Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Брянский государственный аграрный университет»

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

НИКУЛИН В.В.

Методические указания к лабораторно-практическим занятиям

по дисциплинам «Информационная безопасность», «Безопасность и защита информации» для подготовки магистров и бакалавров направления 09.04.03, 09.03.03 «Прикладная информатика»

Брянская область,
2015

УДК 681.3 (07)
ББК 32.973-018.2

Никулин В. В. Методические указания к лабораторно-практическим занятиям по дисциплинам «Информационная безопасность», «Безопасность и защита информации». - Брянск: Издательство БГАУ, 2015. –118 с.

Методические указания содержат много иллюстраций и примеров выполнения заданий по каждой теме лабораторно-практических занятий, облегчающих выполнения заданий, контрольные вопросы.

Пособие предназначено для студентов направления подготовки 09.03.03 Прикладная информатика профиль Прикладная информатика в экономике.

Представленные материалы имеют целью формирование компетенций и освоение обучающимися видов профессиональной деятельности в соответствии с ФГОС ВО и ОПОП ВО по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата).

Рецензенты:
к.э.н., доцент кафедры
информационных систем и технологий БГАУ А.В. Кубышкина

Рекомендовано к изданию решением методической комиссии экономического факультета от 12 ноября 2015 г., протокол №2.

Содержание

Лабораторная работа № 1. Сбор данных об информационной системе с помощью средств администрирования Windows (оснасток MMC).

Для проведения оценки рисков необходимо провести инвентаризацию активов информационной системы (ИС). Если в ИС используются домены Windows, для получения данных о системе можно использовать средства администрирования, реализованные в виде оснасток консоли администрирования (Microsoft management console – mmc).

Используемые в данной работе инструменты могут быть запущены из раздела «Администрирование» меню «Пуск» или через «Панель управления» (Пуск -> Панель управления -> Администрирование).

Целью данной лабораторной работы является сбор данных об имеющихся компьютерах, установленных на них операционных системах, предоставляемых в общий доступ файловых ресурсах.

Из раздела «Администрирование» запустите Active Directory Users and Computers. В раскрывающемся списке объектов выберите Ваш домен, там откройте перечень компьютеров (папка Computers – рис.1).

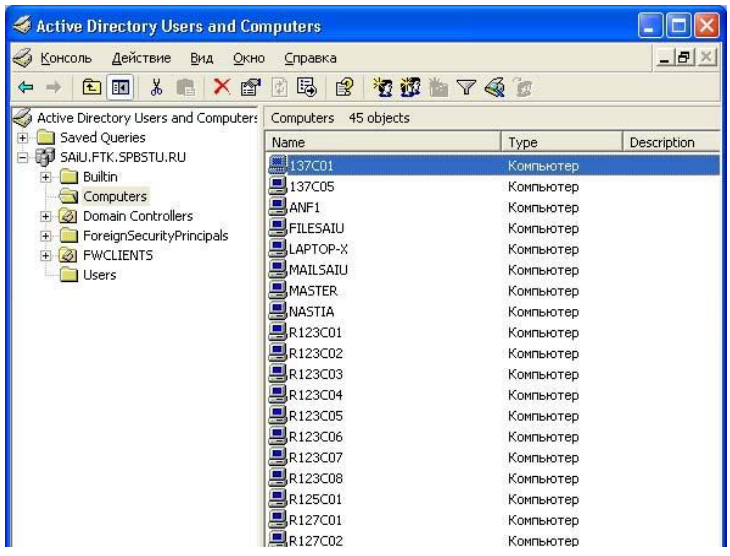


Рис.1. Получение перечня компьютеров домена

С помощью кнопки панели инструментов «Экспорт списка» (на кнопке изображение списка и стрелки) список компьютеров можно экспортировать в текстовый файл для дальнейшей обработки. В свой-

ствах компьютера отображается название и версия установленной операционной системы (рис.2). Также там может быть дополнительная информация, например, описывающая размещение.

Аналогичные данные о контроллерах домена можно получить в разделе Domain Controllers. Данные о пользователях и их группах доступны в разделе Users. Надо отметить, что представленное распределение по разделам не является обязательным. В процессе администрирования могут создаваться новые подразделения (OU - Organization Unit) и объекты (например, пользователи или компьютеры) – помещаться в них.

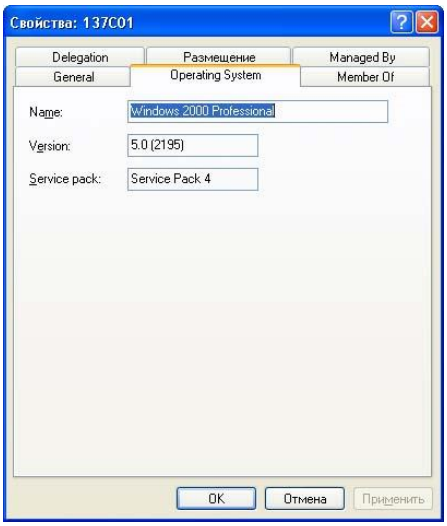


Рис.2. Информация о компьютере.

Информацию о соответствии имен компьютеров IP-адресам можно получить, используя утилиту командной строки nslookup или административную оснастку «DNS». Например, узнать IP-адрес компьютера comp1.mcompany.ru можно с помощью команды **nslookup comp1.mcompany.ru** Часто действующие настройки в сети таковы, что ip-адреса компьютерам выделяются динамически, с использованием службы dhcp, и могут периодически меняться. Как правило, у серверов ip-адреса постоянны.

Теперь перейдем к этапу сбора данных об информационных ресурсах, поддерживаемых на компьютере. Перечень предоставляемых в общий доступ папок можно получить с помощью оснастки «Управление компьютером». На рис.3 представлен пример перечня ресурсов рабочей станции, предоставляемых в общий доступ в служебных целях. Этот список можно также экспортировать в текстовый файл.

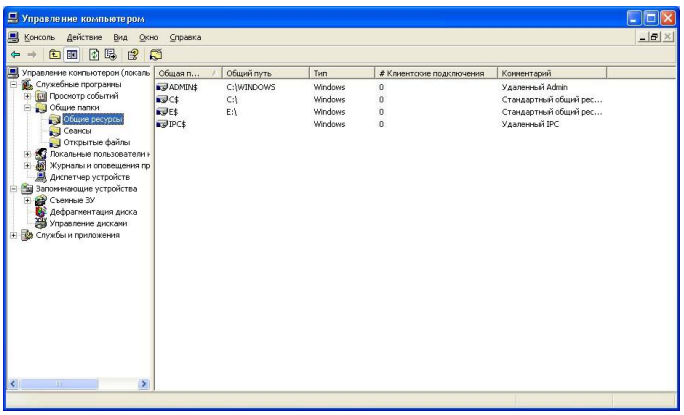


Рис. 3. Пример перечня общих ресурсов рабочей станции.

Более интересен будет подобный список для файлового сервера. Чтобы его увидеть, надо подключить оснастку «Управление компьютером» для сервера. Запустите консоль MMC (Пуск->Выполнить->mmc), в меню выберите добавление новой оснастки (рис. 4), выберите оснастку «Управление компьютером» и укажите, что она будет использоваться для другого компьютера (рис.5).

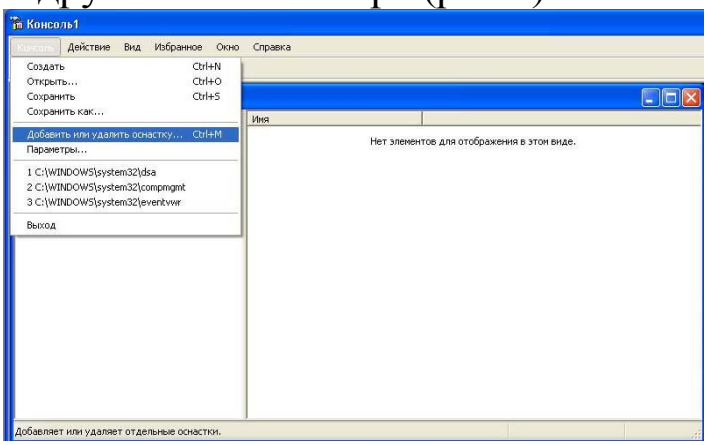


Рис.4. Добавление новой оснастки.

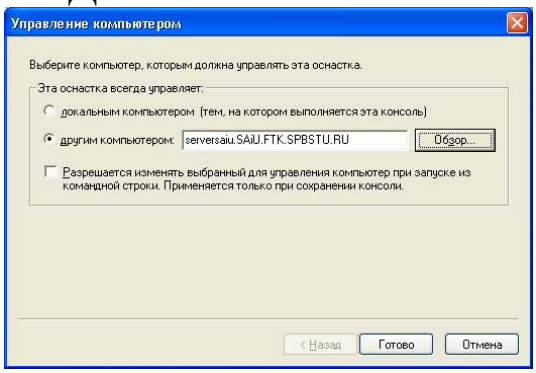


Рис.5. Выбор компьютера.

В остальном для пользователя все будет происходить так же, как и при работе с локальным компьютером.

В свойствах ресурса можно узнать о разрешениях, которые установлены на него как для разделяемого ресурса (рис. 6), а на вкладке

«Безопасность» - разрешениях файловой системы NTFS (если папка расположена на разделе с этой файловой системой, а не с FAT).

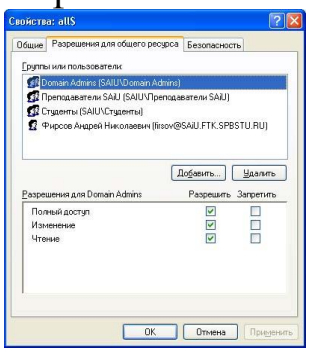


Рис. 6. Разрешения.

Задания к лабораторной работе №1.

1. Получите перечень компьютеров и контроллеров домена. Для указанных преподавателем 1-2 компьютеров выясните установленную операционную систему и используемые ими ip-адреса. *Занесите данные в отчет*.

2. Получите перечень предоставляемых в общий доступ каталогов на вашем компьютере и на компьютерах, данные о которых Вы собирали на этапе 1. Опишите хранимые там данные и охарактеризуйте степень их важности. *Занесите полученную информацию в отчет*.

3. Для указанных ресурсов и выбранных пользователей опишите действующие разрешения на доступ. При этом надо учитывать, что:

- эффективное (действующее) разрешение складывается из разрешений для пользователя лично и разрешений всех групп, в которые пользователь входит;
- запрещение имеет больший приоритет, чем разрешение;
- при комбинации разрешений для общего ресурса с разрешениями NTFS, приоритетными будут разрешения, максимально ограничивающие доступ.

Информацию о членстве пользователя в доменных группах можно получить через оснастку Active Directory Users and Computers, о локальных группах – через «Управление компьютером».

Лабораторная работа № 2. Сбор данных о топологии сети с помощью средства администрирования сетей 3Com Network Supervisor.

Продолжая тему инвентаризации активов информационной системы (ИС), перейдем к рассмотрению средств, позволяющих получить данные о составе и топологии сети. В качестве примера в данной

лабораторной работе будет использоваться утилита 3Com Network Supervisor, которую можно бесплатно получить с сайта компании 3Com (www.3com.com). Аналогичные по функциональности продукты есть и у других производителей сетевого оборудования.

При запуске программы предлагается выбор – строить новую карту сети или открыть существующую. При выборе создания новой карты надо указать, какая подсеть документируется (рис.1). На рисунке выбрана локальная подсеть, т.е. та ip-сеть, к которой относится компьютер, на котором выполняется 3Com Network Supervisor.

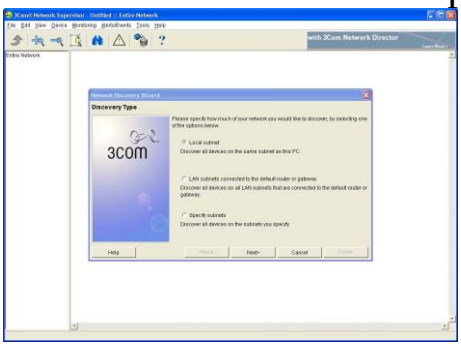


Рис.1 Выбор документируемой сети.

На рис. 2 представлен пример карты сети, которую строит утилита. Надо отметить, что наиболее информативна такая карта будет в том случае, если в сети используется управляемое сетевое оборудование 3Com, поддерживающее, в частности, протокол SNMP. В то же время, польза от составления карты будет и в случае отсутствия в сети подобного оборудования. Для того, чтобы это продемонстрировать, были сделаны следующие настройки. Каждому из компьютеров были присвоены ip-адреса из двух сетей класса C – 192.168.1.0 и 192.168.100.0. Управляемому коммутатору 3Com SuperStack II Switch 3000 назначен адрес 192.168.100.6, т.е. он «виден» только при построении карты сети 192.168.100.0. DNS серверы доступны только в сети 192.168.1.0, поэтому на рисунках, относящихся ко второй сети, компьютеры идентифицируются только ip-адресами. Карта сети 192.168.1.0 представлена на рис.3.

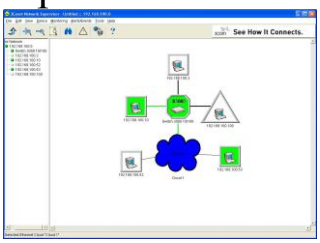


Рис.2. Карта сети 192.168.100.0. Cloud 1 скрывает неуправляемый коммутатор.

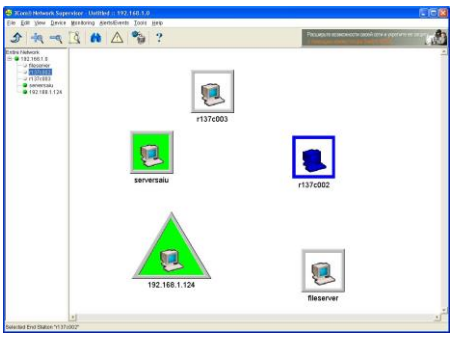


Рис.3 Карта сети 192.168.1.0. Информация от управляемого коммутатора недоступна.

Для выбранного узла можно потребовать провести мониторинг загрузки различных сетевых сервисов или обратиться к средствам удаленного администрирования, использующим протоколы http, telnet или ssh (рис.4,5).

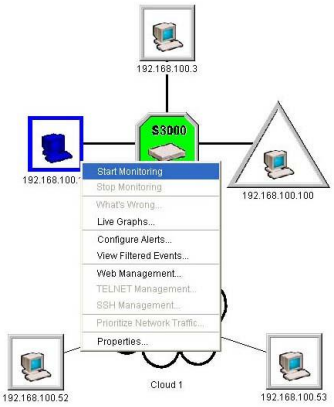


Рис.4. Функции, доступные для выбранного узла.

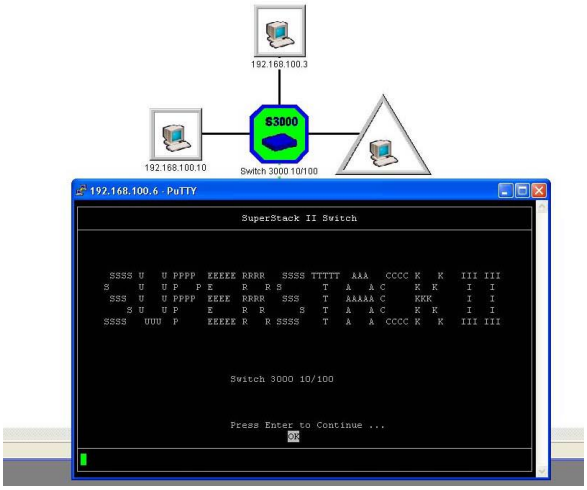


Рис.5. Запуск удаленного терминала для администрирования коммутатора Switch 3000.

Функция поиска (кнопка панели инструментов с изображением бинокля) позволяет, в частности, отобразить информацию о типах используемых сетевых подключений (рис.6,7).

Через свойства управляемого коммутатора доступна информация о том, к какому порту какой узел подключен и графики загрузки (рис.8,9).

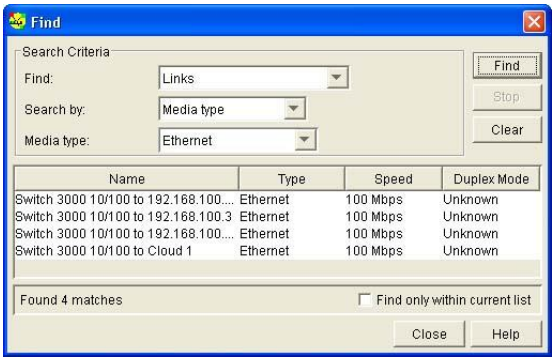


Рис.6. Соединения по типам подключений. Ethernet.

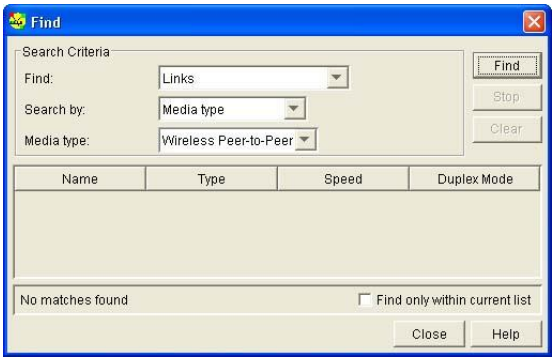


Рис.7. Соединения по типам подключений. Беспроводные подключения (отсутствуют).

Собранная информация может отображаться в виде отчетов, формируемых в формате HTML. Опция доступна через меню Tools пункт Reports. Для задач, связанных с инвентаризацией системы, наибольший интерес представляют отчеты Inventory Report и Topology Report. Примеры «содержательной части» отчетов приведены в табл.1-3.

Табл.1. Inventory Report для сети 192.168.100.0

IP Address	**Device Type**	**MAC Address**	**Device Name**	**Last Discovery Time**
Core Devices				
192.168.100.6	3Com SuperStack II Switch 3000	08-00-4e-50-6d-b3	Switch 3000 10/100	3 Октябрь 2007 г. 22:09
None Core Devices				
192.168.100.10	Generic IP device	00-e0-4c-e9-59-39	192.168.100.10	3 Октябрь 2007 г.

				22:09
192.168.100.100	Generic IP device	00-14-85-d6-50-7d	192.168.100.100	3 Октябрь 2007 г. 22:09
192.168.100.3	Generic IP device	00-11-d8-82-56-d2	192.168.100.3	3 Октябрь 2007 г. 22:09
192.168.100.52	Generic IP device	00-40-f4-70-4f-8f	192.168.100.52	3 Октябрь 2007 г. 22:09
192.168.100.53	Generic IP device	00-30-84-88-09-a7	192.168.100.53	3 Октябрь 2007 г. 22:09

Табл.2. Inventory Report для сети 192.168.1.0

IP Address	**Device Type**	**MAC Address**	**Device Name**	**Last Discovery Time**
Core Devices				
IP Address	**Device Type**	**MAC Address**	**Device Name**	**Last Discovery Time**
None Core Devices				
192.168.1.10	Generic IP device	00-e0-4c-e9-59-39	serversaiu	3 Октябрь 2007 г. 22:35
192.168.1.124	Generic IP device	00-14-85-d6-50-7d	192.168.1.124	3 Октябрь 2007 г. 22:35
192.168.1.3	Generic IP device	00-11-d8-82-56-d2	fileserver	3 Октябрь 2007 г. 22:35
192.168.1.52	Generic IP device	00-40-f4-70-4f-8f	r137c002	3 Октябрь 2007 г. 22:35
192.168.1.53	Generic IP device	00-30-84-88-09-a7	r137c003	3 Октябрь 2007 г. 22:35

Табл.3. Topology Report для сети 192.168.100.0

IP Address	Type	Unit	Port	Linked To	IP Address	Type	Unit	Port
192.168.100.6	3Com SuperStack II Switch 3000	1	6	_____	192.168.100.3	Generic IP device	N/A	N/A
192.168.100.6	3Com SuperStack II Switch 3000	1	5	_____	192.168.100.100	Generic IP device	N/A	N/A
192.168.100.6	3Com SuperStack II Switch 3000	1	12	_____	192.168.100.10	Generic IP device	N/A	N/A
192.168.100.6	3Com SuperStack II Switch 3000	1	4	_____	Unknown	Unknown	N/A	N/A
Unknown	Unknown	N/A	N/A	_____	192.168.100.53	Generic IP device	N/A	N/A
Unknown	Unknown	N/A	N/A	_____	192.168.100.52	Generic IP device	N/A	N/A

Отчет по топологии сети 192.168.1.0 состоит из записи «Нет данных», т.к. данные о топологии программа 3Com Network Supervisor получить не смогла (в этой сети управляемый коммутатор «невидим», т.к. его адрес принадлежит другой ip-сети).

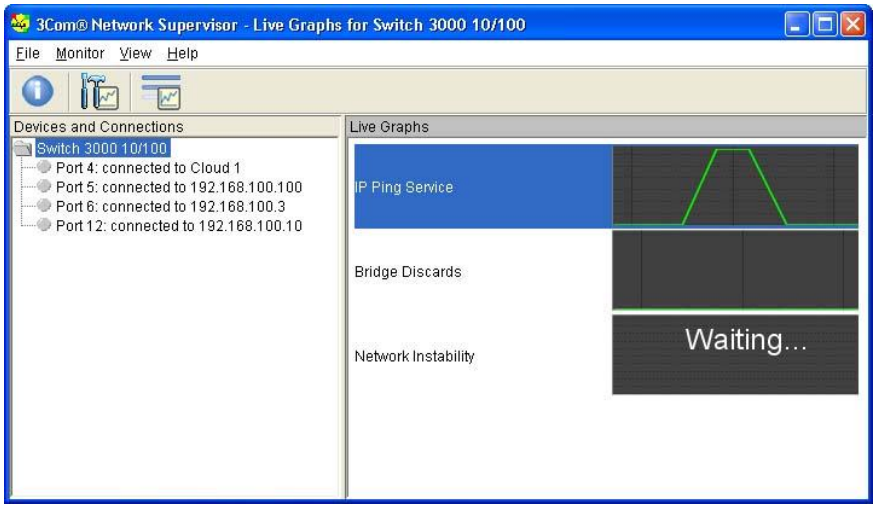


Рис.8. Данные о подключениях и графики.

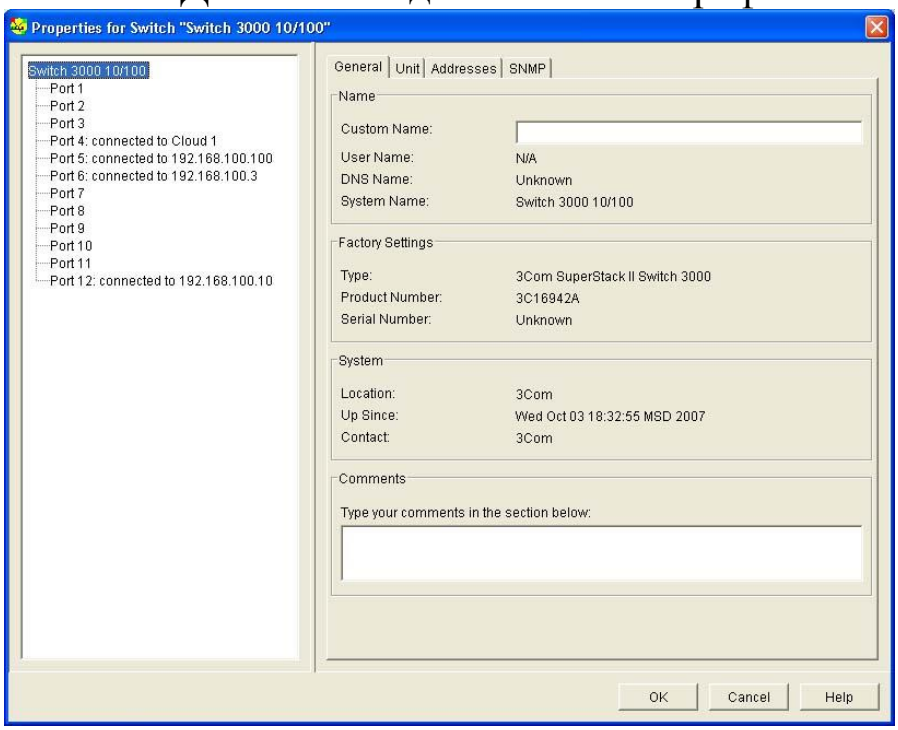


Рис.9. Свойства коммутатора.

Задания к лабораторной работе №1.

С помощью 3Com Network Supervisor постройте карту сети учебной лаборатории. Опишите узлы сети, используемые типы соединений, доступные средства удаленного администрирования.

Перечислите используемые сетевые устройства и укажите, какие последствия будут при выходе из строя (или некорректной работе) каждого из них.

Лабораторная работа №3. Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer.Настройка локальной политики паролей.

Microsoft Baseline Security analyzer – программа, позволяющая проверить уровень безопасности установленной конфигурации операционной системы (ОС) Windows 2000, XP, Server 2003, Vista Server 2008. Также проверяется и ряд других приложений разработки Microsoft. Данное средство можно отнести к разряду систем анализа защищенности. Оно распространяется бесплатно и доступно для скачивания с web-сервера Microsoft (адрес страницы данной утилиты на момент подготовки описания был: http://technet.microsoft.com/ru-ru/security/cc184924(en-us).aspx).

В процессе работы BSA проверяет наличие обновлений безопасности операционной системы, офисного пакета Microsoft Office(для версий XP и более поздних), серверных приложений, таких как MS SQL Server, MS Exchange Server, Internet Information Server и т.д. Кроме того, проверяется ряд настроек, касающихся безопасности, например, действующая политика паролей.

Перейдем к знакомству с программным продуктом. Надо отметить, что при подготовке описания данной лабораторной работы использовалась версия BSA 2.1. К сожалению, продукт не локализован, поэтому использовалась англоязычная версия.

При запуске открывается окно, позволяющее выбрать объект проверки – один компьютер (выбирается по имени или ip-адресу), несколько (задаваемых диапазоном ip-адресов или доменным именем) или просмотреть ранее сделанные отчеты сканирования системы. При выборе сканирования отдельного компьютера по умолчанию подставляется имя локальной станции, но можно указать имя или ip-адрес другого компьютера.

Рис.1. Выбор проверяемого компьютера.

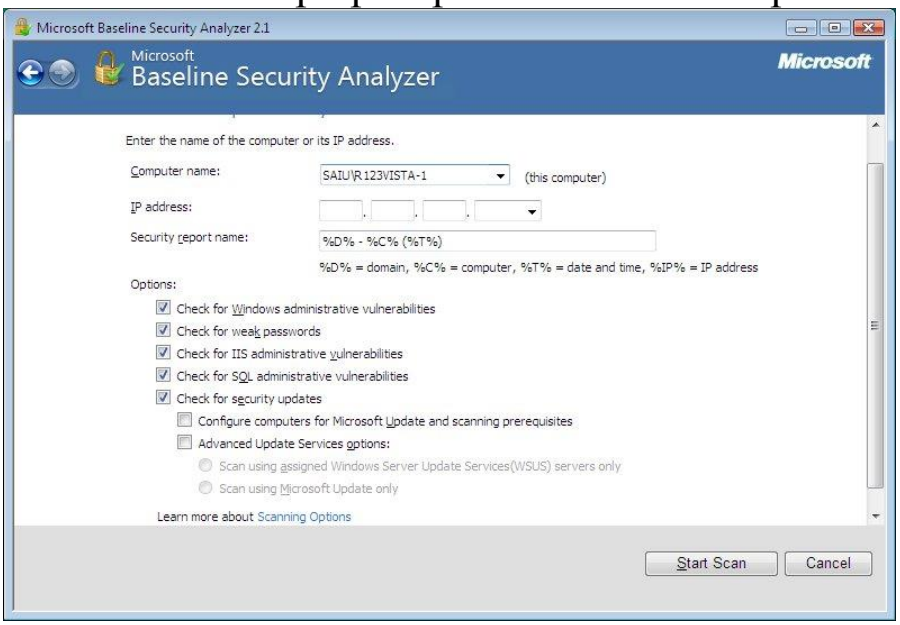


Рис.2. Задание параметров проверки.

Можно задать перечень проверяемых параметров. На рис.2 представлен выбор вариантов проверки:

- проверка на наличие уязвимостей Windows, вызванных некорректным администрированием;
- проверка на «слабые» пароли (пустые пароли, отсутствие ограничений на срок действия паролей и т.д.);
- проверка на наличие уязвимостей web-сервера IIS, вызванных некорректным администрированием;
- аналогичная проверка в отношении СУБД MS SQL Server;
- проверка на наличие обновлений безопасности.

Перед началом работы программа обращается на сервер Microsoft для получения перечня обновлений для ОС и известных уязвимостей. Если на момент проведения проверки компьютер не подключен к Интернет, база уязвимостей не будет обновлена, программа об этом сообщит и дальнейшие проверки выполняться не будут. В подобных случаях нужно отключать проверку обновлении безопасности (сбросив соответствующую галочку на экране рис.2 или с помощью ключа при использовании утилиты командной строки, о чем речь пойдет ниже).

Для успешной проверки локальной системы необходимо, чтобы программа выполнялась от имени учетной записи с правами локального администратора. Иначе проверка не может быть проведена и о чем будет выдано сообщение: «You do not have sufficient permissions to perform this command. Make sure that you are running as the local administrator or have opened the command prompt using the 'Run as administrator' option».

По результатам сканирования формируется отчет, в начале которого дается общая оценка уровня безопасности конфигурации проверяемого компьютера. В приведенном на рис.3 примере уровень риска оценивается как «серьезный» (Severe risk).

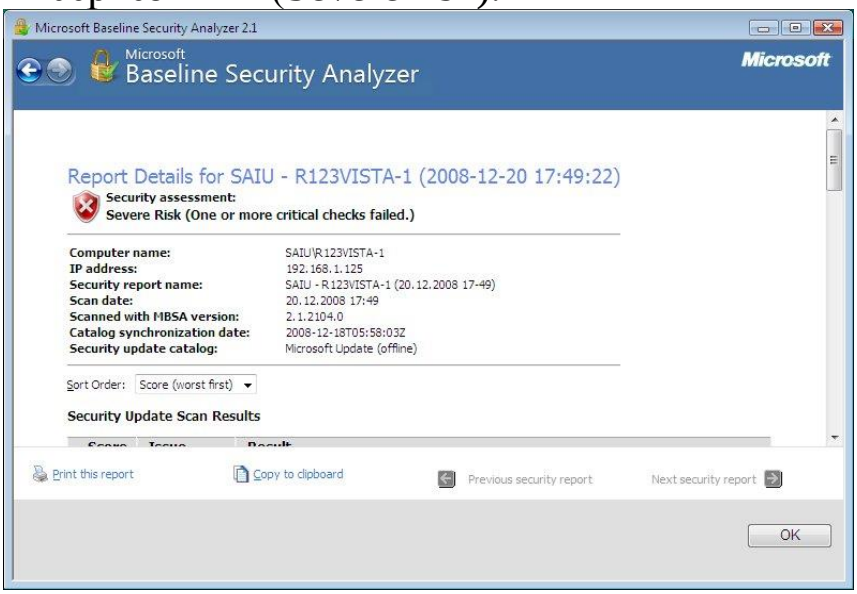


Рис.3. Заголовок отчета.

Далее приводится перечень обнаруженных уязвимостей, разбитый на группы: результаты проверки установки обновлений, результаты проверки Windows и т.д. Надо отметить, что выпускаемые Microsoft обновления бывают различных типов:

Security updates – собственно обновления безопасности, как правило, посвященные исправлению одной уязвимости программного продукта;
Update rollups – набор исправлений безопасности, который позволяет одновременно исправить несколько уязвимостей. Это упрощает обслуживание процесса обновления программного обеспечения (ПО);
Service packs – набор исправлений, как связанных, так и несвязанных с безопасностью. Установка Service pack, как правило, исправляет все уязвимости, обнаруженные с момента выхода предыдущего Service pack, таким образом устанавливать промежуточные обновления уже не надо.
В описании рассматриваемого результата проверки (рис.4) можно выбрать ссылку Result details и получить более подробное описание найденных проблем данной группы. При наличии подключения к Интернет, перейдя по приводимой в отчете ссылке, можно получить информацию об отсутствующем обновлении безопасности и скачать его из сети.
Нужно отметить, что установка обновлений для систем с высокими требованиями в области непрерывности работы, требует предварительной тщательной проверки совместимости обновлений с использующимися приложениями. Подобная проверка обычно производится на тестовых системах с близкой конфигурацией ПО. В то же время, для небольших организаций и пользователей домашних компьютеров такая проверка зачастую неосуществима. Поэтому надо быть готовым к тому, чтобы восстановить систему после неудачного обновления. Для современных ОС семейства Windows это можно сделать, например, используя специальные режимы загрузки ОС – безопасный режим или режим загрузки последней удачной конфигурации.
Также надо отметить еще одну особенность. На данный момент baseline security analyzer не существует в локализованной русскоязычной версии. И содержащиеся там ссылки на пакеты обновлений могут указывать на иные языковые версии, что может создать проблемы при обновлении локализованных продуктов.

Рис.4. Перечень неустановленных обновлений (по группам).

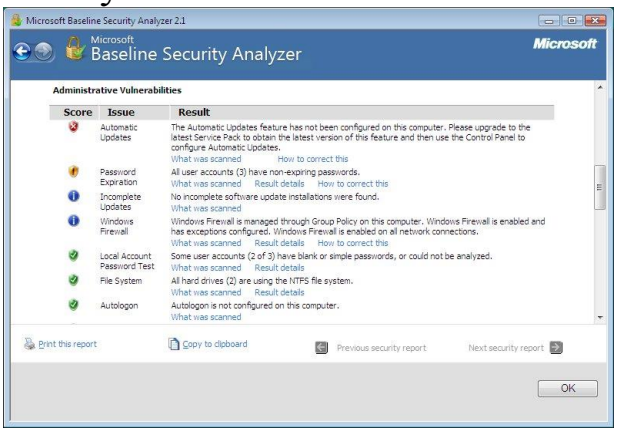


Рис.5. Уязвимости, связанные с администрированием операционной системы.

Аналогичным образом проводится работа по анализу других групп уязвимостей (рис.5). Описывается уязвимость, указывается ее уровень критичности, даются рекомендации по исправлению. На рис. 6 представлено подробное описание результатов (ссылка result details) проверки паролей. Указывается, что 3 учетные записи имеют пароли, неограниченные по сроку действия.

Рис.6. Результаты проверку паролей.

Кроме версии программы с графическим интерфейсом, существует также утилита с интерфейсом командной строки. Называется она mbsacli.exe и находится в том же каталоге, куда устанавливался Baseline security analyzer, например, “C:\Program Files\Microsoft Baseline

Security Analyzer 2". У утилиты есть достаточно много ключей, получить информацию о которых можно запустив ее с ключом "/?".
Запуск без ключей приведет к сканированию локального компьютера с выводом результатов на консоль. Чтобы сохранить результаты сканирования, можно перенаправить вывод в какой-либо файл. Например: mbsacli > mylog.txt Хотелось бы еще раз обратить внимание на то, что при настройках по умолчанию сначала утилита обращается на сайт Майкрософт за информацией об обновлениях. Если соединения с Интернет отсутсвует, то утилиту надо запускать или с ключом /nd (указание «не надо скачивать файлы с сайта Майкрософт») или с ключом /n Updates (указание «не надо проводить проверку обновлений»).
Запуск с ключом /xmlout приводит к запуску утилиты в режиме проверки обновлений (т.е. проверка на уязвимости, явившиеся результатом неудачного администрирования, проводиться не будет), при этом, отчет формируется в формате xml. Например:
mbsacli /xmlout > c:\myxmlog.xml

Локальная политика паролей.

Рассмотрим теперь, какие настройки необходимо сделать, чтобы пароли пользователей компьютера были достаточно надежны. В теоретической части курса мы рассматривали рекомендации по администрированию парольной системы. Потребовать их выполнения можно с помощью политики безопасности. Настройка делается через Панель управления Windows.
Откройте Панель управления → Администрирование → Локальная политика безопасности. Выберите в списке Политика учетных записей и Политика паролей. Для Windows Vista экран консоли управления будет выглядеть так, как представлено на рис. 7.
Значения выбранного параметра можно изменить (рис.8).
Надо понимать, что не все требования политики паролей автоматически подействуют в отношении всех учетных записей. Например, если в свойствах учетной записи стоит «Срок действия пароля не ограничен», установленное политикой требование максимального срока действия пароля будет игнорироваться. Для обычной пользовательской учетной записи, эту настройку лучше не устанавливать. Но в некоторых случаях она рекомендуется. Например, если в учебном клас-

се нужна «групповая» учетная запись, параметры которой известны всем студентам, лучше поставить для нее «Срок действия пароля не ограничен» и «Запретить смену пароля пользователем».
Свойства учетной записи можно посмотреть в Панель управления → Администрирование → Управление компьютером, там выберите Локальные пользователи и группы и Пользователи (или запустив эту же оснастку через Пуск→Выполнить→lusrmgr.msc).

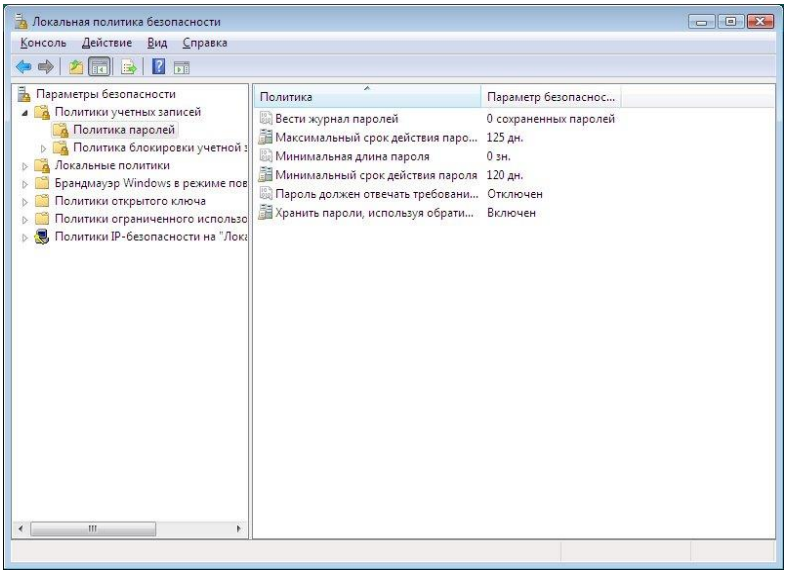


Рис.7. Настройка политики паролей.

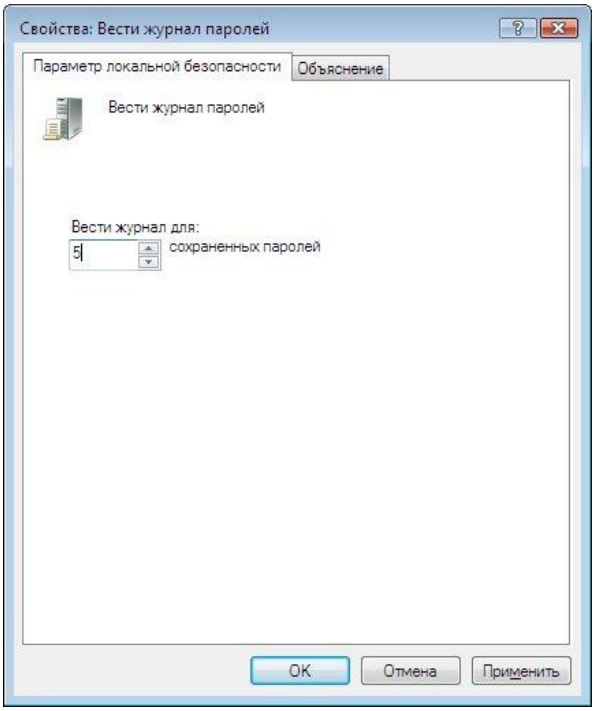


Рис.8. Установка требования ведения журнала паролей.

Задания к лабораторной работе №3.

Задания.1

1. Выполните проверку Вашего компьютера с помощью Microsoft Baseline security analyzer. В отчете о выполнении лабораторной укажите:

- как оценен уровень уязвимости Вашего компьютера;
- какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей;
- опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере.

Проведите анализ результатов – какие уязвимости можно устранить, какие – нельзя из-за особенностей конфигурации ПО или использования компьютера.

2. Выполните удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.
3. Теперь выполните проверку нескольких компьютеров с помощью утилиты mbsacli. Для этого, предварительно создайте текстовый файл с перечнем имен компьютеров или ip-адресов и запускайте mbsacli с ключом /listfile, после которого указывается имя файла с перечнем компьютеров. В результате Вы получите сообщение примерно следующего содержания:

Computer Name, IP Address, Assessment, Report Name

HOME\MYNBOOK, 127.0.0.1, Severe Risk, HOME - MYNBOOK (06.12.2008 13-51)

Для того, чтобы увидеть подробные результаты проверки, надо повторно запустить mbsacli с ключом /ld, после которого указывается имя отчета. Вывод можно перенаправить в текстовый файл для дальнейшей обработки. Например:

mbsacli /ld “HOME - MYNBOOK (06.12.2008 13-51)” > c:\test\report1.txt

После выполнения задания проанализируйте результаты, кратко опишите их в отчете по лабораторной работе.

Задания.2

1. Опишите действующую на вашем компьютере политику паролей.

2. Измените ее в соответствии с рассмотренными в теоретической части курса рекомендациями по администрированию парольной системы.
3. Если в ходе проверки утилитой bsa были выявлены уязвимости связанные с управлением паролями пользователей, опишите пути их устранения или обоснуйте необходимость использования действующих настроек.

Лабораторная работа № 4. Использование сканеров безопасности для получения информации о сети.

Сетевые сканеры безопасности – программные средства, позволяющие проверить уровень уязвимости сетей. Они имитируют различные обращения к сетевым узлам, выявляя операционные системы компьютеров, запущенные сервисы, имеющиеся уязвимости. В некоторых случаях сканеры безопасности также имитируют реализацию различных атак, чтобы проверить уровень подверженности им компьютеров защищаемой сети.

При проведении анализа рисков сканеры безопасности могут использоваться как в процессе инвентаризации ресурсов, так и для оценки уровня уязвимости узлов сети.

В данной лабораторной работе используется ПО Shadow Security Scanner разработки компании Safety-Lab, ознакомительная версия которого бесплатно доступна на сайте www.safety-lab.ru или www.safety-lab.com

После запуска сканера надо начать новую сессию (нажав соответствующую кнопку на панели инструментов). Затем следует выбрать тип проводимых проверок, описываемый правилом (рис.1). К определению проверяемых параметров надо относиться достаточно внимательно. Например, проведение на работающей в штатном режиме информационной системе имитации атак на отказ в обслуживании (DoS tests) может привести к сбою в работе системы, что зачастую недопустимо. Другой пример - сканирование всех TCP и UDP портов (а не только «стандартных») приведет к большим затратам времени, но позволит выявить запушенные службы, использующие нестандартные порты (подробнее об этом см. ниже).

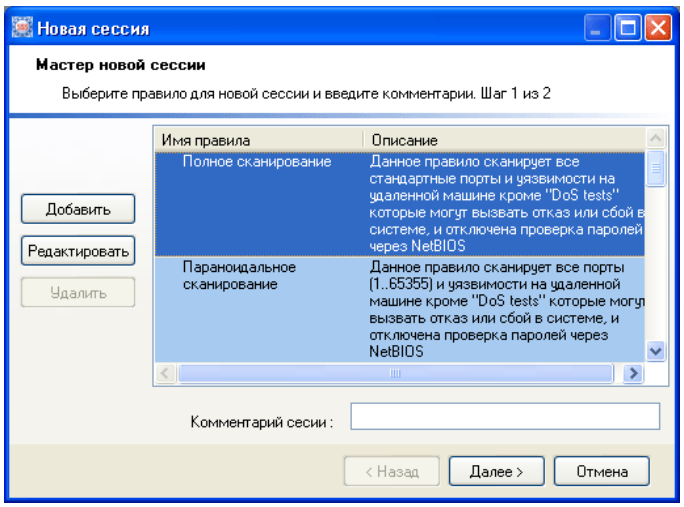


Рис.1. Определение набора проводимых проверок.

Далее определяется перечень проверяемых объектов. Это может быть отдельный компьютер, задаваемый именем или IP-адресом; группа компьютеров, определяемая диапазоном IP-адресов (рис.2) или перечнем имен из заранее подготовленного файла; виртуальные http-узлы, задаваемые именами.

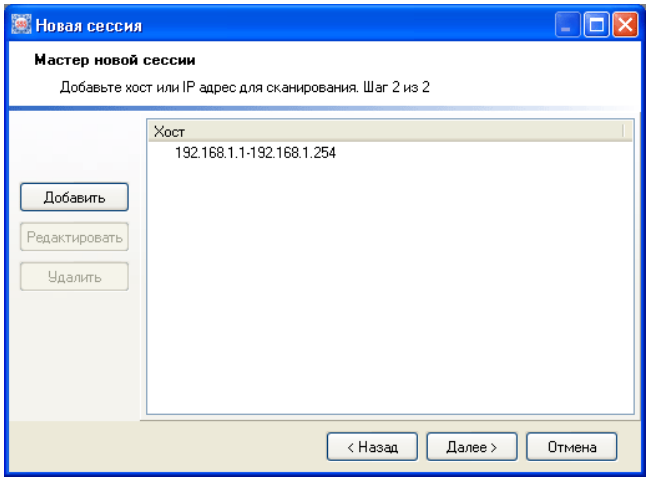


Рис.2. Диапазон проверяемых узлов

Когда параметры сессии определены, проверка запускается кнопкой «Запустить сканирование».

Результаты проверки позволяют получить достаточно полную информацию об узлах сети. На рисунке 3 представлен фрагмент описания результатов сканирования компьютера – указаны имя компьютера, версия операционной системы, перечислены открытые TCP и UDP порты и т.д. Относительно использующихся сетевыми службами портов хотелось бы отметить, что даваемые сканером пояснения не всегда достаточно подробны. В качестве дополнительной информации можно, в частности, порекомендовать техническую статью «Службы и сетевые порты в серверных системах Microsoft Windows» доступ-

ную по ссылке http://support.microsoft.com/?kbid=832017. В качестве справочного материала она приложена к описанию данной лабораторной работы.

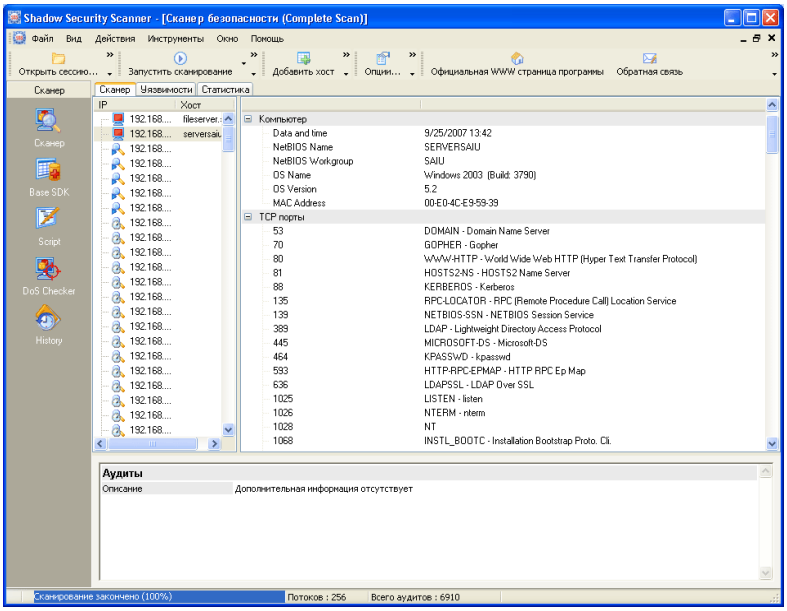


Рис. 3. Результаты сканирования.

Также приводится информация об обнаруженных уязвимостях и степени их критичности, даются ссылки позволяющие найти более подробную информацию и исправления. Ссылки приводятся как на материалы компании-разработчика, так на описания уязвимостей в специализированных каталогах – CVE и bugtraq (рис.4).

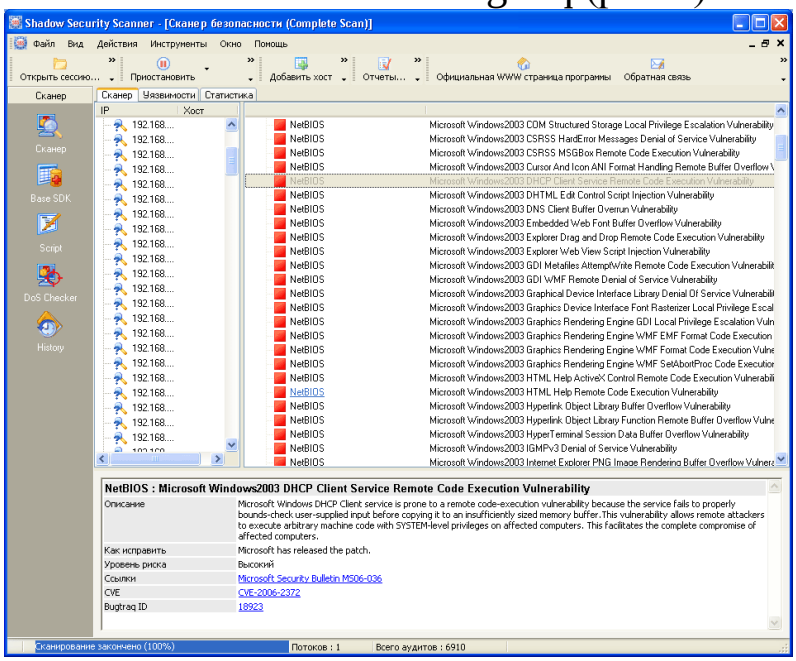


Рис.4. Описание обнаруженных уязвимостей.

К сожалению, опция формирования отчетов в бесплатной версии программы недоступна. Поэтому, при выполнении лабораторной, эту ра-

боту придется делать вручную, перенося описания через буфер из окна программы, например, в тестовый редактор Word.

Задания к лабораторной работе №4

1. Перечислите и охарактеризуйте стандартные правила, определяющие параметры сессии сканирования. На базе одного из них создайте собственное правило.
2. Проведите сканирование указанных преподавателем компьютеров в учебной лаборатории. При сканировании надо учитывать, что часть имеющихся уязвимостей может быть закрыта путем использования встроенного межсетевого экрана (брандмауэра Windows), появившегося в ОС семейства Windows начиная Windows XP. Чтобы получить более полную информацию об исследуемых узлах, лучше провести одно сканирование при включенном, другое - при отключенном межсетевом экране (изменение настройки доступно через Панель управления -> Брандмауэр Windows). Аналогичная ситуация возникает и при использовании других межсетевых экранов.

Опишите результаты проверки – полученные данные о компьютере и сетевых службах, наиболее серьезные из обнаруженных уязвимостей и пути их устранения. Охарактеризуйте уровень безопасности проверенных компьютеров.

Лабораторная работа № 5. Использование Microsoft Security Assessment Tool (MSAT).

В ходе данной лабораторной работы мы познакомимся с разработанной Microsoft программой для самостоятельной оценки рисков, связанных с безопасностью - Microsoft Security Assessment Tool (MSAT). Она бесплатно доступна на сайте Microsoft по ссылке http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=cd057d9d-86b9-4e35-9733-7acb0b2a3ca1

Как отмечают разработчики, приложение предназначается для организаций с числом сотрудников менее 1000 человек, чтобы содействовать лучшему пониманию потенциальных проблем в сфере безопасности. В ходе работы, пользователь, выполняющий роль аналитика, ответственного за вопросы безопасности, отвечает на две группы вопросов.

Первая из них посвящена бизнес-модели компании, и призвана оценить риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Создается так называемый профиль риска для бизнеса (ПРБ).

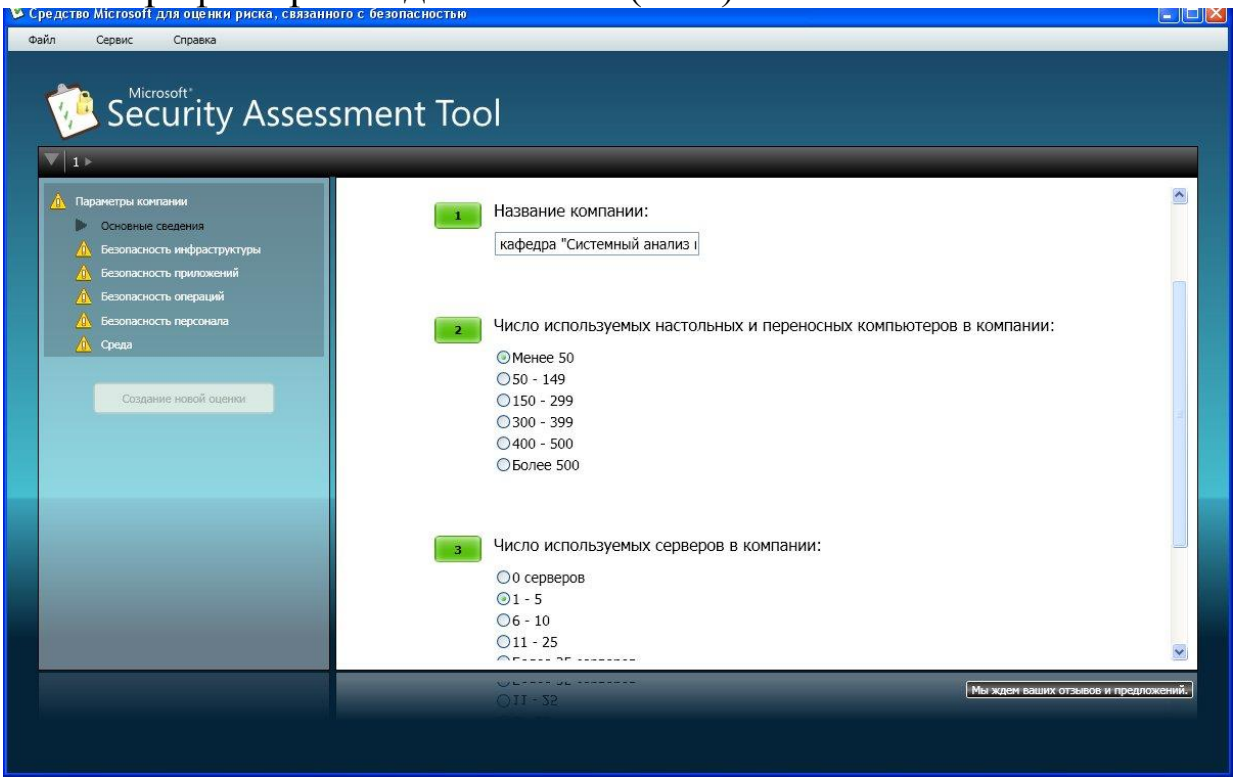


Рис.1. Информация о компании

Вопросы этого этапа разбиты на 6 групп. Первая (рис.1) касается общих сведений о компании – название, число компьютеров, серверов и т.д. Вторая группа вопросов озаглавлена «Безопасность инфраструктуры». Примеры вопросов – «использует ли компания подключение к Интернет», «размещаются ли службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте» и т.д. Остальные группы – «Безопасность приложений», «Безопасность операций», «Безопасность персонала», «Среда».

Надо отметить, что при локализации не все вопросы первого этапа были качественно переведены с английского. Чего стоит вопрос: «Прошла ли ваша организация через «копирование и замена» касающиеся любого основного компонента технологии, за последние 6 месяцев ?»! Однако во всех случаях можно из контекста понять, о чем идет речь (в приведенном примере вопрос был, относительно того, менялись ли используемые технологии обработки информации).

Когда проведен первый этап оценки, полученная информация обрабатывается (для этого требуется подключение к Интернет), после

чего начинается второй этап анализа. Для технических специалистов он будет более интересен, т.к. касается используемых в компании политик, средств и механизмов защиты (рис.2). Стоит сказать, что и перевод вопросов второго этапа выполнен существенно лучше.

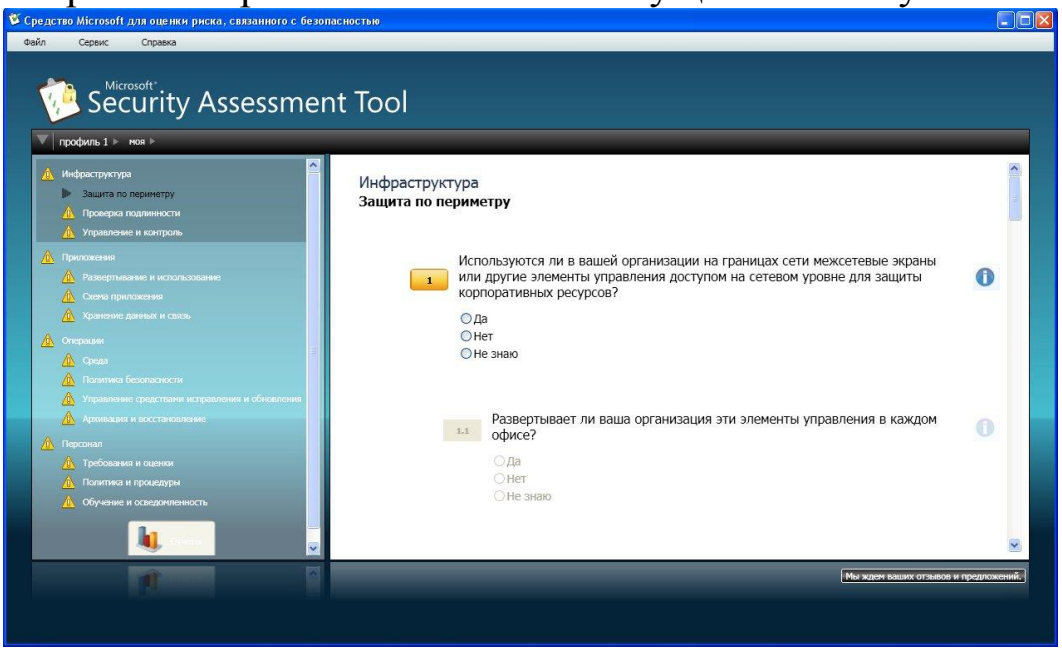


Рис.2. Анализ используемых механизмов защиты.

Вопросы организованы в соответствии с концепцией многоуровневой (эшелонированной) защиты. Сначала рассматривается защита инфраструктуры (защита периметра, аутентификация…), затем вопросы защиты на уровне приложений, далее проводится анализ безопасности операций (определена ли политика безопасности, политика резервного копирования и т.д.), последняя группа вопросов касается работы с персоналом (обучение, проверка при приеме на работу и т.д.).

Во многом тематика вопросов соответствует разделам стандартов ISO 17799 и 27001, рассмотренных в теоретической части курса.

После ответа на все вопросы программа вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес для технических специалистов представляет «Полный отчет». В частности, он содержит предлагаемый список приоритетных действий. Фрагмент списка представлен в табл. 1

Табл. 1

Список предлагаемых действий

Предмет анализа	***Рекомендация***
Высокий приоритет	

Операции > Управление средствами исправления и обновления > Управление средствами исправления	Наличие политики исправлений и обновлений для операционных систем является полезным начальным шагом, однако необходимо разработать такую же политику и для приложений. Разработайте такую политику, пользуясь сведениями, доступными в разделе, посвященном передовым методикам. Сначала установите исправления для внешних приложений и приложений Интернета, затем для важных внутренних приложений и, наконец, для не особо важных приложений.

Задания к лабораторной работе №5

Подробно опишите реально существующее или вымышленное малое предприятие: сферу деятельности, состав и структуру информационной системы, особенности организации процесса защиты информации, применяемые методы и средства.

С помощью программы MSAT проведите оценку рисков для предприятия.

Лабораторная работа № 6. Использование цифровых сертификатов.

В ходе данной лабораторной работы мы познакомимся с некоторыми вопросами использования цифровых сертификатов.

Начнем с их использования протоколом SSL/TSL (на самом деле это два разных протокола, но т.к. TSL разработан на базе SSL, принцип использования сертификатов один и тот же). Этот протокол широко применяется в сети Интернет для защиты данных передаваемых между web-серверами и браузером клиента. Для аутентификации сервера в нем используется сертификат X.509.

Для примера обратимся на сайт Ситибанка (www.citibank.ru), в раздел «Мой банк», предназначенный для ведения банковских операций через Интернет (рис.1).

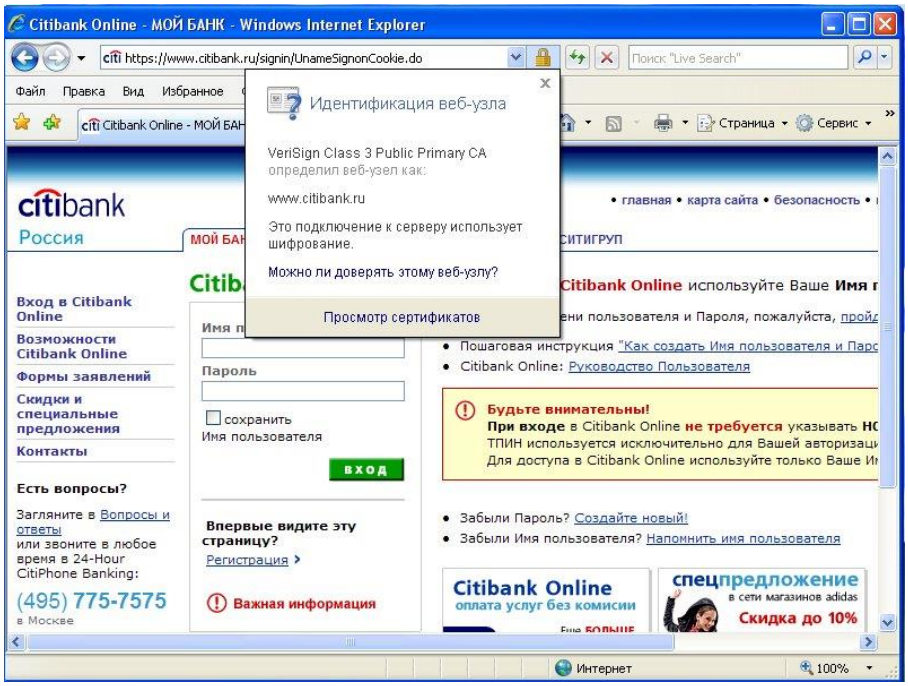


Рис.1. Защищенное соединение.

Префикс https в строке адреса и изображение закрытого замка справа от строки указывают, что установлено защищенное соединение. Если щелкнуть мышью по изображению замка, то увидим представленное на рис. 1 сообщение о том, что подлинность узла с помощью сертификата подтверждает центр сертификации VeriSign. Значит, мы на самом деле обратились на сайт Ситибанка (а не подделанный нарушителями сайт) и можем безопасно вводить логин и пароль.

Выбрав «Просмотр сертификата» можно узнать подробности о получателе и издателе, другие параметры сертификата (рис.2).

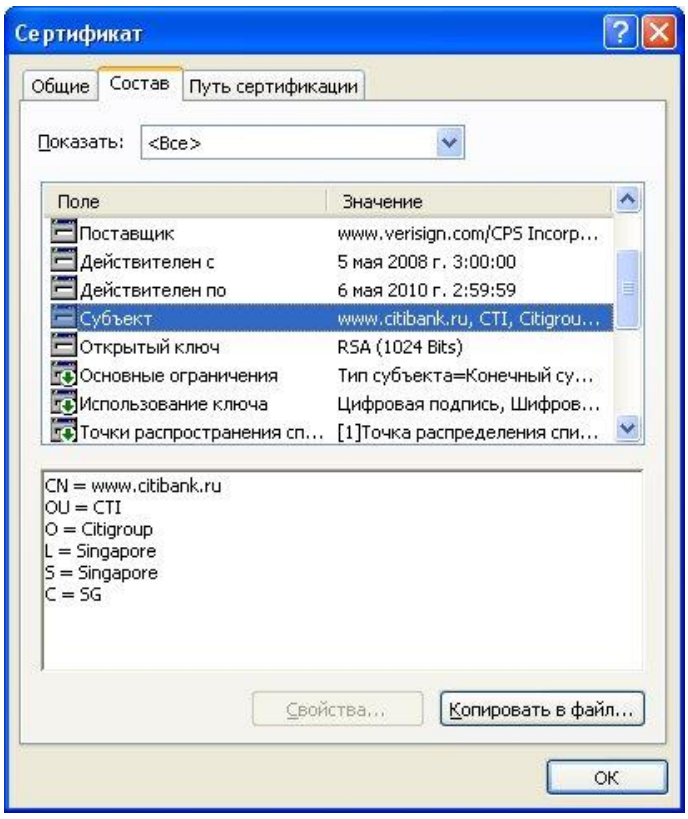


Рис.2 Параметры сертификата.

Задание.

Посмотрите параметры сертификата «электронной сберкассы» Сбербанка – https://esk.sbrf.ru Опишите, кем на какой срок и для какого субъекта сертификат был выдан.

Теперь рассмотрим другой вариант – мы подключаемся по SSL к web-серверу, а браузер не может проверить его подлинность. Подобная ситуация произошла при подключении в раздел Интернет-обслуживания Санкт-Петербургского филиала оператора мобильной связи Tele2 - https://www.selfcare.tele2.ru/work.html (на рис.3).

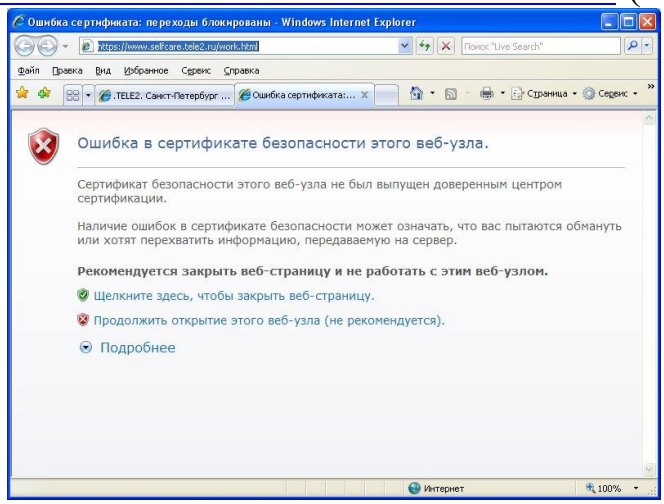


Рис.3. Браузер сообщает о проблеме с сертификатом.

Если нажать ссылка «Продолжить открытие этого web-узла» можно будет просмотреть сертификат.

Задания к лабораторной работе №6

Разберитесь, в чем проблема с указанным сертификатом.

Прим. На всякий случай в конце описания лабораторной приведен ответ.

Теперь рассмотрим, как хранятся сертификаты. Операционная система Windows обеспечивает защищенное хранилище ключей и сертификатов. Работать с хранилищем можно используя настройку консоль управления MMC «Сертификаты».

Из меню Пуск-> Выполнить запустите консоль командой mmc. В меню Консоль выберите Добавить или удалить оснастку, а в списке оснасток выберите Сертификаты. Если будет предложен выбор (а это произойдет, если Вы работаете с правами администратора), выберите пункт «Моей учетной записи».

Таким образом, мы можем просматривать сертификаты текущего пользователя. Если ранее сертификаты не запрашивались, то в разделе «Личные сертификаты» элементов не будет.

В разделе «Доверенные корневые центры сертификации» представлен достаточно обширный список центров, чьи сертификаты поставляются вместе с операционной системой.

Найдите в нем сертификат VeriSign Class 3 Public Primary CA. Благодаря тому, что он уже был установлен, в рассмотренном в начале работы примере с подключением к системам Интернет-банкинга браузер мог подтвердить подлинность узла.

Теперь перейдем к раздел «Сертификаты, к которым нет доверия». Там находятся отозванные сертификаты. Как минимум, там будут находиться два сертификата, которые по ошибке или злому умыслу кто-то получил от имени корпорации Microsoft в центре сертификации VeriSing в 2001 году. Когда это выяснилось, сертификаты отозвали (рис.4).

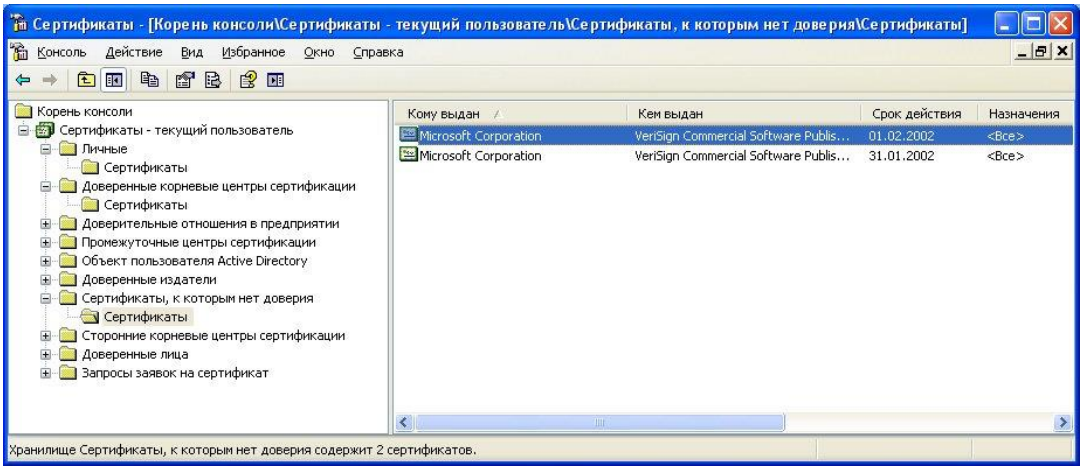


Рис.4. Отозванные сертификаты.

Теперь рассмотрим процесс запроса сертификата. На сайте центра сертификации Thawte http://www.thawte.com можно бесплатно получить сертификат для электронной почты. Для этого в меню сайта Products выберите Free Personal E-Mail Certificates. После этого надо заполнить небольшую анкету, указав имя, фамилию, страну, предпочитаемую кодировку, адрес электронной почты (должен быть обязательно действующим), дальше – пароль и контрольные вопросы для восстановления. Когда все заполнено, на указанный адрес почты будет отправлено письмо со ссылкой для выполнения дельнейших шагов генерации ключей и двумя проверочными значениями, которые нужно ввести, перейдя по ссылке. Таким образом, подлинность и принадлежность адреса будет подтверждена.

Далее система предложит ввести адрес почты (в качестве имя пользователя) и выбранный ранее пароль. После чего можно запросить сертификат X.509. Понадобится указать тип браузера и почтового клиента (например, Internet Explorer и Outlook). После этого потребуется ответить на запросы системы, касающиеся генерации ключей (разрешить выполнение ActiveX элемента, выбрать криптопровайдер, разрешить генерацию).

После завершение этого этапа на почтовый адрес будут выслано второе письмо, подтверждающее запрос сертификата. А спустя некоторое время – третье, со ссылкой для получения сертификата.

Пройдя по ссылке, надо будет снова ввести имя и пароль и на странице нажать кнопку «Install Your Cert» и согласиться с добавлением сертификата.

В результате в оснастке Сертификаты появится личный сертификат выпущенный издателем Thawte Personal Freemail Issuing CA для

субъекта Thawte Freemail Member с указанным вами адресом почты (рис.5).

Если использовать сертификат для защиты почты, дальнейшая настройка зависит от почтового клиента. Если это Microsoft Outlook, можно использовать встроенную в него поддержку протокола S/MIME. В Outlook 2003 для выбора сертификата надо войти в меню Сервис -> Параметры там выбрать вкладку Безопасность и там в параметрах шифрованной электронной почты выбрать используемый сертификат и алгоритмы (рис.6).

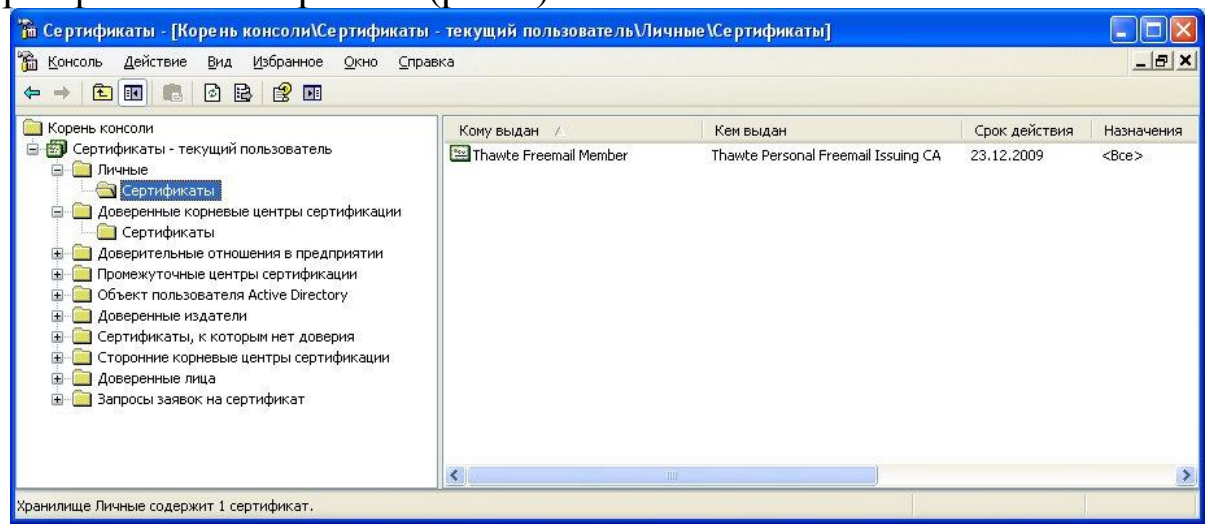


Рис.5. Полученный сертификат.

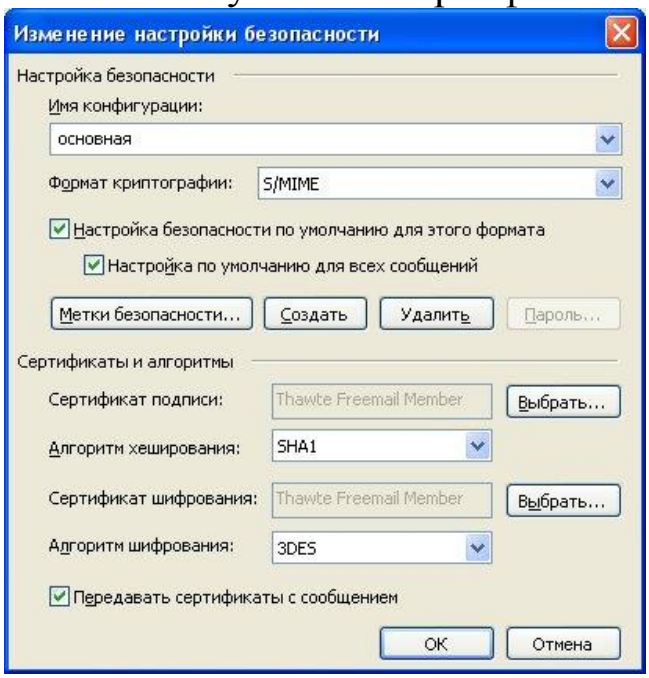


Рис.6. Выбор сертификата для защиты почты с помощью S/MIME в Outlook.

Задания к лабораторной работе №6

Запросите сертификат в Thawte и настройте почтовый клиент для использования S/MIME.

Ответ на задание про сертификат на сайте Tele2

Проблема была в том, что сертификат «самоподписанный»: он был выдан центром сертификации www.selfcare.tele2.ru самому себе. Браузер сообщает о невозможности удостовериться в подлинности узла из-за того, что данный центр сертификации отсутствует в списке доверенных, а проверить его подлинность с помощью «вышестоящего» по иерархии центра не представляется возможным (т.к. вышестоящего центра нет).

Доверять или нет такому сертификату - каждый решает самостоятельно.

Лабораторная работа № 7. Создание центра сертификации (удостоверяющего центра) в Windows Server 2008.

Предыдущая лабораторная работа была посвящена вопросам использования цифровых сертификатов X.509 конечными пользователями. А сейчас мы рассмотрим возможности, которые предоставляет Windows Server 2008 по созданию собственно центра сертификации (Certification Authority – CA) на предприятии.

Соответствующие службы присутствовали в серверных операционных системах семейства Windows, начиная с Windows 2000 Server.

В Windows Server 2008 для того, чтобы сервер смог работать как центр сертификации, требуется сначала добавить серверу роль Active Directory Certificate Services. Делается это помощью оснастки Server Manager, которую можно запустить из раздела Administrative Tools в стартовом меню.

В Server Manager раскроем список ролей и выберем добавление роли (Add Roles) – рис.1.

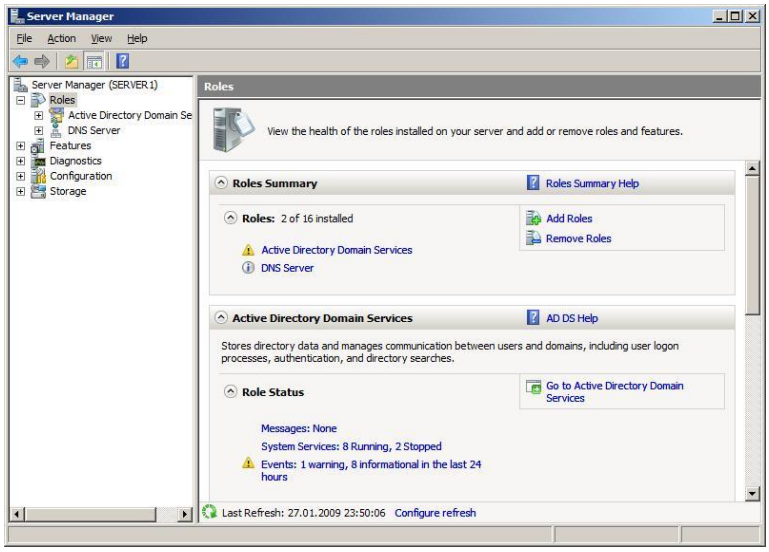


Рис.1. Добавление роли.

В нашем примере, роль добавляется серверу, являющемуся членом домена Windows. Так как это первый CA в домене, он в нашей сети будет играть роль корневого (Root). Рассмотрим по шагам процедуру установки.

В списке доступных ролей выбираем требующуюся нам (Active Directory Certificate Services) и нажимаем Next (рис.2). После этого запускается мастер, который сопровождает процесс установки.

В дополнение к обязательному компоненту «Certification Authority», могут быть установлены дополнительные средства, предоставляющие web-интерфейс для работы пользователей с CA (рис.3). Это может понадобиться, например, для выдачи сертификатов удаленным или внешним, не зарегистрированным в домене, пользователям. Для выполнения данной лабораторной работы это не понадобится.

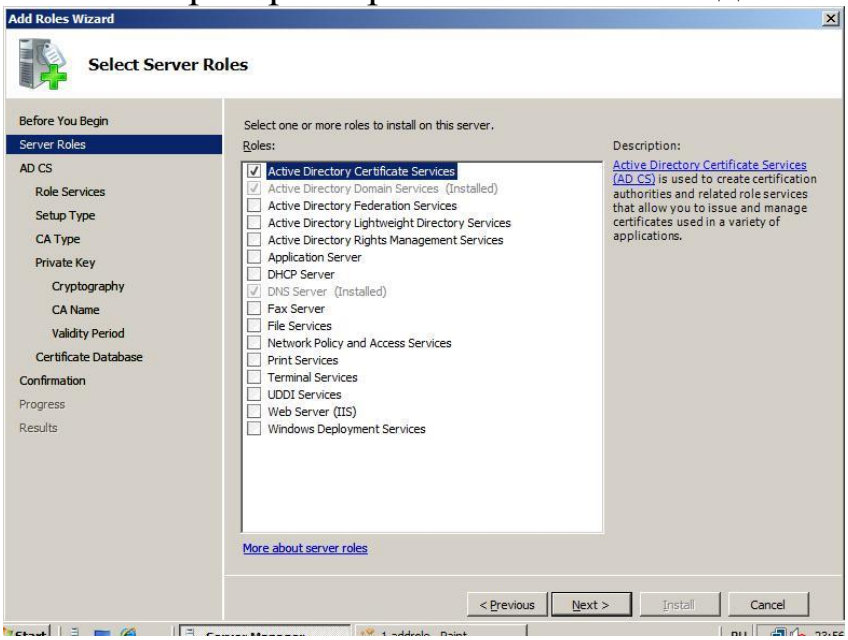


Рис.2. Выбор добавляемой роли.

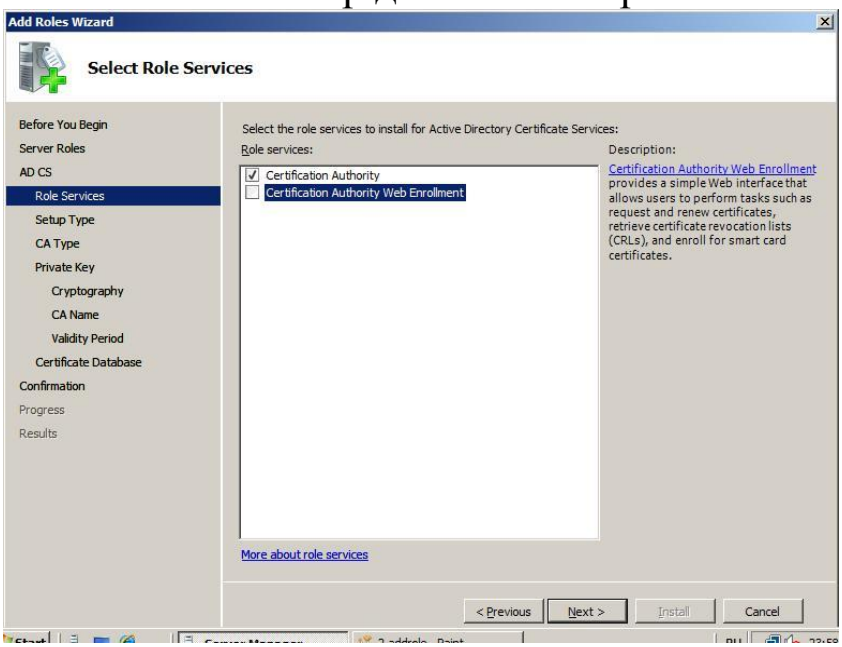


Рис.3. Выбор устанавливаемых компонент.

Следующий шаг – определения типа центра сертификации. Он может быть корпоративным (Enterprise) или отдельностоящим (Standalone) – рис.4. Разница заключается в том, что Enterprise CA может быть установлен только на сервер, являющийся членом домена, т.к. для его работы требуется служба каталога Active Directory. Standalone CA может работать вне домена, например, обрабатывая запросы пользователей, полученные через web-интерфейс. Для выполнения лабораторной работы нужно выбрать версию Enterprise.

Следующее окно мастера позволяет определить, создается корневой (Root) или подчиненный (Subordinate) CA – рис.5. В нашем примере создаваемый CA является первым и единственным, поэтому выбираем вариант Root.

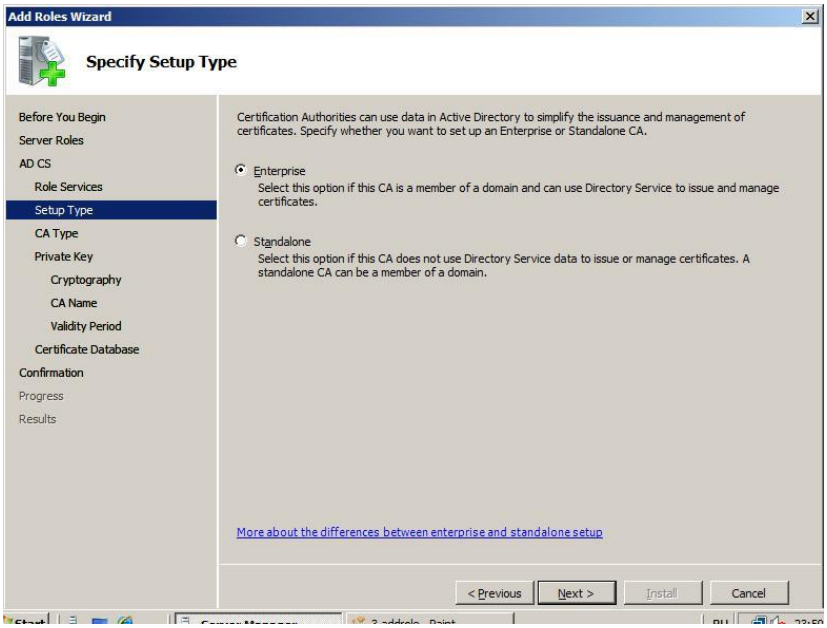


Рис.4. Выбор типа центра сертификации.

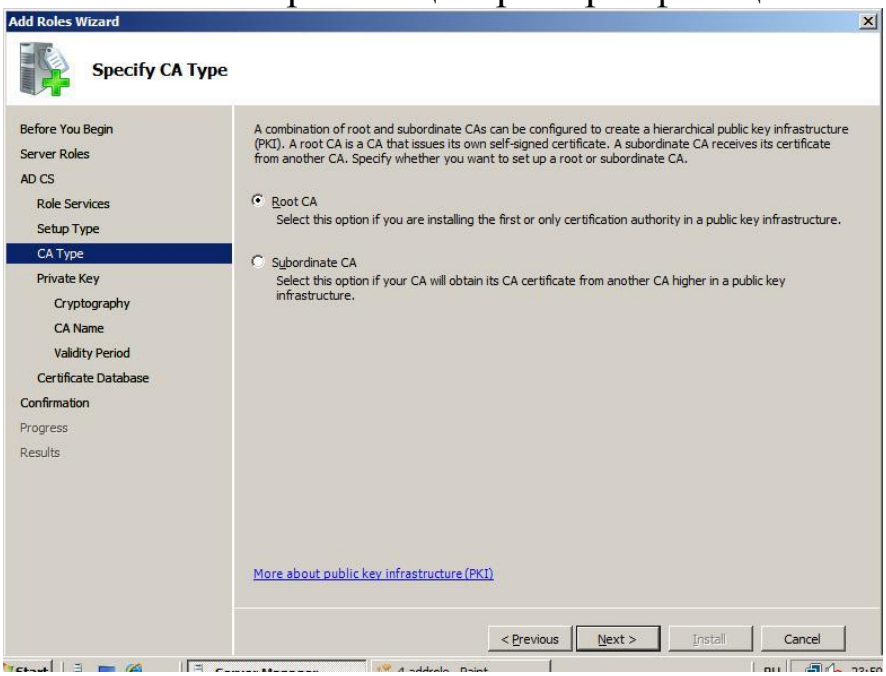


Рис.5. Выбор типа центра сертификации (продолжение).

Создаваемый центр сертификации должен будет использовать при работе как минимум одну ключевую пару – открытый и секретный ключ (иначе он не сможет подписывать выпускаемые сертификаты). Поэтому для продолжения установки мастер запрашивает, нужно ли создать новый секретный ключ или будет использоваться уже существующий (тогда надо будет указать, какой ключ использовать). В нашем примере надо создать новый ключ. При этом, потребуется выбрать «криптографический провайдер» (программный модуль, ре-

ализующий криптоалгоритмы) и алгоритм хеширования. Согласимся с настройками по умолчанию (рис.6).

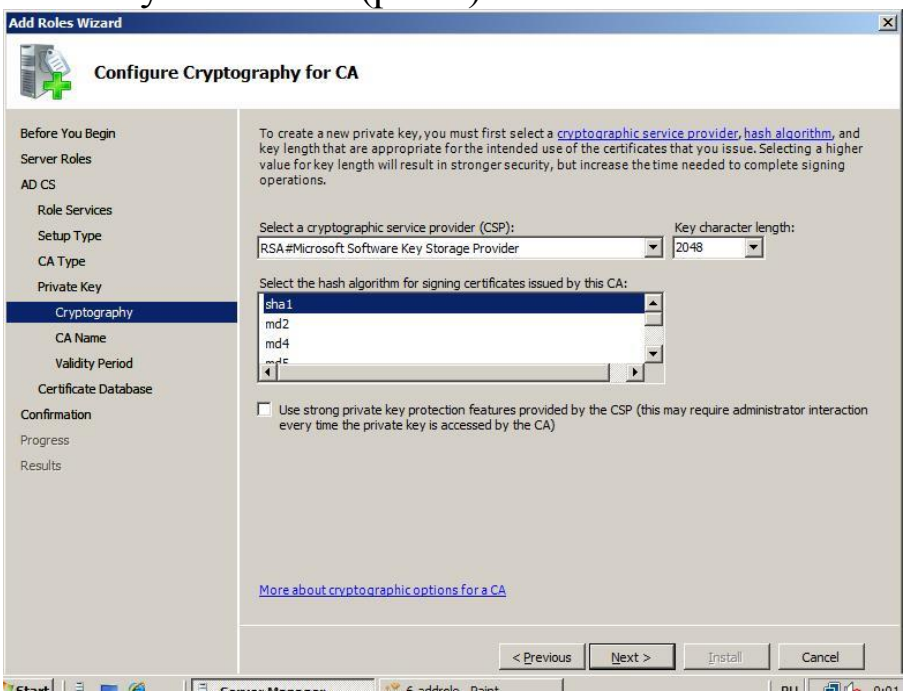


Рис.6. Выбор криптографического провайдера и алгоритма хеширования.

Далее потребуется указать имя CA, размещение базы сертификатов и лог-файлов, и подтвердить сделанные настройки. После этого, роль будет установлена.

Задания к лабораторной работе №7

На учебном сервере или виртуальной машине установите роль Active Directory Certificate Services с настройками, аналогичными рассмотренным выше.

Управлять работой CA можно из оснастки Certification Authority, которая должна появиться в разделе Administrative Tools (рис.7).

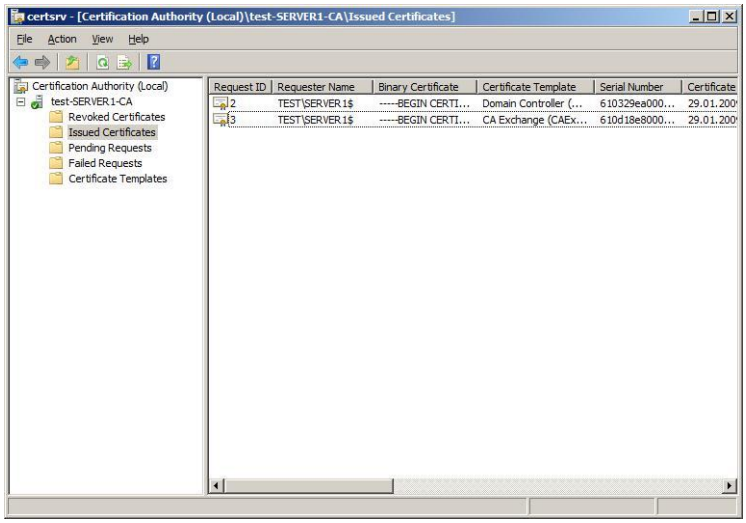


Рис.7. Управление центром сертификации.

Как видно на рисунке, только что установленный Enterprise CA уже выпустил некоторое количество сертификатов для служебных целей (в частности, сертификаты контроллеров домена). В свойствах данного сервера (пункт Properties контекстного меню) можно посмотреть сделанные настройки. В частности, если выбрать закладку Policy Module и там нажать кнопку Properties, можно увидеть текущую настройку, определяющую порядок выдачи сертификатов (рис.8).

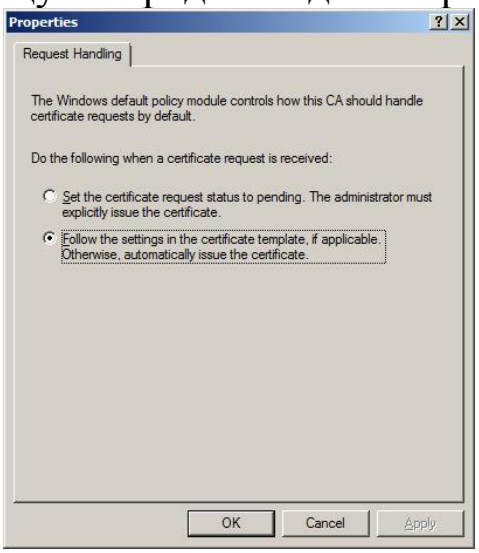


Рис.8. Настройки, определяющие порядок выпуска сертификатов.

В выбранном на рисунке случае, после запроса сертификат выдается в соответствии с настройками шаблона сертификата (или автоматически, если настроек нет). Возможен вариант, когда запрос помещается в очередь ожидающих, и сертификат выпускается только после утверждения администратором.

Задание.

Ознакомьтесь с текущими настройками центра сертификации.

Опишите, какие шаблоны сертификатов (Certificate Templates) определены и для каких целей служит каждый тип сертификатов.
Посмотрите, какие сертификаты выпущены (Issued Certificates), есть ли отозванные сертификаты (Revoked Certificates).
Теперь рассмотрим процесс получения цифрового сертификата. Сделать это можно с помощью оснастки Certificates, с которой мы познакомились в лабораторной № 6. Если она не установлена, запустите консоль mmc и добавьте эту оснастку для текущей учетной записи.
Запустим оснастку, откроем раздел, посвященный сертификатам пользователя (Personal) и запросим сертификат (рис.9). Из перечня предложенных шаблонов сертификатов выберем User. Данный тип сертификатов может использоваться для шифрования файлов с помощью EFS, защиты электронной почты и аутентификации пользователей.
Для пользователя будет сгенерирована ключевая пара, и на основе данных, взятых из базы службы Active Directory и шаблона, будет выпущен сертификат, удостоверяющий открытый ключ.
Этот сертификат будет виден и в оснастке Certification Authority, в списке выпущенных данным сервером.

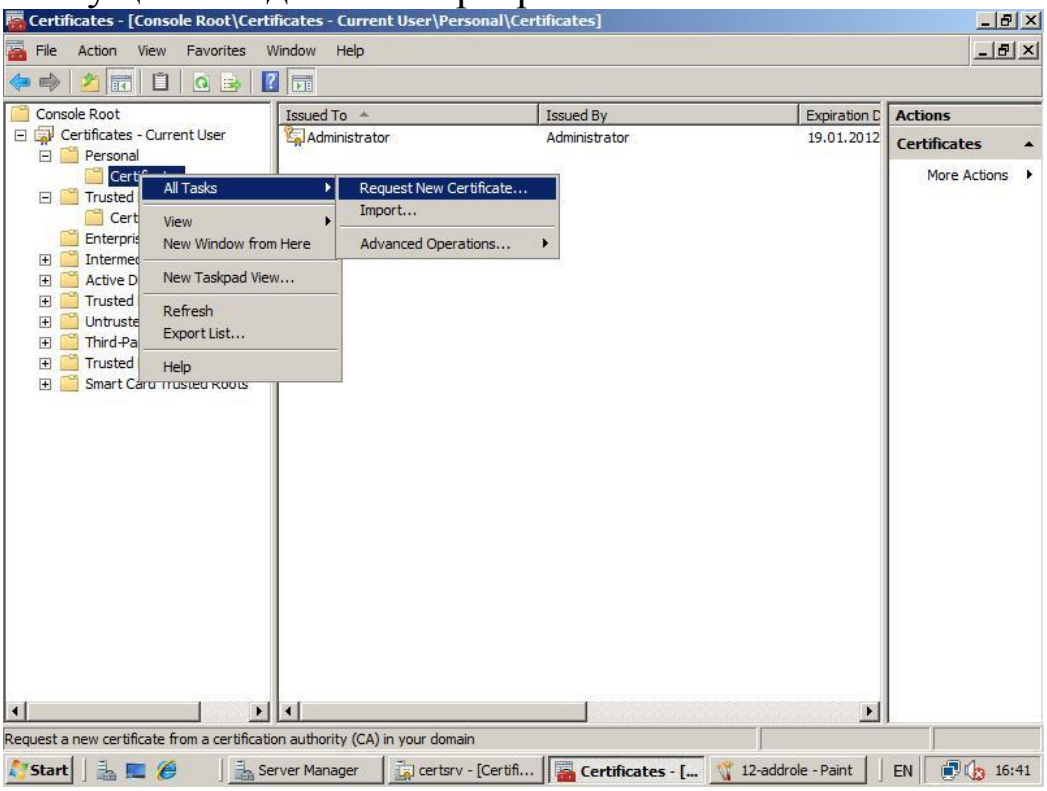


Рис.9. Запрос сертификата.

Задание.

1. Запросите сертификат для одного из пользователей.

2. После получения, изучите состав сертификата, его назначение.
3. Выполните экспорт сертификата (в оснастке Certificates выделите сертификат и в контекстном меню выберите All Tasks -> Export). Обратите внимание, что можно экспортировать только сертификат или сертификат вместе с секретным ключом (private key). Второй вариант надо использовать аккуратно, чтобы кто-нибудь не узнал ваш секретный ключ шифрования. Такой тип экспорта нужен, если вы хотите сохранить резервную копию ключевой пары и сертификата.

Лабораторная работа № 8. Шифрование данных при хранении - EFS.

Шифрующая файловая система (Encrypting File System – EFS) появилась в операционных системах семейства Windows, начиная с Windows 2000. Она позволяет шифровать отдельные папки и файлы на томах с файловой системой NTFS. Рассмотрим этот механизм подробнее.

Сначала несколько слов о рисках, которые можно снизить, внедрив данный механизм. Повышение мобильности пользователей приводит к тому, что большое количество конфиденциальных данных (предприятий или личных) оказывается на дисках ноутбуков, на съемных носителях и т.д. Вероятность того, что подобное устройство будет украдено или временно попадет в чужие руки, существенно выше чем, например, для жесткого диска корпоративного персонального компьютера (хотя и в этом случае, возможны кражи или копирование содержимого накопителей). Если данные хранить в зашифрованном виде, то даже если носитель украден, конфиденциальность данных нарушена не будет. В этом и заключается цель использования EFS.

Следует учитывать, что для передачи по сети, зашифрованный EFS файл будет расшифрован, и для защиты данных в этих случаях надо использовать дополнительные механизмы.

Рассмотрим работу EFS. Пусть, у нас имеется сервер Windows Server 2008, входящий в домен, и три учетные записи, обладающие административными правами на сервере (одна из них - встроенная административная запись Administrator).

Пользователь User1 хочет защитить конфиденциальные файлы. Тут надо отметить, что хотя шифровать с помощью EFS можно и отдельные файлы, рекомендуется применять шифрование целиком к папке.

User1 с помощью оснастки Certificates запрашивает сертификат (можно выбрать шаблон User или Basic EFS). Теперь у него появляется ключевая пара и сертификат открытого ключа, и можно приступать к шифрованию.

Чтобы зашифровать папку, в ее свойствах на вкладке General нажимаем кнопку Advanced и получаем доступ к атрибуту, указывающему на шифрование файла.

Рис.1. В свойствах папки устанавливаем шифрование.

Работа EFS организована так, что одновременно сжатие и шифрование файлов и папок осуществляться не может. Поэтому нельзя разом установить атрибуты Compress contents to save disk и Encrypt contents to secure data (рис.1).

При настройках по умолчанию, зашифрованная папка выделяется в проводнике зеленым цветом. Для зашифровавшего файл пользователя порядок работы с ним не изменится.

Теперь выполним «переключение пользователей» и зайдем в систему под другой учетной записью, обладающей административными правами, но не являющейся встроенной административной записью. Пусть это будет User2.

Несмотря на то, что User2 имеет такие же разрешения на доступ к файлу, что и User1, прочитать он его не сможет (рис.2).

Также он не сможет его скопировать, т.к. для этого надо расшифровать файл. Но надо учитывать, что User2 может удалить или переименовать файл или папку.

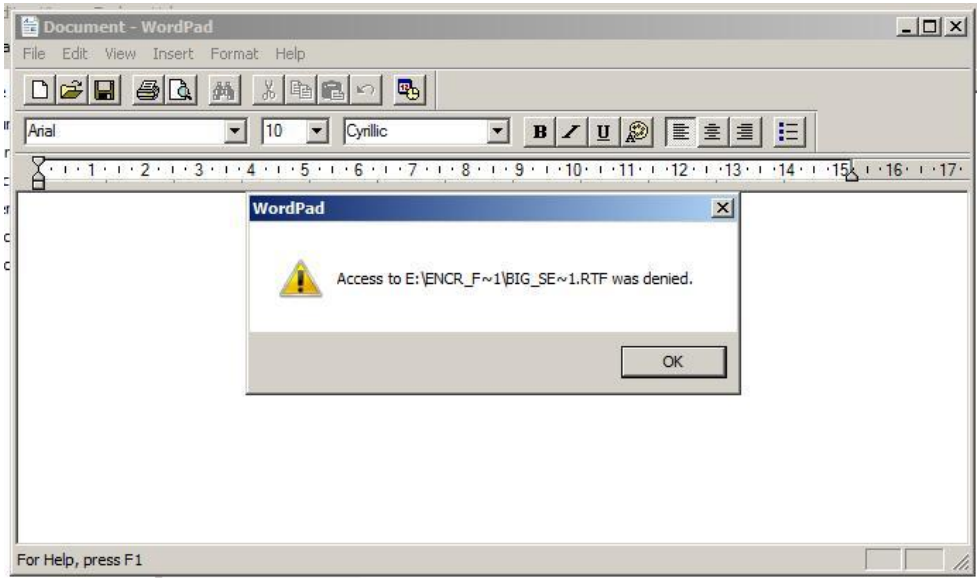


Рис.2. Другой пользователь прочитать файл не сможет.

<u>Задание</u> к лабораторной работе №8

1. Работая под первой учетной записью, запросите сертификат (если он не был получен ранее), после чего зашифруйте папку с тестовым файлом, который не жалко потерять. Проверьте, что будет происходить при добавлении файлов, переименовании папки, копировании ее на другой диск с файловой системой NFTS на том же компьютере, копировании папки на сетевой диск или диск с FAT.
2. Убедитесь, что другой пользователь не сможет прочитать зашифрованный файл.
3. Снова зайдите под первой учетной записью. В оснастке Certificates, удалите сертификат пользователя (несмотря на выдаваемые системой предупреждения). Завершите сессию пользователя в системе и войдите заново. Попробуйте открыть зашифрованный файл.

Как вы убедились, если сертификат и соответствующая ему ключевая пара удалены, пользователь не сможет прочитать зашифрованные им же данные. В частности поэтому, в EFS введена роль агента восстановления. Он может расшифровать зашифрованные другими пользователями данные.

Реализуется это примерно следующим образом. Файл шифруется с помощью симметричного криптоалгоритма на сгенерированном системой случайном ключе (назовем его K1). Ключ K1 шифруется на открытом ключе пользователя, взятом из сертификата, и хранится

вместе с зашифрованным файлом. Также хранится K1, зашифрованный на открытом ключе агента восстановления. Теперь либо пользователь, осуществлявший шифрование, либо агент восстановления могут файл расшифровать.

При настройке по умолчанию роль агента восстановления играет встроенная учетная запись администратора (локального, если компьютер не в домене, или доменная).

Задание.

Зайдите в систему под встроенной учетной записью администратора и расшифруйте папку.

То, какой пользователь является агентом восстановления, задается с помощью групповых политик. Запустим оснастку Group Policy Management. В политике домена найдем группу Public Key Policies и там Encrypting File System, где указан сертификат агента восстановления (рис.3). Редактируя политику (пункт Edit в контекстном меню, далее Policies->Windows Settings-> Security Settings -> Public Key Policies -> Encrypting File System), можно отказаться от присутствия агентов восстановления в системе или наоборот, указать более одного агента (рис.4).

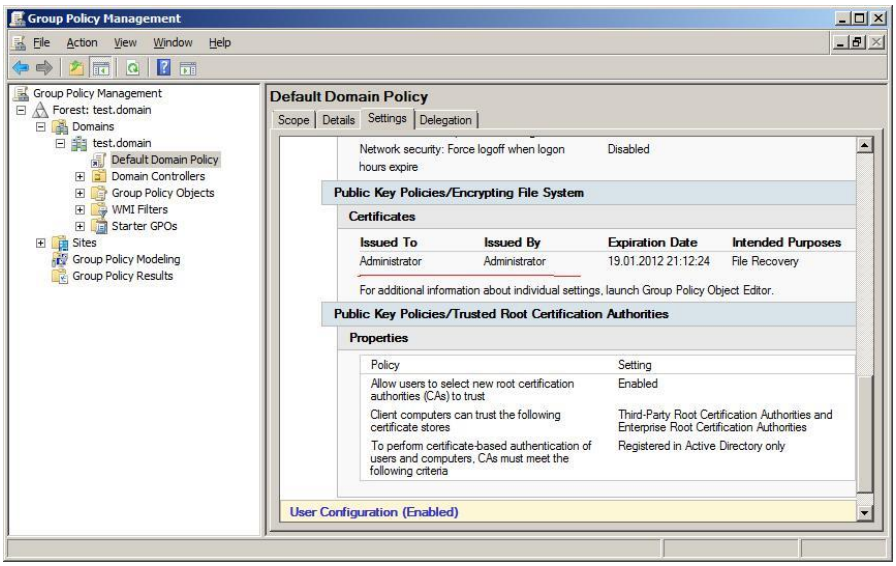


Рис.3. Агент восстановления.

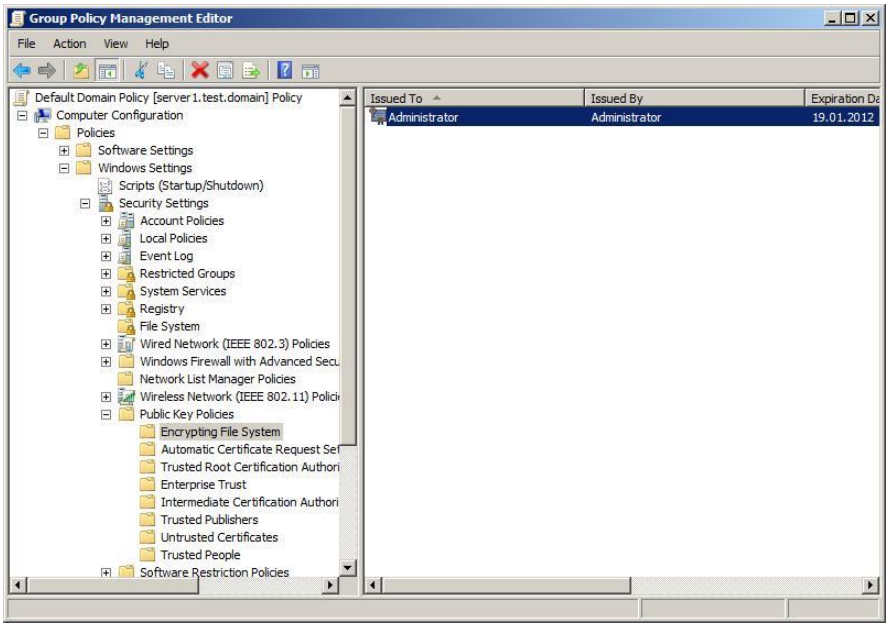


Рис.4. Изменение агента восстановления.

Задание.

1. Отредактируйте политику таким образом, чтобы убрать из системы агента восстановления (удалите в политике сертификат). Выполнив команду «gpupdate /force» (меню Start->run-> gpupdate /force) примените политику.
2. Повторив действия из предыдущих заданий, убедитесь, что теперь только тот пользователь, который зашифровал файл, может его расшифровать.
3. Теперь вернем в систему агента восстановления, но будем использовать новый сертификат. В редакторе политик находим политику Encrypting File System и в контекстном меню выбираем Create Data Recovery Agent. Это приведет к тому, что пользователь Administrator получит новый сертификат и с этого момента сможет восстанавливать шифруемые файлы.

Теперь рассмотрим, как можно предоставить доступ к зашифрованному файлу более чем одному пользователю. Такая настройка возможна, но делается она для каждого файла в отдельности.

В свойствах зашифрованного файла откроем окно с дополнительными параметрами, аналогичное представленному на рис.1 для папки. Если нажать кнопку Details, будут выведены подробности относительно того, кто может получить доступ к файлу. На рис. 5 видно, что в данный момент это пользователь User1 и агент восстановления Administrator. Нажав кнопку Add можно указать сер-

тификаты других пользователей, которым предоставляется доступ к файлу.

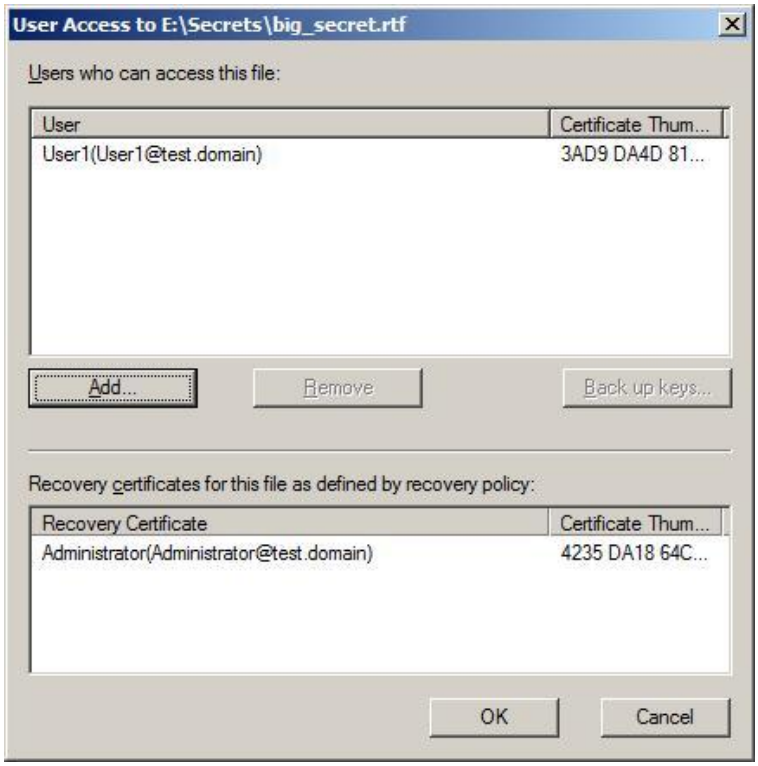


Рис.5. Данные о пользователях, которые могут расшифровать файл.

Задание.

Зашифруйте файл. Предоставьте другому пользователю, не являющемуся агентом восстановления, возможность также расшифровать данный файл. Проверьте работу выполненных настроек.

Лабораторная работа № 9. Управление разрешениями на файлы и папки.

Данная лабораторная работа посвящена вопросам управления разрешениями на файлы и папки Windows. Правильно настроенное управление доступом к файлам позволяет избежать многих проблем, связанных с безопасностью, как на рабочей станции, так и на серверах (в особенности, выполняющих роль файлового сервера).

Начнем с небольшого теоретического обзора.

Пользователи (как доменные, так и локальные), группы пользователей и компьютеры (далее будем называть их всех субъектами) имеют уникальные идентификаторы безопасности – SID. Под этим

идентификатором система и «знает» субъекта. SID имеет уникальное значение в пределах домена и формируется во время создания пользователя или группы, либо когда компьютер регистрируется в домене.

Когда пользователь при входе в систему вводит имя и пароль, ОС выполняет проверку правильности пароля и, если пароль правильный, создает маркер доступа для пользователя. Маркер включает в себя SID пользователя и все SID'ы групп, в которые данный пользователь входит.

Для объектов подлежащих защите (таких как файлы, папки, реестр Windows) создается дескриптор безопасности. С ним связывается список управления доступом (Access Control List – ACL), который содержит информацию о том, каким субъектам даны те или иные права на доступ к данному объекту. Чтобы определить, можно ли предоставить запрашиваемый субъектом тип доступа к объекту, ОС сравнивает SID в маркере доступа субъекта с SID, содержащимися в ACL.

Разрешения суммируются, при этом запрещения являются более приоритетными, чем разрешения. Например, если у пользователя есть разрешение на чтение файла, а у группы, в которую он входит – на запись, то в результате пользователь сможет и читать, и записывать. Если у пользователя есть разрешение на чтение, а группе, в которую он входит, чтение запрещено, то пользователь не сможет прочитать файл.

Если говорить о файлах и папках, то механизмы защиты на уровне файловой системы поддерживаются только на дисках с файловой системой NTFS. Файловая система FAT (и ее разновидность – FAT32) не предполагает возможности хранения ACL, связанного с файлом.

Теперь перейдем к практической части работы. Выполняться она будет на компьютере с операционной системой Windows Server 2008, входящем в домен. Для выполнения работы понадобятся две учетные записи – администратора (далее будем называть его Administrator) и пользователя, не входящего в группу администраторов (будем называть его TestUser). Также понадобится тестовая группа (TestGroup). Все группы и учетные записи доменные, поэтому управление ими будем производить с помощью оснастки Active Directory Users and Computers.

Начнем с того, что работая под учетной записью Administrator, создадим новую папку Test. В ее свойствах выберем вкладку Security (рис.1). В отличие от предыдущих версий операционных систем Windows, в Windows Vista и Windows Server 2008 на этой вкладке можно только просматривать имеющиеся разрешения. Чтобы их изменять, надо нажать кнопку Edit, что даст возможность изменять список контроля доступа к файлу (рис.2).

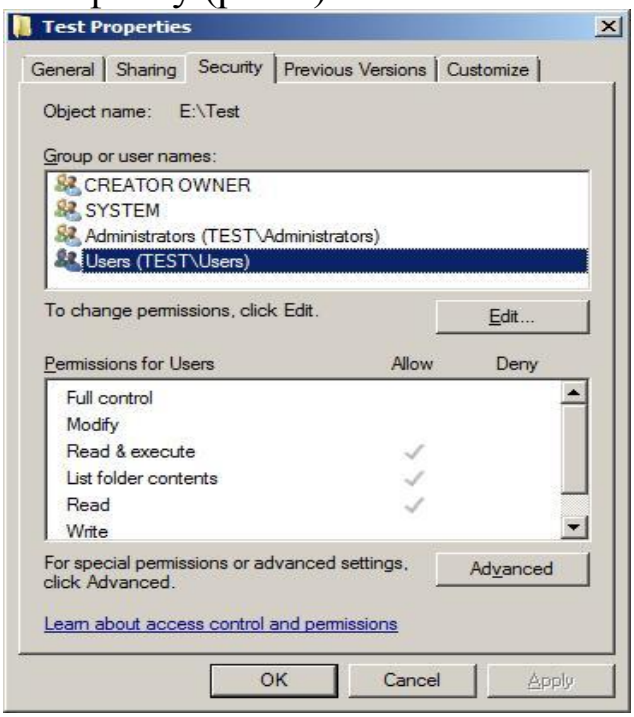


Рис.1. Просмотр разрешений.

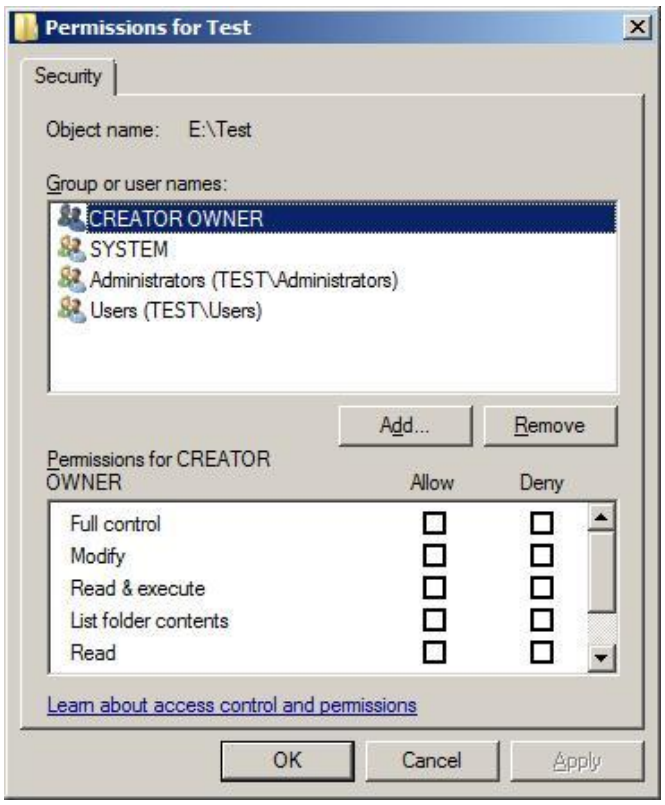


Рис.2. Изменение разрешений.

Задания к лабораторной работе №9

Выполните действия, аналогичные описанным выше. Убедитесь, что пользователь TestUser отсутствует в списке доступа к папке, но есть в группе Users (последнее проверяется с помощью оснастки Active Directory Users and Computers, т.к. пользователь и группа доменные).

Выполните переключение пользователей, зайдите в систему под учетной записью TestUser, попробуйте открыть папку и создать в ней новый файл. Какие из этих действий удались? Почему ?

Снова выполните переключение пользователей. Под учетной записью Administrator добавьте в список доступа к файлу пользователя TestUser и дайте ему разрешение на изменение (modify). Пробуйте снова выполнить задание.

Как мы убедились, можно добавлять пользователей в список доступа. Теперь попробуем под учетной записью Administrator удалить группу Users. Сделать это не удастся и появится предупреждение (рис.3) о том, что эти разрешения наследуются от родительского объекта. Для того, чтобы отменить наследование надо на вкладке Security (рис.1) нажать кнопку Advanced. В появившемся окне (рис.4) видно,

что отмечено свойство Include inheritable permissions from this object's parent. Это значит, что объект наследует родительский ACL, а в его собственный можно только добавлять разрешения или запрещения. Если нажать кнопку Edit и сбросить эту галочку будет задан вопрос, что делать с унаследованным списком – его можно скопировать (Copy) в ACL объекта или убрать (Remove). Чаще всего, чтобы не потерять нужные настройки, выполняется копирование, а потом уже список исправляется.

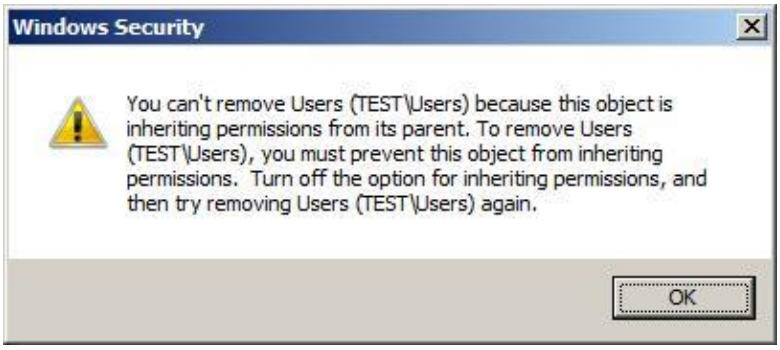


Рис.3. Предупреждение.

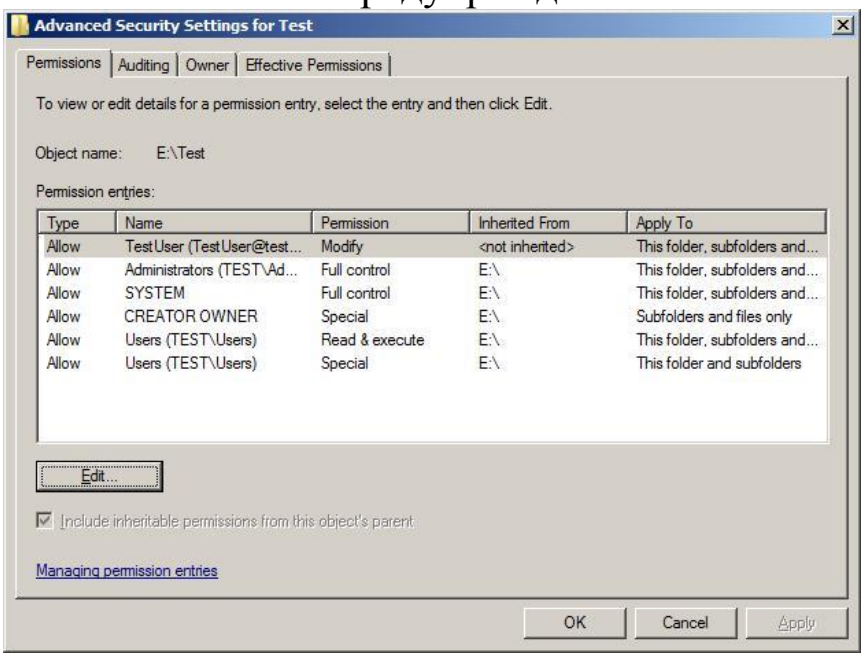


Рис.4. Дополнительные параметры безопасности.

Задание.

Удалите группу Users из ACL для папки.

Если редактировать разрешения пользователя из окна дополнительных параметров безопасности, то увидим список разрешений, отличный от того, что был ранее (рис.5).

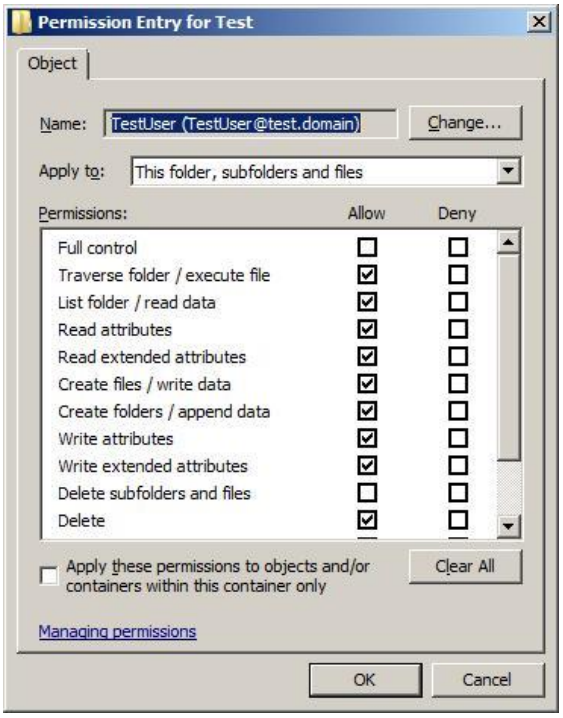


Рис.5. Специальные разрешения.

Это так называемые специальные разрешения. Виденные ранее стандартные разрешения (чтение/read, запись/write и т.д.) состоят из специальных. Соответствие между ними описано на рис.6 (набор разрешений для папок и файлов несколько отличается, но понять какие к чему относятся можно по названиям). Более подробно с этой темой можно ознакомиться, например, по справочной системе Windows.

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

Рис.6. Соответствие между специальными и стандартными разрешениями.

Как уже ранее отмечалось, при определении разрешения на доступ, учитываются разрешения и запрещения, как для самого пользо-

вателя, так и для всех групп, в которые он входит. Для того, чтобы узнать действующее (эффективное) разрешение, можно воспользоваться вкладкой Effective Permissions (рис.4). Там, нажав кнопку Select, можно выбрать пользователя или группу, для которой будет показано эффективное разрешение.

Задание.

Проверьте, чтобы у пользователя TestUser на папку, с которой работаем, было разрешение modify. Проверьте действующее эффективное разрешение.

Не заканчивая сеанса пользователя, переключитесь в сеанс пользователя Administrator. Добавьте в список разрешений на папку запрещение для группы TestGroup всех видов доступа (выберите Deny для разрешения Full Control). Внесите пользователя TestUser в группу TestGroup. Посмотрите эффективное разрешение для пользователя TestUser.

Переключитесь в сеанс пользователя TestUser. Попробуйте открыть папку и создать документ. Завершите сеанс TestUser (выполните выход из системы) и снова войдите в систему. Повторно попробуйте открыть папку и создать документ. Как можно объяснить полученный результат (подсказка есть в начале описания лабораторной)?

Теперь рассмотрим вопросы, связанные с владением папкой или файлом. Пользователь, создавший папку или файл, становится ее владельцем. Текущего владельца объекта можно узнать, если в окне дополнительных параметров безопасности (рис.4) выбрать вкладку Owner.

Владелец файла может изменять разрешения на доступ к этому файлу, даже в том случае, если ему самому доступ запрещен.

Порядок смены владельца файла в Windows Server 2008 отличается от того, что было в предыдущих версиях ОС. Ранее, администратор или пользователь, имеющий на файл (папку) право Take Ownership могли стать владельцами файла. Причем, владельцем мог быть или конкретный пользователь, или группа Администраторы (Adminisrators) – другую группу владельцем было не назначить.

В Windows Server 2008 администратор (или член группы администраторов) может не только сам стать владельцем, но и передать право владения произвольному пользователю или группе. Но эта опера-

ция рассматривается как привилегированная, и доступна не всякому пользователю, имеющему право на файл.

На рис. 7 показано, что Администратор сделал владельцем папки Test группу TestGroup.

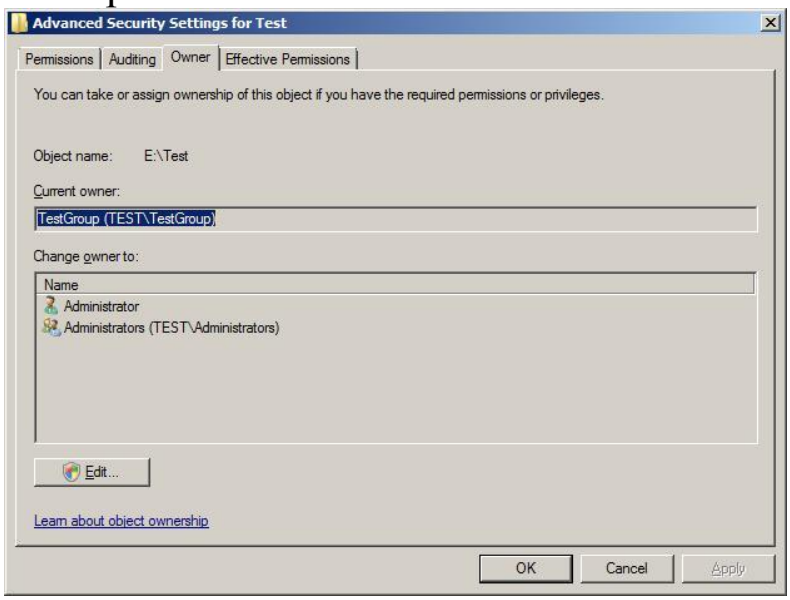


Рис.7. Смена владельца объекта.

Задание.

Выполните передачу права владения группе TestGroup, куда входит пользователь TestUser. Зайдя под этой учетной записью, измените разрешения так, чтобы TestUser смог работать с папкой.

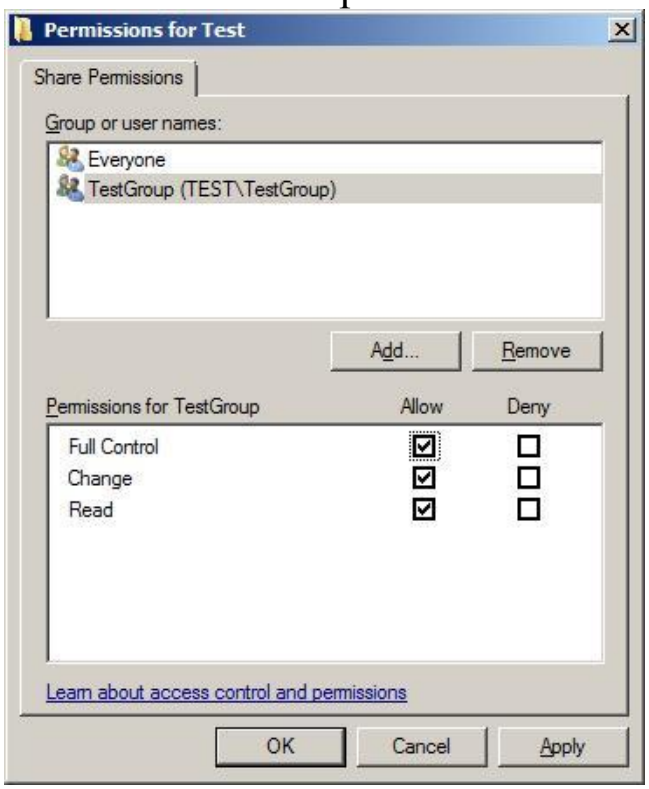


Рис.8. Разрешения на общую папку.

При использовании компьютера с Windows Server 2008 в качестве файлового сервера, важно учитывать, что на предоставляемые в общий доступ папки, отдельно устанавливаются разрешения, регулирующие доступ к ним по сети. Сделать это можно в свойствах папки на вкладке Sharing (рис.8). В этом случае, при доступе по сети действуют и разрешения на общую папку, и разрешения NTFS. В результате получаем наиболее строгие ограничения. Например, если на общую папку установлено «только чтение», а в разрешениях NTFS – «изменение», то в итоге, подключающийся по сети пользователь сможет только читать файлы. А тот же пользователь при локальном доступе получает право на изменение (разрешения на общую папку влиять не будут).

Лабораторная работа №10. Настройка протокола IPSec.

В данной лабораторной работе мы рассмотрим порядок настройки защищенного с помощью протокола IPSec соединения между клиентом и сервером.

Итак, у нас есть домен test.domain, в который входит сервер Server1, работающий под управлением операционной системы Windows Server 2008. В домен также входит рабочая станция Vista1, которая работает под управлением ОС Windows Vista. В домене развернут центр сертификации.

Целью работы является настройка протокола IPSec для шифрования всех данных, передаваемых между указанным сервером и рабочей станцией.

Для работы с политиками IPSec существует оснастка IPSecurity Policy Management. Если запустить консоль mmc и добавить эту оснастку, появится запрос, для какого объекта будет использоваться оснастка (рис.1)

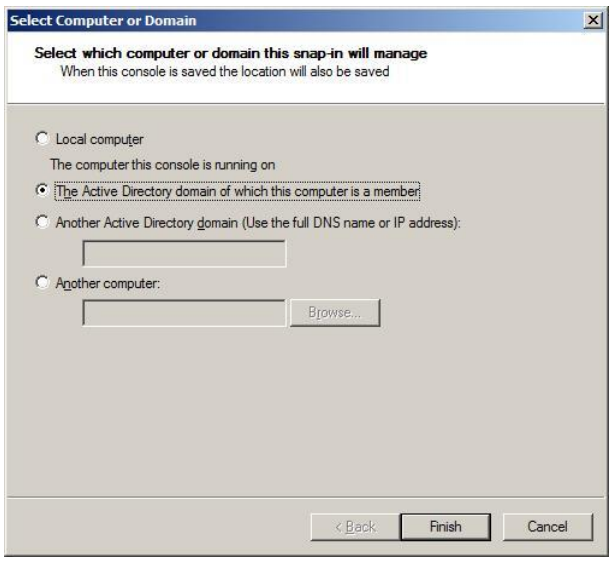


Рис.1. Выбираем объект для работы.

Настройку будем делать с помощью доменной политики, что и выбираем.

В ней существуют уже три предопределенные политики (рис.2). Но нам нужна будет новая, управляющая работой конкретного сервера и клиента. Поэтому в контекстном меню выбираем пункт Create new security policy. И по запросу мастера назначаем ей имя Server1_Vista1.

Настройка в следующее окне понадобится в случае, если используются предыдущие (по сравнению с Windows Server 2008 / Windows Vista) версии операционных систем.

Выбрав в окне (рис.4) пункт Edit Properties переходим непосредственно к созданию настроек.

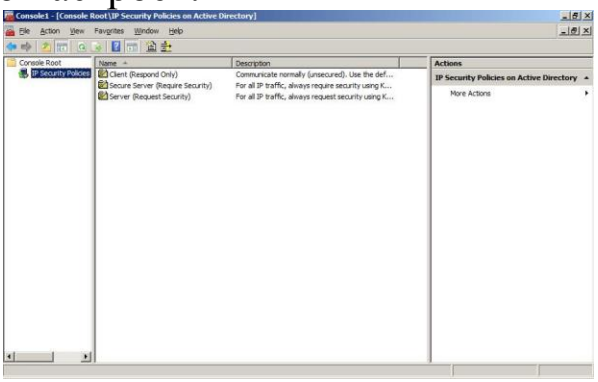


Рис.2. Предопределенные политики IPSec.

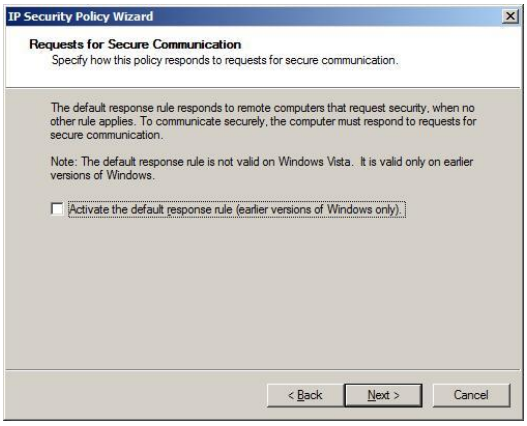


Рис.3. Окно мастера IP Security Policy.

Рис.4 Окно мастера IP Security Policy.

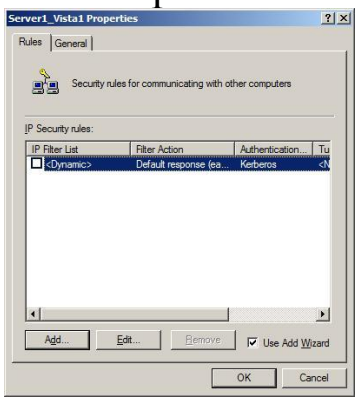


Рис.5 Добавляем правило.

Нам понадобится новое правило, поэтому в окне, представленном на рис.5 нажимаем кнопку Add. В следующем окне указываем, надо ли определять туннель. Так как мы планируем использовать IPSec в транспортном режиме, это не понадобится.

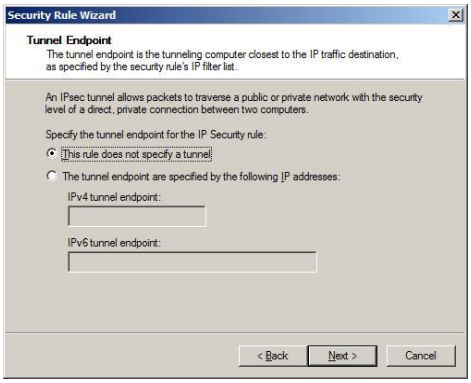


Рис.6. Выбор типа соединения.

Следующий запрос касается того, для каких подключений действует правило – для всех, подключений из локальной сети или извне. Нас устроит вариант «для всех» (All network connections). После этого, будет предложено определить, в отношении какого типа трафика действует создаваемая политика (рис.7).

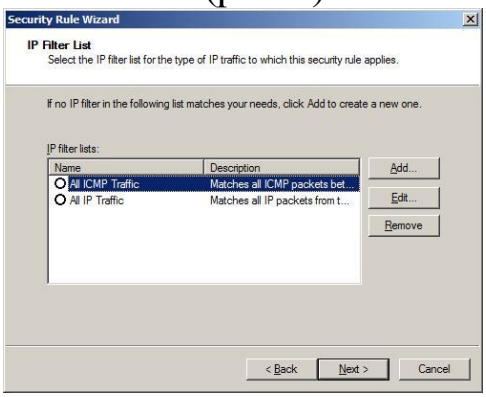


Рис.7 Фильтры позволяют определить, какие пакеты будут защищаться IPSec.

Предустановленные правила нас не устраивают, т.к. нам нужно защищенное соединение между двумя конкретными узлами. Нажимаем кнопку Add, чтобы добавить новый список фильтров (рис.8). Задаем ему имя и нажимаем кнопку Add, что приводит к запуску очередного мастера.

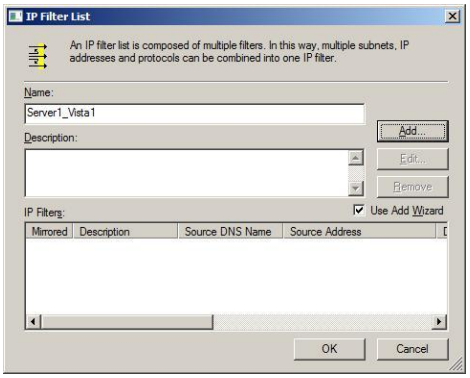


Рис.8. Добавляем новый список фильтров.

Работая с мастером, определим источник (source) пакетов (в выпадающем списке выберем A specific DNS name и укажем имя Vista1.test.domain, для простоты будем считать, что IP-адрес этого хоста неизменен), получатель server1.test.domain. Далее можно выбрать защищаемый протокол. В нашем примере – любой (Any).

Таким образом, мы создали фильтр и теперь нужно отметить его, как использующийся (рис.9).

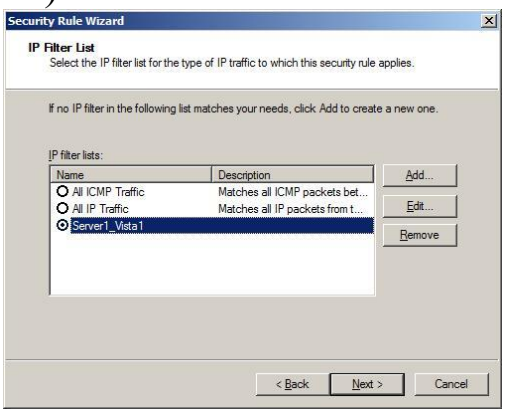


Рис.9. Выбираем созданный фильтр.

В следующем окне запрашивается действие, если приходит незащищенный пакет. Его можно принять, при этом отвечая защищенной посылкой, а можно заблокировать (для этого предопределенного правила нет, нужно создать новое, нажав кнопку Add). Выбранный на рис.10 вариант Require Security предполагает, что сервер может принимать незащищенные пакеты, но в ответ предлагает установку защищенного соединения.

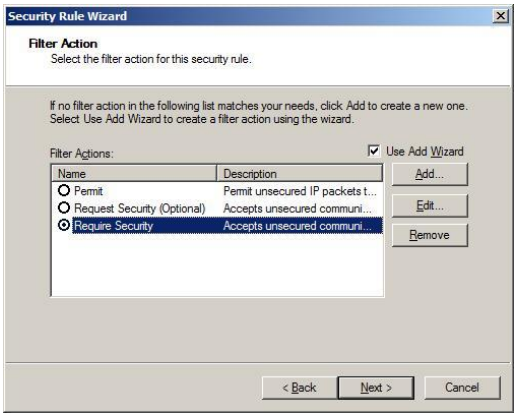


Рис.10.Действия при получении незащищенного пакета.

Далее предлагается выбрать метод аутентификации (рис.11). Выбор делается между Kerberos, сертификацией на основе цифровых сертификатов и предопределенным ключом. Последний вариант наименее надежен. Что же касается первых двух, то если подключения производятся внутри домена, можно выбрать Kerberos. Если узел внешний,

но например, для него нашим корпоративным центром сертификации выпущен сертификат, можно применить второй метод аутентификации.

Таким образом, мы создали новую политику. Теперь ее надо назначить (Assign). Сделать это можно в редакторе доменной политики (Start-> Administrative Tools-> Group Policy Management найти Default Domain Policy и в контекстном меню выбрать Edit, после чего в разделе Computer Configuration ->Policies-> Windows Settings->Security Settings найти политики IPSec, выбрать нужную и в контекстном меню выбрать Assign – рис.12).

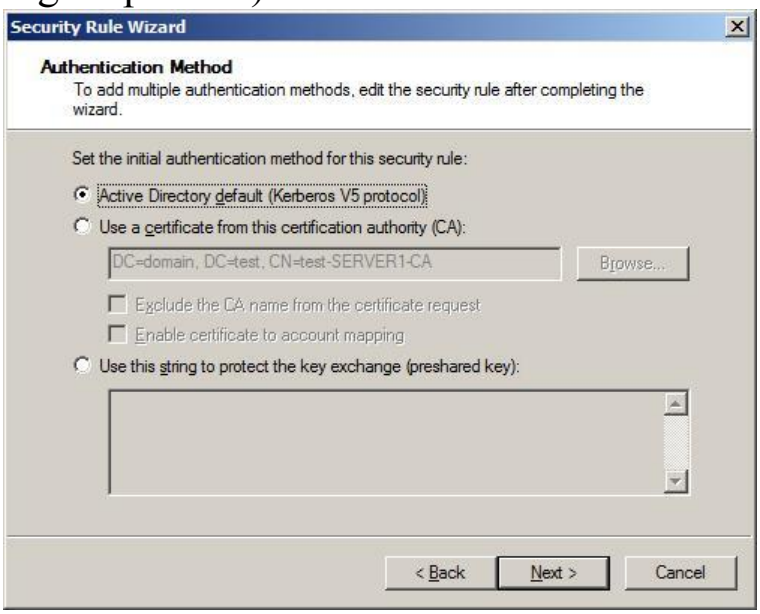


Рис.11. Выбор метода аутентификации.

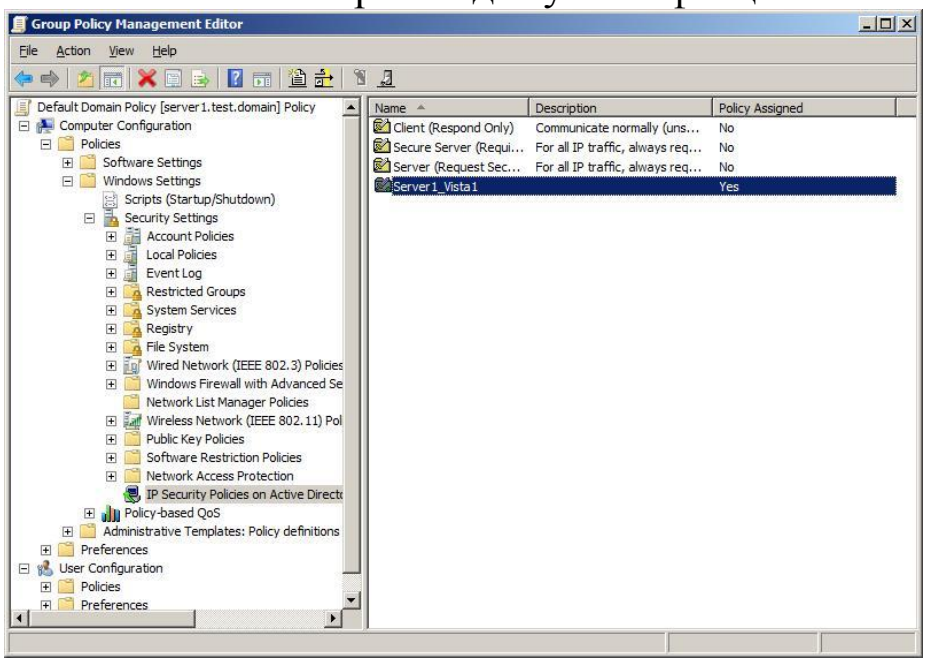


Рис.12.Назначение политики.

Задания к лабораторной работе №10

Создайте политику IPSec.

Применив политику, проверьте соединение между компьютерами.

Вполне возможно, что сразу установить соединение не получится. Проблемы может вызвать использование межсетевых экранов (как встроенных в Windows, так и отдельных решений), трансляция адресов (NAT), если она применяется. Возможны и другие причины.

При выяснении причин неправильной работы может использоваться оснастка MMC IPSec Monitor (по умолчанию она не устанавливается, ее надо добавлять) – рис.13.

Помощь может также оказать использование утилиты Network Monitor и анализ журналов межсетевых экранов (для встроенного МЭ Windows порядок работы описан в предыдущей лабораторной).

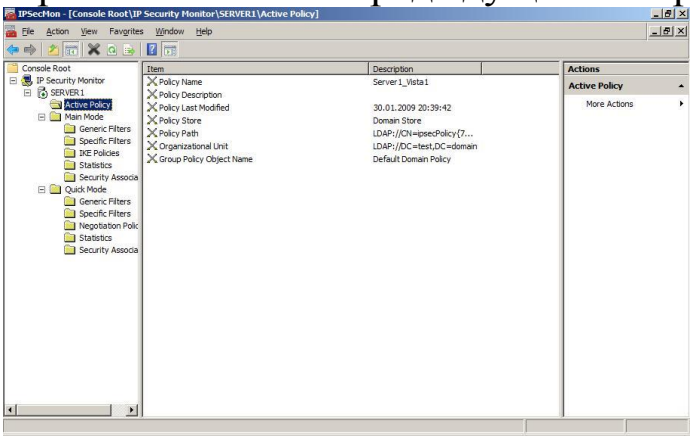


Рис.13 Оснастка IPSec Monitor.

Лабораторная работа №11. Основные признаки присутствия на компьютере вредоносных программ

Аннотация: Эта лабораторная работа позволяет получить практические навыки по выявлению вредоносных программ на локальном компьютере под управлением Microsoft Windows NT -подобной операционной системы. В процессе выполнения этой работы будут изучены явные признаки заражения компьютера на примере модификации настроек браузера, исследованы возможные места скрытых проявлений: запущенные процессы, элементы автозапуска, сетевая активность.

Ключевые слова:

Сценарий. Умение своевременно найти и обезвредить вредоносную программу - один из ключевых навыков компьютерной грамотности. Для этого необходимо знать основные признаки присутствия вируса,

уметь оценивать действия, выполняемые той или иной программой на предмет их вредоносности и знать, что в первую очередь следует предпринять, если компьютер все же оказался заражен.

Все виды проявлений вируса на компьютере можно разбить на три группы: явные, косвенные и скрытые. К первым относятся изменение настроек браузера, всплывающие сообщения и несанкционированный дозвон в Интернет. К косвенным можно отнести блокирование работы антивируса, доступа к сайтам антивирусных компаний, сбои в работе системы или других приложений, почтовые уведомления о рассылаемых Вами вирусах. Первое задание этой лабораторной работы посвящено изучению явных признаков на примере несанкционированного изменения настроек браузера.

Некоторые вредоносные программы умеют достаточно хорошо скрывать от пользователя свою деятельность - такие проявления, называемые скрытыми, обычно под силу обнаружить только антивирусной программе. Однако в любом случае, если возникло хоть малейшее подозрение на наличие вируса, необходимо уметь провести простейшую диагностику системы, чтобы либо подтвердить заражение, или опровергнуть его. Во втором задании этой лабораторной работы изучается список запущенных на компьютере процессов (фактически, список работающих в данный момент программ), в третьем - элементы автозапуска, а четвертое посвящено исследованию сетевой активности.

Подготовка

Перед началом лабораторной работы убедитесь, что Ваш компьютер:

- Включен
- На нем загружена операционная система **Microsoft Windows XP** или **Microsoft Windows 2000 Professional**
- Выполнен вход в систему под учетной записью, обладающей правами администратора

Задание к лабораторной №11.

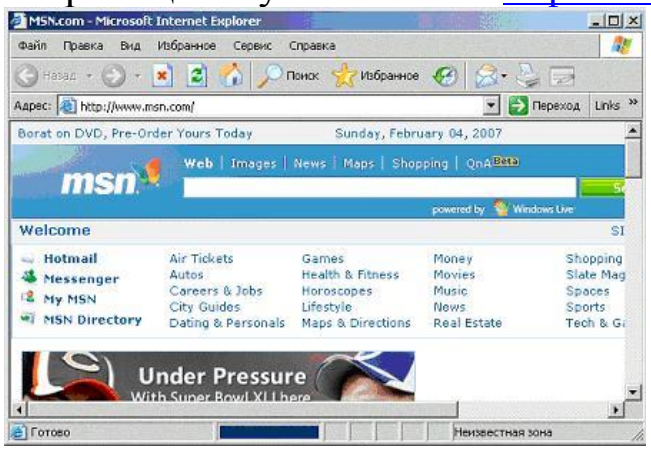
Изучение настроек браузера

Как уже говорилось выше, вирусные проявления бывают явными, косвенными и скрытыми. Если первые обычно видны невооруженным глазом, то косвенные и тем более скрытые требуют от пользова-

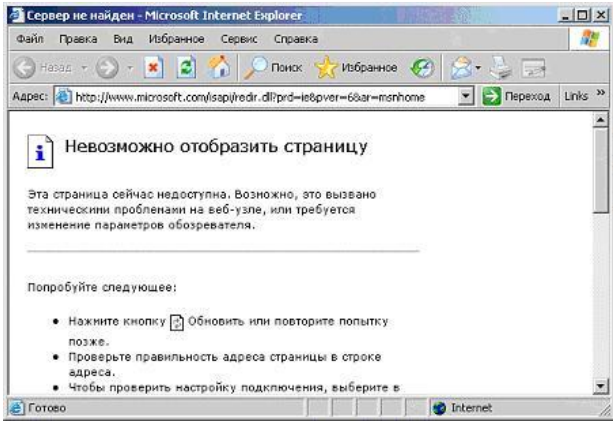
теля проявления изрядной доли интуиции. Они часто не мешают работе и для их обнаружения требуется знать где и что нужно искать.
Явные проявления обычно выражаются в неожиданно появляющихся рекламных сообщениях и баннерах - обычно это следствие проникновения на компьютер рекламной утилиты. Поскольку их 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. Они вынуждены быть явными, поскольку используемые ими приложения сложно использовать незаметно от пользователя.
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

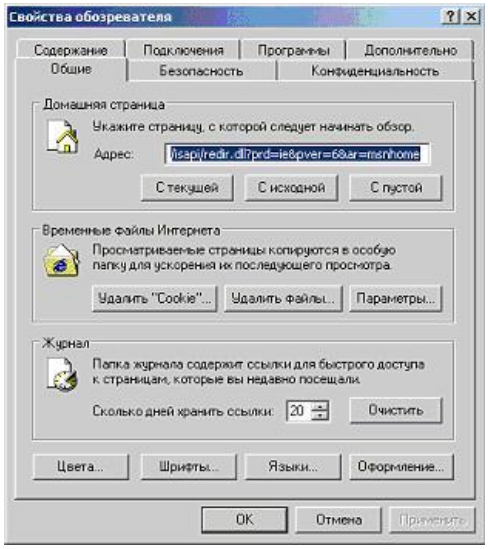


Если доступ в Интернет не настроен, то выведется соответствующее уведомление:

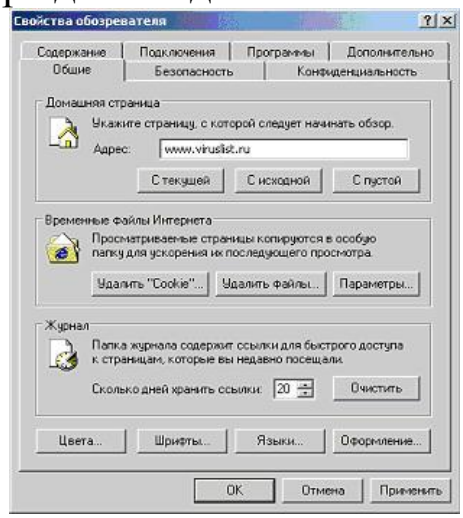


3. Проверьте значение параметра, отвечающего за стартовую страницу. Для этого нужно воспользоваться меню **Сервис**. Откройте его и выберите пункт **Свойства обозревателя**

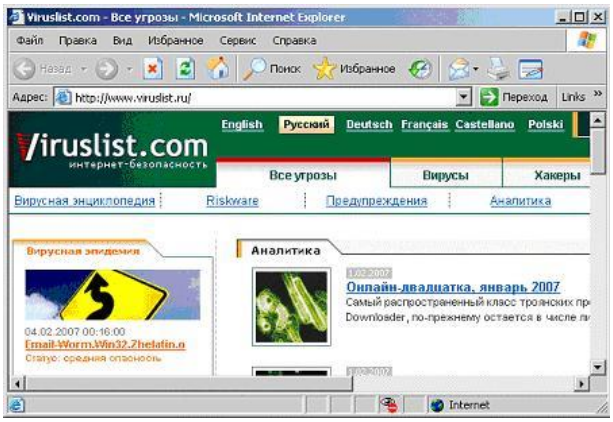
4. Адрес стартовой страницы указан в первом же поле открывшегося окна **Свойства обозревателя**, на закладке **Общие**. Значение этого поля совпадает с тем адресом, который был автоматически задан при открытии браузера.
Измените это поле, введя адрес www.viruslist.ru



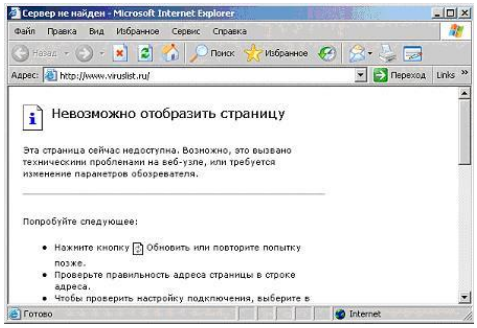
5. Далее для подтверждения сделанных изменений нажмите **ОК**



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 посторонний сайт, 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.

Задание 2. Подозрительные процессы

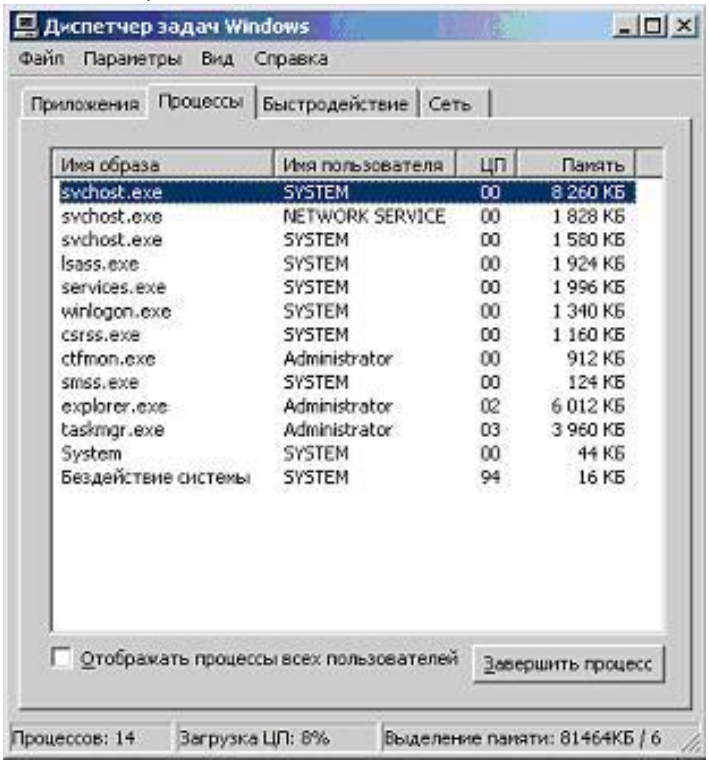
Одним из основных проявлений вредоносных программ является наличие в списке запущенных процессов подозрительных программ. Исследуя этот список и особенно сравнивая его с перечнем процессов, которые были запущены на компьютере сразу после установки системы, то есть до начала работы, можно сделать достаточно 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 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 **Microsoft Windows NT** -подобную операционную систему, в том числе **Microsoft Windows XP**. С ее помощью можно в режиме реального времени отслеживать выполняющиеся приложения и запущенные процессы, оценивать загруженность системных ресурсов компьютера и использование сети.

Познакомьтесь с интерфейсом **Диспетчера** и проследите за изменениями в системе на примере запуска программы **Paint**. Изучение сетевой активности с помощью **Диспетчера задач Windows** будет продолжено в одном из последующих заданий.

1. Перейдите к **Диспетчеру задач Windows**, нажав одновременно клавиши **Ctrl**, **Shift** и **Esc**.



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, **Процессы .**

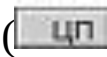
2. Внимательно изучите представленный в окне список процессов. Если на компьютере не запущены никакие пользовательские программы, он должен содержать только служебные процессы операционной системы.

При работе с домашним компьютером рекомендуется сразу после установки операционной системы ознакомиться со списком запускаемых ею процессов. В дальнейшем, при подозрении на заражение, можно будет вывести перечень процессов и сразу исключить из рассмотрения те, что были с самого начала.

Описание большинства процессов можно найти в Интернете. Поэтому если к Вам закрались подозрения, немедленно обратитесь к всемирной сети.

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.

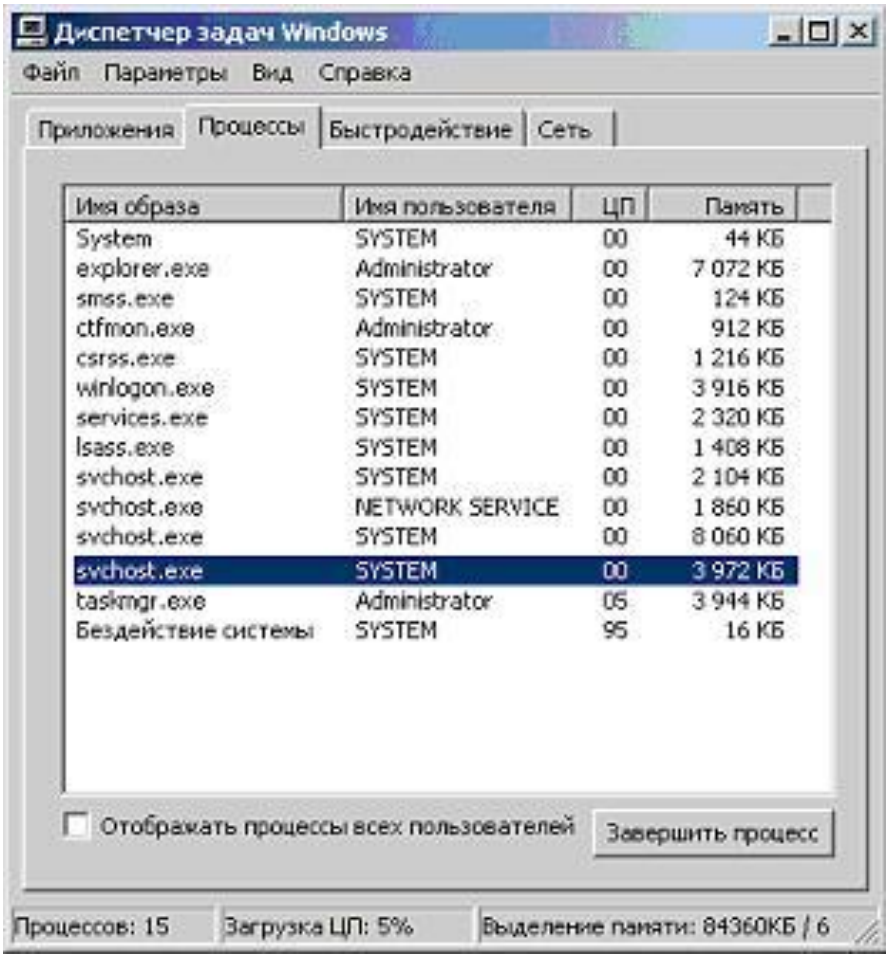
Загрузка процессора представлена в процентах от максимальной. Поэтому для удобства пользователя в списке всегда присутствует пункт "Бездействие системы". С его помощью можно быстро узнать насколько загружен, вернее свободен процессор.

Отсортируйте все процессы по использованию ресурсов процессора. Для этого нажмите на заголовок поля **ЦП** (

)

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 %.

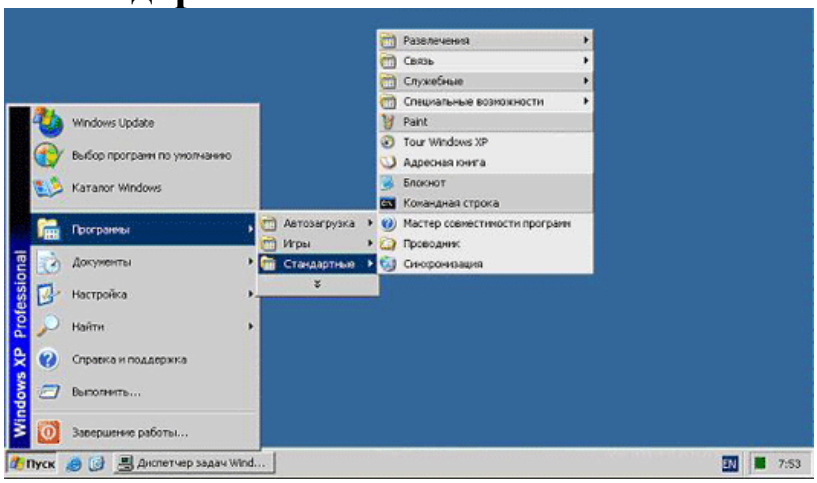
Этот метод также можно использовать для того, чтобы в случае заметного снижения производительности определить, какая программа виновна в этом: столбец **ЦП** покажет загрузку процессора, а **Память** - оперативную память.



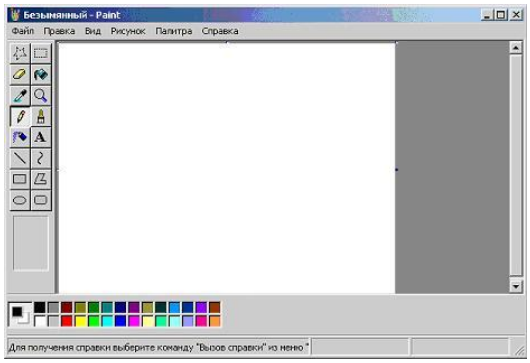
В ряде случаев может потребоваться вручную завершить некий процесс. Это можно сделать с помощью кнопки **Завершить процесс.**
Например, Вы обнаружили подозрительный процесс, на сайте вирусной энциклопедии www.viruslist.ru прочитали, что он однозначно принадлежит вирусу или троянской программе, но антивирусной 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 запущенные 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**



Дождитесь запуска **Paint**

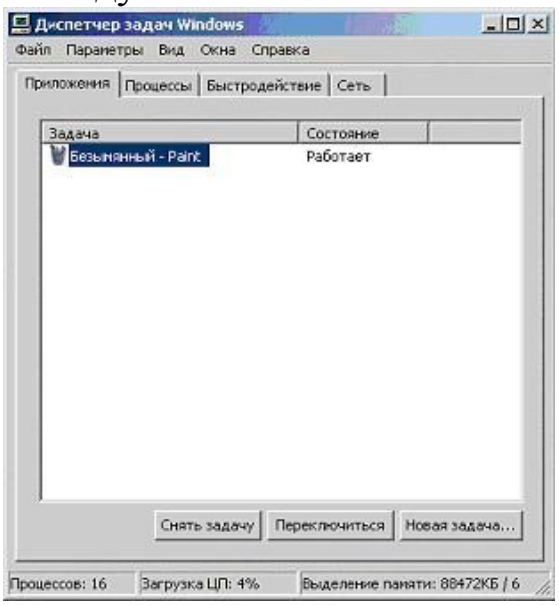


8. Не закрывая приложение **Paint**, вернитесь к окну **Диспетчера задач Windows** и проследите за изменениями на закладке **Приложения**

9. Список запущенных приложений должен содержать строку, соответствующую **Paint**. Поскольку она сейчас работает, это же записано в строке **Состояние.**

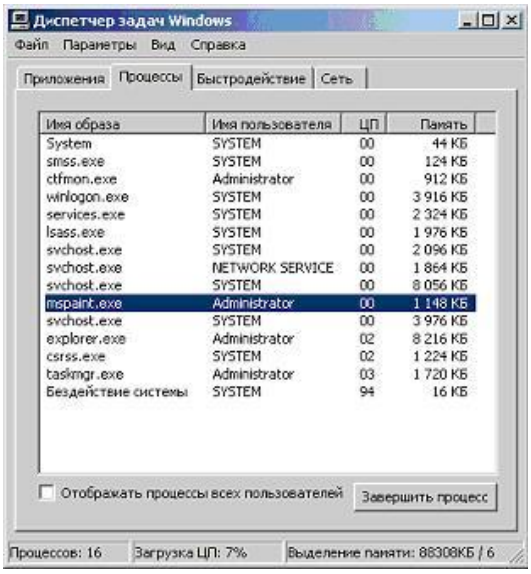
Иногда случается так, что программа вызывает ошибку - тогда в ее состоянии будет написано "Не отвечает". Если некое ранее бесперебойно работающее приложение начало часто без видимых причин переходить в состояние "Не отвечает", это может быть косвенным признаком заражения.

Тогда первое, что можно сделать - это воспользоваться кнопкой **Снять задачу** и начать поиски причин. В иных случаях пользоваться этой кнопкой не рекомендуется.



10. Перейдите к закладке **Процессы**

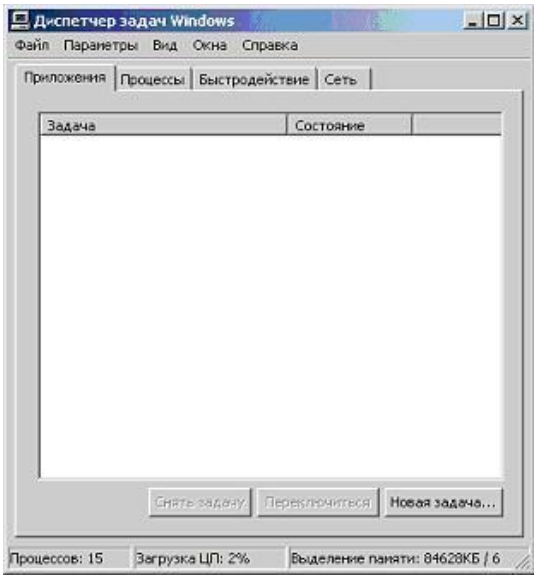
11. Сравните список запущенных сейчас процессов с перечнем, составленным на шаге 5 этого задания. Найдите отличие



12. 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

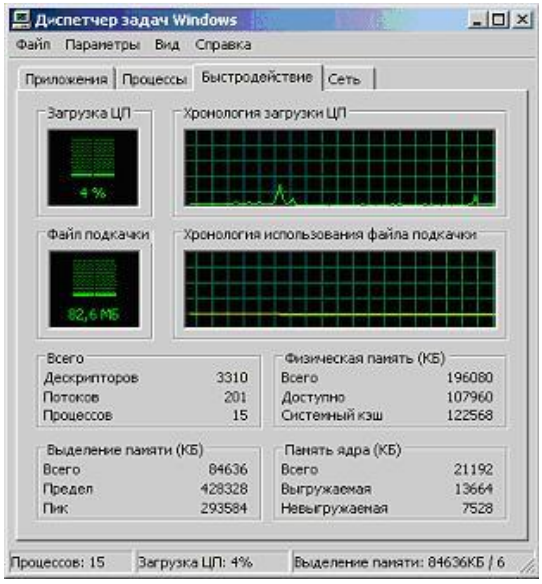
13. Проследите, что из списка запущенных процессов пропал mspaint.exe

14. Вернитесь к закладке **Приложения** и убедитесь, что она снова пуста



15. Перейдите к закладке **Быстродействие**

16. 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



17. Закройте окно **Диспетчера задач Windows**

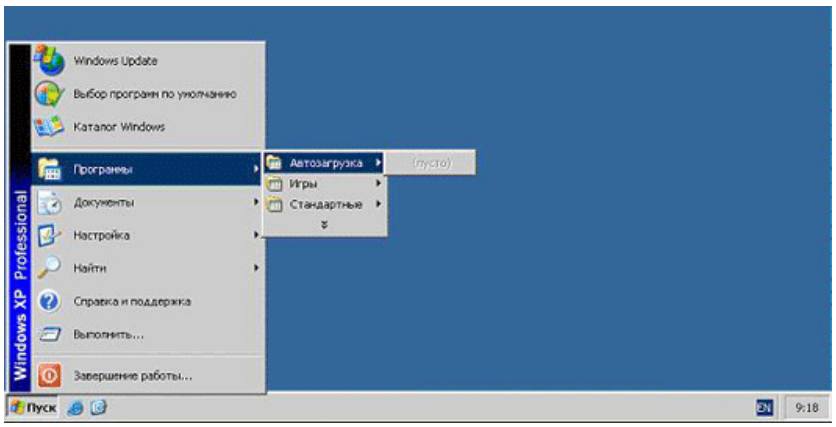
Задание 3. Элементы автозапуска

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 стартовал (используются обманные методы), 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.

В этом задании предлагается изучить элементы операционной системы, отвечающие за автозапуск программ при ее загрузке, а именно: группу **Автозагрузка** в меню **Пуск** и утилиту msconfig.exe.

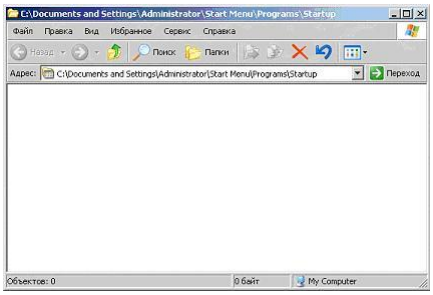
1. Самый простой способ добавить какую-либо программу в автозагрузку - это поместить ее ярлык в раздел **Автозагрузка** системного меню **Пуск / Программы**. По умолчанию, сразу после установки операционной системы этот раздел пуст, поскольку ни одной прикладной программы еще не установлено.

Проверьте папку **Автозагрузка** на Вашем компьютере. Она должна быть пустой

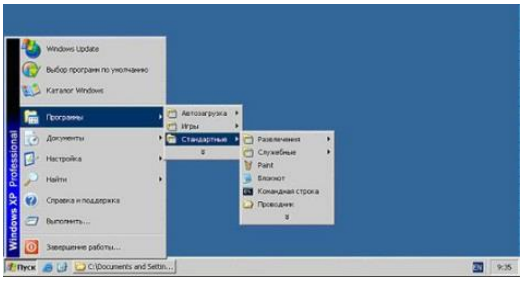


Добавьте в список автозагрузки свою программу. Для этого дважды щелкните левой клавишей мыши по названию группы **Автозагрузка**

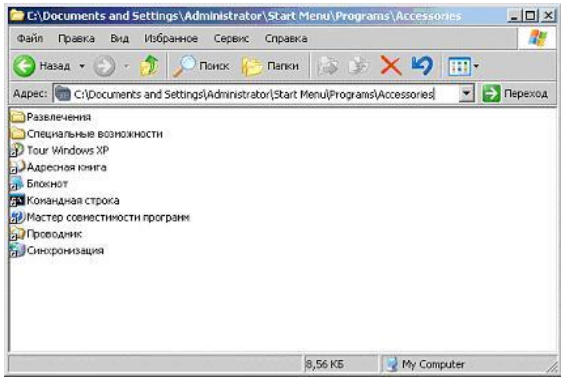
2. В результате должно открыться соответствующее окно папки автозагрузки. Обратите внимание на полный адрес открывшейся папки. Все что нужно сделать, чтобы некая программа запускалась автоматически при старте операционной системы - это поместить в эту папку ее ярлык



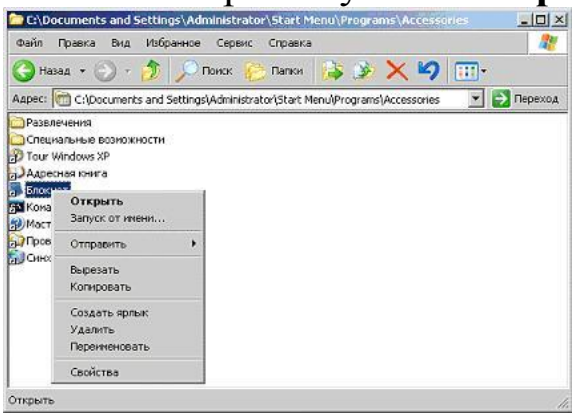
3. Повторите действия пункта 2, но только для папки **Пуск / Программы / Стандартные**



4. В открывшемся окне найдите ярлык " **Блокнот** ". Щелчком правой клавиши мыши на нем выведите контекстное меню

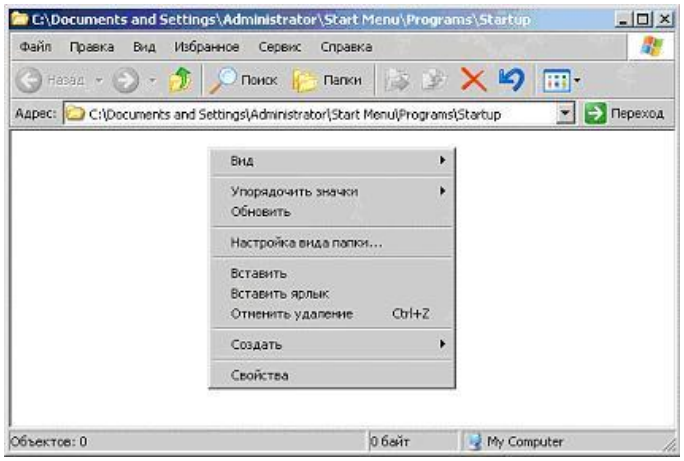


5. В контекстном меню выберите пункт **Копировать**

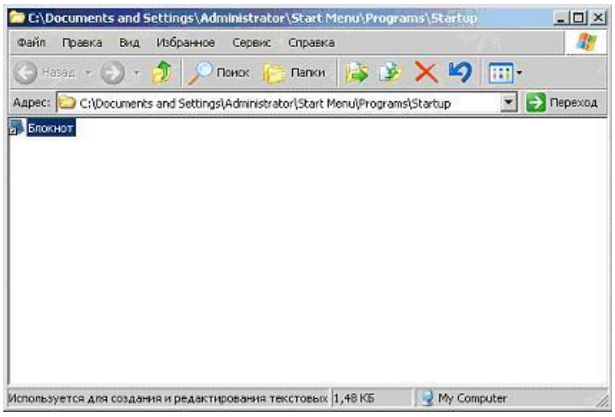


6. Закройте окно стандартных программ и вернитесь в окно автозагрузки

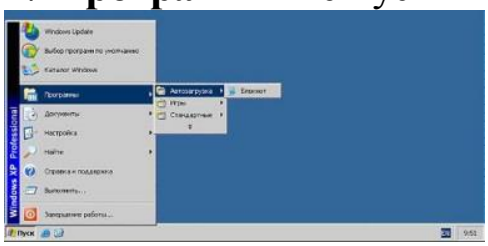
7. В окне автозагрузки щелкните правой клавишей мыши где-нибудь на белом поле окна и в открывшемся контекстном меню выберите **Вставить**



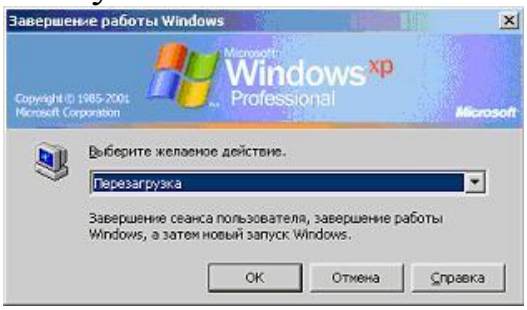
8. В результате этих действий в окне должна появиться копия ярлыка **Блокнота**



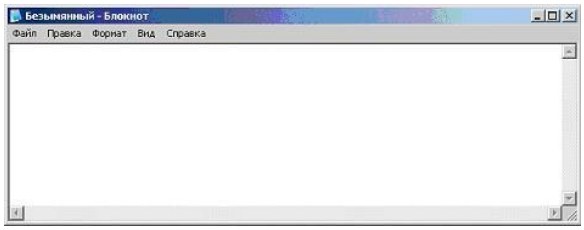
9. Закройте окно и убедитесь, что теперь раздел **Автозагрузка** в системном меню **Пуск / Программы** не пуст



10. Перезагрузите компьютер (**Пуск / Завершение работы**) и войдите в систему под своей учетной записью



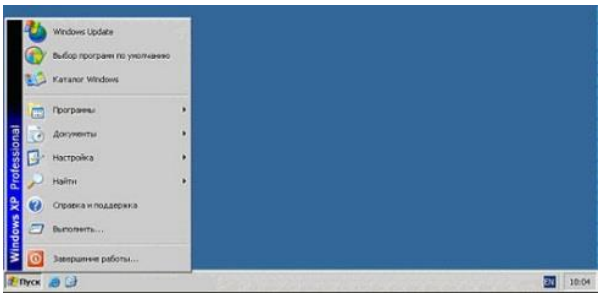
11. Убедитесь, что по завершению загрузки автоматически запустилась программа **Блокнот**



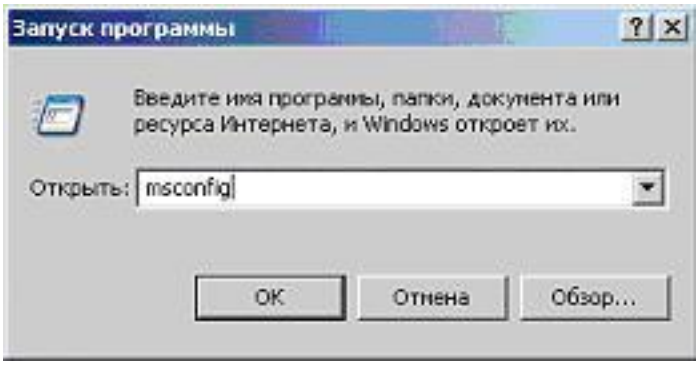
12. При обследовании компьютера нужно помнить, что отсутствие подозрительных ярлыков в разделе **Автозагрузка** системного меню **Пуск / Программы** не гарантирует, что ни одно приложение не запускается автоматически. Технически для автозапуска нужно добавить соответствующую запись в системный реестр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

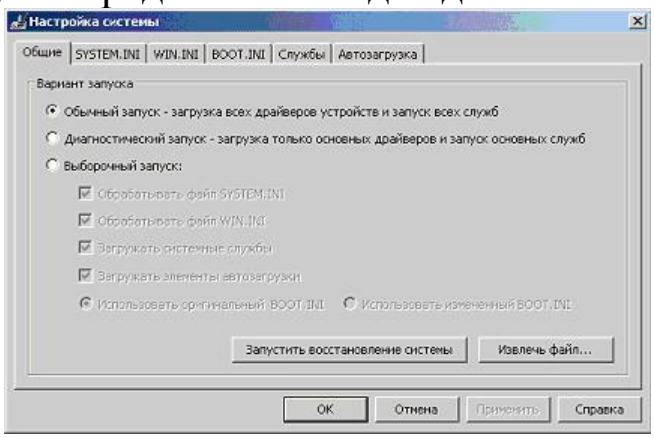


13. В открывшемся окне **Запуск программы** наберите msconfig и нажмите **ОК**



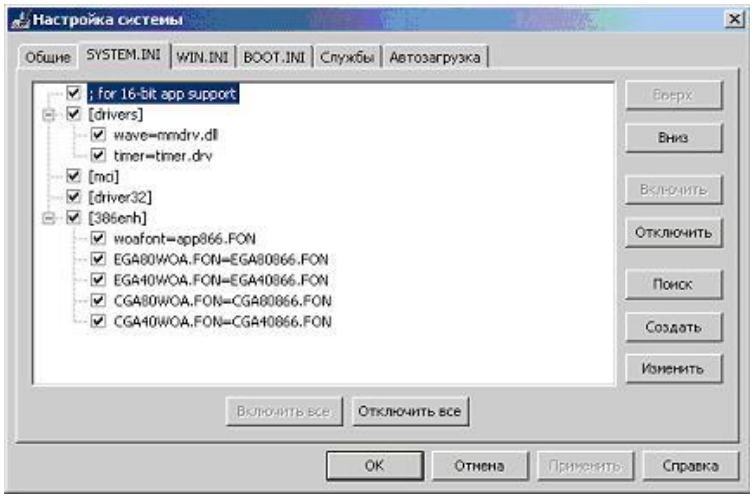
14. Ознакомьтесь с внешним видом окна утилиты **Настройка системы**.

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

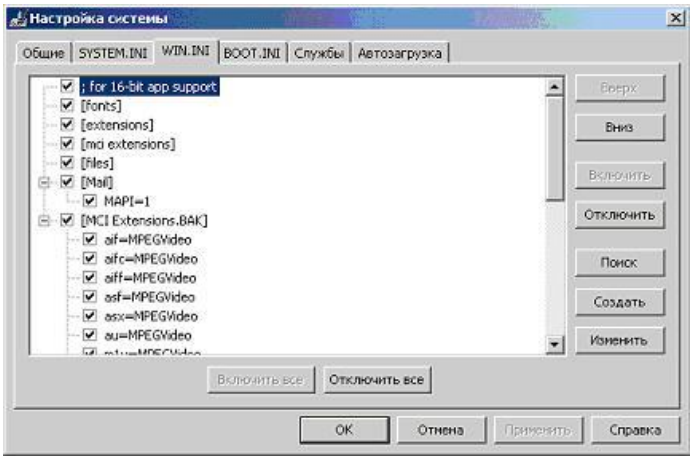


Второй режим, **Диагностический запуск**, рекомендуется использовать также при подтвердившемся вирусном инциденте - если компьютер уже заражен, сразу установить антивирус в ряде случаев нельзя, например, если вирус сознательно блокирует запуск ряда антивирусных программ. Тогда, если нет возможности удалить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

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

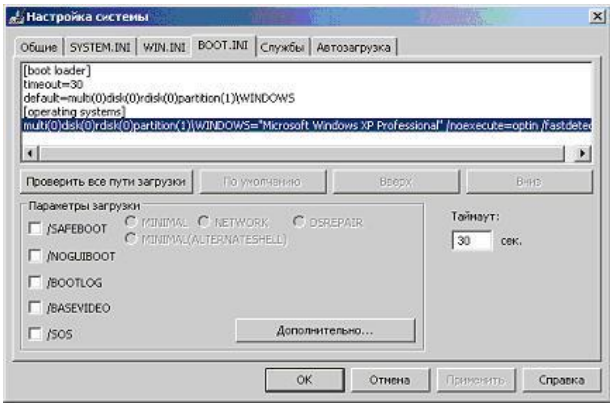


16. Перейдите к аналогичной закладке WIN.INI и ознакомьтесь с ее содержимым



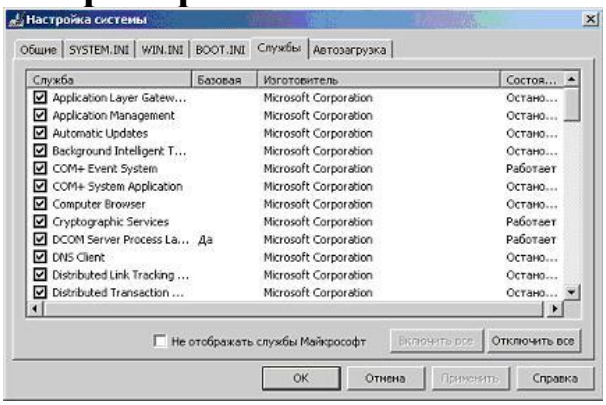
17. Следующая закладка, BOOT.INI, также отображает данные из одноименного файла. Как и предыдущие две, она также содержит си-

стемную информацию. Изменять ее можно только обладая соответствующими знаниями. Однако ознакомиться со стандартным видом и в случае подозрений обнаружить следы вируса под силу и непрофессионалу

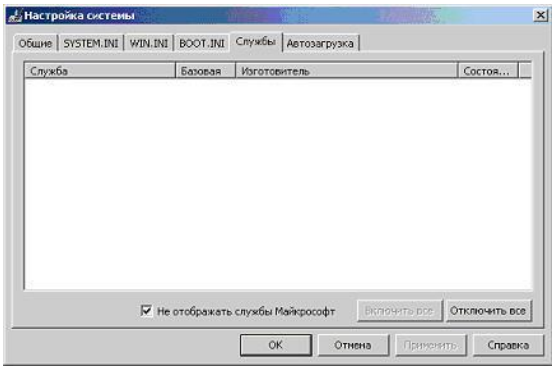


18. Перейдите на закладку **Службы**. Здесь представлен список всех служб, установленных в системе. Каждая служба представляет собой некое приложение, работающее в фоновом режиме. Например, антивирусный комплекс, обеспечивающий постоянную защиту, также встраивает свою службу, следовательно, она должна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

Однако сейчас никаких посторонних служб, кроме системных, установлено быть не должно. Убедитесь в этом, отметив флаг: **Не отображать службы Майкрософт**

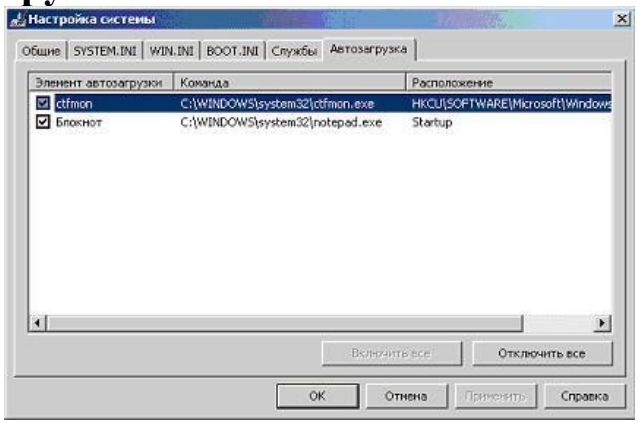


19. Если посторонних приложений действительно нет, список должен опустеть

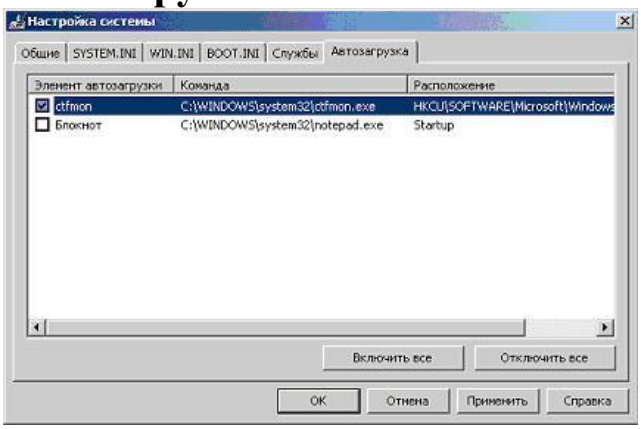


20. Перейдите к последней закладке, **Автозагрузка**, и убедитесь, что в списке приложений, автоматически запускаемых при загрузке системы, есть **Блокнот**.

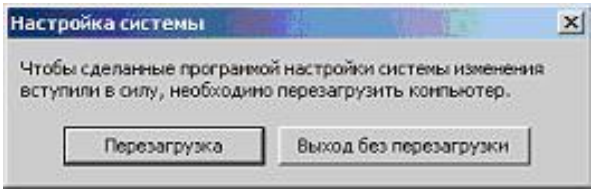
Отметим, что список в окне **Настройки системы** может содержать дополнительные элементы, не отображаемые в разделе **Пуск / Программы / Автозагрузка**



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



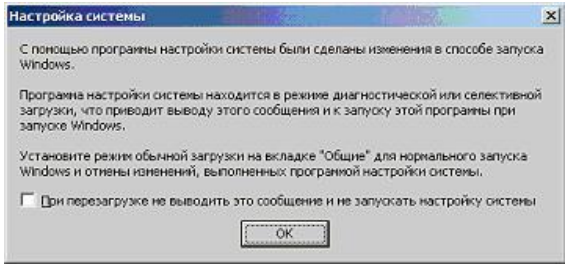
22. В открывшемся окне согласитесь провести перезагрузку, выбрав **Перезагрузка**



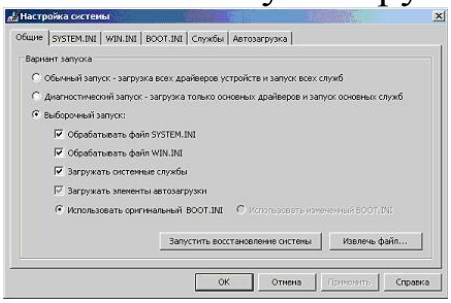
23. Дождитесь окончания перезагрузки и войдите в систему под своей учетной записью

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

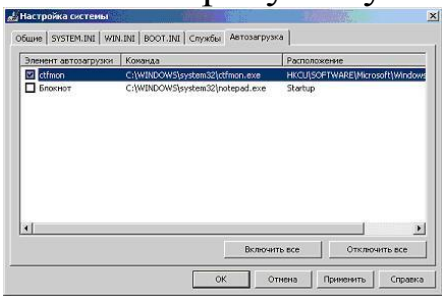
Внимательно прочитайте текст и нажмите **ОК**



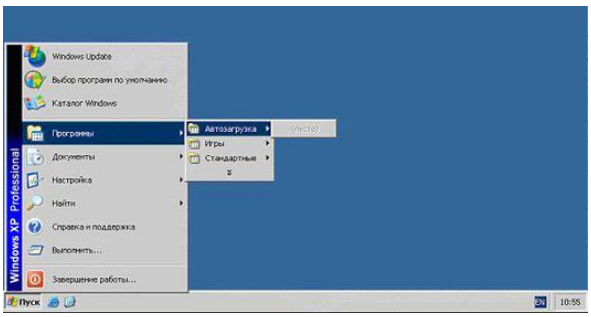
25. Это приведет к открытию окна **Настройка системы**. Обратите внимание, что теперь используется не обычный запуск, а выборочный. При этом полностью обрабатываются все элементы файлов SYSTEM.INI, WIN.INI и BOOT.INI, загружаются все службы (поскольку мы их не трогали), но флаг **Загружать элементы автозагрузки**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



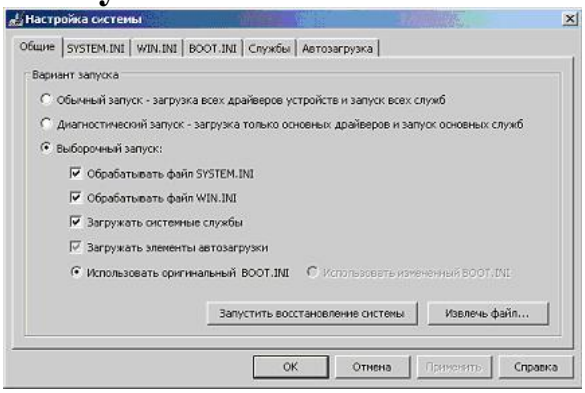
26. Перейдите к закладке **Автозагрузка** и убедитесь, что ее вид не изменился - **Блокнот** все так же присутствует в списке, но отключен



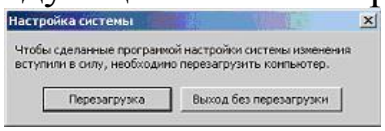
27. Не закрывая окна **Настройка системы** проверьте, что **Блокнот** автоматически не запустился и раздел **Пуск / Программы / Автозагрузка** теперь пуст



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

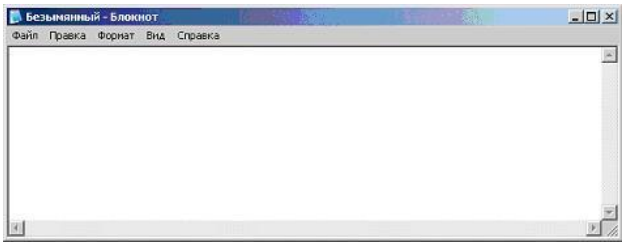


28. Нажмите **ОК** и в следующем окне выберите **Перезагрузка**

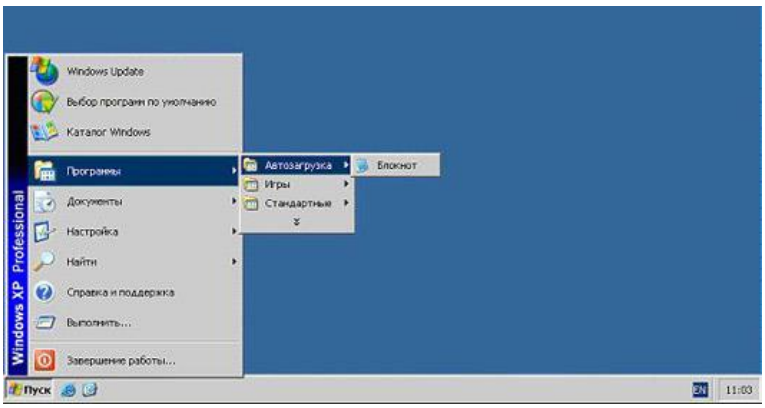


29. Дождитесь окончания перезагрузки, войдите в систему под своей учетной записью и убедитесь, что сообщение о выборочном запуске (как было в пункте 25) не появляется

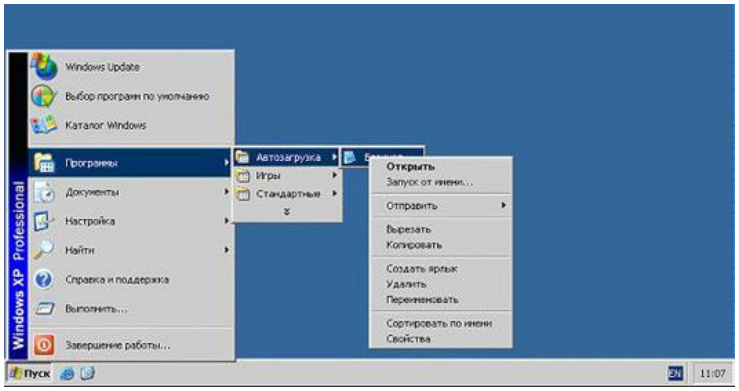
30. Однако поскольку флаг, снятый на шаге 22, при переключении в режим **Обычный запуск** вернулся (**Обычный запуск** предполагает загрузку всех зарегистрированных компонентов), приложение **Блокнот** снова автоматически запускается по завершении перезагрузки операционной системы



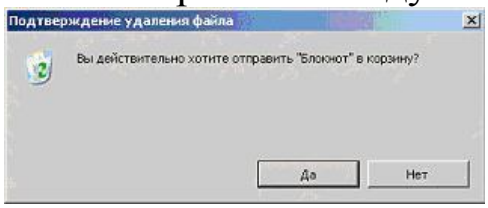
31. Убедитесь, что в **Пуск / Программы / Автозагрузка** вернулся ярлык **Блокнота**



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



Для подтверждения своих намерений в следующем окне нажмите **Да**



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

Задание 4. 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

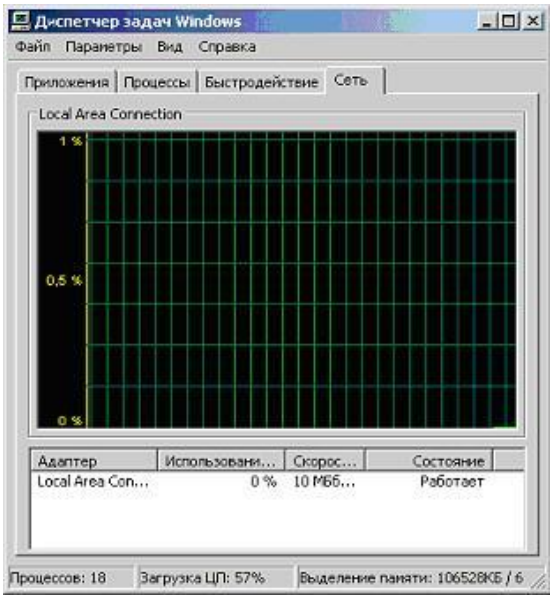
какие программы и приложения вызвали эту подозрительную активность.

Изучить и проанализировать сетевую активность можно с помощью встроенных в операционную систему инструментов или же воспользовавшись специальными отдельно устанавливаемыми приложениями. В этом задании это предлагается сделать с помощью **Диспетчера задач Windows** и встроенной утилиты netstat, которая выводит на экран мгновенную статистику сетевых соединений.

1. Откройте окно **Диспетчера задач Windows**, нажав одновременно клавиши **Ctrl**, **Shift** и **Esc**, и перейдите к закладке **Сеть.**

Поскольку сейчас не инициируется ни одного сетевого соединения, график должен быть пуст, вернее представлять собой прямую на уровне 0 %.

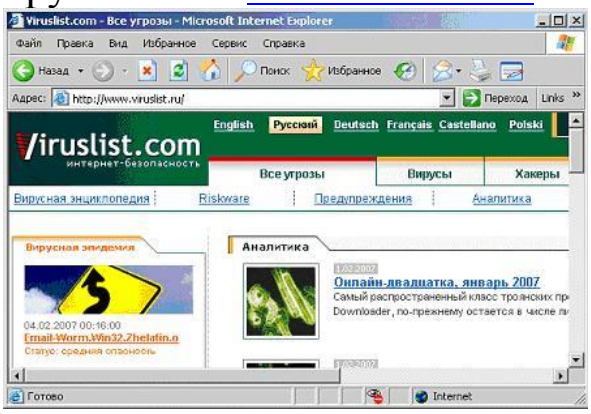
В нижней части окна расположен перечень всех установленных в системе сетевых адаптеров. Обычно он один. В столбце **Использование сети** приводится моментальное значение доли используемого канала, а в **Скорость линии** - пропускная способность. **Состояние** отображает статус.



Если на Вашем компьютере нет ни одного активного адаптера, окно **Диспетчера задач** на закладке **Сеть** будет выглядеть так:

В этом задании предполагается, что как минимум один адаптер установлен и работает.

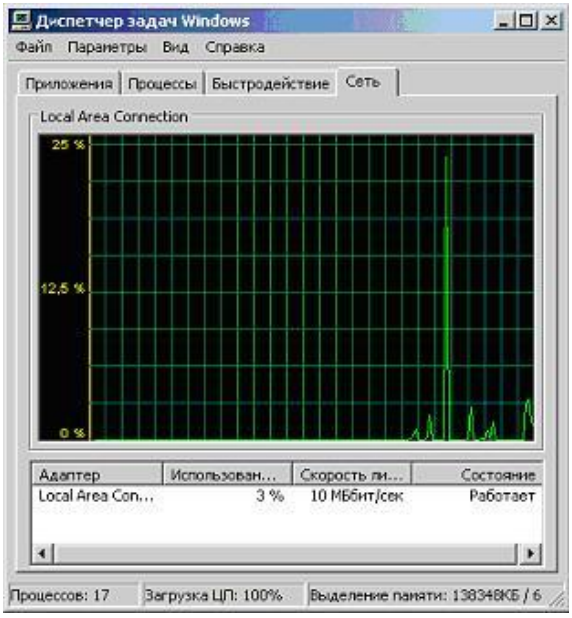
2. Инициируйте какое-нибудь сетевое соединение. Например, откройте браузер и загрузите сайт www.viruslist.ru .



При отсутствии выхода в Интернет, зайдите на сетевой ресурс, указанный преподавателем

3. Проследите за изменениями на графике **Диспетчера задач**: все Ваши действия отобразятся на графике в виде пиков сетевой активности, а значение поля **Использование сети** на время перестанет быть равным нулю.

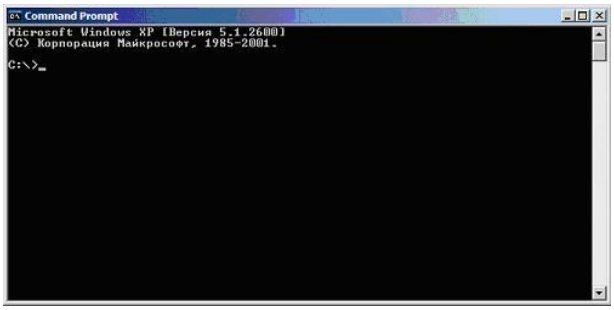
Таким образом, если Вы, закрыв все прикладные программы, которые могут инициировать сетевые соединения, обнаруживаете, что сеть все равно использоваться продолжает, нужно искать причину



4. **Диспетчер задач Windows** показывает только самую общую информацию. Для получения более подробных данных можно воспользоваться утилитой netstat.

Закройте окно **Диспетчера задач Windows** и перейдите к системному меню **Пуск / Программы / Стандартные / Командная строка**

5. В открывшемся окне нужно набирать команды, оканчивающиеся нажатием клавиши **Enter**. Такой способ взаимодействия называется работой через командную строку. Утилита netstat подразумевает именно такой режим

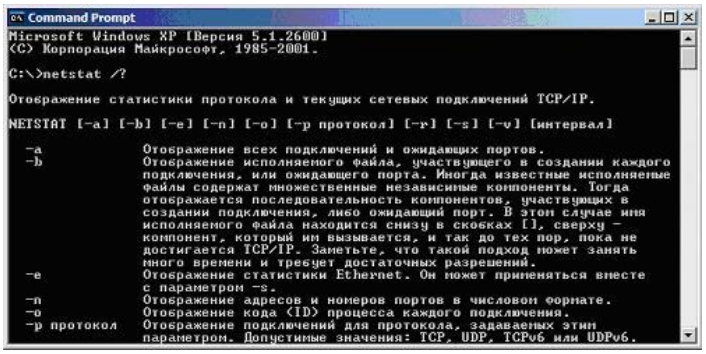


Наберите

```
netstat /?
```

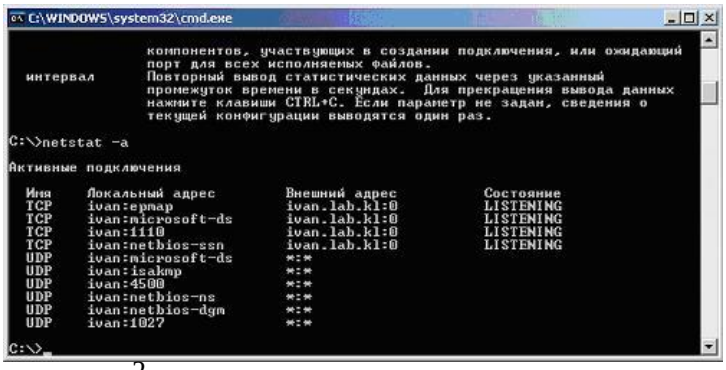
и нажмите **Enter**

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



7. Наберите
`netstat -a`
и нажмите **Enter**

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

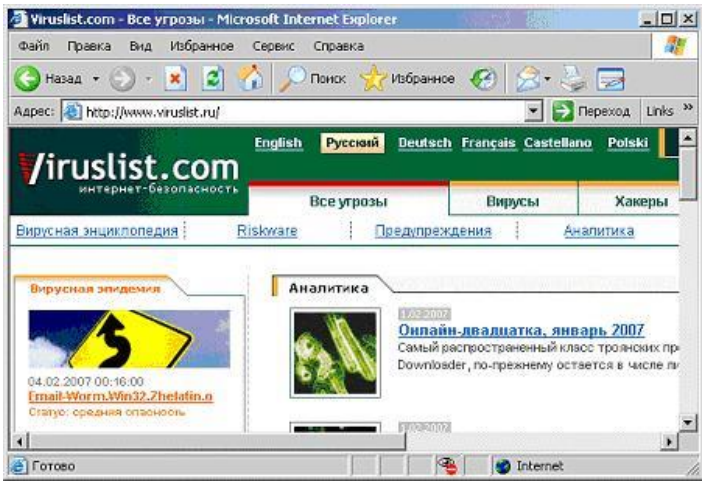


Открытые TCP-порты[2] обозначаются строкой " LISTENING " в колонке состояние. Часть портов связана с системными службами **Windows** и отображается не по номеру, а по названию - epmap, microsoft-ds, netbios-ssn. Порты, не относящиеся к стандартным службам, отображаются по номерам.

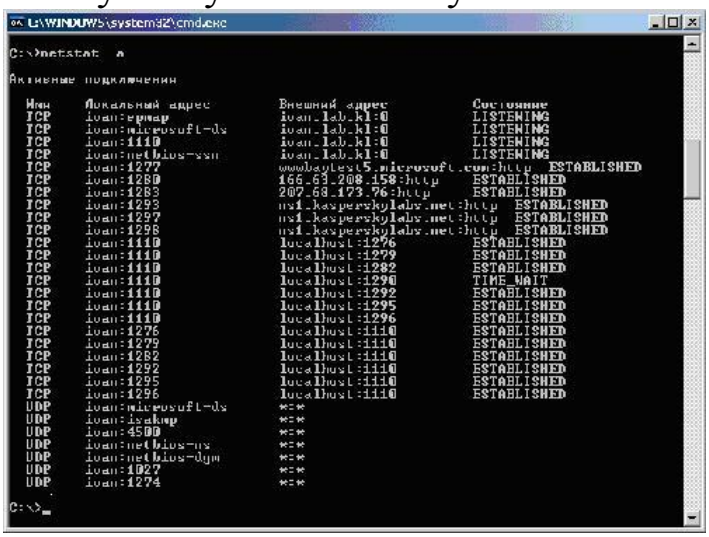
UDP -порты обозначаются строкой " UDP " в колонке **Имя**. Они не могут находиться в разных состояниях, поэтому специальная пометка " LISTENING " в их отношении не используется. Как и TCP -порты они могут отображаться по именам или по номерам.

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[3].

9. Проверьте, как изменится статистика, отображаемая netstat при инициировании новых соединений. Для этого повторите пункт 2



10. Команда netstat, в отличие от **Диспетчера задач Windows**, не работает в режиме реального времени, а отображает мгновенную статистику. Следовательно, ее нужно снова запустить.
Вернитесь к окну командной строки, введите
`netstat -a`
и нажмите **Enter**
11. Исследуйте полученную статистику



12. Закройте браузер, повторите команду
`netstat -a`
и нажмите **Enter**
13. Убедитесь, что все вызванные ранее сетевые соединения закрыты, а перечень активных соединения не отличается от данных, полученных на шаге 9
14. Закройте окно командной строки. Для этого введите команду
`exit`
и нажмите **Enter**

Заключение

В этой лабораторной работе были изучены явные признаки заражения компьютера на примере модификации настроек браузера, исследованы возможные места скрытых проявлений: запущенные процессы, элементы автозапуска, сетевая активность. В совокупности с полученными из курса теоретическими знаниями выполнение практических заданий призвано дать слушателям навыки обнаружения на своем компьютере подозрительных программ вручную, без использования антивирусных средств.

Иногда собранные данные позволяют определить имя вируса, тогда можно обратиться например, к вирусной энциклопедии www.viruslist.com, чтобы вручную ликвидировать последствия заражения. Если однозначного ответа получить не удается, необходимо собрать все подозрительные проявления и обратиться к Интернету. На сегодняшний день существует достаточно много сайтов, содержащих описания неопасных процессов, например, www.processlibrary.com. Сравнив полученные в результате анализа данные с представленными в библиотеке описаниями, нужно оставить только не заявленные как легальные процессы и объекты и проследить их расположение на диске.

Дальнейшие действия зависят от того, используется ли на компьютере антивирусная программа или нет. Если нет, то полученные файлы нужно исследовать с помощью антивирусной программы, например онлайн сканера http://www.kaspersky.ru/virusscanner, позволяющего бесплатно проверять отдельные объекты.

Если на компьютере антивирус уже установлен, после выделения подозрительных файлов следует обратиться в службу технической поддержки антивирусной компании, чей продукт используется на компьютере, прикрепив к сообщению обнаруженные подозрительные объекты. Вполне возможно, они содержат новый, еще не известный вирус.

Лабораторная работа №12. Обеспечение ИБ средствами Windows XP

Возможности Windows XP для обеспечения информационной безопасности.

· Как определить параметры компьютерной системы.

· Причины возникновения физических дефектов магнитных дисков и меры их профилактики.

· Как использовать стандартные средства Windows XP для устранения логических дефектов дисков.

· Порядок использования служебной программы «Очистка диска» для очистки магнитных носителей на компьютере.

· Что такое фрагментация файла, почему она возникает, как влияет на скорость операций чтения информации с диска и как выполнить дефрагментацию файлов.

· Порядок использования стандартной программы архивации для защиты данных компьютера от случайной утери, если в системе возникнет сбой оборудования или носителя.

Обеспечение информационной безопасности средствами Windows XP

Windows XP содержит обширный набор средств, которые обеспечивают конфиденциальность и безопасность пользовательских данных и помогают достичь максимальной производительности работы компьютера.

Защита файлов Windows

В версиях Windows, предшествующих Windows 2000, установка дополнительного программного обеспечения операционной системы могла привести к перезаписи общих файлов системы, таких, как библиотеки динамической компоновки (файлы .dll) и исполняемые файлы (файлы .exe), что могло вызвать нестабильную работу программ и сбои операционной системы. В операционных системах Windows 2000 и Windows XP имеется средство защиты файлов Windows, которое предотвращает замещение защищенных системных файлов, таких, как файлы .sys, .dll, .ocx, .ttf, .fon и .exe.

Защита компьютера

Для обеспечения безопасности компьютера Windows позволяет заблокировать его на время отсутствия пользователя на рабочем месте и настроить экранную заставку, защищенную паролем.

Управление информационной безопасностью с использованием средства «Параметры безопасности»

Изменение настройки системы безопасности на компьютере обеспечивает средство «Параметры безопасности» - правила для одного или нескольких компьютеров для защиты ресурсов или сети. С помощью средства «Параметры безопасности» можно изменить параметры безопасности нескольких компьютеров, зависящих от измененного объекта групповой политики, с компьютера, присоединенного к домену.

Параметры безопасности позволяют контролировать следующие действия:

- проверку подлинности пользователей при входе в сеть или в компьютер;
- ресурсы, которые пользователи могут использовать;
- включение и отключение записи действий пользователя или группы в журнале событий;
- принадлежность к группам.

Для обеспечения целостности, подлинности и конфиденциальности данных, а также защиты от повторений для трафика TCP/IP используется IPSec (Internet Protocol Security). Управление IPSec осуществляется посредством политики IPSec, для настройки и назначения которой используется оснастка «Управление политикой безопасности IP».

Управление доступом

Важным средством безопасности является оснастка «Локальные пользователи и группы», которая позволяет ограничить возможные действия пользователей и групп путем назначения им прав и разрешений. Право дает возможность пользователю выполнять на компьютере определенные действия, например архивирование файлов и папок или завершение работы компьютера. Разрешение представляет собой правило, связанное с объектом (файлом, папкой, принтером и т. д.), которое определяет, каким пользователям и какого типа доступ к объекту разрешен.

Предоставление пользователям, группам и компьютерам определенных прав на доступ к объектам называется ***управлением доступом***. С управлением доступом связаны следующие понятия: владение объектами, разрешения и наследование разрешений.

При создании объекта ему назначается владелец. По умолчанию владельцем объекта становится его создатель. Какие разрешения ни

были бы установлены для объекта, владелец объекта всегда может их изменить.

Разрешения определяют тип доступа к объекту или его свойству, допустимый для пользователя или группы. Например, группе пользователей финансового отдела можно предоставить разрешения на чтение и запись для файла платежной ведомости payment.dat. Разрешения применяются к защищенным объектам, таким как файлы, объекты Active Directory или объекты реестра. Рекомендуется назначать разрешения группам.

Разрешения, назначаемые объекту, зависят от его типа. Например, разрешения, которые могут быть назначены для файла, отличаются от разрешений, допустимых для раздела реестра. Однако некоторые разрешения являются общими для большинства типов объектов:

- чтение разрешений;
- смена разрешений;
- смена владельца;
- удаление.

При установке разрешений необходимо определить уровень доступа для групп и пользователей. Например, одному пользователю можно разрешить читать содержимое некоторого файла, другому - вносить изменения в файл, а всем остальным пользователям вообще запретить доступ к этому файлу. Так же можно устанавливать разрешения на доступ к принтерам, чтобы одни пользователи могли настраивать принтер, а другие — только печатать на нем.

Если требуется изменить разрешения для отдельного объекта, можно просто запустить нужную программу и внести изменения в свойства объекта. Например, чтобы изменить разрешения на доступ к файлу, запустите проводник, щелкните имя файла правой кнопкой мыши и выберите команду **Свойства**. На вкладке **Безопасность** можно изменить разрешения для файла.

Для облегчения администраторам задачи назначения разрешений и управления ими используется механизм наследования. Благодаря ему разрешения, установленные для контейнера, автоматически распространяются на все объекты этого контейнера. Например, файлы, создаваемые в папке, наследуют разрешения этой папки.

Доступ пользователей к объектам можно подвергнуть аудиту (проверке). События, связанные с безопасностью, можно просматри-

вать в журнале безопасности, используя программу просмотра событий.

Создание надежных паролей

Защита компьютера предполагает использование надежных паролей для входа в сеть и учетной записи администратора на компьютере.

Надежный пароль должен отвечать следующим требованиям.

1. Пароль должен состоять не менее чем из семи знаков. Наиболее надежные пароли состоят из семи или четырнадцати знаков. Причиной надежности таких паролей является способ кодировки.
2. Пароль должен содержать знаки, относящиеся к каждой из следующих трех групп: букв, цифр и других символов (все знаки, не являющиеся буквами или цифрами).
3. Пароль не должен содержать фамилии или имени пользователя и должен содержать не менее одного символа в позициях со второй по шестую. В качестве пароля нельзя использовать распространенное слово или имя.

Чтобы защитить учетные записи пользователей в случае, если они забыли пароль, каждому из локальных пользователей рекомендуется создать дискету сброса пароля и хранить ее в надежном месте. Тогда, если пользователь забудет пароль, при помощи дискеты сброса пароля можно сбросить пароль и снова получить доступ к локальной учетной записи пользователя.

Уровни защиты информации

Существуют три уровня защиты, предоставляемых пользователям. Они предоставляются пользователям через членство в группах «Пользователи», «Опытные пользователи» или «Администраторы».

Добавление пользователей в группу «Пользователи» является наиболее безопасным действием, поскольку разрешения по умолчанию, предоставленные этой группе, не позволяют пользователям изменять параметры операционной системы или данные других пользователей. Участники группы «Пользователи» гарантированно могут запускать только сертифицированные для Windows программы и часто не могут запускать устаревшие приложения.

Административный доступ рекомендуется использовать только для выполнения следующих действий:

- установки операционной системы и ее компонентов (например, драйверов устройств, системных служб и т. д.);
- установки пакетов обновления;
- обновления операционной системы;
- восстановления операционной системы;
- настройки важнейших параметров операционной системы(политики паролей, управления доступом, политики аудита, настройки драйверов в режиме ядра и т. д.);
- вступления во владение файлами, ставшими недоступными;
- управления журналами безопасности и аудита;
- архивирования и восстановления системы.

На практике учетные записи администраторов часто должны использоваться для установки и запуска программ, написанных для предыдущих версий Windows.

Группа «Опытные пользователи» поддерживается, в основном, для совместимости с предыдущими версиями и выполнения несертифицированных приложений. Разрешения по умолчанию, предоставленные этой группе, позволяют членам группы изменять параметры компьютера. Если необходима поддержка несертифицированных приложений, конечные пользователи должны быть членами группы «Опытные пользователи».

Члены группы «Опытные пользователи» имеют больше разрешений, чем члены группы «Пользователи», и меньше, чем члены группы «Администраторы». Опытные пользователи могут выполнять любые задачи с операционной системой, кроме задач, зарезервированных для группы «Администраторы».

Опытные пользователи могут:

- выполнять приложения, сертифицированные для Windows 2000и Windows XP Professional, а также устаревшие приложения;
- устанавливать программы, не изменяющие файлы операционной системы, и системные службы;
- настраивать ресурсы на уровне системы, включая принтеры, дату, время, параметры электропитания и другие ресурсы панели управления;
- создавать и управлять локальными учетными записями пользователей и групп;

- останавливать и запускать системные службы, не запущенные по умолчанию.

Безопасное хранение данных на основе шифрования

Для повышения уровня безопасности хранения данных можно хранить данные на диске в зашифрованной форме.

Шифрование - это процесс преобразования данных в формат, недоступный для чтения другим пользователям. После того как файл был зашифрован, он автоматически остается зашифрованным в любом месте хранения на диске.

Расшифровка - это процесс преобразования данных из зашифрованной формы в его исходный формат. После того как файл был расшифрован, он остается расшифрованным в любом месте хранения на диске.

Для повышения уровня безопасности хранения данных на основе шифрования используется шифрованная файловая система - Encrypting File System (EFS). Она предоставляет следующие возможности:

- Пользователи могут зашифровывать свои файлы при сохранении их на диске. Шифрование можно разрешить, установив флажок в диалоговом окне Свойства данного файла.
- Доступ к зашифрованным файлам можно получить простои быстро. При доступе пользователей к своим файлам с диска данные отображаются в виде обычного текста.
- Шифрование данных выполняется автоматически и является полностью прозрачным для пользователя.
- Для расшифровки файла пользователь должен снять флажок шифрования в диалоговом окне Свойства данного файла,

Шифрованная файловая система использует алгоритм шифрования Data Encryption Standard (DESX). Администраторы могут восстанавливать данные, зашифрованные другим пользователем. Это позволяет получить доступ к данным, если пользователь, зашифровавший данные, в настоящее время недоступен или соответствующий закрытый ключ утерян.

EFS позволяет зашифровывать данные только при сохранении их на диске. Для шифрования данных при их передаче по сети TCP/IP

доступны две дополнительных возможности - безопасность протокола IP (IPSEC) и шифрование PPTP.

При использовании стандартной конфигурации шифрованной файловой системы никаких действий администратора не требуется - пользователи могут сразу начинать шифрование файлов. Шифрованная файловая система автоматически создает пару ключей шифрования для пользователя, если она отсутствует.

Сведения о системе

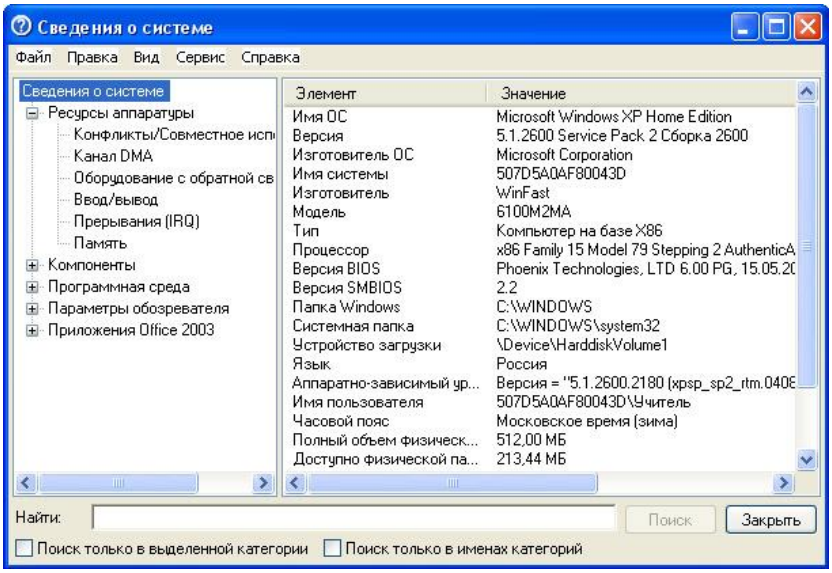


Рис. 1. Окно программы Сведения о системе

Для эффективного использования компьютерной системы и при устранении неполадок, связанных с конфигурацией системы, очень важно знать параметры этой системы. Для сбора данных о компьютере используется стандартная программа «Сведения о системе». Она собирает и отображает данные о конфигурации системы, как для локальных, так и для удаленных компьютеров. Эти данные включают информацию о конфигурации оборудования, компонентах компьютера, а также о программном обеспечении. Для хранения данных о системе предназначены файлы с расширением .nfo. Кроме того, программа «Сведения о системе» работает с файлами форматов .cab и .xml.

Для запуска программы выберите в меню **Пуск** команду **Программы-Стандартные-Служебные-Сведения** о системе. Как показано на рис. 1, в левой области окна программы находится дерево категорий, похожее на дерево папок проводника Windows. В правой части окна программы находится об-

ласть сведений, в которой выводятся данные, относящиеся к элементу, выделенному в дереве категорий.

«Сведения о системе» - это корневой узел в дереве категорий программы. Когда он выделен, в области сведений отображаются данные общего характера о компьютере и его операционной системе. Здесь можно узнать название операционной системы, ее версию, изготовителя и местоположение системного каталога. Кроме того, можно сверить версию BIOS, тип процессора и объем памяти.

В категории «Ресурсы аппаратуры» сведений о системе собраны данные о назначениях ресурсов и возможных конфликтах, обусловленных совместным использованием каналов DMA, оборудования с обратной связью, портов ввода-вывода, линий IRQ и адресов памяти.

В категории «Компоненты» собраны сведения о следующих элементах системы: мультимедиа, CD-ROM, звуковое устройство, дисплей, инфракрасные устройства, ввод, модем, сеть, порты, запоминающие устройства, печать, устройства с ошибками, USB и т.п.

В категорию «Программная среда» включены данные о конфигурации системы, в том числе сведения о системных драйверах, переменных среды и имеющихся заданиях печати.

Для просмотра данных о системе дважды щелкните категорию в дереве консоли, а затем щелкните элемент, чтобы вывести его содержимое в правой области окна. Так, например, на рис. 2 отображаются сведения о клавиатуре компьютера. Если требуется выполнить поиск данных о системе, в нижней части окна программы в поле *Найти* введите слово (или слова), соответствующее искомым сведениям о системе, затем установите необходимые параметры поиска. Например, для поиска в отдельной части дерева консоли установите флажок **Поиск только в выделенной категории**. В этом случае поиск будет выполнен в выделенной категории и во всех ее подкатегориях. Чтобы выполнить поиск во всем дереве, снимите этот флажок. Для поиска только в названиях категорий дерева консоли (без учета области сведений) установите флажок **Поиск только в именах категорий**. Чтобы выполнить поиск и в дереве консоли, и в области сведений, снимите этот флажок. Для поиска по всем категориям в обеих областях окна программы снимите оба флажка. Для начала поиска нажмите кнопку «Поиск». По окончании поиска в области сведений будут отображены данные об искомом компоненте системы.

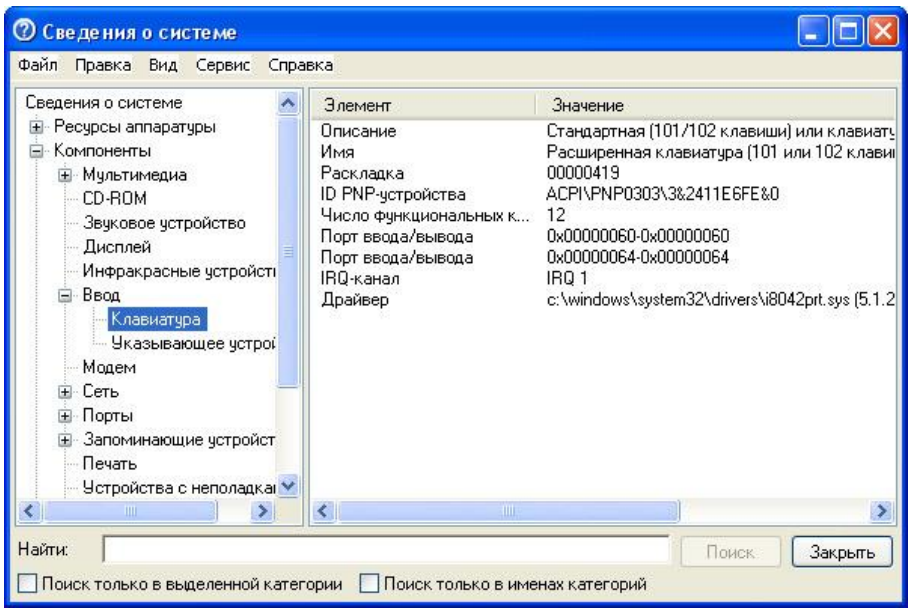


Рис. 2. Просмотр сведений о клавиатуре

Примечание. Если панель поиска отсутствует в нижней части окна программы, в меню Правка выберите команду Скрыть поиск, чтобы снять флажки и восстановить настройку средства поиска.

Чтобы сохранить файл данных, программы «Сведения о системе» выберите в меню **Файл** команду **Сохранить**, затем в поле *Папка* выберите расположение файла, в поле *Имя файла* введите имя файла, в поле *Тип файла* выберите необходимый формат файла и нажмите кнопку «Сохранить».

Примечание. По умолчанию данные о системе сохраняются в формате .nfo, совместимом с текущей версией программы «Сведения о системе».

К программно-техническим мерам обеспечения информационной безопасности можно отнести обеспечение бесперебойной работы дисковой системы компьютера.

Магнитные диски компьютера в настоящее время являются основными носителями информации, предназначенными для длительного и надежного ее хранения. В процессе работы персонального компьютера непрерывно происходит обмен информацией между дисками и оперативной памятью, при этом наиболее интенсивно происходит обмен с жестким диском. Несмотря на высокое качество изготовления дисков и дисковых устройств, в практике регулярной работы на компьютере нередко возникают ситуации, когда не удается прочитать информацию с дисков, происходят нарушения в работе файловой системы, значительно сокращается свободное пространство на дисках

или диски оказываются переполненными. Нередко ошибочно удаляются нужные файлы.

Эти нарушения в работе дисков могут возникать по следующим причинам:

- при физическом повреждении диска;
- при загрязнении магнитной поверхности диска;
- при аварийном отключении компьютера;
- при несвоевременном извлечении дискет из дисководов;
- при перезагрузке операционной системы после аварийного завершения задания;
- при воздействии программных вирусов.

Кроме того, при эксплуатации компьютера на магнитных дисках накапливаются такие изменения в расположении файлов, которые, если не принимать мер, могут привести к существенному замедлению обмена с ними информацией.

Дефекты дисков

Различают физические и логические дефекты магнитных дисков. *Физические дефекты* возникают главным образом из-за механических повреждений, воздействия электромагнитных полей или старения магнитного покрытия диска. Наличие физического дефекта делает непригодными к использованию некоторые сектора и кластеры. Если оказывается, что какой-либо файл располагается в таких дефектных секторах или кластерах, то полностью спасти находящуюся в файле информацию не представляется возможным. Дефектные сектора диска должны быть исключены из дальнейшего использования. *Логические дефекты* диска связаны с повреждениями системной области диска, включающей таблицу разделов жесткого диска, таблицу размещения файлов, загрузочный сектор, каталоги диска. Такие нарушения могут возникать при аварийном отключении питания, сбоях, зависании ошибочно работающих программ, воздействии компьютерных вирусов и других причинах. Во всех этих случаях оказываются незавершенными процедуры работы с дисками, файлами или каталогом. В результате на диске образуются потерянные кластеры, которые или не принадлежат ни одному файлу, или, наоборот, принадлежат сразу нескольким.

Логические дефекты приводят к разрушению файловой системы, «засорению» дискового пространства, когда кластеры считаются занятыми, но не принадлежат ни одному из файлов, а некоторые файлы оказываются «связанными» друг с другом общими кластерами.

Для обнаружения ошибок файловой системы и поврежденных секторов на жестком диске можно использовать служебную программу проверки диска. Для этого откройте окно *Мой компьютер* и выберите локальный диск, который требуется проверить. В меню **Файл** выберите команду **Свойства**. На вкладке **Сервис** в группе Проверка диска нажмите кнопку «Выполнить проверку», как показано на рис. 3. В группе Параметры проверки диска установите флажок **Проверять и восстанавливать поврежденные сектора**.

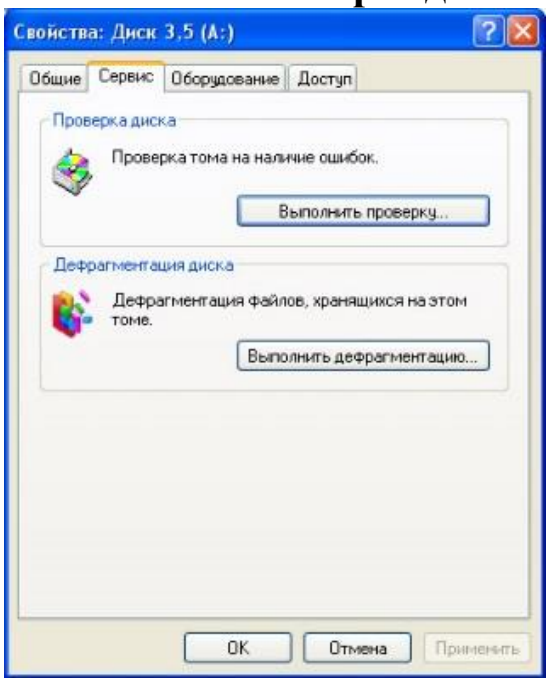


Рис. 3. Запуск процедуры проверки диска

Примечание. Перед запуском проверки диска следует закрыть все файлы на нем. Если том используется, на экран будет выведено сообщение с предложением выполнить проверку диска после перезагрузки системы. При положительном ответе проверка диска будет запущена после перезагрузки компьютера. Во время проверки диск недоступен для выполнения других задач.

После выполнения операции проверки диска на экран будет выведено сообщение о результатах работы программы.

Рекомендуется использовать служебную программу проверки диска примерно раз в месяц для контроля жесткого диска. Разумеется, это нужно делать и в том случае, если появляются подозрения на

сбой работы жесткого диска (иногда он может быть вызван и заражением компьютерными вирусами). Особо паниковать при появлении сбойных участков на жестком диске не стоит - дело это обычное, если таких участков немного. Утилита сканирования помечает их и исключает из работы. Если появление сбойных участков участилось и они заметно сказываются на общей емкости жесткого диска, значит настала пора его менять на новый. Гибкие диски со сбойными участками лучше вообще не применять.

Очистка диска

Во время работы за компьютером на жестком диске накапливается большое количество ненужной информации. Это всевозможные временные файлы, скачанные из Интернета web-страницы, а также не используемые файлы приложений. Чем больше программ вы устанавливаете и запускаете, чем чаще выходите в Интернет, тем больше шансов появления на жестком диске разного бесполезного мусора, который занимает драгоценное свободное место. Для поддержания порядка на своем компьютере необходимо периодически устраивать уборку. В операционной системе Windows XP для этих целей используется служебная программа под названием «Очистка диска». Для ее запуска активируйте меню «**Пуск**», затем выберите **Программы-Стандартные-Служебные-Очистка диска**. После запуска утилиты на экране появится рабочее окно программы, в котором необходимо выбрать логический диск, который будет подвергнут процедуре очистки. По умолчанию выбранным всегда является диск (C:).

Примечание. Также можно запустить мастер очистки, зайдя в «Мой компьютер», выбрав соответствующий диск и щелкнув на нем правой кнопкой, активировать закладку «Очистка диска». Тогда процедура очистки будет сразу же запущена специально для выбранного диска. После того как вы определите диск, который желаете очистить, можно нажимать кнопку «ОК». При этом мастер очистки диска перейдет к процедуре проверки состояния файлов на данном диске. После завершения анализа текущего состояния диска утилита представит отчет о проделанной работе, указав, сколько места можно освободить.

Как показано на рис. 4, мастер выведет на экран сводную информацию о том, за счет чего может быть освобождено пространство на диске.

В окне приводится перечень категорий файлов, которые могут быть удалены или сжаты без ущерба для работы системы. Тем не менее, пользователю предлагается самостоятельно определить, что подлежит удалению, а что удалять не следует. Галочкой отмечаются группы файлов, подлежащие удалению. В конце каждой строки отображается объем в килобайтах, который можно высвободить удалением данной категории файлов.

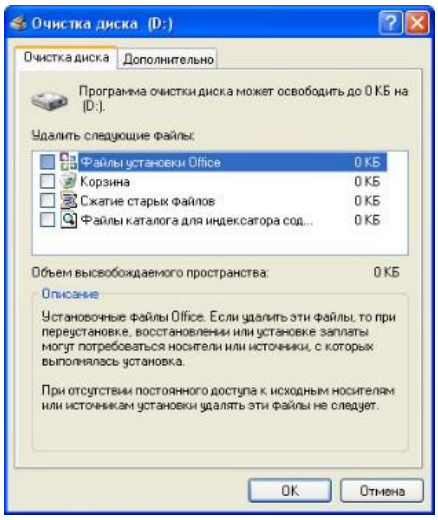


Рис. 4. Окно Очистки диска

Для того чтобы уверенно сделать выбор, необходимо знать, что представляют собой перечисленные файловые группы.

Папка «Downloaded Program Files» предназначена для временного хранения элементов ActiveX и приложения Java, автоматически загружаемых из Интернета, при загрузке и просмотре различных web-страниц. Папка в любой момент может быть смело подвергнута очистке. В каталоге «Temporary Internet Files» находятся web-страницы, автоматически сохраняющиеся на жестком диске во время работы в Интернете, для быстрого просмотра при повторном обращении к ним. При хорошем соединении время загрузки web-страниц не очень велико, а потому нет смысла оберегать содержимое данной папки. Поскольку в ней скапливается достаточно большое количество файлов, ее нужно стараться очищать достаточно регулярно. В Корзину помещаются файлы после их удаления с диска. Очистка Корзины избавит диск от уже ранее удаленных файлов. Некоторые программы очень часто хранят временную информацию в файлах, в специально

отведенной для этого папке TEMP. Как правило, перед закрытием таких программ эти файлы обычно удаляются. Тем не менее, это происходит не

всегда, а потому в папке может накапливаться масса ненужной информации. Временные файлы, которые хранятся больше недели, можно смело удалять. Временные автономные файлы представляют собой локальные копии недавно использовавшихся сетевых файлов, автоматически помещенных в кэш. Это дает возможность получить к ним доступ в отключенном от сети состоянии.

Служба WebClient/WebPublisher сохраняет на диске файлы, к которым был осуществлен доступ соответствующим образом. Они необходимы для увеличения быстродействия, а потому также могут быть безболезненно удалены. Одним из способов экономии места является процедура сжатия файлов, к которой давно не было обращений. При этом Windows сохраняет возможность в любой момент обратиться к данным файлам, и никакая информация не удаляется. Правда, информация об освобождаемом пространстве в данном случае будет приблизительной, поскольку файлы сжимаются с различной степенью. Служба индексирования призвана ускорить поиск файлов на дисках. Создавая индексы существующих на диске файлов, данная служба значительно расширяет возможности обнаружения необходимой информации. Тем не менее, старые индексы могут сохраняться со времен последней операции индексирования и подлежат удалению.

Таким образом, ознакомившись с отчетом мастера очистки диска, можно определить, какие именно из обнаруженных файлов необходимо удалить. При необходимости, выделив какую-либо группу файлов из предлагаемого списка, можно просмотреть ее содержимое. Для этого достаточно нажать кнопку «Просмотр файлов». Это удобно тогда, когда из всей группы необходимо сохранить лишь несколько файлов. Их можно переписать в другой каталог, а остальные файлы удалить.

Щелкнув на вкладке «**Дополнительно**», можно освободить дополнительное место на диске, удалив неиспользуемые компоненты Windows или установленные программы. Каждый пользователь должен постараться определиться с тем, какие именно приложения он использует при работе за компьютером. Все остальное может быть

удалено. После того как определена вся информация, подлежащая удалению, нажмите кнопку «ОК» в окне отчета мастера очистки. Все выбранные файлы будут удалены, а утилита «Очистка диска» автоматически завершит свою работу.

Дефрагментация диска

Операционная система Windows записывает файлы на диск физическими блоками, называемыми кластерами. ***Кластер*** - минимальный объем дисковой памяти, который может быть выделен для размещения файла. Все файловые системы, используемые Windows для работы с жесткими дисками, основаны на кластерах, которые состоят из одного или нескольких смежных секторов. Чем меньше размер кластера, тем более эффективно используется дисковая память. Если размер кластера не задан во время форматирования, он выбирается Windows в зависимости от объема диска. Стандартные значения подобраны таким образом, чтобы снизить потерю дискового пространства и степень возможной фрагментации тома.

После форматирования диска или в том случае, когда на нем имеется достаточно свободного пространства, операционная система записывает файл в смежные, примыкающие друг к другу кластеры. Считывание информации из такого файла происходит при минимальном перемещении магнитных головок. По мере записи на том новых файлов свободное пространство на нем уменьшается.

Примечание. Том - раздел или логический диск, расположенный на жестком магнитном диске.

При недостаточном размере непрерывного свободного пространства на диске операционная система использует для размещения нового файла имеющиеся свободные участки, помещая в них отдельные цепочки кластеров файла - фрагменты файла. При этом фрагменты могут располагаться на значительном расстоянии друг от друга, что приводит к существенному увеличению времени на перемещение магнитных головок и соответственно времени считывания или записи файла.

Файл, который занимает на диске более одного непрерывного участка, называется ***фрагментированным***. Фрагментация диска - это появление на диске множества свободных участков, разделенных занятыми участками.

Как было описано выше, для увеличения свободного пространства диска производят его чистку. Однако удаление файлов еще больше способствует фрагментации, так как освободившиеся участки будут использоваться операционной системой для размещения фрагментов новых файлов. При этом может возникнуть ситуация, при которой свободного пространства на диске много, но все оно состоит из множества разбросанных по диску мелких участков, недостаточных для размещения файлов целиком. Если в процессе длительной эксплуатации диска, особенно жесткого, не принимать специальных мер, то фрагментированной окажется большая часть файлов, и это может замедлить работу диска и соответственно программ, взаимодействующих с ним, в несколько раз. Кроме того, наличие фрагментации всегда ухудшает прогноз восстановления удаленных файлов и каталогов.

В настоящее время разработаны и широко применяются специальные программы, устраняющие фрагментацию дисков. Все эти программы выполняют ***дефрагментацию диска***, т.е. реорганизуют физическое расположение всех файлов и каталогов таким образом, чтобы минимизировать перемещение магнитных головок дисководов. Программа дефрагментации выполняет две процедуры:

- объединяет все неиспользуемые участки диска и помещает их в конец диска, образуя сплошное пространство;
- объединяет фрагменты файлов, располагая все кластеры каждого файла в виде одного сплошного участка.

Все эти операции, которые программа производит с дисковой информацией, называют оптимизацией диска.

В операционной среде Windows для дефрагментации лучше использовать стандартную служебную программу **Дефрагментация диска**. Программа **Дефрагментация диска** - это системная служебная программа, выполняющая анализ локальных томов и объединяющая фрагментированные файлы и папки таким образом, чтобы каждый файл или папка тома занимали единое непрерывное пространство.

Примечания.

1. Дефрагментацию дисков также можно запустить из командной строки с помощью команды **c:\windows\ system32\ defrag.exe.** Перед запуском программы оптимизации диска необходимо выполнить следующие процедуры:

- удалить ненужные файлы;
- восстановить случайно удаленные файлы, так как после дефрагментации это сделать будет уже невозможно;
- проверить и при необходимости устранить нарушения в логической структуре диска, иначе программа дефрагментации, обнаружив нарушения, прекратит дефрагментацию.

Для запуска программы **Дефрагментации диска** следует выбрать в меню **Программы** пункт **Стандартные**, затем **Служебные**, а затем выбрать пункт **Дефрагментация диска**. После этого нужно выбрать диск и нажать кнопку «Анализ». По завершении анализа тома программа дефрагментации диска выводит результаты анализа и сообщение о том, нуждается ли данный том в дефрагментации, как показано на рис. 5. Для того чтобы просмотреть отчет об анализе, содержащий более подробные сведения о томе, и список наиболее фрагментированных файлов, нажмите кнопку «Вывести отчет». Если вы считаете дефрагментацию необходимой, то щелкните кнопку «Дефрагментация», иначе - «Закрыть».

Если вы запустили процедуру Дефрагментация диска, то после выполнения этой процедуры результаты будут отображены в графическом представлении с цветовой кодировкой в полях результатов анализа и дефрагментации. Чтобы просмотреть отчет о дефрагментации, содержащий подробные сведения о дефрагментированном томе, нажмите кнопку «Вывести отчет».

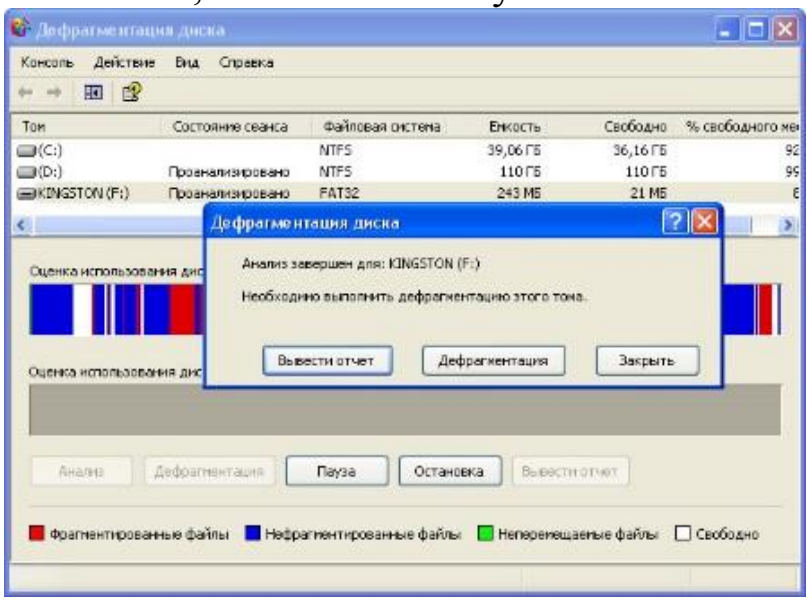


Рис. 5. Окно Сообщение с результатами анализа

2. В полях результатов анализа и дефрагментации отображается приблизительное представление фрагментации тома, так как поля результатов анализа и дефрагментации недостаточно велики, чтобы отображать цветную вертикальную линию для каждого кластера диска в составе тома. Каждая линия в полях результатов анализа и дефрагментации представляет собой десятки или даже сотни кластеров в зависимости от размера тома и кластера. Поскольку в одной группе кластеров могут находиться и фрагментированные файлы, и нефрагментированные файлы, и неперемещаемые файлы (файлы, текущее положение которых на диске не может быть изменено), и свободное пространство, цвет каждой вертикальной линии определяется следующими правилами.

Цвет	Описание
Красный	Большинство кластеров являются частью фрагментированного файла.
Синий	Большинство кластеров в группе содержат только свободное пространство и нефрагментированные файлы.
Зеленый	Большинство кластеров являются частью неперемещаемого файла.
Белый	Большинство кластеров представляют свободное пространство.

Для получения точных числовых значений используйте отчеты об анализе и дефрагментации, которые содержат подробные сведения о томе, проверенном на наличие фрагментированных файлов и папок, включая размер тома и свободного пространства, число фрагментированных файлов и папок, а также среднее число фрагментов в файле.

Советы и рекомендации при дефрагментации

1. Перед дефрагментацией проанализируйте тома. Анализ рекомендуется проводить регулярно, а дефрагментацию только после соответствующей рекомендации программы дефрагментации диска. Анализ томов рекомендуется выполнять не реже одного раза в неделю. Если потребность в дефрагмен-

тации возникает редко, интервал выполнения анализа томов можно увеличить до одного месяца.

2. Анализируйте тома на фрагментированность после добавления большого числа файлов, так как после добавления их или папок тома могут стать сильно фрагментированными.
3. Перед дефрагментацией убедитесь, что на диске не менее 15% свободного пространства. Программа Дефрагментация диска использует этот объем как область для сортировки фрагментов файлов. Если объем составляет менее 15% свободного пространства, то программа **Дефрагментация диска** выполнит только частичную дефрагментацию.
4. Дефрагментируйте тома после установки программного обеспечения, после выполнения обновления или чистой установки Windows, так как после установки программного обеспечения тома часто фрагментируются.

Архивация данных

Для защиты данных компьютера от случайной утери в случае, если в системе возникнет сбой оборудования или носителя, используется стандартная программа архивации. С помощью программы архивации можно создать резервную копию данных на жестком диске, а затем создать архив на другом устройстве хранения данных. Носителем архива может быть логический диск (например, жесткий диск), отдельное устройство (такое, как съемный диск) или целая библиотека дисков или лент.

Программа архивации предоставляет следующие возможности:

- архивация выбранных файлов и папок на магнитном диске;
- восстановление архивированных файлов и папок на локальный жесткий диск или любой другой доступный диск;
- использование средства аварийного восстановления системы для сохранения и восстановления всех системных файлов и параметров конфигурации, необходимых для восстановления системы после сбоя;
- создание копии данных из любого внешнего хранилища или данных, хранящихся на присоединенных дисках;

- создание копии данных состояния системы локального компьютера;
- создание копии системного раздела, загрузочного раздела и файлов, необходимых для загрузки системы в случае сбоя компьютера или сети;
- планирование периодического выполнения архивации для получения текущих версий архивов.

Создание архива данных

Для архивации в файл необходимо задать имя файла и место, где он будет сохранен. Файлы архива обычно имеют расширение BKF, но его можно сменить на любое другое. Файл архива можно сохранить на жестком диске, дискете или на любом другом съемном либо несъемном носителе, на котором возможно сохранение файлов. Для архивации данных на ленту необходимо, чтобы к компьютеру был подключен накопитель на магнитной ленте, а для управления накопителями на магнитной ленте имелась оснастка Съемные ЗУ.

Чтобы заархивировать данные состояния системы, запустите приложение Архивация, выбрав в меню Пуск команды **Программы-Стандартные-Служебные-Архивация данных**. По умолчанию программа архивации запускается в режиме мастера, если этот режим не отключен. Для переключения в расширенный режим нажмите кнопку «Расширенный» в окне мастера архивации. Вкладка **Добро пожаловать** предоставляет пользователю выбор из трех вариантов использования программы: Мастер архивации, Мастер восстановления и Мастер аварийного восстановления системы.

Для архивации выбранных файлов и папок на жестком диске перейдите на вкладку **Архивация** и установите флажки в списке **Установите флажки** для всех объектов, которые вы хотите заархивировать, как показано на рис. 6.

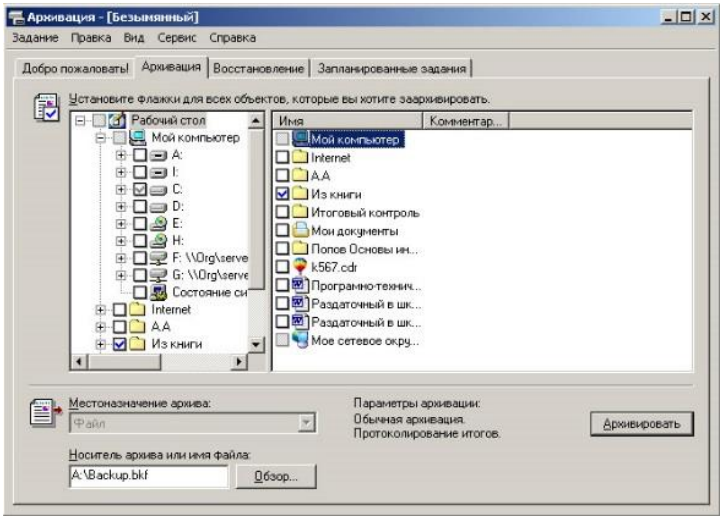


Рис. 6. Определение объектов для архивации

Восстановление файлов и папок из архива

Для восстановления файлов и папок запустите программу **Архивация данных**, на вкладке **Восстановление и управление носителем** на дереве архивированных файлов и папок выберите объекты для восстановления, затем выберите один из трех вариантов размещения восстанавливаемых файлов и папок из архива, как показано на рис. 7.

Различие в вариантах размещения восстанавливаемых файлов и папок из архива заключается в следующем:

Восстановление в исходную папку (или папки), из которой была выполнена архивация, применяется при восстановлении поврежденных или утерянных файлов и папок.

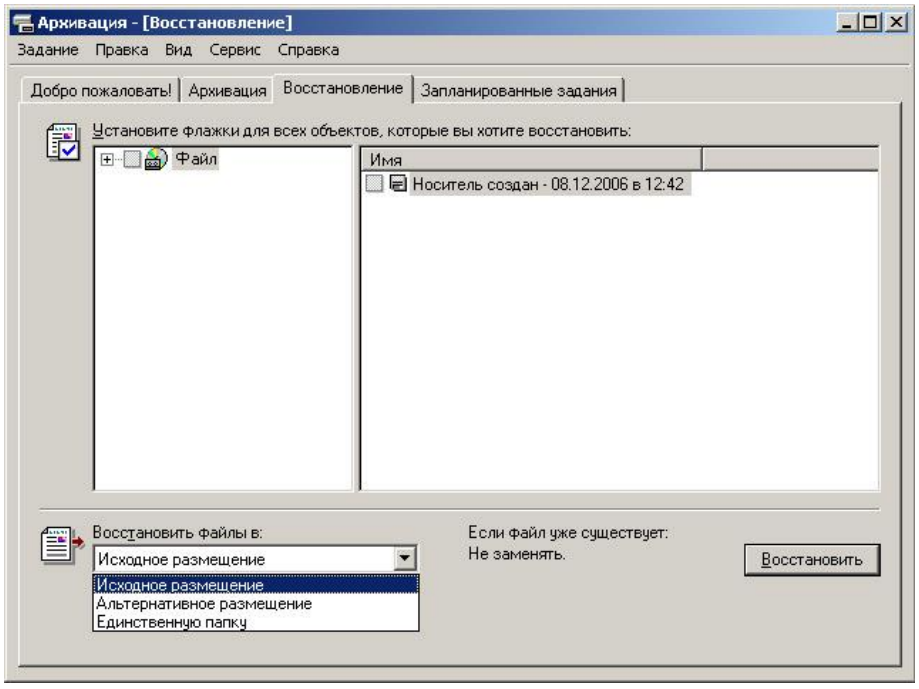


Рис. 7. Выбор объектов для восстановления

Восстановление в любую альтернативную папку применяется, если требуется извлечь несколько старых файлов, но нельзя заменять все остальные текущие файлы и папки на диске.

Восстановление архивированных файлов в одну папку с сохранением структуры архивированных файлов и папок используется при поиске файла, если неизвестно его расположение.

Для выбора способа восстановления файлов и папок выберите в меню **Сервис** команду **Параметры**, после чего в окне *Параметры* выберите один из трех вариантов, как показано на рис. 8, и щелкните на кнопке «ОК».

Различия между способами восстановления уже имеющихся файлов следующие:

1. Выбор варианта **Не заменять файл на компьютере** предотвратит замену файлов, находящихся на жестком диске. Этот вариант является самым безопасным режимом восстановления уже имеющихся файлов.
2. Выбор варианта **Заменять файл на компьютере**, только если он старее, будет гарантировать, что если со времени последней архивации данных были изменены какие-либо файлы, то внесенные изменения не будут утеряны.
3. Вариант **Всегда заменять файл на компьютере** приведет к потере внесенных со времени последней архивации данных изменений в уже имеющиеся файлы.

Для завершения определения параметров восстановления щелкните на кнопке «ОК», а затем нажмите кнопку «Восстановить» для начала процесса.

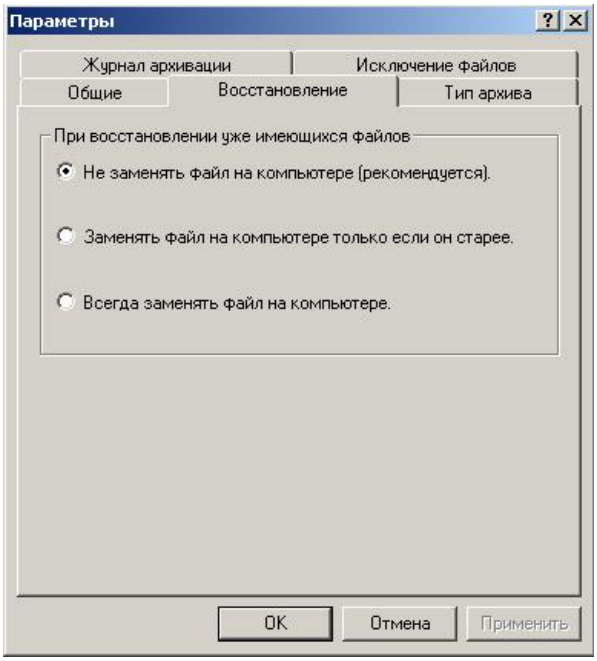


Рис. 8. Выбор способа восстановления файлов и папок

Задания к лабораторной работе №12

1. Используя программу Сведения о системе, определите следующие параметры компьютерной системы: сведения об имеющихся на компьютере портах, звуковом устройстве, о системных драйверах и автоматически загружаемых программах.
2. Используя стандартную программу Windows Проверка диска, проверьте диск A: на наличие поврежденных секторов и ошибок файловой системы. При этом если будут обнаружены ошибки, то задайте режим восстановления поврежденных секторов диска автоматического исправления системных ошибок.
3. Используя стандартную программу Очистка диска, выполните очистку диск D:.
4. Используя стандартную программу Дефрагментация диска, выполните оценку фрагментированности файлов на диске D: и, если требуется, то выполните дефрагментацию этого диска.
5. Используя служебную программу Архивация данных, архивируйте данные из папки C:\Program Files\Microsoft OfficeYTemplates вархив с именем Templates на диске D:.

Контрольные вопросы

1. Почему при эксплуатации компьютерной системы важно знать ее параметры?
2. Какие стандартные средства Windows XP обеспечивают пользователю возможность определения параметров компьютерной системы?
3. Почему обеспечение бесперебойной работы дисковой системы компьютера является одной из основных мер обеспечения информационной безопасности?
4. Опишите причины нарушений в работе магнитных дисков.
5. Почему необходима процедура очистки диска?
6. Что такое фрагментация файла? Почему она возникает и как влияет на скорость операций чтения информации с диска?
7. В каких случаях рекомендуется выполнить дефрагментацию диска?
8. С какой целью выполняется архивация данных компьютера?
9. Что такое дискета аварийного восстановления? Какой программой она создается?
10. Какие вы знаете программы восстановления информации на магнитных дисках?

Список используемых источников

1. . Галатенко В. А. Основы информационной безопасности. – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2008. – 208 с.

2. Астахов А. Анализ защищенности корпоративных автоматизированных систем // Jet Info [Эл. ресурс] – URL: www.jetinfo.ru\2002\7\1\article1.7.2002.html

3. Доля А. Внутренние угрозы ИТ-безопасности. // Byte-Россия [Эл. ресурс] – N 12, 2004. – URL: www.bytemag.ru/?ID=603365

4. Доля А. Внутренние ИТ-угрозы в России 2006 // Компьютер-Пресс N 5, 2007.

5. Грудзаев С. Полезные мелочи - Aladdin Security Solution // LAN [Эл. ресурс] – URL: http://www.osp.ru/lan/2008/05/5068377/

6. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред.В.Ф. Шаньгина.-2-е изд., перераб. и доп. - М.: Радио и связь, 2001. - 376 с.

7. Галатенко В. А. Стандарты информационной безопасности. – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2005. - 264 с.

8. Lonely R. Алгоритм шифрования данных с открытым ключом RSA. [Эл. ресурс] – URL: www.rusdoc.ru/material/raznoe/rsa.shtml

9. Лапонина О. Р. Криптографические основы безопасности: курс лекций для Интернет-университета информационных технологий.

10. Антивирусная защита компьютерных систем: курс лекций для Интернет-университета информационных технологий от лаборатории Касперского – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2007. – URL: www.intuit.ru/department/security/antiviruskasp/

11. Вирусы и средства борьбы с ними: курс лекций для Интернету-ниверситета информационных технологий от лаборатории Касперского – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2007. – URL: www.intuit.ru/department/security/viruskasper/

12. Атака через Интернет / Медведовский И. Д., Семьянов П. В., Платонов В. В.; под ред. П. Д. Зегжды. - СПб.: изд. НПО «Мир и семья-95», 1997.

13. Мэйволд Э. Безопасность сетей: курс лекций для Интернетуниверситета информационных технологий – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2006. – URL: www.intuit.ru/department/security/netsec/

14. Кобб М. Джост М. Безопасность IIS: курс лекций для Интернетуниверситета информационных технологий – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2006. – URL: www.intuit.ru/department/internet/iissecurity/

15. Бейс Р. Введение в обнаружение атак и анализ защищенности // НИП «Информзащита» [Эл. ресурс] - URL: http://bugtraq.ru/library/books/icsa/

16. Семенов Ю. А. Процедуры, диагностики и безопасность в Интернет: курс лекций для Интернет-университета информационных технологий – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2007. – URL: www.intuit.ru/department/network/pdsi/

17. Пировских А. Взлом WPA // TNG.ru [Эл. ресурс] - URL: www.thg.ru/network/20050806/print.html

18. Таранов А., Слепов О. Безопасность систем электронной почты // Jet Info [Эл. ресурс] - № 6, 2003. – URL: www.citforum.ru/security/internet/email/article1.6.2003.html#AEN11

19. Иржавский А. Безопасность электронной почты // CIO - № 8, 2003. – URL:offline.cio-world.ru/2003/18/29383/index.html

20. Карпов В. Е., Коньков К. А. Основы операционных систем. – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2005. - 536 с.

21. Коньков К. А. Устройство и функционирование ОС Windows. – М.: Интернет-университет информационных технологий - ИНТУИТ.ру, БИНОМ. Лаборатория знаний, 2008. - 208 с.

22. Коньков К. А. Основы организации операционных систем Microsoft Windows: курс лекций для Интернет-университета информационных технологий – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2007. – URL: www.intuit.ru/department/os/osmswin/

23. Казарин О. В. Безопасность программного обеспечения компьютерных систем. – М.: МГУЛ, 2003. – 212 с. – URL: www.citforum.ru/security/articles/kazarin/#1-5

24. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Уч. пособие для вузов. – М.: Горячая линия – Телеком, 2004. – 280 с.

25. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещериков, А. А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

26. Грушо А. А. Тимонина Е. Е. Теоретические основы защиты информации. - М.: Изд. агентства «Яхтсмен», 1996. – 72 с.

27. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. – М.: Юниор, 2003. – 504 с.

28. Ярочкин В. И. Информационная безопасность. Учебное пособие для студентов непрофильных вузов. — М.: Междунар. отношения, 2000. — 400 с.

29. Корнюшин П. Н. Костерин С. С. Информационная безопасность. – Владивосток: ДВГУ, 2003. – 155 с.

30. Халяпин Д. Б. Защита информации. Вас подслушивают? Защищайтесь! – М.: НОУ ШО «Баярд», 2004. – 432 с.

31. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: Наука и Техника, 2004. – 384 с.

32. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003. – 368 с.

33. Будко В. Н. Информационная безопасность и защита информации. Конспект лекций. – Воронеж: ВГУ, 2003. – 86 с.

34. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003. — 328 с.

35. Биккенин Р. Р. Стеганография — современный метод обеспечения безопасности информации // Информация и космос. - N 2, 2006. – С. 89-93.

36. Девянин П. Н. Модели безопасности компьютерных систем: учеб. пособие для студентов высш. учеб. заведений. – М.: Изд. центр «Академия», 2005. – 144 с.

37. Белоусов С. А., Гуц А. К., Планков М. С. Троянские кони. Принципы работы и методы защиты: учебное пособие. – Омск: изд. Наследие. Диалог-Сибирь, 2003. – 84 с.

38. Аналитический бюллетень Secure List – URL: http://www.securelist.com/ru/

39. Электронный учебник по разработке информационной безопасности компьютеров // Help Antivirus – URL: http://help antivirus.ru/developmentsafety/Menu.php

40. Хогланд Г., Мак-Гроу Г. Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 400 с.

41. Макаренко С. И. Анализ математического аппарата расчета качества обслуживания информационно-вычислительной сети на сетевом уровне эталонной модели взаимодействия открытых систем // VII Всероссийская конф. молодых ученых по математическому модели-

рованию и информационным технологиям / ИВТ СО РАН, 2006. [Эл. ресурс] - URL: http://www.ict.nsc.ru/ws/YM2006/10566/article.htm

42. Макаренко С. И. Расчетные соотношения для определения числовых характеристик вероятностной оценки времени задержки трафика в проводном, спутниковом и радио каналах связи // Сборник докладов Всероссийской научно-технической школы-семинара «Передача, обработка и отображение информации при быстропротекающих процессах» / РАРАН, октябрь 2006, г. Сочи. - М.: РПА «АПР», 2006. – С. 147-149.

43. Макаренко С. И., Кихтенко А. В. Вывод расчетных соотношений для времени обслуживания и эффективной пропускной способности спутникового и радио каналов связи.: Ставропольское высшее военное инженерное училище (военный институт). – Ставрополь: 2006. – 24 с. - Библиогр.: с. 19. - Деп. в СИФ ЦВНИ Минобороны РФ 14.05.2007, № 15246. - СИФ ЦВНИ Минобороны РФ, инв. № В6554.

44. Макаренко С. И. Методика оценки времени задержки пакета в канале связи в условиях нестабильности входного трафика // Инфокоммуникационные технологии. 2007. Т. 5. № 3. С. 95-96.

45. Макаренко С. И., Кихтенко А. В. Методика оценки времени задержки пакета в спутниковой сети связи в условиях нестабильности входного трафика // Системы управления и информационные технологии. 2007. № 1.3 (27). С. 344-348.

46. Макаренко С. И., Кихтенко А. В. Показатели качества обслуживания информационно-вычислительной сети АСУ реального времени в условиях нестационарности потоков данных // Авиакосмические технологии и оборудование. Казань-2006: Мат. Международной научно-практической конференции. 15-16 августа 2006 года. - Казань: изд. КГТУ им. А. Н. Туполева, 2006. – С. 173–174.

Учебное издание

Никулин Валерий Владимирович

Методические указания к лабораторно-практическим занятиям по дисциплине «Информационная безопасность», «Безопасность и защита информации»

Компьютерный набор произвел Никулин В.В.

Редактор Лебедева Е.М.

Подписано к печати Формат 60x84. 1/16. Бумага печатная
Усл.п.л. 7,37. Тираж 100 экз. Изд.№

Издательство Брянского государственного аграрного университета
243365, Брянская обл., Выгоничский район, п. Кокино, БГАУ