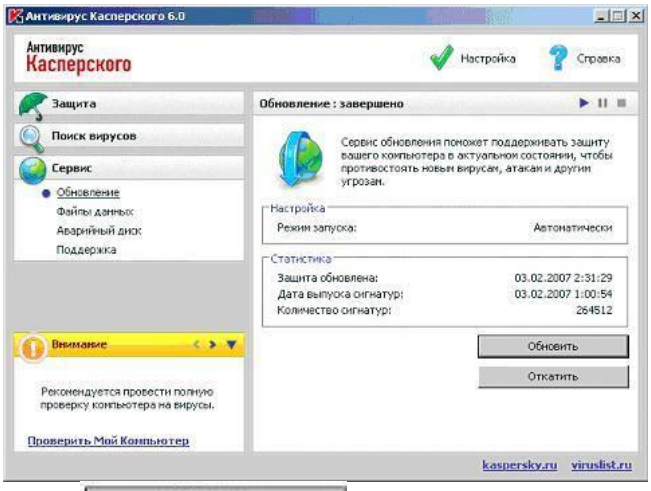
9. Закройте окно настройки обновлений, нажав ОК

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



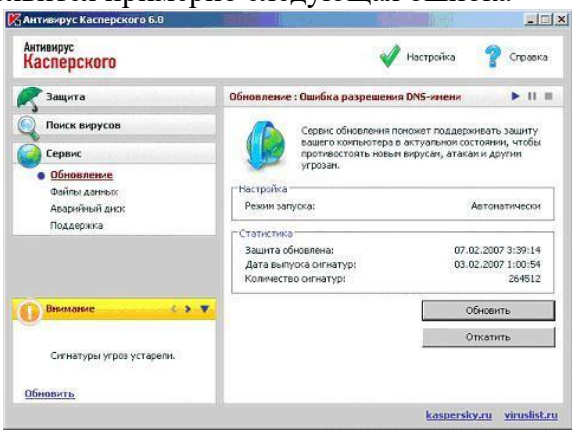
11. Выберите Режим запуска Автоматически, нажмите кнопку Применить и Ок.

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

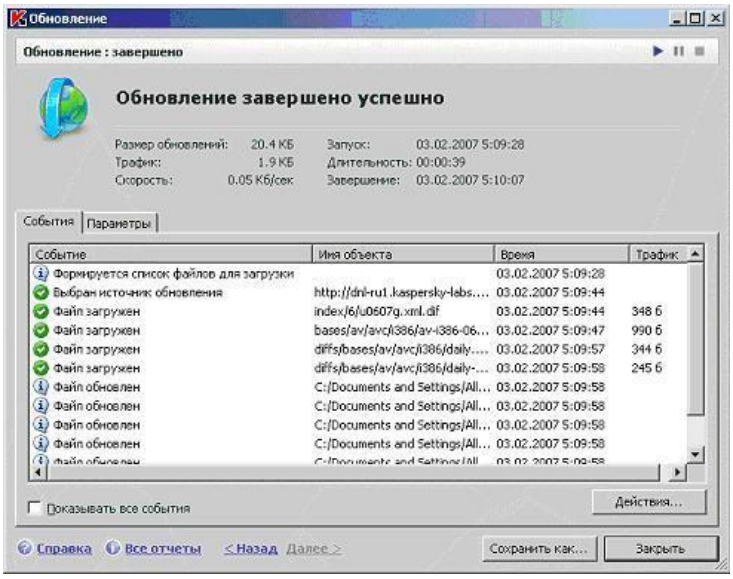


13. Нажмите кнопку  для запуска процедуры Обновления.

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»



Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader, антивирус Касперского.

Указания по технике безопасности: к выполнению практических занятий
допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Как можно просмотреть статистику антивируса?
2. Как произвести настройку обновления?
3. Какие три режима обновления существуют в Антивирусе Касперского?
4. В каких случаях необходимо приостановить работу антивируса?
5. На какие три части можно разделить работу с постоянной защитой?

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.

2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.

3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.

OILCO, 1992.

5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.

6. Групер Ш. Электронные ключи с энергонезависимой памятью //КомпьютерПресс.-1993.-N8.-С.60-62.

7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.

8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.

9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьтерПресс.-1993.-N7.-С.49-52.

10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер-Пресс.-1991.-N10.-С.19-24.

11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.

12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

Практическое занятие №8

Оценка технологической безопасности программ на базе модели Нельсона

Цель работы: Познакомиться с встроенными компонентами защиты операционной системы Microsoft Windows и настроить их.

Теоретическая часть

Брандмауэр Windows

Задачу защиты от несанкционированного доступа и сетевых атак домашнего компьютера успешно решает персональная программа-брандмауэр. Она может быть как встроенной в операционную систему (например, брандмауэр Windows), так и устанавливаемой отдельно (например Outpost FireWall).

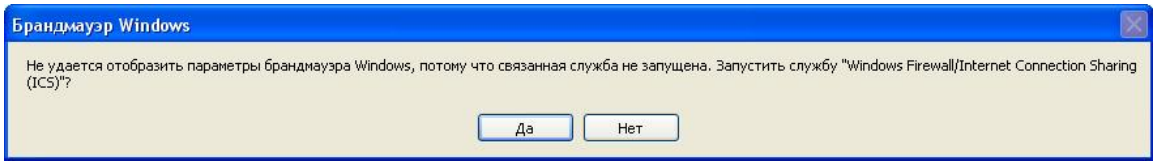
Самая, пожалуй, популярная на сегодняшний день операционная система домашнего компьютера - Microsoft Windows XP содержит встроенный Брандмауэр Windows. Более поздние версии Microsoft Windows, Vista и Seven (находится в стадии разработки, в начале 2009 года будет представлена beta-версия) содержат в себе дополнительные компоненты защиты от несанкционированного доступа и шпионских программ, например Windows Defender.

Встроенные брандмауэры отличаются весьма ограниченной функциональностью, что с другой стороны компенсируется отсутствием конфликтов с операционной системой и бесплатностью. Брандмауэры же третьих производителей, устанавливаемые отдельно, обеспечивают обычно более удобную и приятную работу с возможностью более точной настройки различных параметров.

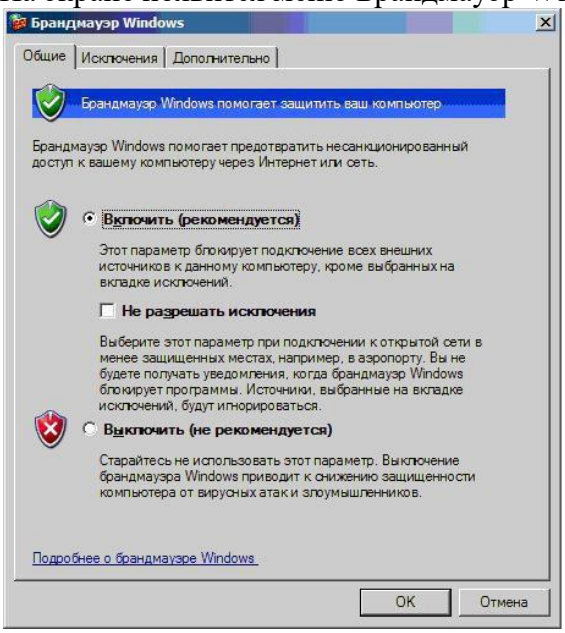
1. После загрузки операционной системы Microsoft Windows XP (в Microsoft Virtual PC), Брандмауэр Windows будет отключен. Для его включения выполните следующие действия:

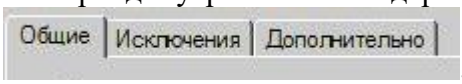
Нажмите Меню Пуск – Панель управления – Брандмауэр Windows

2. Появится сообщение операционной системы, информирующее вас о выключенной службе Брандмауэра Windows. Включите службу, нажав кнопку Да.



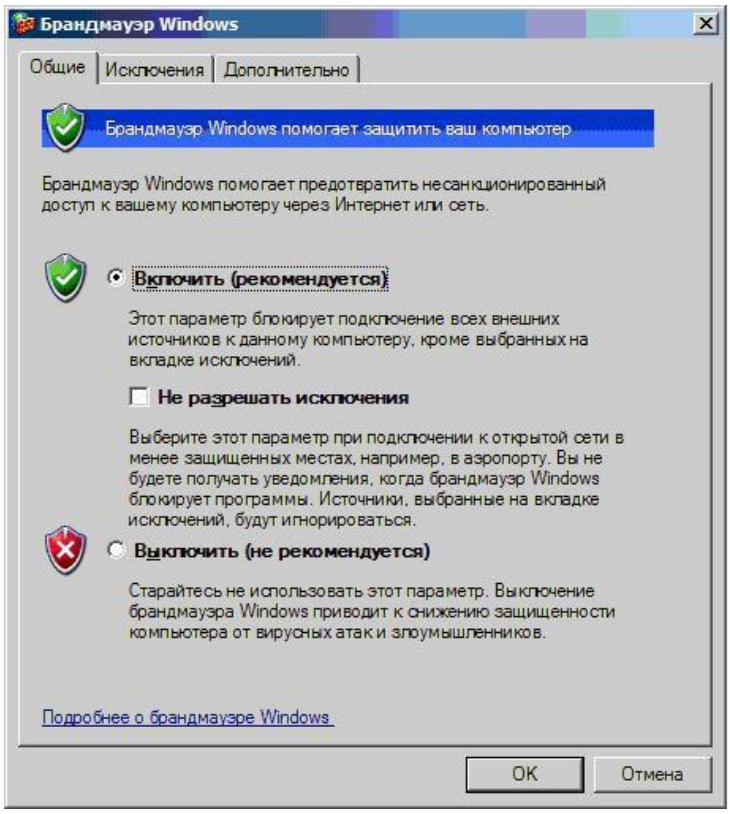
На экране появится меню Брандмауэр Windows



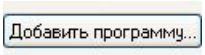
3. Меню Брандмауэр Windows содержит 3 вкладки – Общие, Исключения, Дополнительно 

. Выберите каждую вкладку и просмотрите ее содержимое.

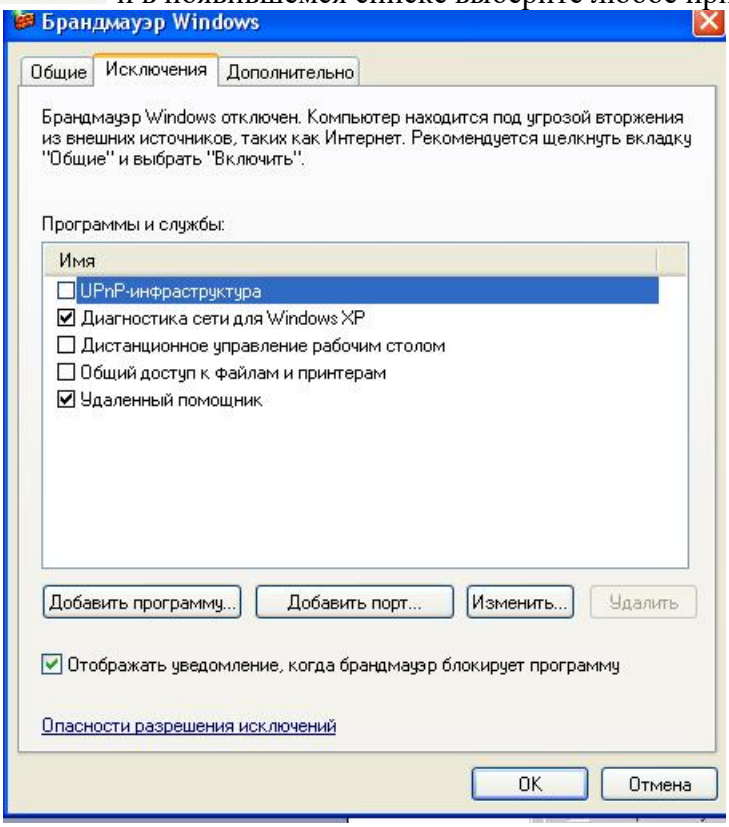
4. Вкладка Общие позволяет менять режим работы Брандмауэра Windows. Можно Включить брандмауэр (после установки Операционной системы Microsoft Windows XP, система автоматически включает Брандмауэр Windows) или Выключить его (при установке другого Брандмауэра на ваш компьютер, Брандмауэр Windows будет выключен автоматически). Отключите Брандмауэр Windows, а затем вновь включите его.



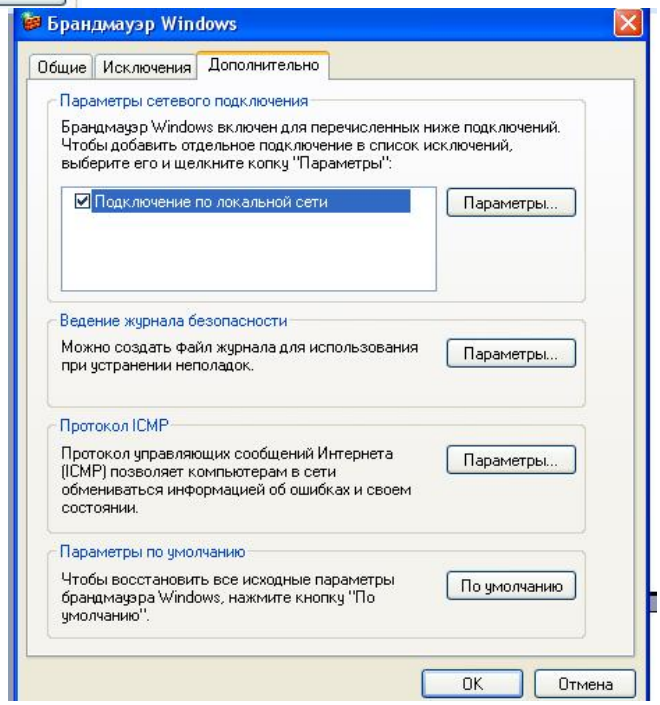
5. Вкладка Исключения позволяет создавать исключения для нужных служб и приложений. Например, если вы точно уверены, что конкретное приложение не будет выполнять несанкционированных удаленных соединений или Брандмауэр Windows заблокировал сетевой доступ приложения, можно создать Исключение и блокировка будет снята. Добавьте исключение для программы, нажав кнопку Добавить программу

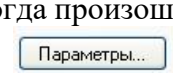


и в появившемся списке выберите любое приложение.

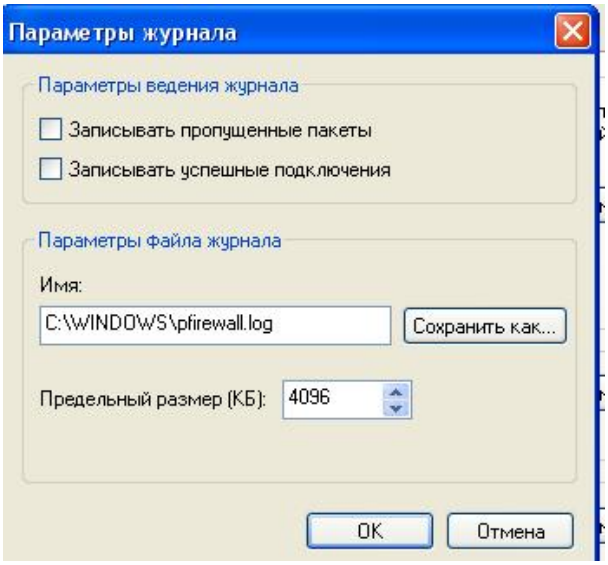


6. Вкладка Дополнительно позволяет включить или отключить Брандмауэр Windows для конкретных сетевых подключений, заблокировать или разблокировать сетевые службы. Выберите нужно сетевое Подключение и нажмите кнопку Параметры

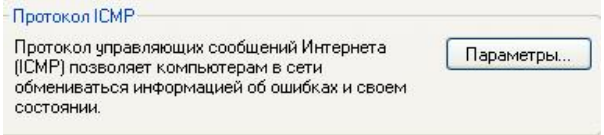


7. При устранении неполадок, можно воспользоваться Журналом Безопасности, для того, чтобы выяснить, когда произошла неполадка и при каких обстоятельствах. Нажмите кнопку Параметры 

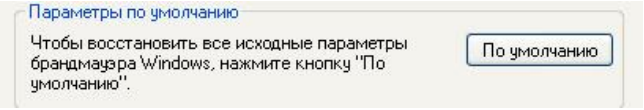
в блоке Ведение журнала безопасности. В появившемся окне произведите настройки, согласно предложенному рисунку и нажмите Ок.



8. Блок Протокол ICMP служит для приема и отправки сообщений об ошибках и состоянии компьютеров в сети. Так же этот протокол используют некоторые вредоносные программы, с периодичностью показывая различные сообщения о якобы произошедших ошибках в операционной системе.



9. Блок Параметры по умолчанию служит для восстановления исходных настроек Брандмауэра Windows.

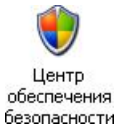


Центр Обеспечения безопасности Windows

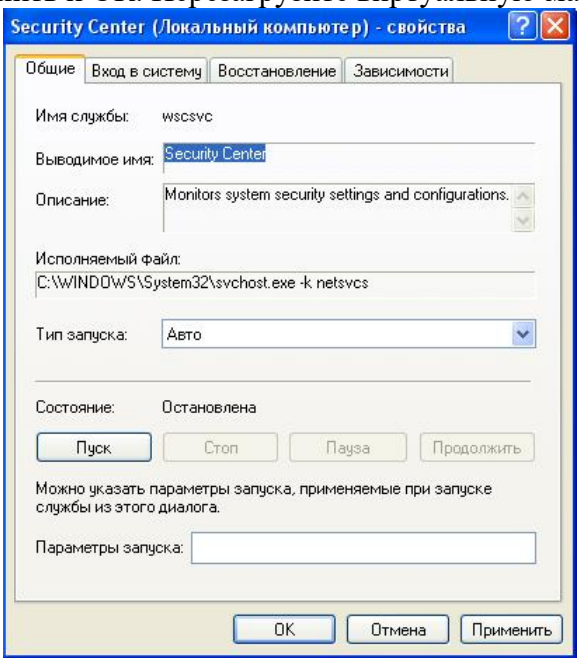
Если ваш компьютер подключен к компьютерной сети (неважно, Интернет это или Интранет), то он уязвим для вирусов, атак злоумышленников и других вторжений. Для защиты компьютера от этих опасностей необходимо, чтобы на нем постоянно работали межсетевой экран (брандмауэр) и антивирусное ПО (с последними обновлениями). Кроме того, необходимо, чтобы все последние обновления были также установлены на вашем компьютере.

Не каждый пользователь может постоянно следить за этим. Не каждый пользователь знает, как это осуществить. И даже если пользователь компетентен в этих вопросах, у него просто может не хватать времени на такие проверки. Компания Microsoft позаботилась обо всех этих пользователях, включив в состав SP2 (и SP3) для Windows XP такой инструмент. Он называется Центр обеспечения безопасности Windows (Windows Security Center).

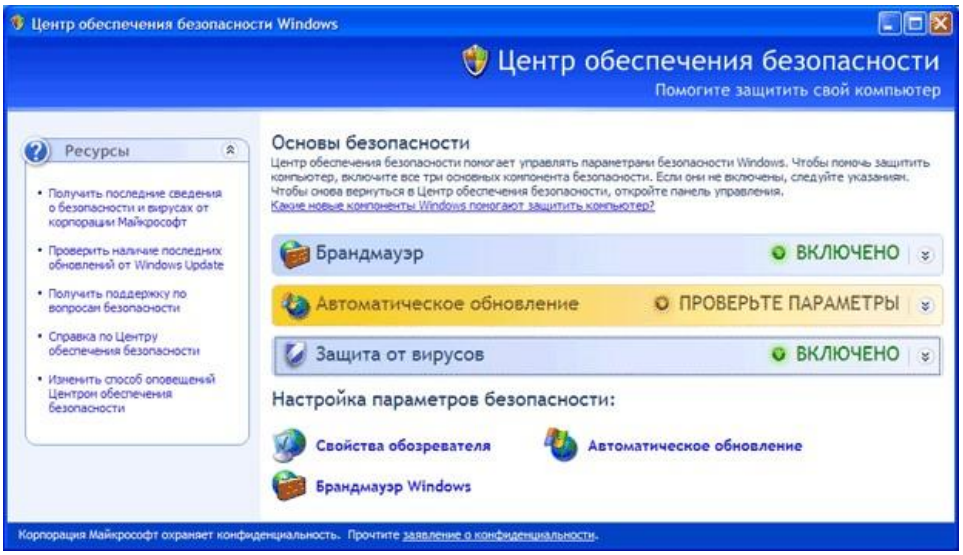
1. Нажмите Меню Пуск – Панель управления – Центр обеспечения безопасности



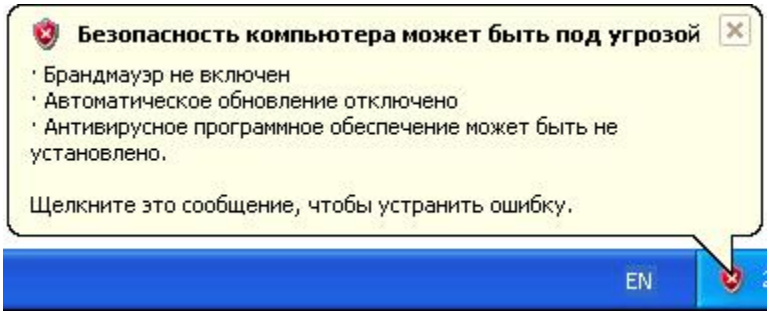
Для включения Центра обеспечения безопасности Windows, нажмите Пуск – Панель управления – Администрирование – Службы. В списке служб найдите службу Security Center, нажмите 2 раза на на этой службе, выберите тип запуска Авто, нажмите кнопку Применить и ОК. Перезагрузите виртуальную машину.



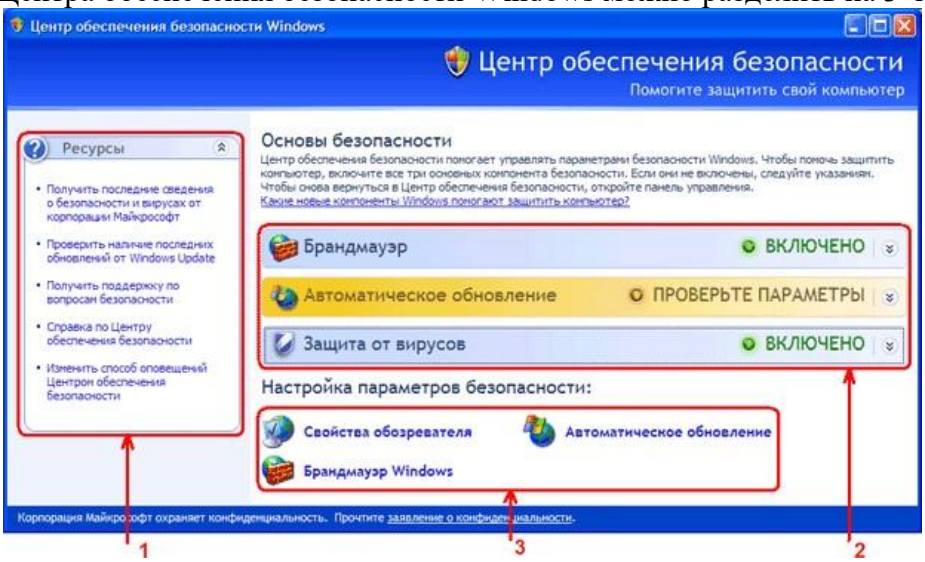
2. На экране появится меню Центра обеспечения безопасности Windows.



3. Основное назначение этого инструмента - информировать и направлять пользователя в нужном направлении. Во-первых, он постоянно контролирует состояния трех основных компонентов ОС (брандмауэр, антивирус, система автоматического обновления). Если параметры любого из этих компонентов не будут удовлетворять требованиям безопасности компьютера, то пользователь получит соответствующее уведомление.



Меню Центра обеспечения безопасности Windows можно разделить на 3 части



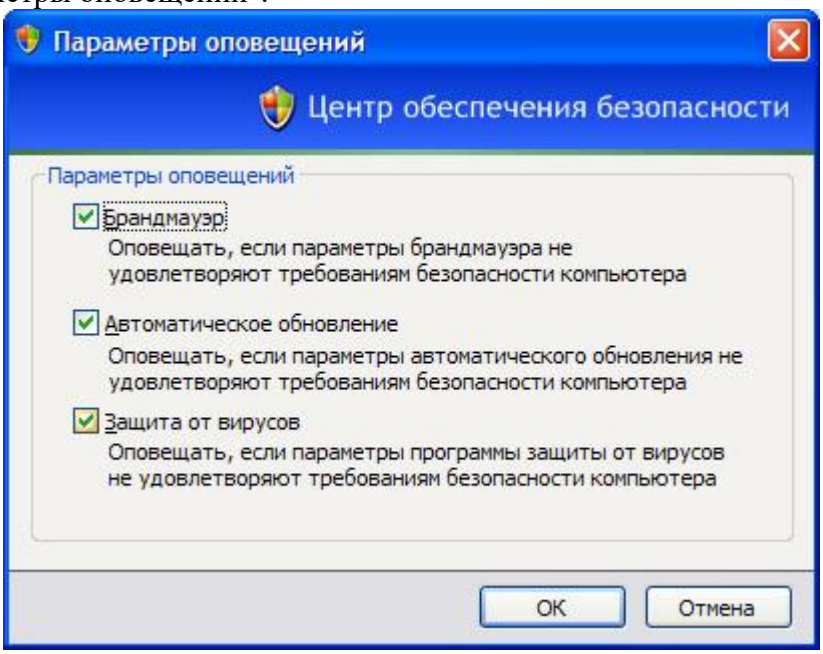
1. Ресурсы. Здесь располагаются ссылки для перехода к Интернет-ресурсам, к встроенной в Windows справочной службе и к окну настройки параметров оповещений.

2. Компоненты безопасности. Здесь располагаются информационные элементы трех основных компонентов безопасности: брандмауэр, автоматическое обновление, антивирусная защита.

3. Параметры безопасности. Здесь располагаются кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, брандмауэр Windows.

Рассмотрим эти части более подробно.

4. В части 1 первые три ссылки предназначены для перехода на соответствующие страницы на сайте Microsoft. Предпоследняя ссылка предназначена для открытия справочной службы Windows на странице "Общие сведения о центре обеспечения безопасности Windows". Последняя ссылка предназначена для открытия окна "Параметры оповещений".



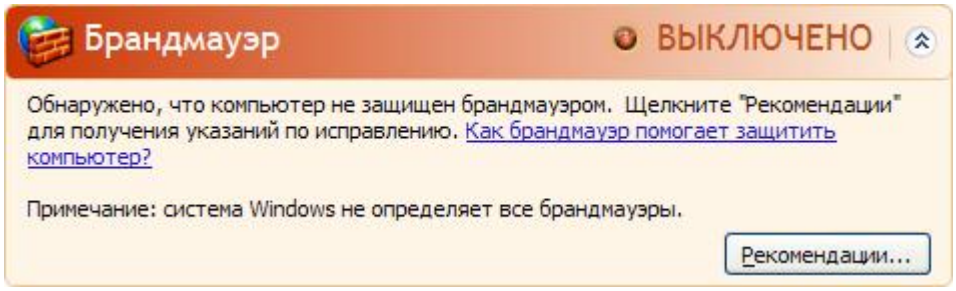
Если на компьютере установлен брандмауэр и антивирусное ПО, не определяемое Центром обеспечения безопасности, вы можете отключить соответствующие оповещения

5. В части 2 каждое информационное табло сообщает о состоянии соответствующего компонента. На рисунке представлены возможные состояния.

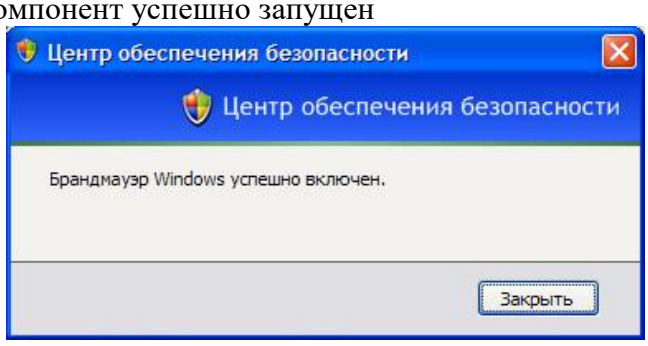
A	ВКЛЮЧЕНО
B	ПРОВЕРЬТЕ ПАРАМЕТРЫ
C	ВЫКЛЮЧЕНО
D	НЕ НАЙДЕНО
E	СРОК ИСТЕК
F	НЕ НАБЛЮДАЕТСЯ

Состояния A-C понятны без комментариев. Состояние D - "Не найдено" - соответствует невозможности определить присутствие соответствующего ПО (например, антивирус или брандмауэр). Состояние E - "Срок истек" - возможно для антивирусной защиты, когда обновления антивирусных баз устарели. Состояние F - "Не наблюдается" - соответствует отключенному контролю над соответствующим компонентом.

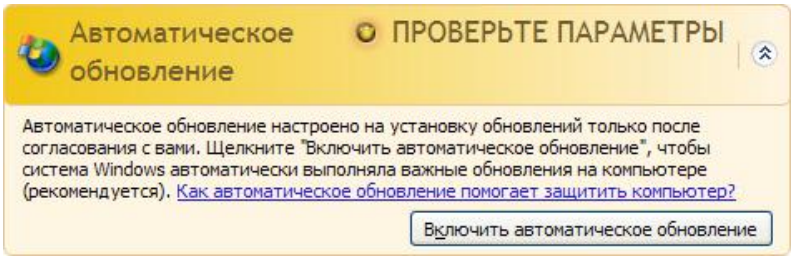
6. Выключите один из компонентов защиты. Состояние этого компоненты примет вид, показанный на рисунке (например, если отключить Брандмауэр Windows)



7. Включите отключенный компоненты защиты, на экране появится сообщение Ваш компонент успешно запущен



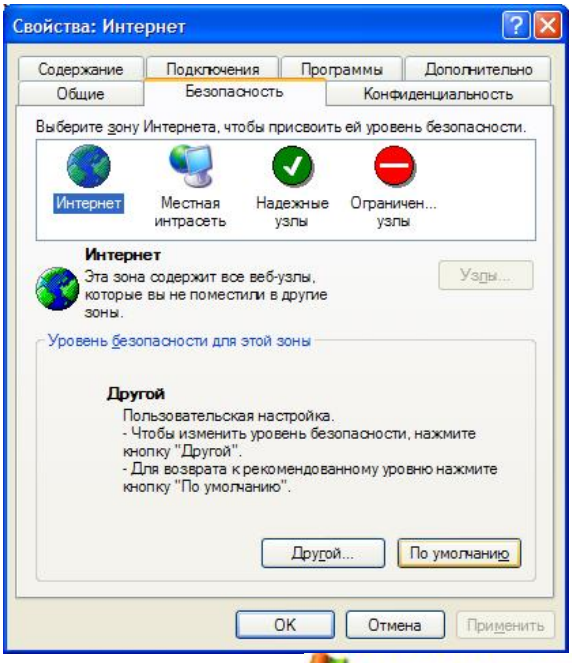
8. Если один из компонентов не может выполнить нужное действие (например, автоматические обновления устанавливаются по выбору пользователя), статус компонента примет вид, показанный на рисунке.



9. Как уже было указано ранее, в разделе 3 расположены кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, брандмауэр Windows.

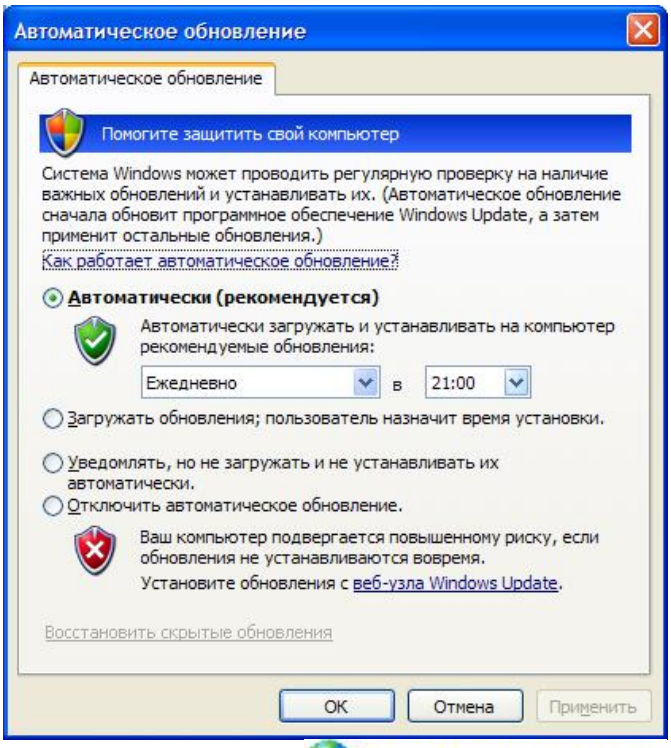
10. Нажав кнопку 

, вы попадете на закладку "Безопасность" в окне настроек обозревателя Internet Explorer.



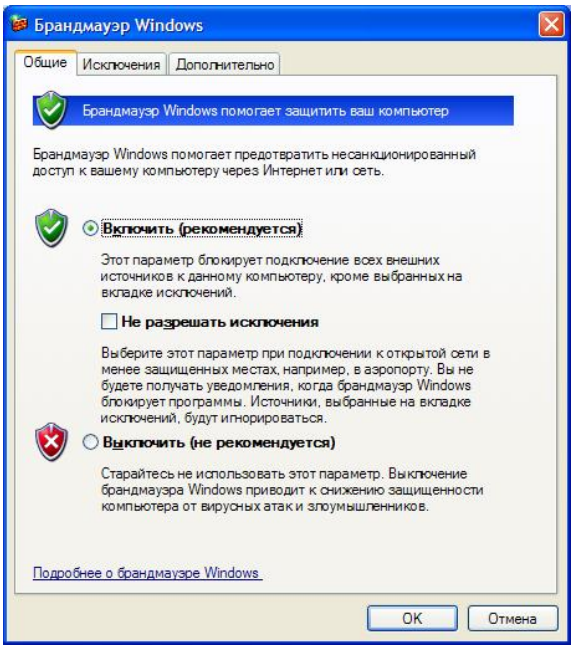
11. Нажав кнопку 

, вы откроете окно настроек "Автоматического обновления".



12. Нажав кнопку 

, вы попадете в соответствующее окно настроек.



Измените различные настройки безопасности компонентов Internet Explorer, Автоматического обновления и Брандмауэра Windows.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader.

Указания по технике безопасности: к выполнению практических занятий допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Дайте определение «несанкционированный доступ», «хакерская атака».
2. Что такое персональная программа-брандмауэр? Какие задачи она решает?
3. Перечислите плюсы и минусы брандмауэров.
4. Как вкл/выкл брандмауэр?
5. Для чего нужен журнал безопасности брандмауэра?
6. Для чего служит блок протокол ICMP?
7. Как защитить компьютер от сетевых хакерских атак?
8. В чем заключается назначение Центра обеспечения безопасности Windows (Windows Security Center)?

10. Какие действия необходимо выполнить для активации Брандмауэра Windows?

Список литературы, рекомендуемый к использованию по данной теме:

1. Агеев А.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.

2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.

3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.

4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация OILCO, 1992.

5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.

6. Групер Ш. Электронные ключи с энергонезависимой памятью //КомпьютерПресс.-1993.-N8.-С.60-62.

7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF, 1996, ил., 336 с.

8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.

9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьютерПресс.-1993.-N7.-С.49-52.

10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер-Пресс.-1991.-N10.-С.19-24.

11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.

12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.

Практическое занятие №9

Организация защиты программ от потенциально опасных инструментальных средств

Цель работы: Ознакомиться с процедурами создания ученых записей пользователей и управления их нравами.

Теоретическая часть

Пользователи

Локальный пользователь или группа - это учетная запись, которой могут быть предоставлены разрешения и права на вашем компьютере. Домен или глобальные пользователи и группы управляются сетевым администратором. Имеется возможность добавить локальных пользователей, глобальных пользователей и глобальные группы в

локальные группы. Однако невозможно добавить локальных пользователей и локальныегруппы в глобальные группы.

Пользователи и группы важны для безопасности Windows XP. поскольку позволяют ограничить возможность пользователей и групп выполнять определенные Действия путем назначения им прав и разрешений. Право даст возможность пользователю выполнять на компьютере определенные действия, такие как архивирование файлов и папок или

завершение работы компьютера. Разрешение представляет собой правило, связанное с объектом (например, файлом, папкой пли принтером), которое определяет, каким пользователям и какого тина доступ к объекту разрешен.

Операционная система содержит несколько встроенных учетных записейпользователей и групп, которые не могут быть удалены.

Краткая информация о встроенных учетных записях.

Учетная запись администратора

Учетная запись пользователя е именем «Администратор» используется при первой установке рабочей станции пли рядового сервера. Эта учетная запись позволяет выполнять необходимые действия до того, как пользователь создаст спою собственную учетную запись. Учетная запись администратора является членом группы администраторов на

рабочей станции или рядовом сервере.

Учетную запись «Администратор» нельзя удавить, отключить или вывести ИЗ группы администраторов, что исключает возможность случайной потери доступа к компьютеру после уничтожения всех учетных записей администраторов. Это свойство отличает пользователя «Администратор» от остальных членов локальной группы

«Администраторы»

Учетная запись гостя

Учетная запись гостя используется теми, кто не имеет реальной учетной записи на компьютере. Если учетная запись пользователя отключена (но не удалена), он также может воспользоваться учетной записью «Гость». Учетная запись гостя не требует пароля. Учетная запись гостя по умолчанию отключена, но не может включена.

Учетной записи пользователя «Гость», как и любой другой учетной записи, можно предоставлять права и разрешения на доступ к объектам. Учетная запись «Гость» по умолчанию входит во встроенную группу «Гости», что позволяет пользователю войти в систему с рабочей станции или рядового сервера. Дополнительные права, как любые разрешения, могут быть присвоены группе «Гости» членом группы администраторов.

1. Группы

Администраторы

Пользователи, входящие в группу «Администраторы», имеют полный доступ на управление компьютером. Это единственная встроенная группа, которой автоматически предоставляются все встроенные нрава и возможности в системе.

Операторы архива

Члены группы «Операторы архива» могут архивировать и восстанавливать файлы на компьютере, независимо от всех разрешений, которыми защищены эти файлы. Также они могут входить на компьютер и выключать его, но не могут изменять параметры

безопасности.

Опытные пользователи

Члены группы опытных пользователей могут создавать учетные записи пользователей, но могут изменять и удалять только созданные ими учетные записи. Они могут создавать локальные группы и удалять пользователей из локальных групп, которые они создали. Они также могут удалять пользователей из групп «Опытные пользователи»,

«Пользователи» и «Гости»

Они не могут изменять группы «Администраторы» и «Операторы архива», не могут являться владельцами файлов, не могут выполнять архивирование и восстановление каталогов, не могут загружать и выгружать драйверы устройств или управлять журналами безопасности и аудита.

Пользователи

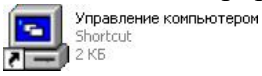
Члены группы пользователей могут выполнять наиболее распространенные задачи, например запуск приложений, использование локальных и сетевых принтеров, завершение работы и блокировка рабочих станций. Пользователи могут создавать локальные группы, но изменять могут только те, которые они создали. Пользователи не могут организовыватьобщий доступ к каталогам или создавать локальные принтеры.

Гости

Группа «Гости» позволяет случайным или разовым пользователям войти в систему со встроенной учетной записью гостя рабочей станции и получить ограниченные возможности. Члены группы «Гости» могут только прекратить работу компьютера.

2. Управление учетной записью пользователя

Для управления учетными записями используется компонент «Управление компьютером». Чтобы открыть окно этого компонента, нажмите Пуск-Панель управления.

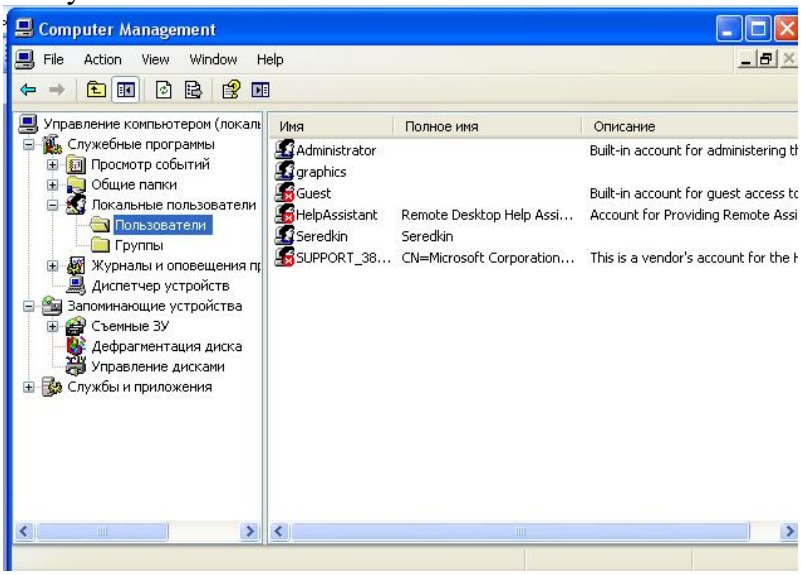
Дважды щелкните значок Администрирование , затем дважды щелкните значок Управление компьютером 

.

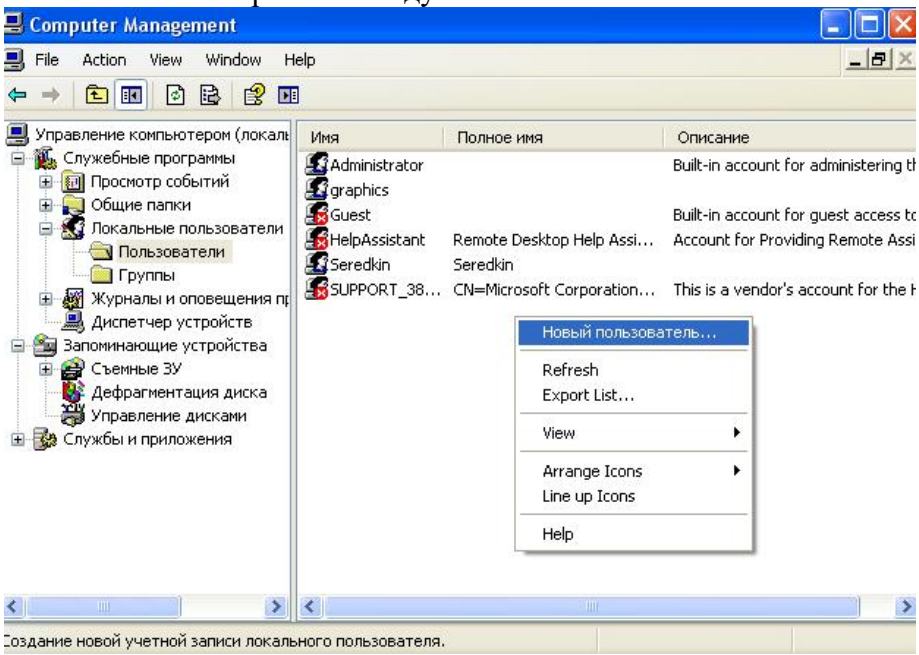
Создание новой учетное записи пользователя:

1. Откройте компонент «Управление компьютером».

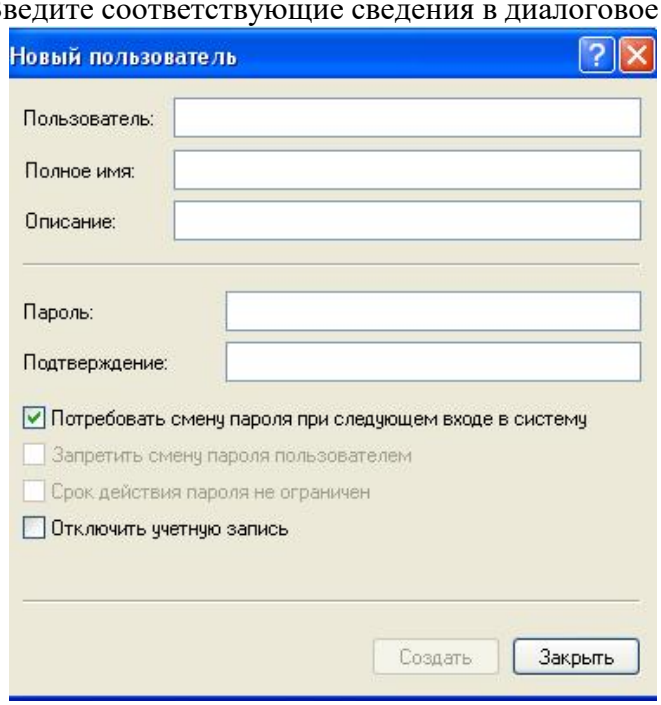
2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Пользователи



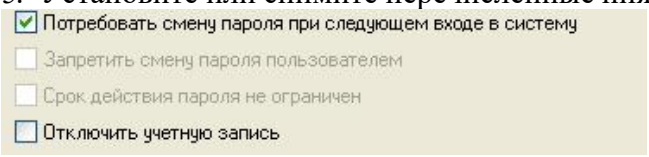
3. Нажмите правой кнопкой мыши в окне со списком пользователей и в появившемся меню выберите команду Новый пользователь.



4. Введите соответствующие сведения в диалоговое окно.



5. Установите или снимите перечисленные ниже флажки.



Потребовать смену пароля при следующем входе в систему – при входе в систему пользователю будет выведено сообщение о смене пароля.

Запретить смену пароля пользователем – пользователь не сможет изменять пароли других пользователей в системе.

Срок действия пароля не ограничен – по истечению срока действия пароля, при входе в систему пользователю будет выводиться сообщение о блокировке учетной записи.

Отключить учетную запись – вход в систему для данного пользователя будет не возможен.

6. Выполните одно из следующих действий.

Чтобы создать дополнительного пользователя, нажмите кнопку Создать и повторите шаги 2 и 3.

Чтобы завершить работу, нажмите кнопку Создать, а затем Закрыть.

Изменение учетной записи пользователя

1. Откройте компонент «Управление компьютером».
2. В дереве консоли выберите компонент «Локальные пользователи н группы» и щелкните в нем учел Пользователи
3. Выберите учетную запись, которую требуется изменить.
4. В меню Действие выберите команду Свойства и произведите изменения.
5. Внесите нужные изменения и нажмите кнопку ОК.

Изменение пароля для пользователя

1. Откройте компонент «Управление компьютером».
2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Пользователи.
3. Выберите учетную запись, которую требуется изменить.
4. В меню Действие выберите команду Установка пароли.

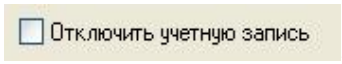
Отключение и активизации учетной записи пользователи

1. Откройте компонент «Управление компьютером».

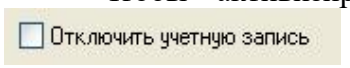
2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Пользователи

3. Выберите учетную запись, которую требуется изменить.

4. В меню Действие выберите команду Свойства.

5. Чтобы отключить выбранную учетную запись пользователя, установите флажок 

.

Чтобы активизировать выбранную учетную запись пользователя, снимите флажок 

.

Удаление учетной записи пользователи

1. Откройте компонент «Управление компьютером».

2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Пользователи

3. Выберите учетную запись, которую требуется удалить.

4. В меню Действие выберите команду Удалить

5. В окне подтверждения удаления нажмите кнопку ОК.

6. В отвез на приглашение подтвердить удаление нажмите кнопку Да.

Переименование учетной записи пользователя

1. Откроите компонент «Управление компьютером».

2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Пользователи

3. Выберите учетную запись, которую требуется переименовать.

4. В меню Действие выберите команду Переименовать.

5. Введите новое имя пользователя и нажмите клавишу ENTER.

Управление группами пользователей

Пользователь, принадлежащий группе, имеет все права на разрешения,

предоставленные этой Группе. Пользователь, являющийся членом нескольких групп, имеетвсе права и разрешения, предоставленные каждой из этих трупп.

При удалении локальной группы удаляется учетная запись группы. Учетные записи пользователей и глобальных групп, являющихся членами удаленной группы, при этом не удаляются.

Создание новой локальной группы

1. Откройте компонент «Управление компьютером».

2. В дереве консоли выберите компонент «Локальные пользователи и труппы» и щелкните в нем узел Группы.

3. В меню Действие выберите команду Новая группа.

4. Введите имя новой группы в поле Имя группы

5. Введите описание новой группы в поле Описание

6. Выполните одно из следующих действий.

Чтобы создать другую группу, нажмите кнопку Создать и повторите шаги 2 и 3. Чтобы завершить работу, нажмите кнопку Создать, а затем Закрыть.

Добавление пользователя в группу

1. Откроите компонент «Управление компьютером».

2. В дереве консоли выберите компонент «Локальные пользователи и группы» и выберите в нем узел Группы.

3. Выберите нужную группу.

4. В меню Действие выберите команду Свойства.

5. Нажмите кнопку Добавить.

6. В нижнее поле введите имена пользователей или групп, которые нужно добавить,или выберите имена пользователей или групп из верхнего поля и нажмите кнопку Добавить.

7. Если необходимо проверить имена добавляемых пользователей или групп.

Нажмите кнопку Проверить имена.

8. Добавив имена всех требуемых пользователей, нажмите кнопку ОК.

Удаление локальной группы

1. Откройте компонент «Управление компьютером».

2. В дереве консоли выберите компонент «Локальные пользователи и группы» и щелкните в нем узел Группы.

3. Выберите Группу, которую следует удалить.

4. В меню Действие выберите команду Удалить.

5. В ответ на приглашение Подтвердить удаление нажмите кнопку Да.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows 7 и программными продуктами: MS Word, Adobe Reader.

Указания по технике безопасности: к выполнению практических занятий допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Дайте определение «локальный пользователь или группа».
2. Почему пользователи и группы важны для безопасности ОС?
3. Какие встроенные учетные записи вы знаете?
4. Расскажите об учетной записи администратора, гостя.
5. Поясните следующие группы: администраторы, операторы архива, опытные пользователи, пользователи, гости.
6. Как осуществляется управление учетной записью пользователя?
7. Как создать новую учетную запись пользователя?
8. Как изменить учетную запись пользователя?
9. Как осуществляется управление группами пользователей?
10. Как создать новую локальную группу? Как добавить пользователя в группу?

Список литературы, рекомендуемый к использованию по данной теме:

1. АгеевА.С. Организация работ по комплексной защите информации/ Информатика и вычислительная техника. 1993, №1.

2. Андрианов В.И., Бородин В.А., Соколов А.В. “Шпионские штучки” и устройства для защиты объектов и информации / Под общей редакцией Золотарева С.А.

3. Афанасьев В.В., Манаев Ю.А. О возможностях защиты информации при ее обработке на ПК. Мир ПК. 1990, № 4.

4. Богумирский Б.С. Руководство пользователя ПЭВМ. ч.2. СПб., Ассоциация

5. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия/ Под ред. акад. Б.П. Смагоринского - М.: Право и Закон, 1996. - 182 с.

6. Групер Ш. Электронные ключи с энергонезависимой памятью //КомпьютерПресс.-1993.-N8.-С.60-62.

7. Жельников Владимир Криптография от папируса до компьютера. - М., ABF,1996, ил., 336 с.

8. Иванов В., Залогин Н. Активная маскировка побочных излучений вычислительных систем. Компьютер Пресс. 1993, № 10.

9. Макаров В. Суперкодированная связь. М., Красная звезда, 1992. Мельников В. Опасная безопасность //КомпьтерПресс.-1993.-N7.-С.49-52.

10. Моисеенко И. Основы безопасности компьютерных систем //Компьютер- Пресс.-1991.-N10.-С.19-24.

11. Моисеенко И. Американская классификация и принципы оценивания безопасности компьютерных систем. Компьютер Пресс, 2/92, 3/93.

12. Пашков Ю.Д., Казеннов В.Н. Организация защиты информации от несанкционированного доступа в автоматизированных системах. С-П, Лаборатория ППШ. 1995.