МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО БРЯНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

Институт энергетики и природопользования
Кафедра информатики, информационных систем и технологий

В.В. НИКУЛИН

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
Лабораторный практикум

Учебно-методическое пособие для студентов направления подготовки 09.03.03 «Прикладная информатика»

Брянская область, 2021

УДК 004.056.5 (076)
ББК 32.97
Н 65

Никулин, В. В. Информационная безопасность. Лабораторный практикум: учебно-методическое пособие для студентов направления подготовки 09.03.03 Прикладная информатика / В. В. Никулин. – Брянск: Изд-во Брянский ГАУ, 2021. – 84 с.

Учебно-методическое пособие адресовано бакалаврам, обучающимся по направлению подготовки 09.03.03 Прикладная информатика изучающих дисциплину «Информационная безопасность».

Рецензенты:
ст. преподаватель кафедры информатики,
информационных систем и технологий
Брянского ГАУ Л.И. Бишутина

Рекомендовано методической комиссией института энергетики и природопользования от 30.08.2021, протокол № 1.

Содержание

Введение

Курс с названием «Информационная безопасность» (Information Security) входит в целый ряд государственных образовательных стандартов по различным специальностям, например, 090102 – «Компьютерная безопасность», 090105 – «Комплексное обеспечение информационной безопасности автоматизированных систем», 090106 – «Информационная безопасность телекоммуникационных систем» и других.

Тематика курса разрабатывается многими авторами, ими к настоящему времени подготовлено достаточно много книг, в том числе и учебных пособий. Обилие этих книг говорит об огромной величине рассматриваемой области, ее постоянном изменении и увеличении.

Актуальность тематики обеспечена высокой динамикой развития информационных технологий и большой зависимостью их от обеспечения информационной безопасности.

Все книги написаны известными специалистами в области информационной безопасности и во многом основаны на передовом зарубежном и отечественном опыте. Однако даже за прошедшее время с момента выхода книг произошли существенные изменения в данной области, например, вышли новые стандарты и рекомендации по вопросам информационной безопасности и новым технологиям, приняты новые законы и другие акты. В связи с этим должно быть переработано и дополнено содержание всех этих книг и курса на их основе. По-видимому, в последующем также надо будет учесть и процесс гармонизации международных и отечественных стандартов, особенности новых.

В настоящее время приобрело популярность получение международных сертификатов путем сдачи соответствующих квалификационных экзаменов.

Одними из наиболее признанных являются сертификаты CISA и CISSP, выдаваемые Международным Информационным Консорциумом по Сертификации Защиты Систем (Information Security Certification Consortium (ISC) 2 – www.isc2.org). Содержание курса должно учитывать требования и соответствующие разделы программ этих экзаменов, чтобы в последующем позволить студентам сдать данные экзамены без больших дополнительных усилий.

В настоящее время в России идет процесс формирования системы требований информационной безопасности для 6 организаций банковской системы, созданы несколько стандартов, система сертификации, методика проверки требований. Конечно, при этом использовался зарубежный опыт, но отечественные разработчики и специалисты по информационной безопасности внесли много нового в этот процесс.

Лабораторная работа №1. Создание виртуальной машины в Windows 10 с помощью диспетчера Hyper-V

Содержание

- Добавляем компоненты Hyper-V.
- Запуск Hyper-V.
- Настройка сети.
- Создание виртуальной машины.
- Изменение параметров виртуальной машины.
- Оборудование. - Управление.

Мы добавим компоненты Hyper-V в Windows 10, рассмотрим вариант создания виртуальной машины с помощью Hyper-V, а также рассмотрим её параметры.

Добавляем компоненты Hyper-V.

Запускаем "Выполнить" любым из двух способов:

1. Жмём правой кнопкой по меню "Пуск" и выбираем "Выполнить». (Рис.1) 2. Нажимаем сочетание клавиш "Win"+"R".

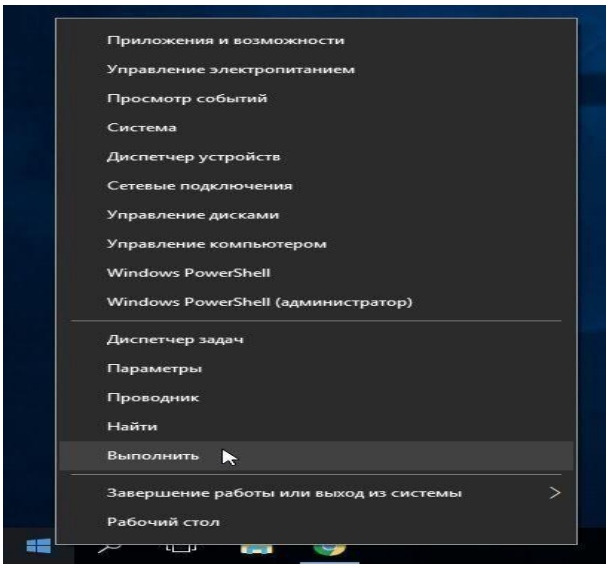


Рисунок 1 - Правой кнопкой "Пуск" -> "Выполнить"

Вводим appwiz.cpl (Рис.2)

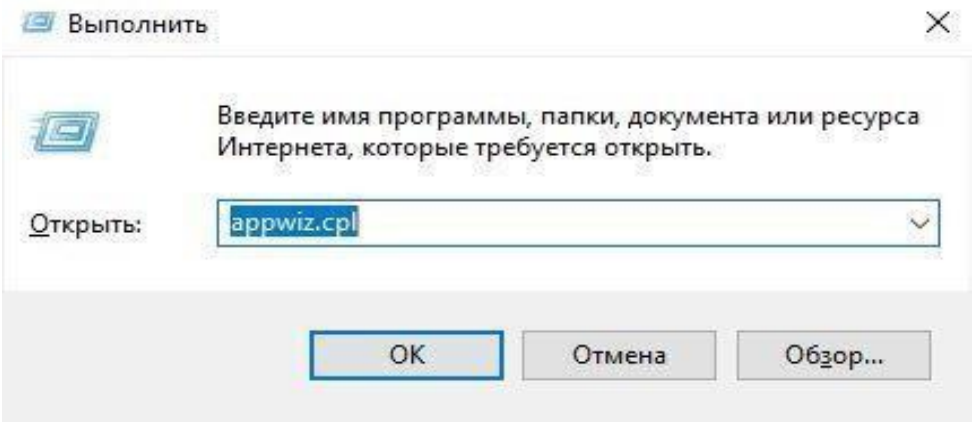


Рисунок 2 - Вводим appwiz.cpl

Откроется окно "Программы и компоненты". Слева нажимаем "Включение или отключение компонентов Windows" (Рис.3).

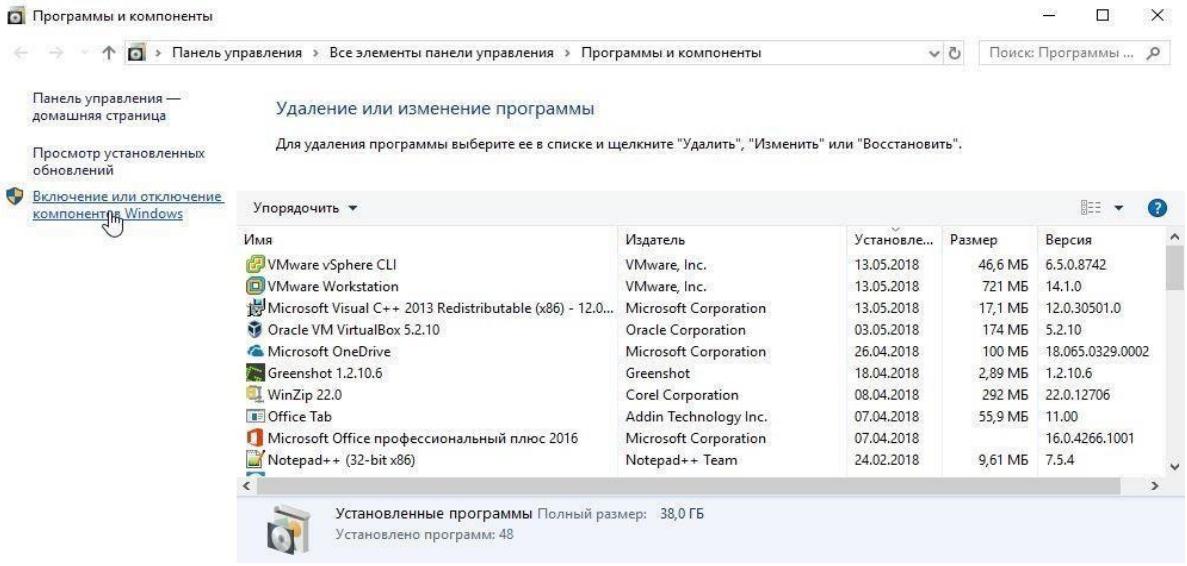


Рисунок 3 - Программы и компоненты

Откроется окно "Компоненты Windows". Выбираем всё что есть в разделе Hyper-V. (Рис.4). Жмём "Ок".

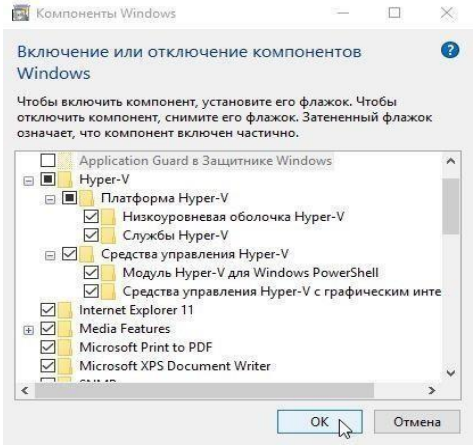


Рисунок 4 - Выбор компонентов Hyper-V

Ждём установку компонентов - Применение изменений, и нажимаем "Перезагрузить сейчас".(Рис.5)

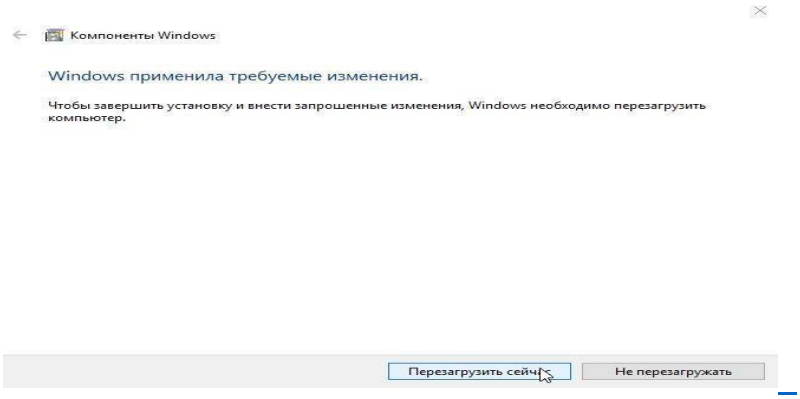


Рисунок 5 - Применение компонентов, перезагрузка системы

На этом Добавление компонентов закончено. Приступаем к работе с Hyper-V **Запуск Hyper-V.**

В меню **"Пуск"** -> **"Средства администрирования Windows"** появился ярлык **"Диспетчер Hyper-V"**. Запускаем его.(Рис.6).

Рисунок 6 - Запускаем Диспетчер Hyper-V

Перед нами стартовое окно **"Диспетчера Hyper-V"**.(Рис.7)

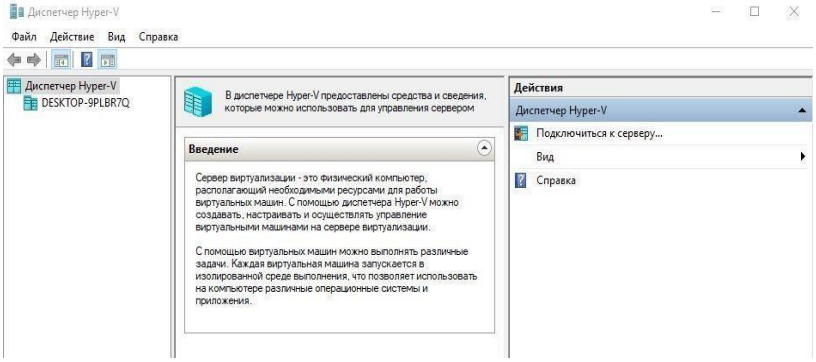


Рисунок 7 - Стартовое окно Диспетчера Hyper-V

Настройка сети.

Выбираем слева наш компьютер, у меня это - **DESKTOP-9PLBR7Q**, справа появится меню **"Действия"**, Нажмите на пункт **"Диспетчер виртуальных коммутаторов"**(Рис.8).

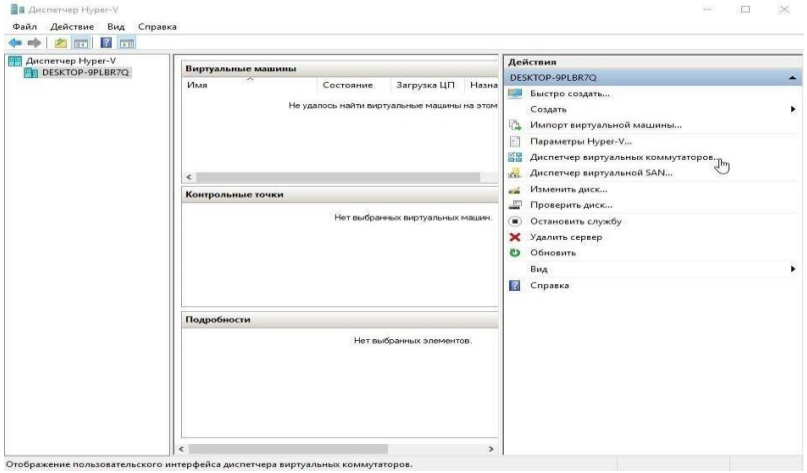


Рисунок 8 - Заходим в Диспетчер виртуальных коммутаторов

В **"Диспетчере виртуальных коммутаторов"** нажмите **"Создать виртуальный коммутатор"**(Рис.9)

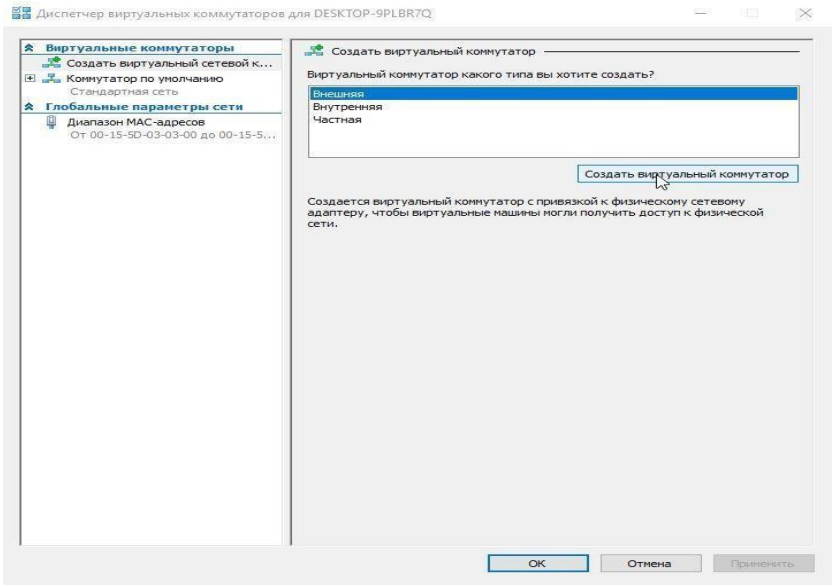


Рисунок 9 - Создаём виртуальный коммутатор

Введите **Имя**, у меня это - **Hypernet** и примечание, у меня это - **Сеть Hyper-V**.(Рис.10) Так же выберете **Тип подключения**. Я выбрал подключение к **Внешней сети** через мою сетевую карту - **"Realtek PCIe GBE Family Controller"**. А также установил галочку в чекбоксе **"Разрешить управляющей операционной системе предоставлять общий доступ к этому сетевому адаптеру"**. Жмём **"Применить"**.

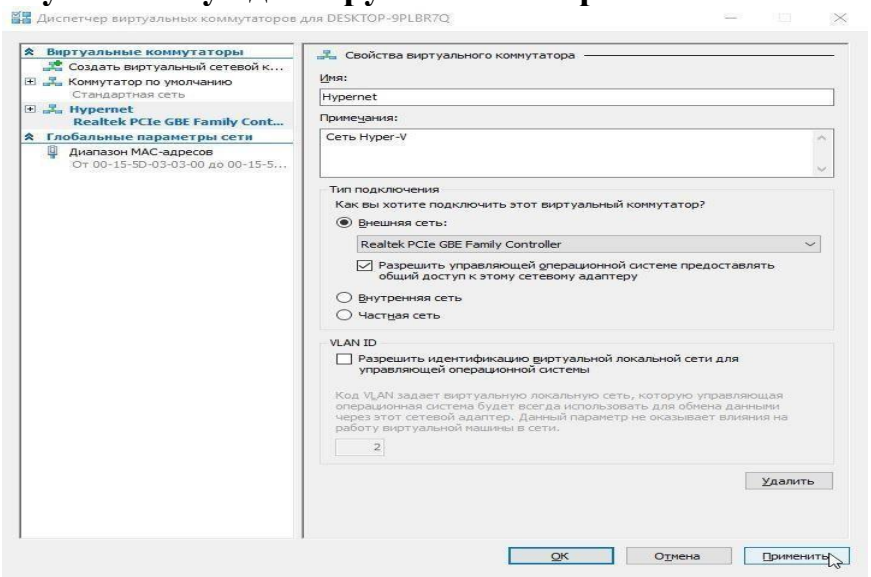


Рисунок 10 - Свойства виртуального коммутатора

Выскакивает предупреждение **"Ожидающие изменения могут нарушить сетевое подключение"** (Рис.11). Я предполагаю, что это будут

читать новички, а значит они вряд ли будут пошагово повторять за мной, используя задействованный сервер, своего предприятия. Следовательно, ничего страшного в том, что мы можем на некоторое время потерять сетевое подключение. Жмём **"Да"** и ждём **"Применение изменений"**.

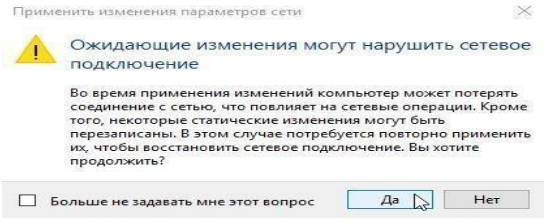


Рисунок 11 - Предупреждение о возможном нарушении сетевого подключения

Теперь зайдя в **"Сетевые подключения" -> "Настройка параметров адаптера"**.

Мы можем увидеть наш только что созданный **vEthernet (Hypernet)**, так же с ним соседствует не подключенный **vEthernet (Коммутатор по умолчанию)** - "Стандартная сеть" автоматически предоставляет виртуальным машинам доступ к сети компьютера с помощью преобразования сетевых адресов (**NAT**). **NAT** на данный момент нам не интересен. И коммутатор этот трогать мы не будем (Рис.12).

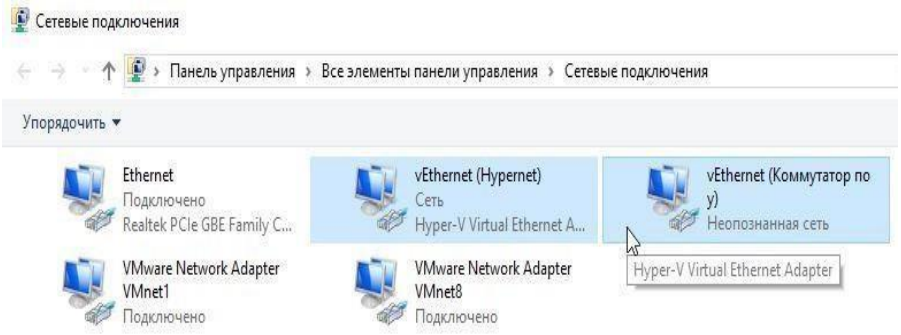


Рисунок 12 - Сетевые подключения -> Настройка параметров адаптера

На этом настройка сети закончена. Переходим к самому главному, тому для чего и создана система виртуализации **Hyper-V** - **Создание виртуальной машины**. **Создание виртуальной машины.** Жмём правой кнопкой по нашему компьютеру **-> "Создать" -> "Виртуальная машина"**.
(Рис.13)

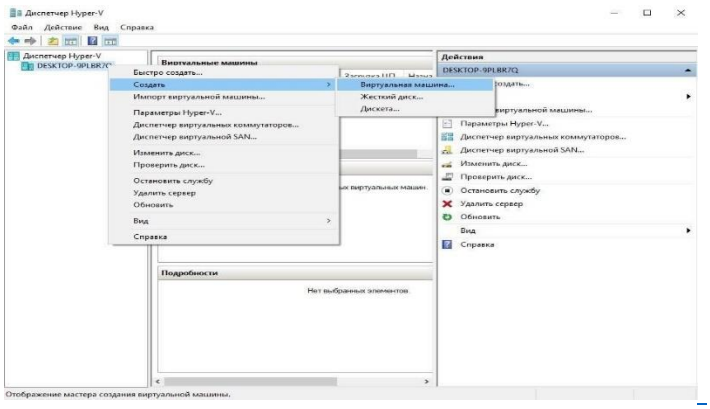


Рисунок 13 - Создание виртуальной машины Hyper-V

Откроется "Мастер создания виртуальной машины".(Рис.14)

- Нажмите кнопку **"Готово"**, чтобы создать виртуальную машину с настройками по умолчанию.
- Нажмите кнопку **"Далее"**, чтобы создать виртуальную машину с особыми параметрами конфигурации.

Жмём **"Далее"** чтобы выбрать нужные нам параметры.

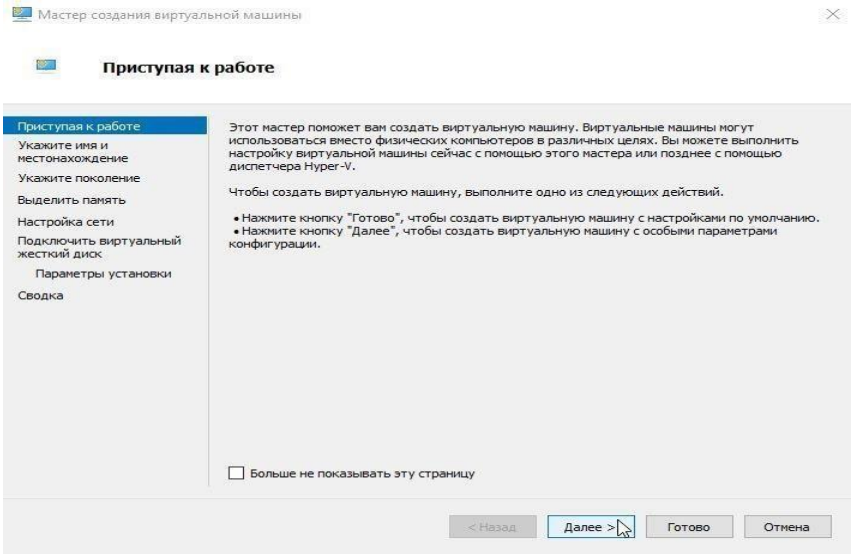


Рисунок 14 - Мастер создания виртуальной машины

Указываем Имя виртуальной машины и её расположение (Рис.15). Я решил протестировать при помощи **Ubuntu Server 18.04** или другую ОС семейства Windows . Поэтому у меня так:

- **Имя:** ubuntuserver 18.04.
- **Расположение:** E:\hyper-v ubuntu server 18.04\.

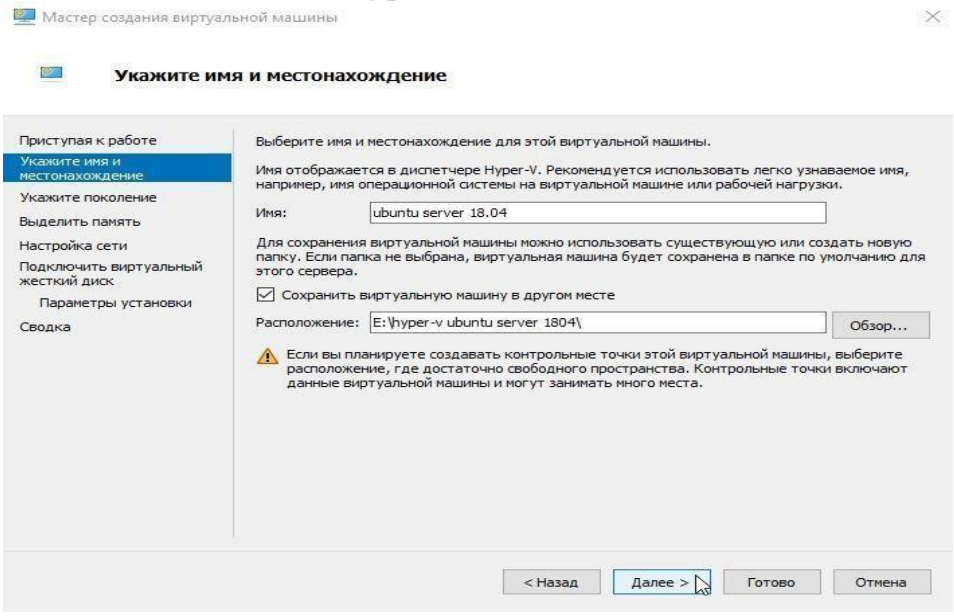


Рисунок 15 - Указываем Имя виртуальной машины и её расположение

Выбираем поколение виртуальной машины (Рис.16) В большинстве случаев стоит выбрать второе поколение, но если вы устанавливаете что-то **32-bit**ное то стоит выбрать - **Поколение -1**.

Лично у меня **Ubuntu Server 18.04 64-bit с** поддержкой **UEFI**, следовательно, я выбираю - **Поколение 2.**

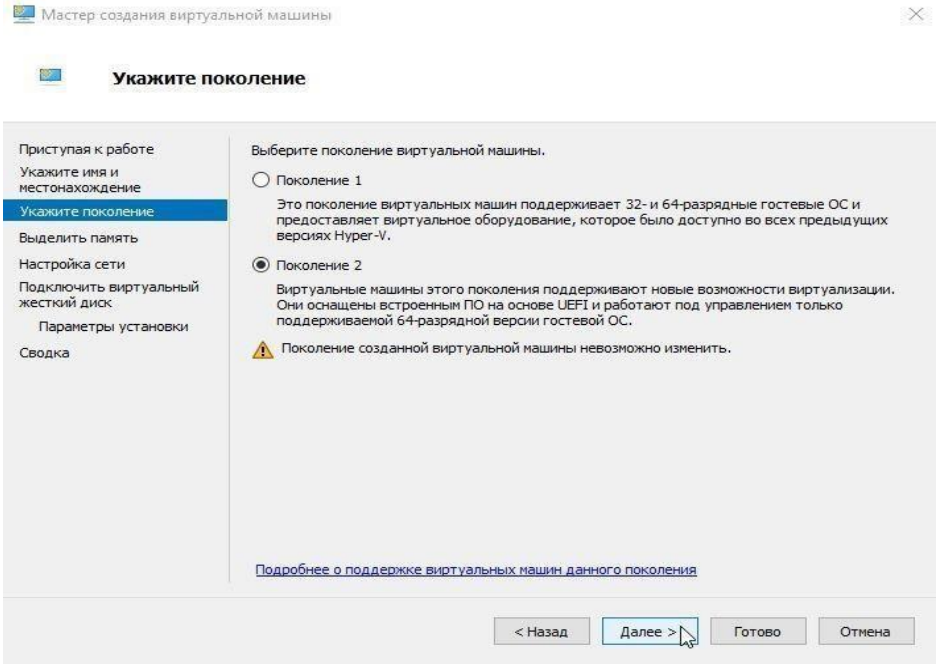


Рисунок 16 - Выбираем поколение виртуальной машины

Выделяем количество оперативной памяти (Рис.17). Моей операционной системе хватит **1Gb ОЗУ** => Я оставляю по умолчанию вписанные **1024 Mb**. Идём **"Далее"**.

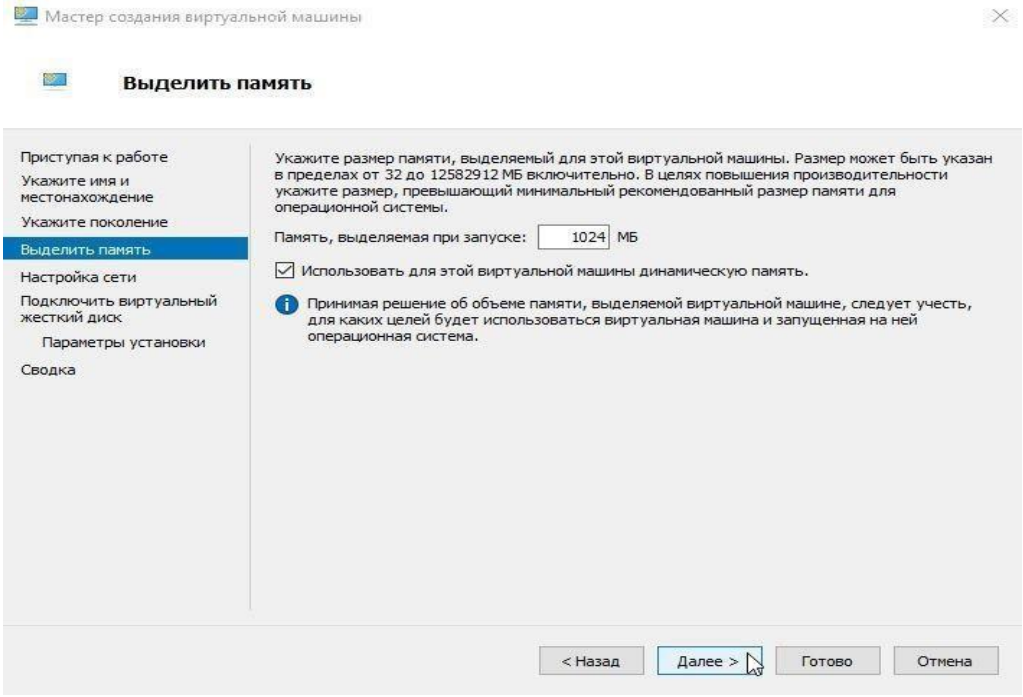


Рисунок 17 - Выделяем количество оперативной памяти

Выбираем к какому коммутатору будет подключен наш сетевой интерфейс. (Рис.18) Выбираем наш **"Hypernet"**, идём **"Далее"**.

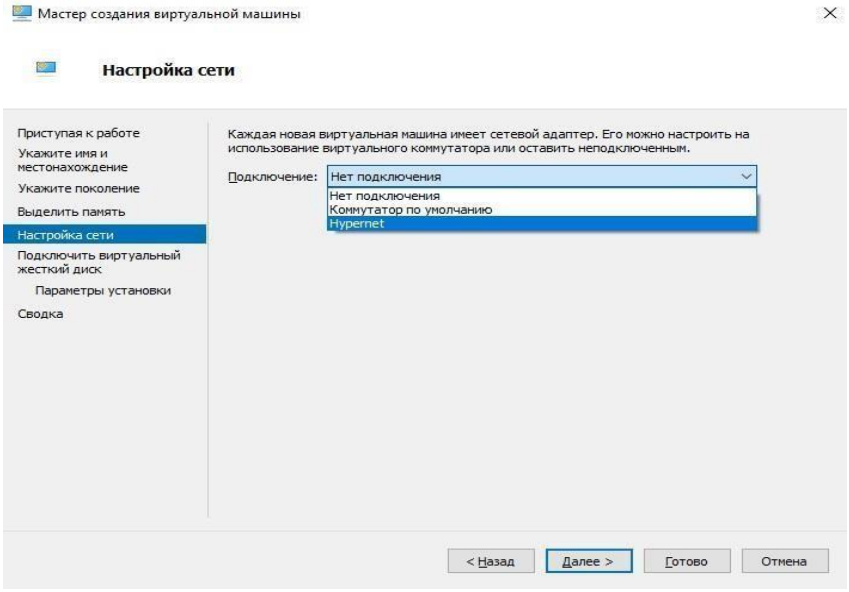


Рисунок 18 - Настройка сети

Создаём виртуальный жёсткий диск (Рис.19).

Указываем **Имя**, **Расположение** и максимальный **Размер** файла виртуального **HDD.**

У меня так:

- **Имя:** ubuntu Server 18.04. vhdx.
- **Расположение:** E:\hyper-v ubuntu server 1804\.
- **Размер:** 10 ГБ.

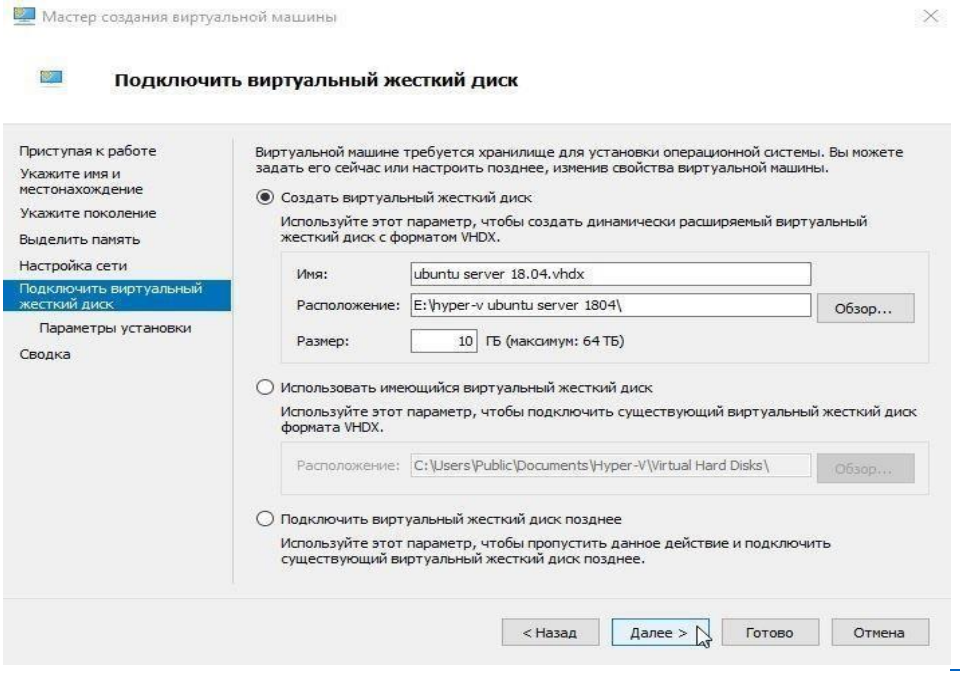


Рисунок 19 - Создаём виртуальный жёсткий диск

Выбираем **ISO-образ** с которого будем устанавливать операционную систему. (Рис.20) Выбираем пункт **"Установить операционную систему из файла загрузочного образа"** > Нажимаем **"Обзор"** -> Выбираем **iso-образ**. -> Жмём **"Далее"**.

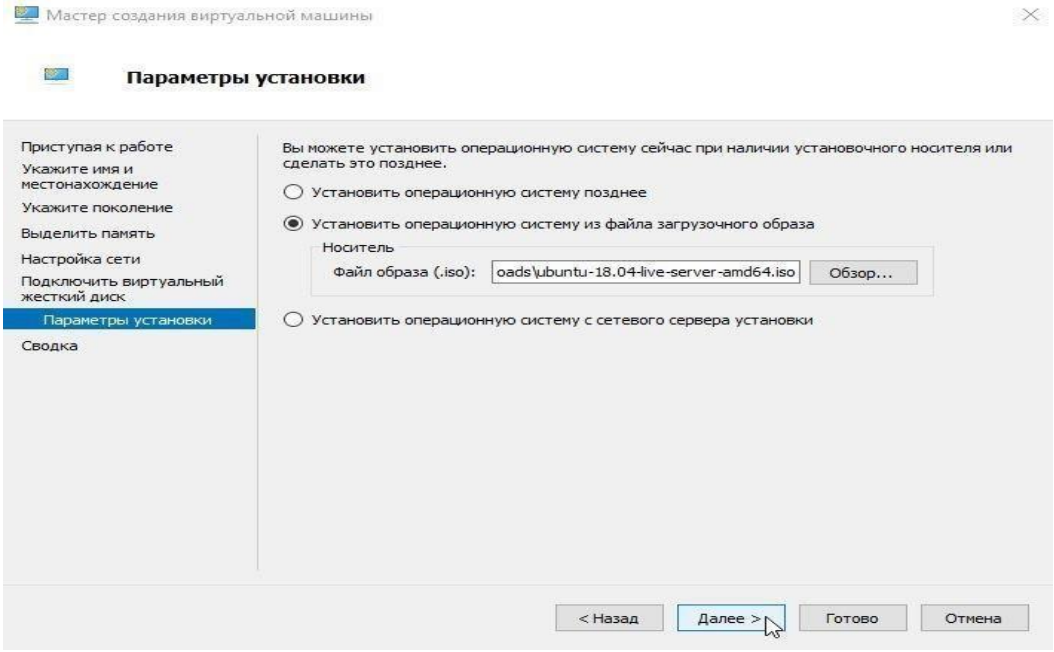


Рисунок 20 - Выбор образа ОС

Завершение работы мастера создания виртуальной машины (Рис.21) Жмём **"Готово"**.

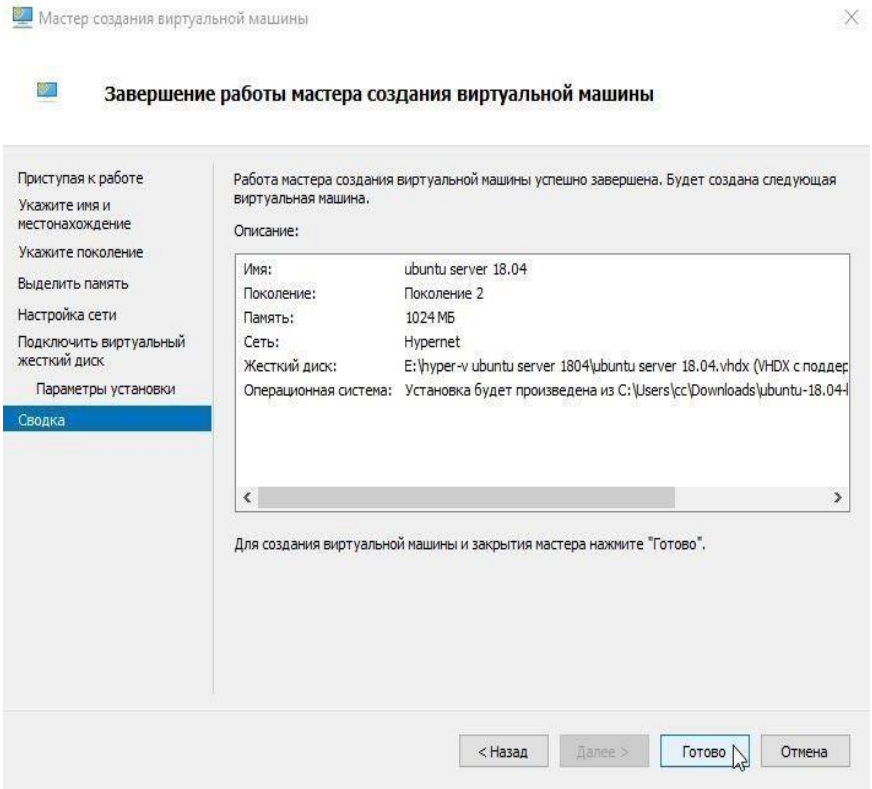


Рисунок 21 - Завершение работы мастера создания виртуальной машины

Теперь в **Диспетчере Hyper-V** мы видим, только что созданную, виртуальную машину - **ubuntu Server 1804**. (Рис.22)

Нажимаем на нее правой кнопкой мыши - > **"Подключить"**.

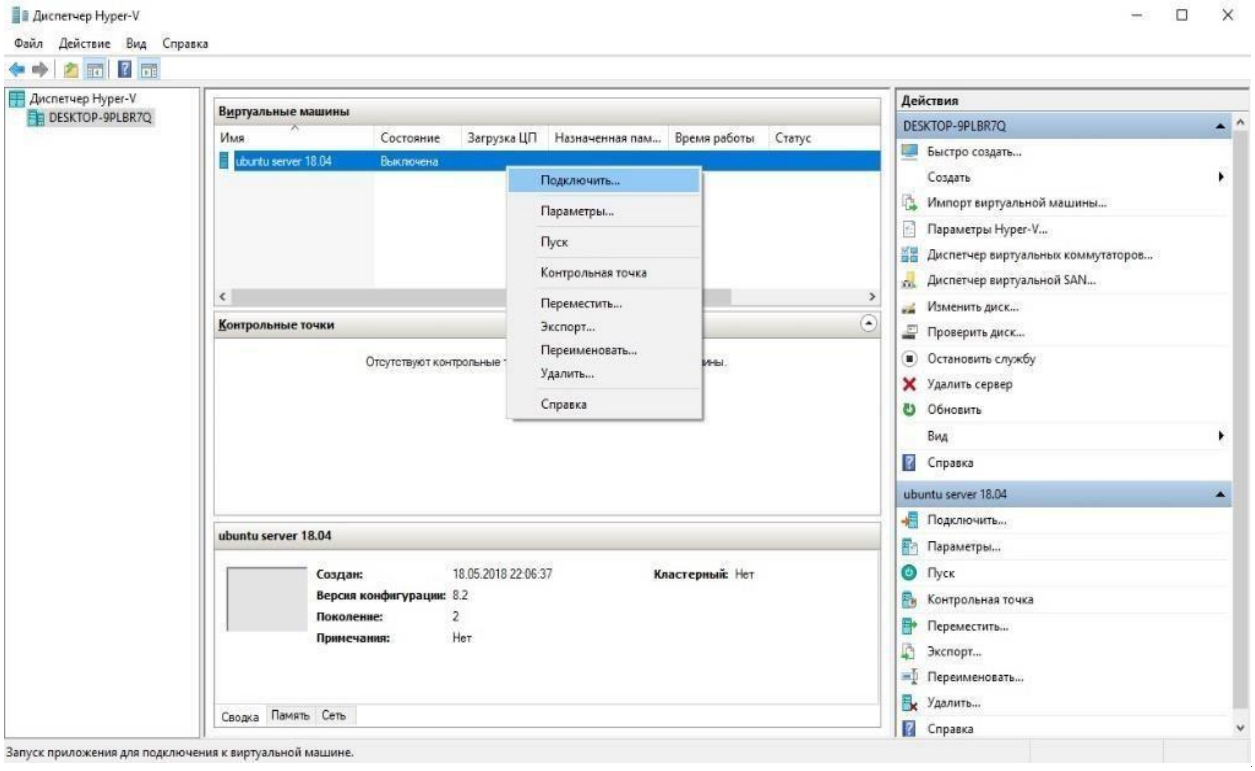


Рисунок 22 - Диспетчер Hyper-V, Новая виртуальная машина

Появится окно **"Подключение к виртуальной машине"** (Рис.23). Если вы хотите установить систему **Windows,** то при нажатии на кнопку **"Пуск"** у вас должна запуститься установка, без каких любо ошибок.

Но для того чтобы запустился **Ubuntu Server 18.04** Пришлось в **"Файл"** - > **"Параметры"** -> **"Безопасность"** отключить **"Безопасную загрузку"**.(Рис.24)

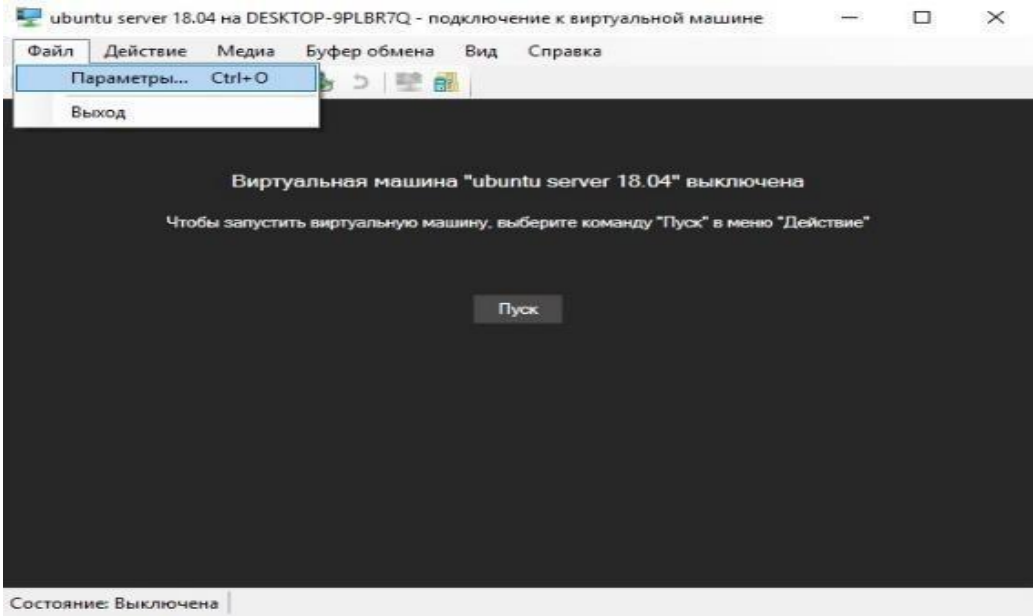


Рисунок 23 - Подключение к виртуальной машине

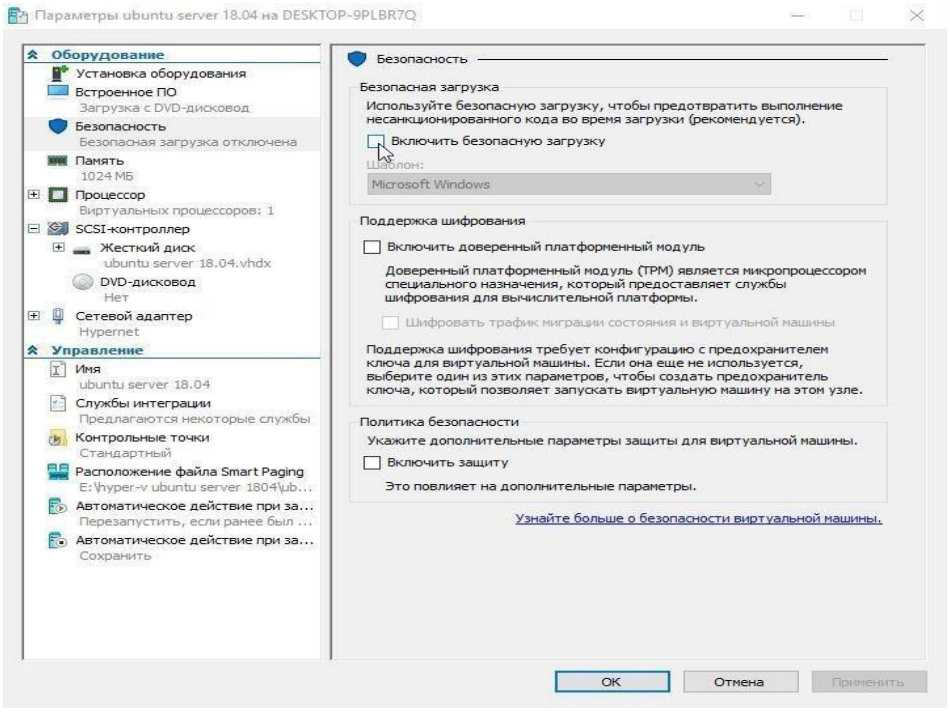


Рисунок 24 - Отключаем Безопасную загрузку

Включаем виртуальную машину (Рис.25)

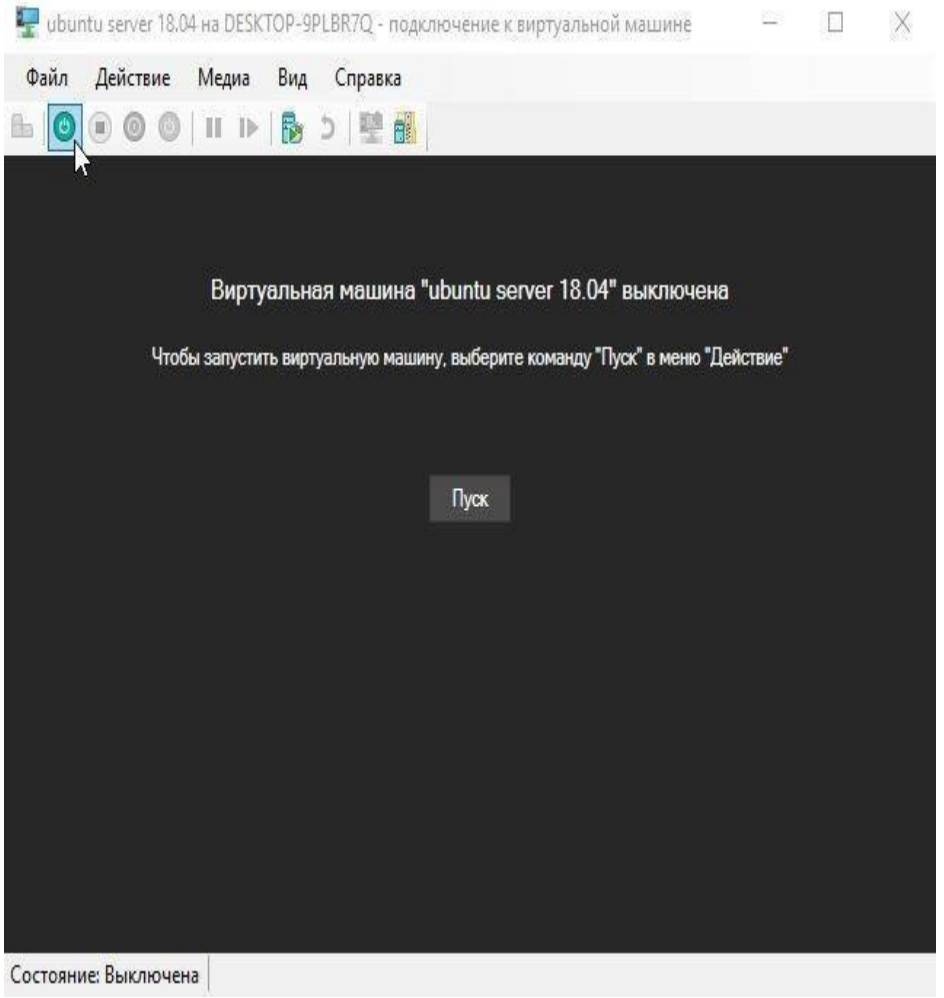


Рисунок 25 - Включаем виртуальную машину

Всё отлично виртуальная машина запустилась. Нас встречает установщик **Ubuntu Server 18.04.**(Рис.26)

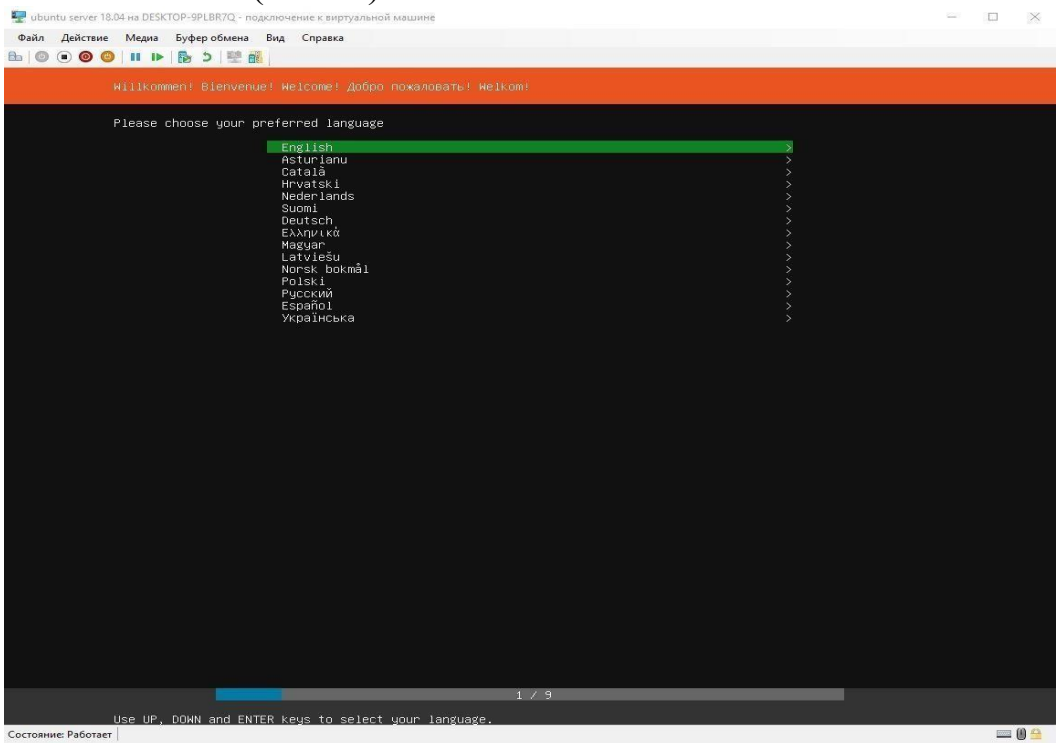


Рисунок 26 - Запущенная виртуальная машина.
Установщик Ubuntu Server 18.04

Изменение параметров виртуальной машины

Сделаем небольшой обзор параметров виртуальной машины, чтобы вы могли посмотреть основные функции до того, как примете решение пользоваться системой виртуализации **Hyper-V**.
Заходим в **"Файл"** - > **"Параметры "Встроенное ПО"** - можно изменить приоритет загрузки устройств в виртуальной машине. (Рис. 27)

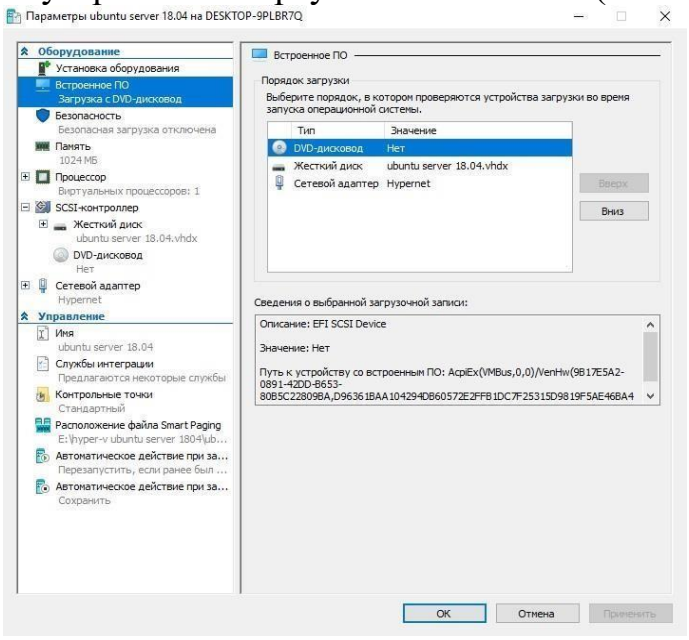


Рисунок 27 - Выбор приоритета загрузки

"Безопасность" - можно **"Включить/Выключить безопасную загрузку"**, "**Включить/Выключить поддержку шифрования"**(Рис.28).

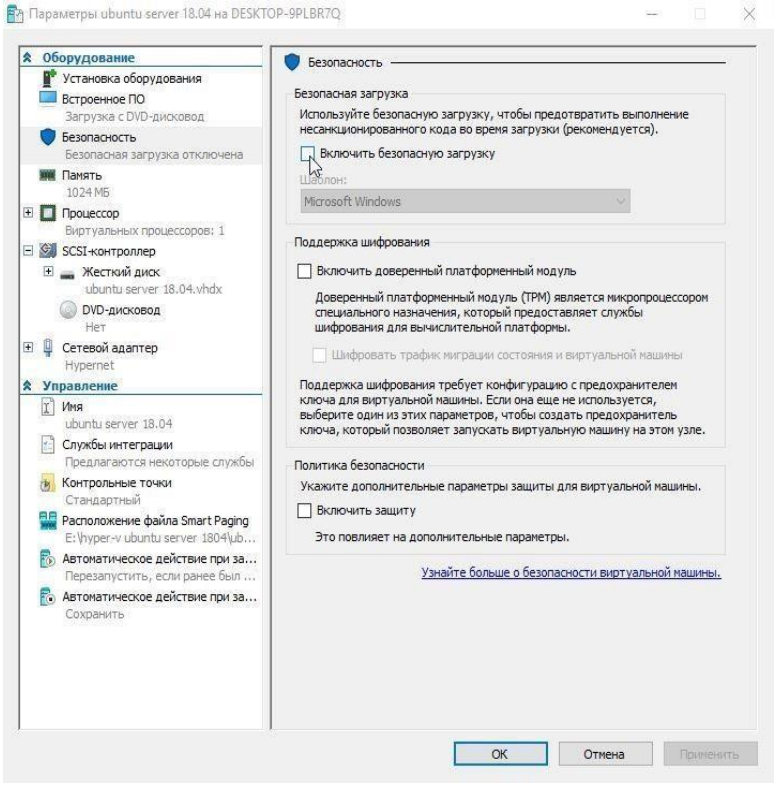


Рисунок 28 - Параметры безопасности виртуальной машины

"Память" - можно отредактировать количество выделяемой **ОЗУ, Включить/Выключить** функцию **Динамическая память** (Рис.29)

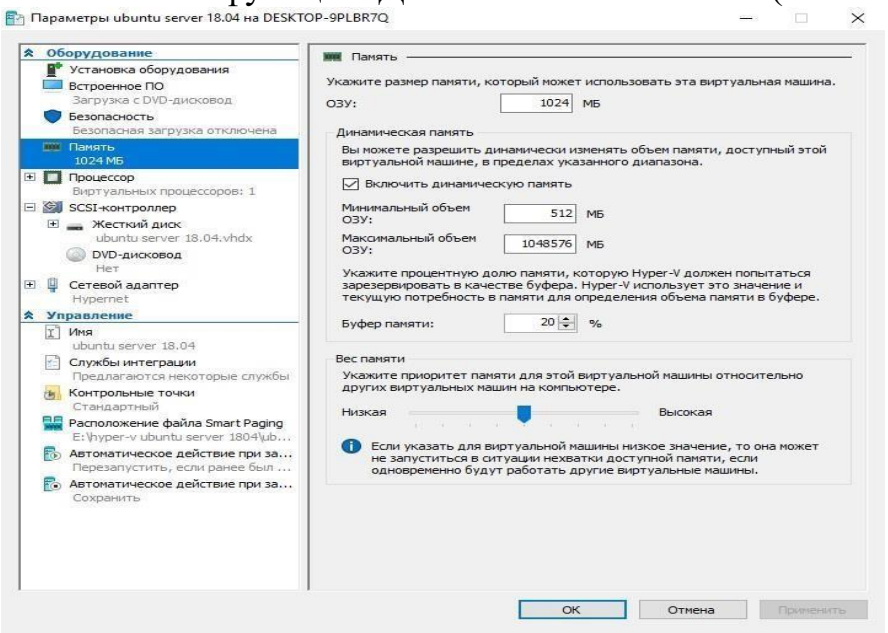


Рисунок 29 - Параметры оперативной памяти

"Процессор" - можно отредактировать число виртуальных процессоров в соответствии с числом процессоров на физическом компьютере (Рис.30). Также можно распределить нагрузку в **"Управление ресурсами"**.

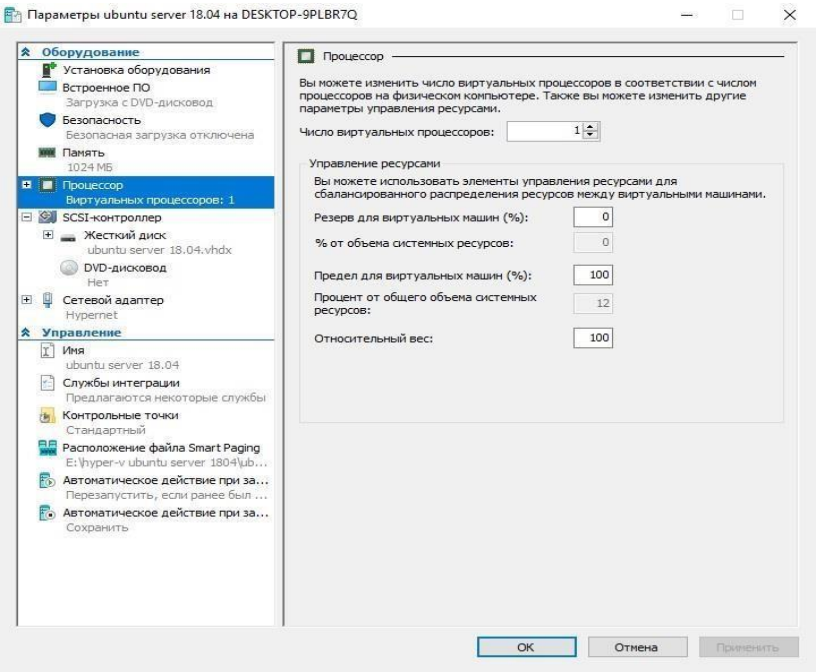


Рисунок 30 - Параметры процессора

"SCSI-контроллер" можно добавить **Жёсткий диск**, **DVD-дисковод** или **Общий диск** (Рис.31).

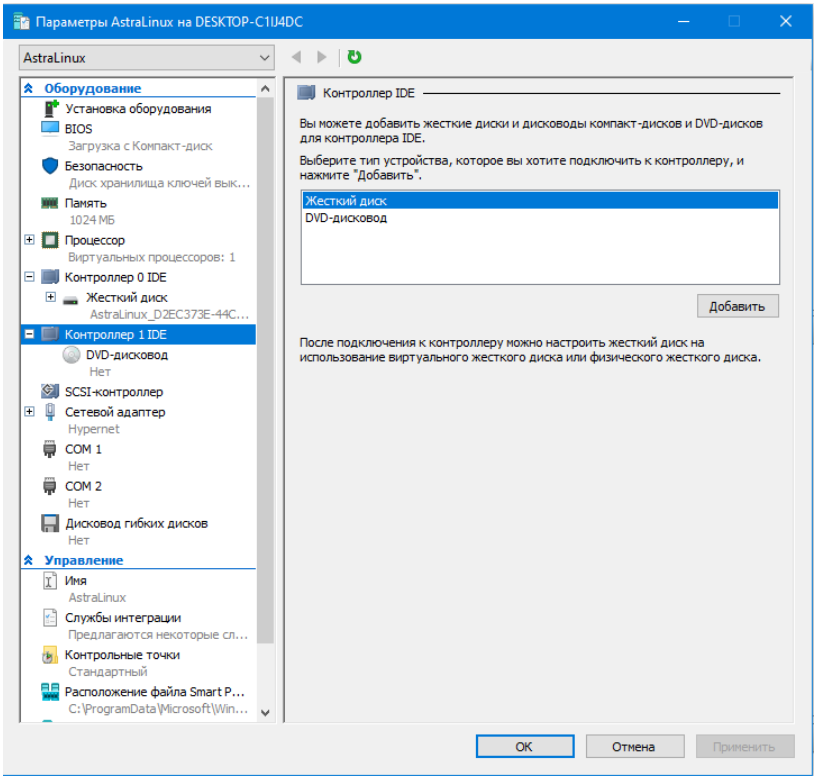


Рисунок 31 – Параметры жесткого диска

Задание

1. Включить диспетчер виртуальных машин hyper-V в Windows 10 создать и настроить виртуальную машину.
2. изучить интерфейс диспетчер виртуальных машин hyper-V.
3. Составить отчет о проделанной работе.

Лабораторная работа № 2. 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).

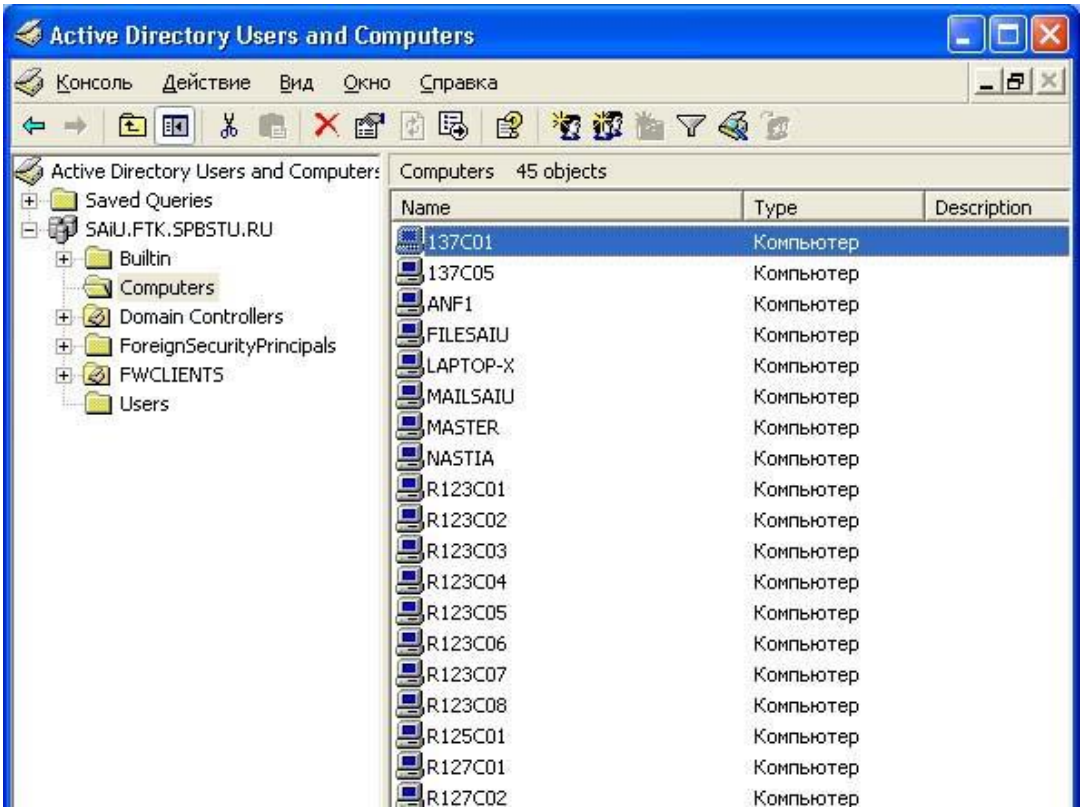


Рисунок 1 - Получение перечня компьютеров домена

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

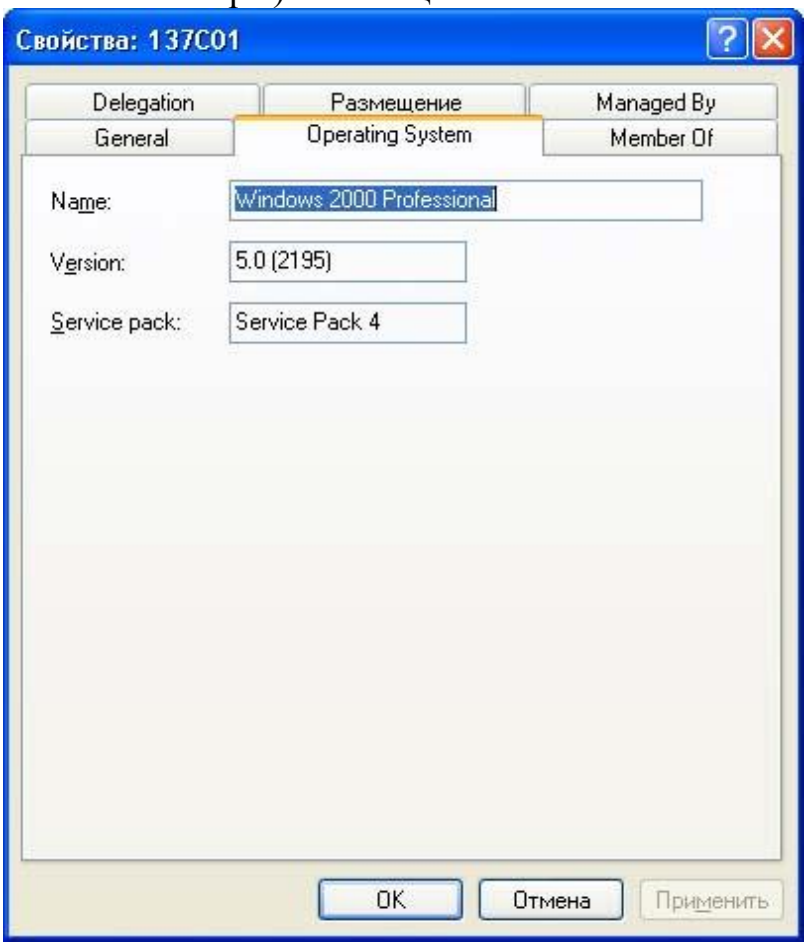


Рисунок 2 - Информация о компьютере

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.

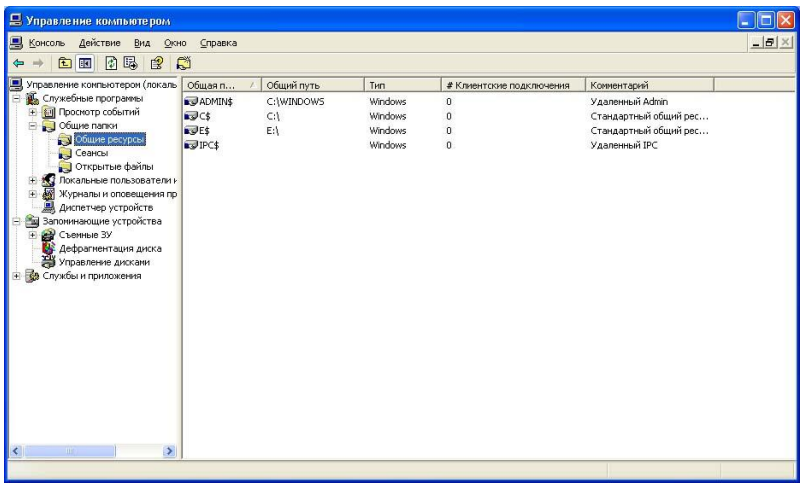


Рисунок 3 - Пример перечня общих ресурсов рабочей станции

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).

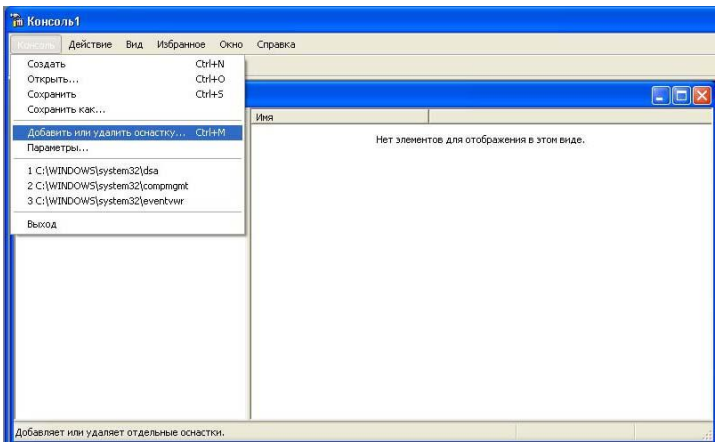


Рисунок - 4 Добавление новой оснастки

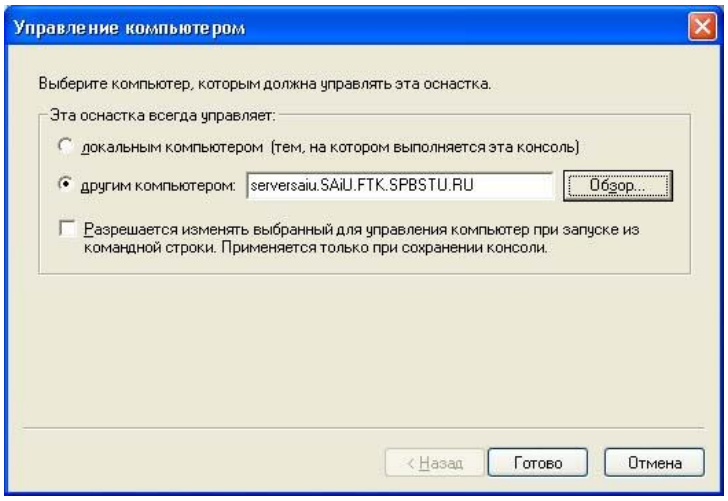


Рисунок 5 - Выбор компьютера

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).

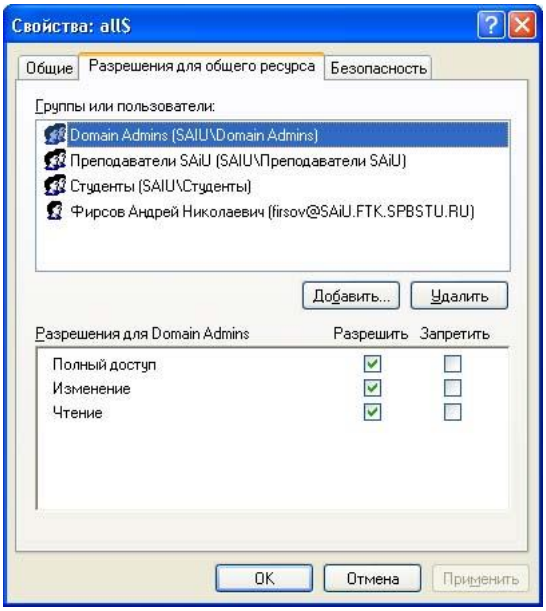


Рисунок 6 - Разрешения

Задания.

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 № 3. 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.

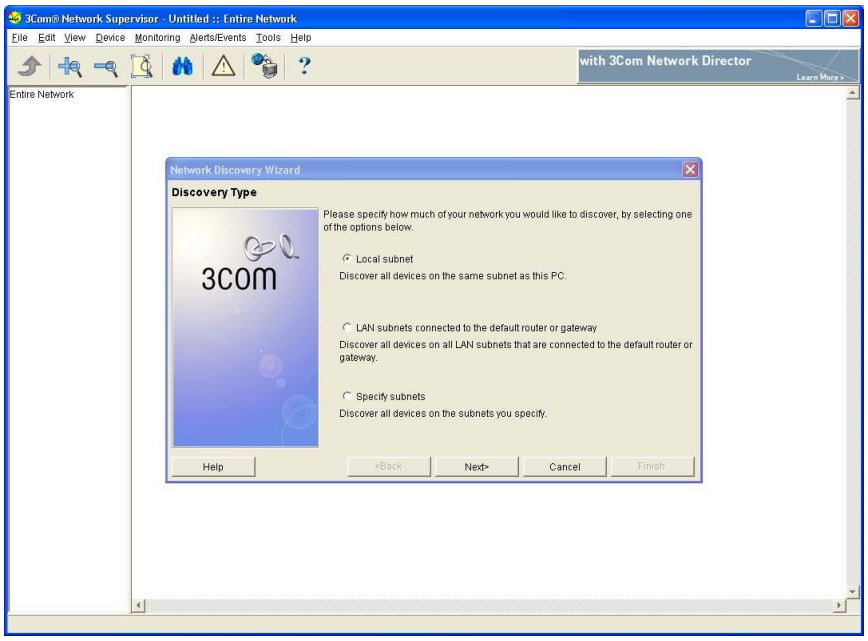


Рисунок 1 - Выбор документируемой сети

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.

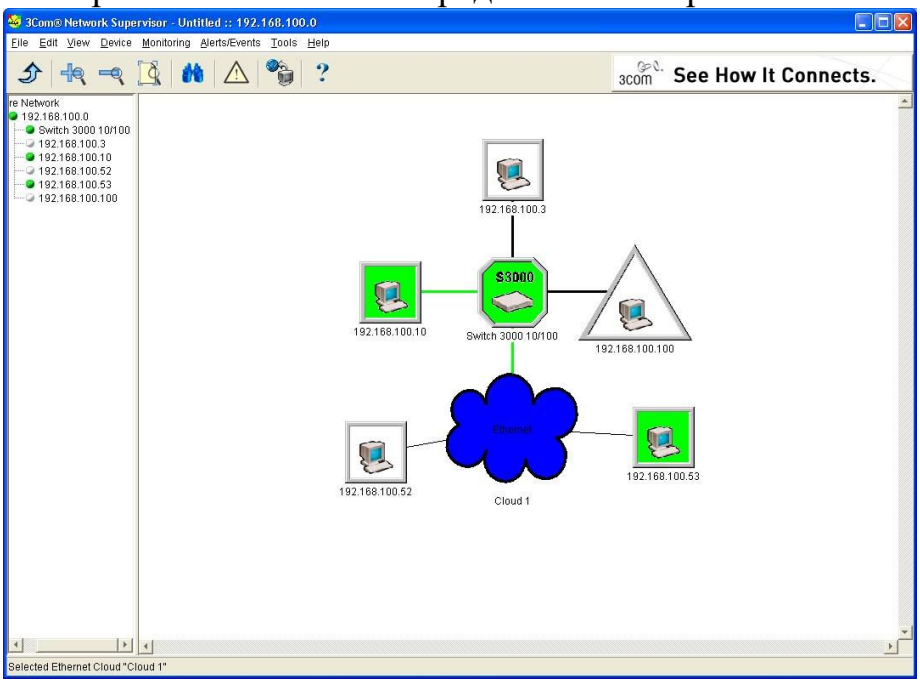


Рисунок - 2. Карта сети 192.168.100.0. Cloud 1 скрывает неуправляемый коммутатор

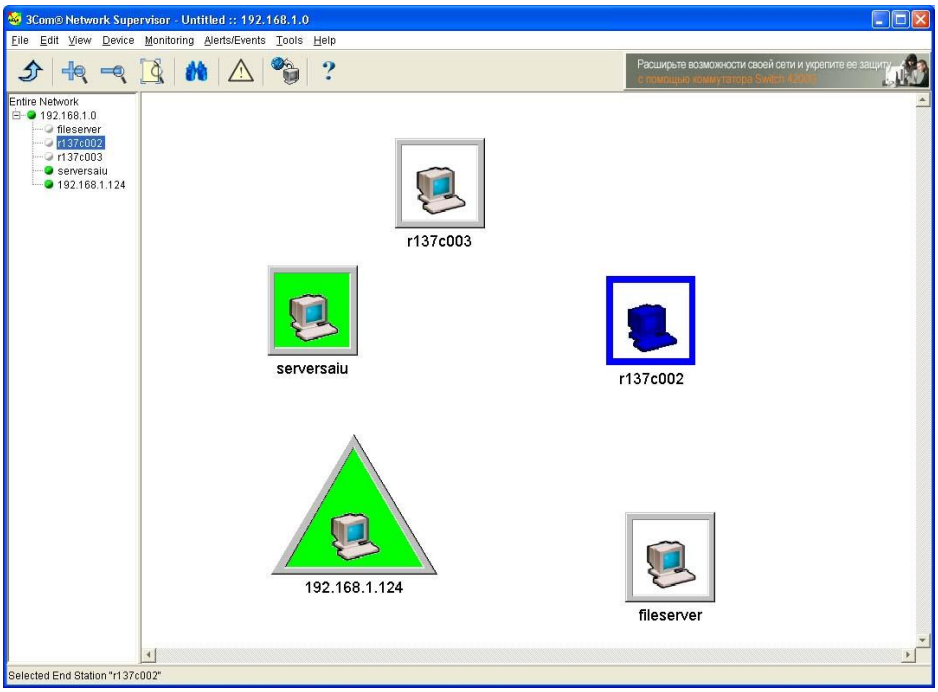


Рисунок 3 - Карта сети 192.168.1.0. Информация от управляемого коммутатора недоступна

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).

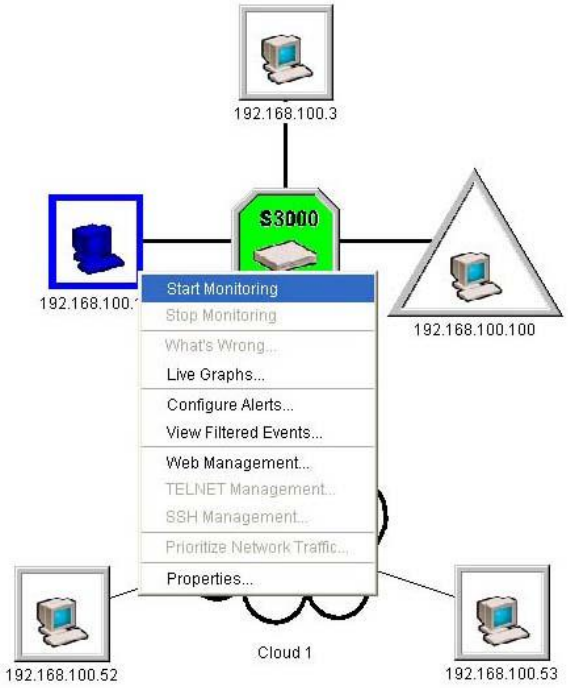


Рисунок 4 - Функции, доступные для выбранного узла

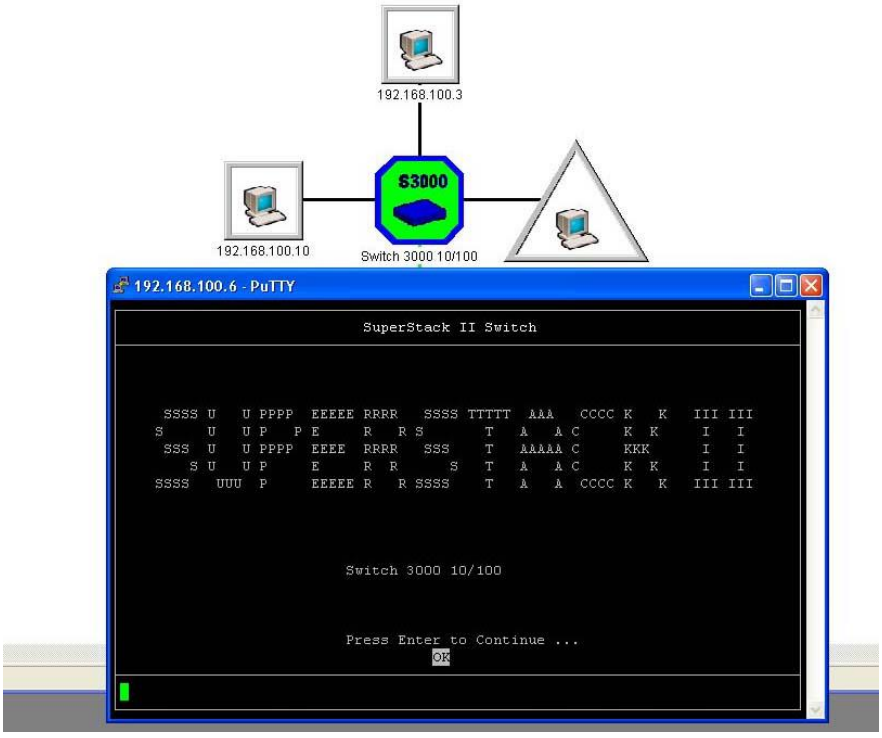


Рисунок 5 - Запуск удаленного терминала для администрирования коммутатора Switch 3000

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).

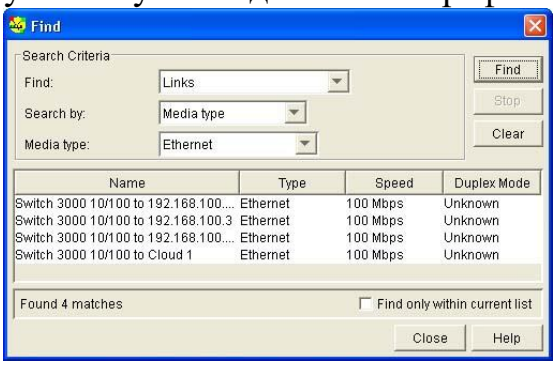


Рисунок 6 - Соединения по типам подключений. Ethernet

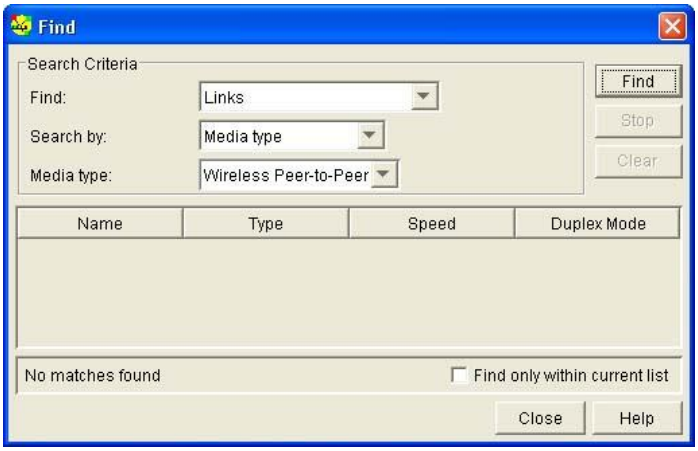


Рисунок 7 - Соединения по типам подключений. Беспроводные подключения (отсутствуют)

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).

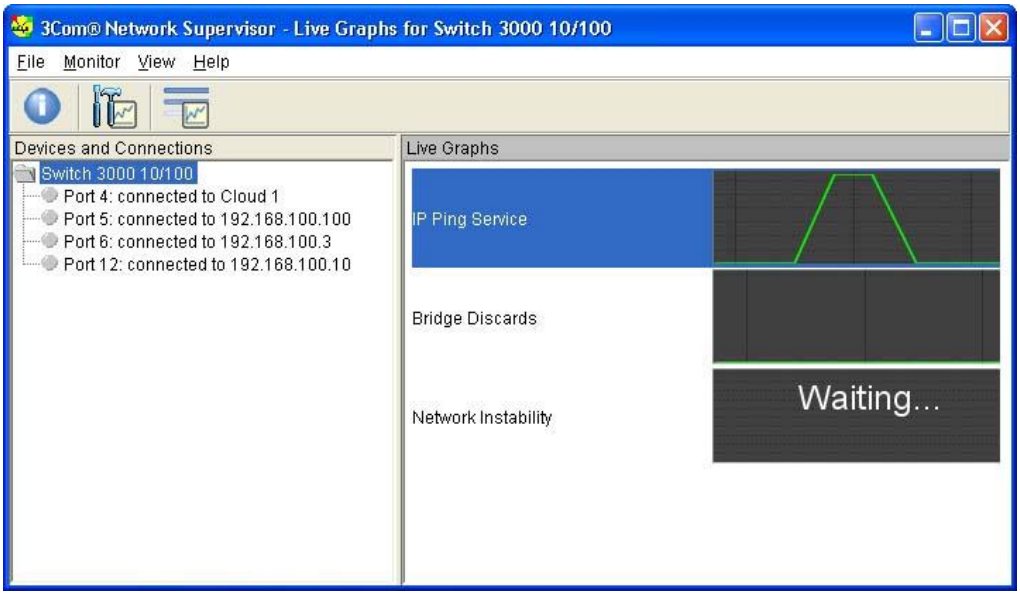


Рисунок 8 - Данные о подключениях и графики

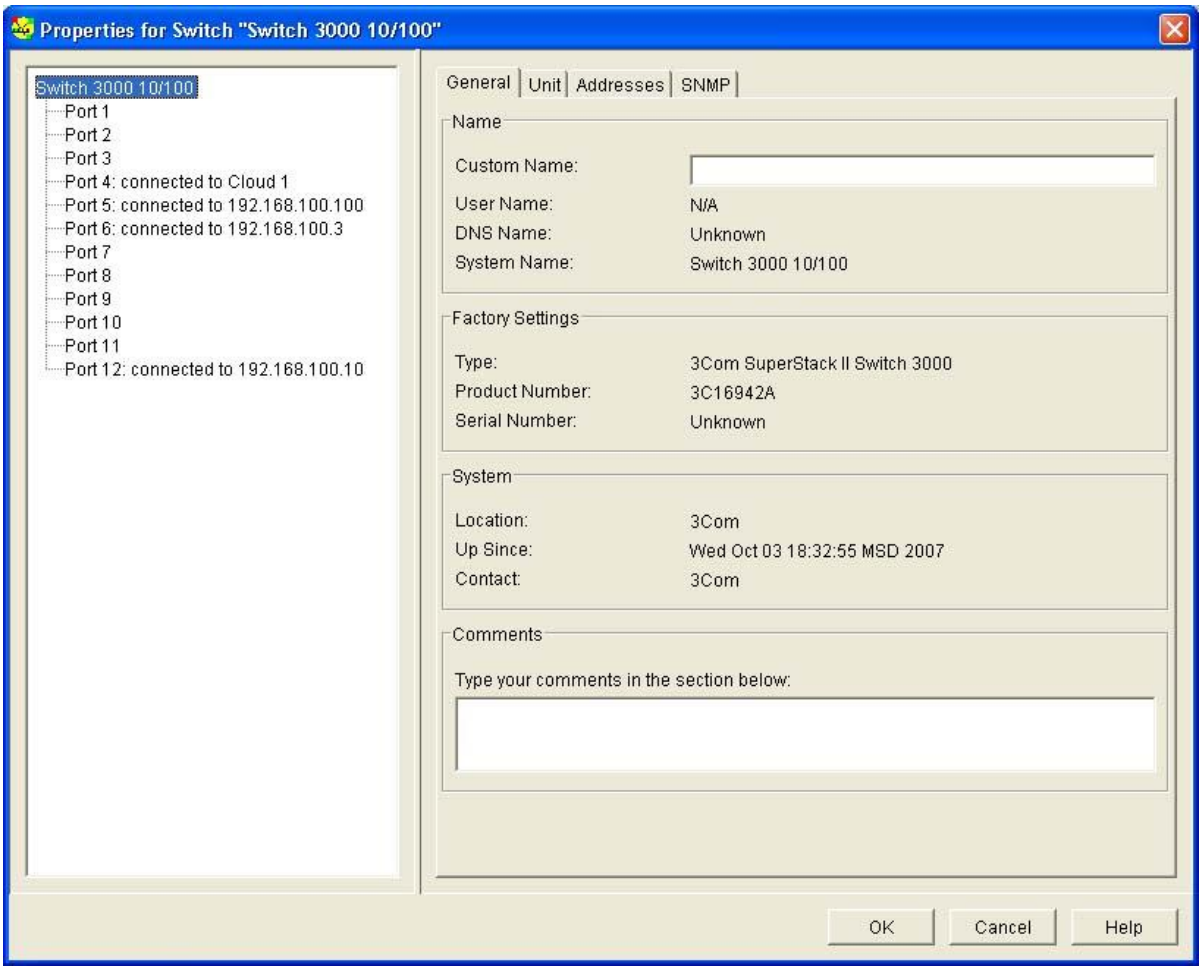


Рисунок 9 - Свойства коммутатора

Задание

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.

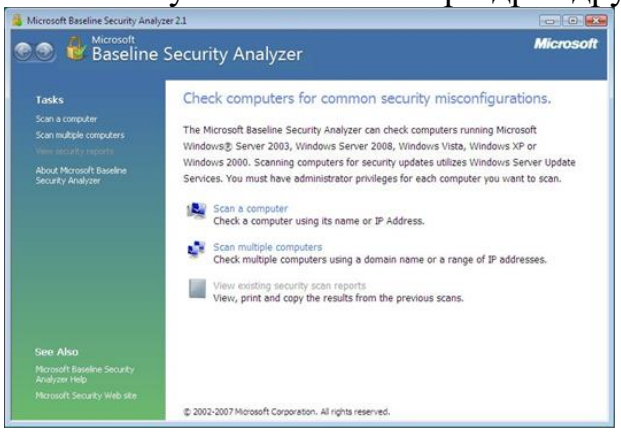
Лабораторная работа №4. Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer.Настройка локальной политики паролей

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.



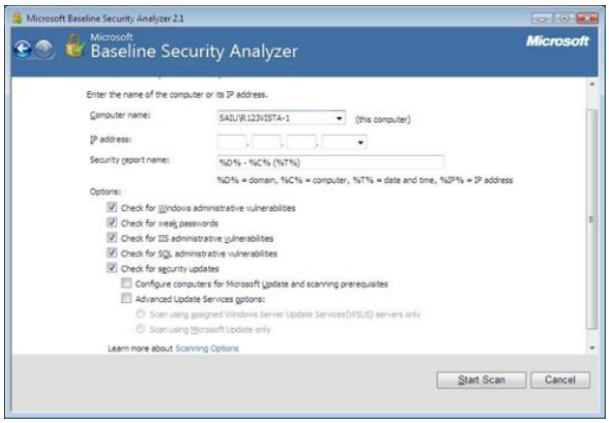


Рисунок 1 - Выбор проверяемого компьютера

Рисунок 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).

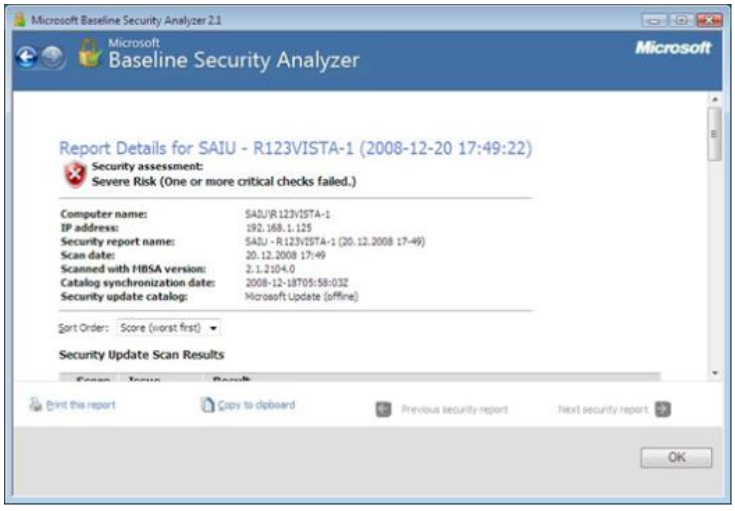


Рисунок 3 - Заголовок отчета

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.

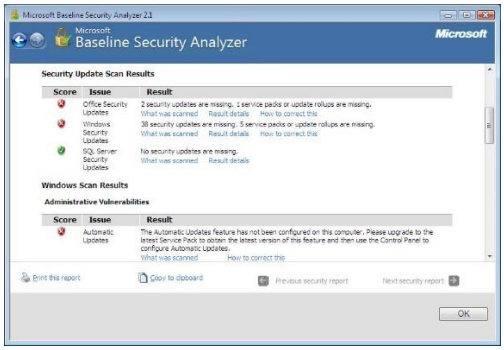


Рисунок 4 - Перечень неустановленных обновлений (по группам)

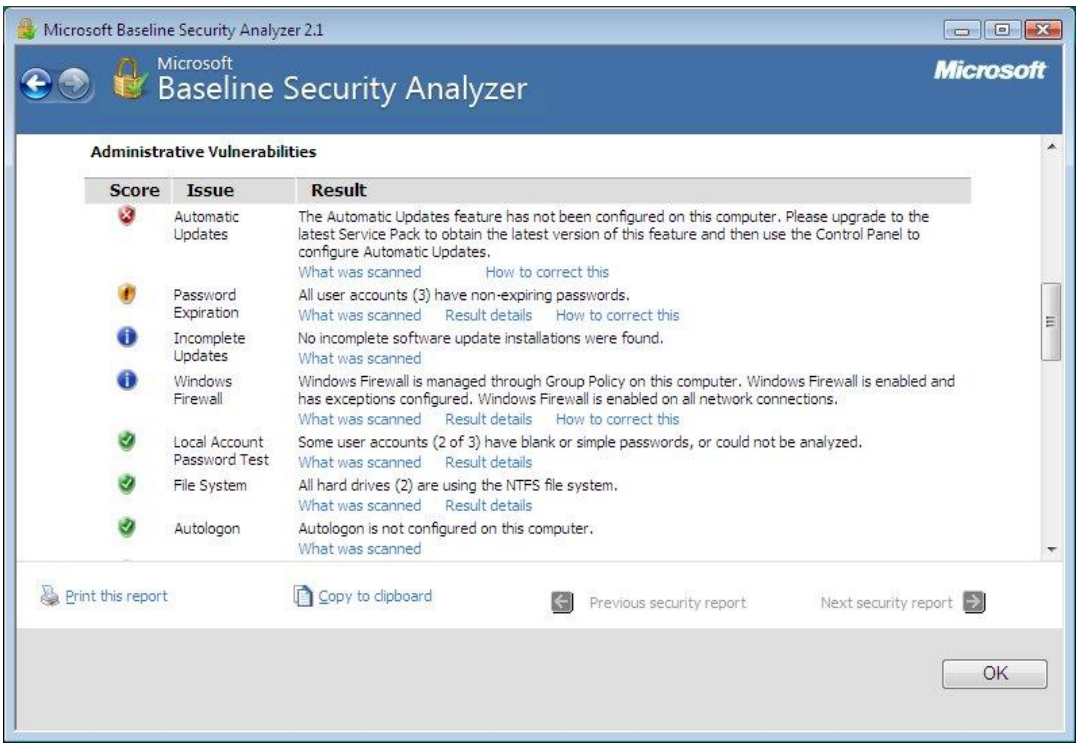


Рисунок 5 - Уязвимости, связанные с администрированием операционной системы

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.

Рисунок 6 - Результаты проверки 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 отсутствует, 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 классе 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).

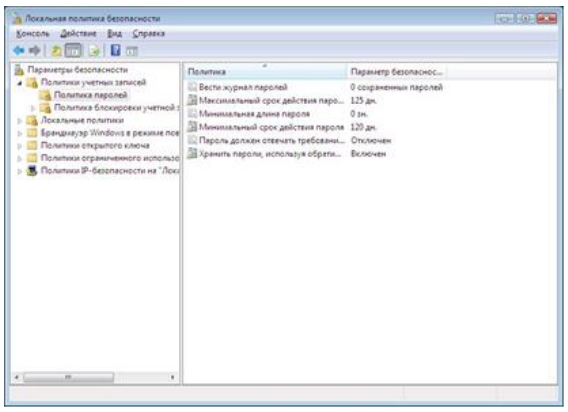


Рис. 7. Настройка политики паролей

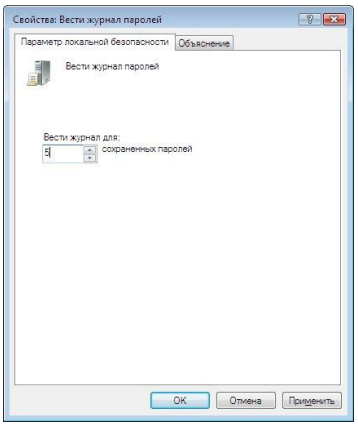


Рис. 8. Установка требования ведения журнала паролей

Задания 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 № 5. Использование сканеров безопасности для получения информации о сети

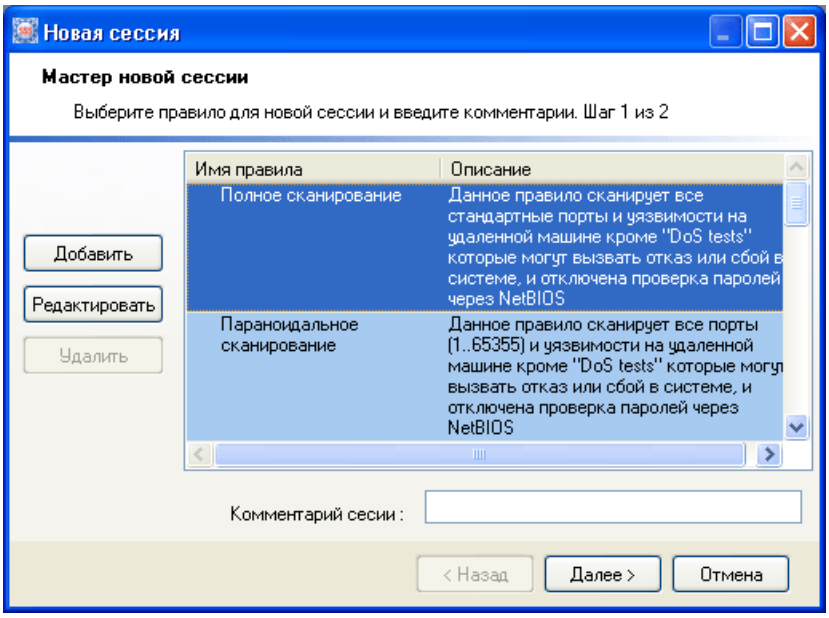


Рис. 1. Определение набора проводимых проверок

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.

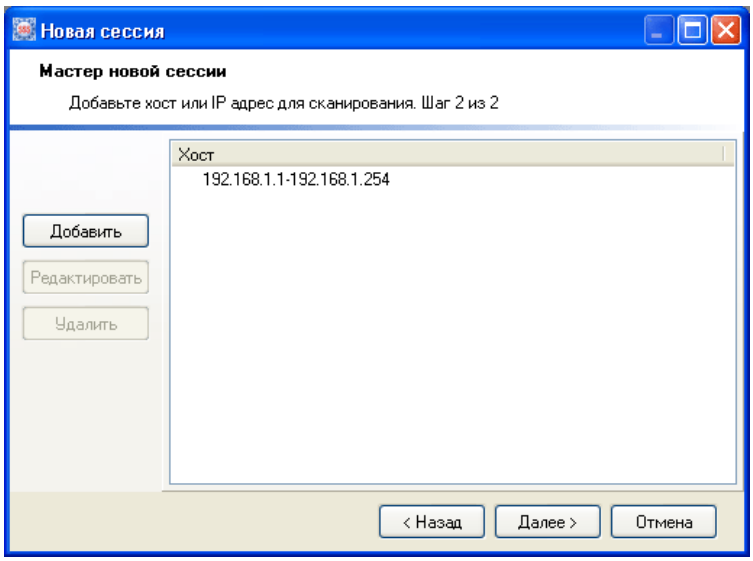


Рис. 2. Диапазон проверяемых узлов

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

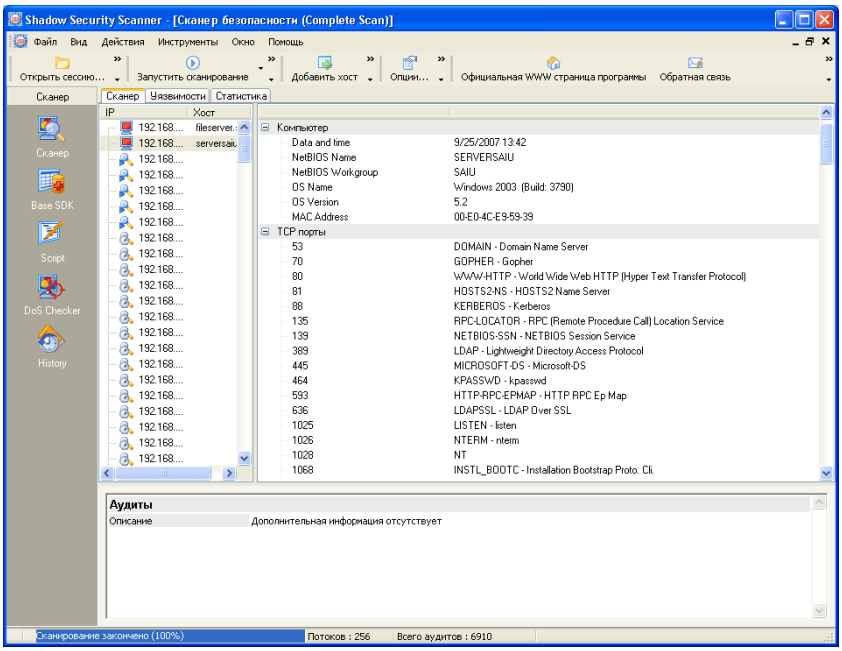


Рис. 3. Результаты сканирования

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).

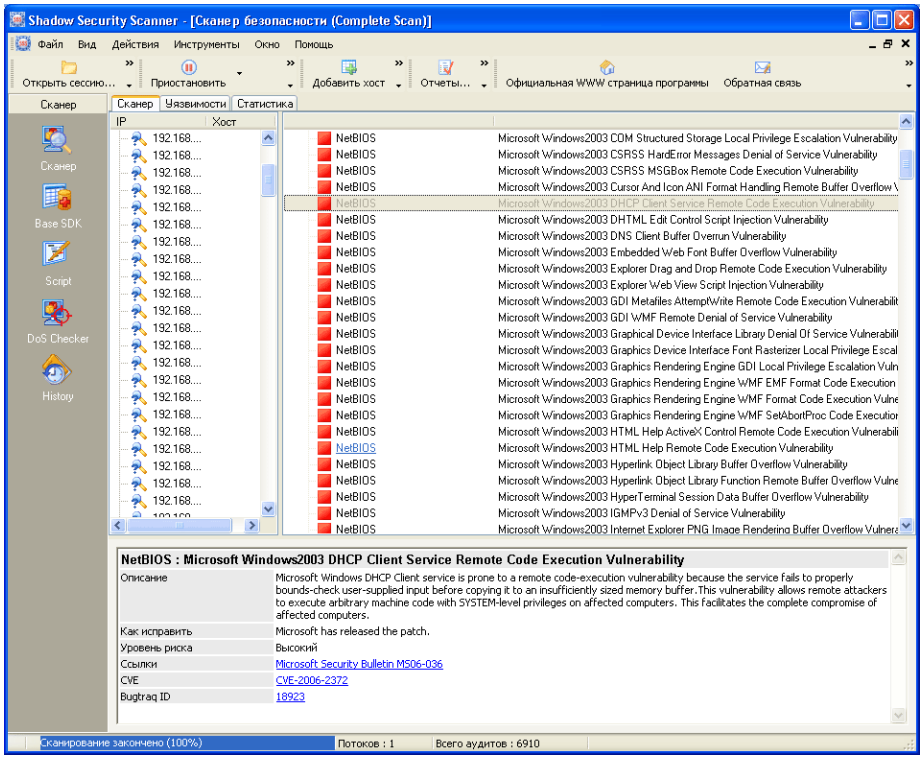


Рис. 4. Описание обнаруженных уязвимостей

К сожалению, опция формирования отчетов в бесплатной версии программы недоступна. Поэтому, при выполнении лабораторной, эту работу придется делать вручную, перенося описания через буфер из окна программы, например, в тестовый редактор Word.

Задание.

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 № 6. Использование Microsoft Security Assessment Tool (MSAT) для оценки рисков безопасности.

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).

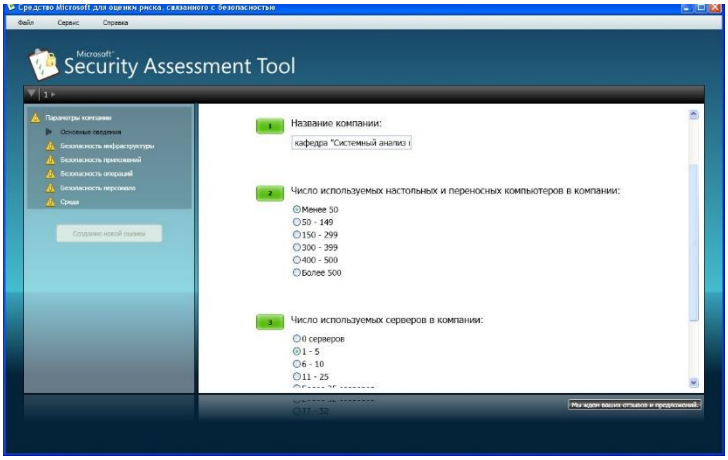


Рис. 1. Информация о компании

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.

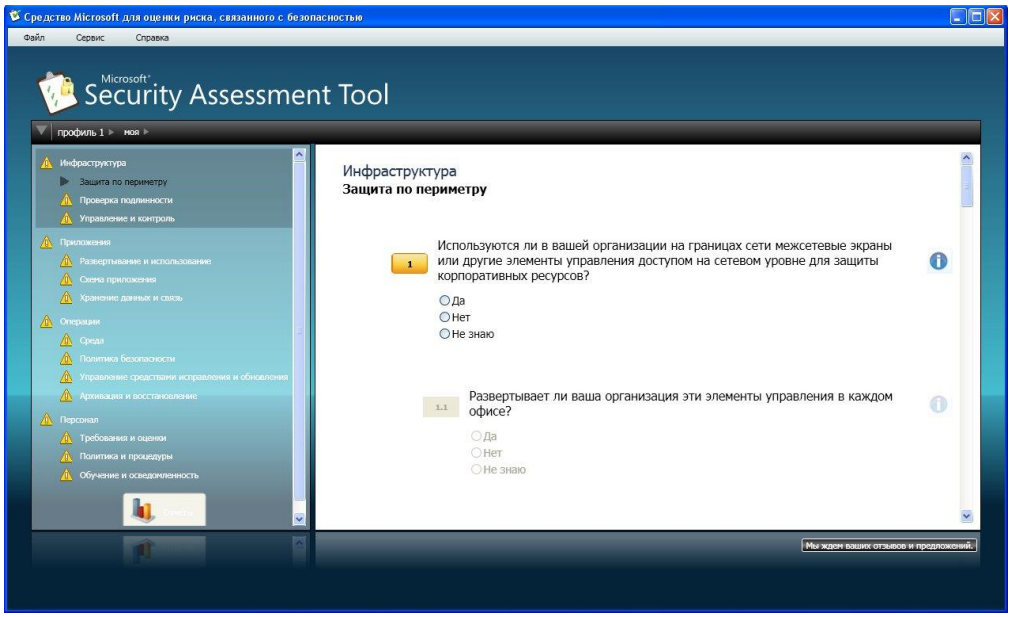


Рис.2. Анализ используемых механизмов защиты

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

Список приоритетных 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.

Индивидуальные задания к лабораторной работе

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 № 7. 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).

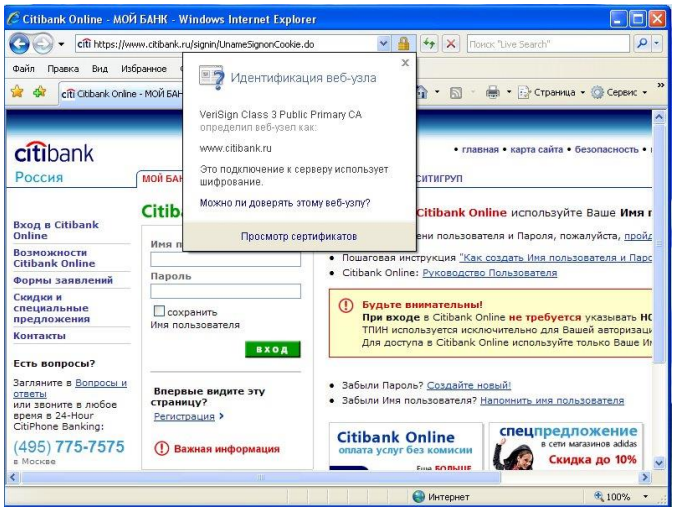


Рис. 1. Защищенное соединение

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).

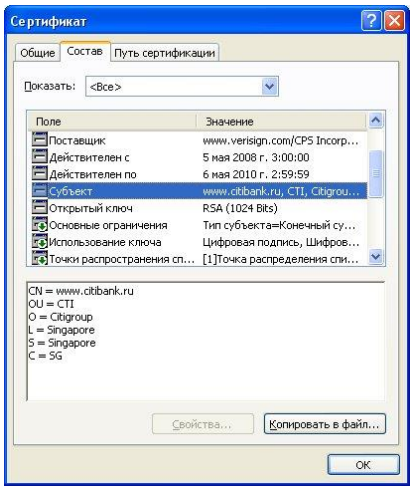


Рис. 2. Параметры сертификата

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).

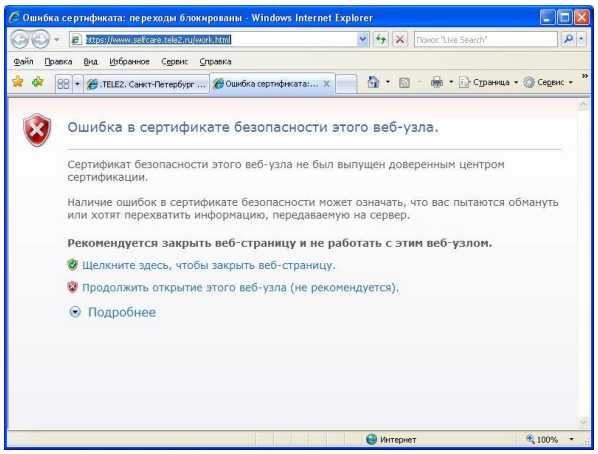


Рис. 3. Браузер сообщает о проблеме с сертификатом

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

Задание.

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 разделу «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).

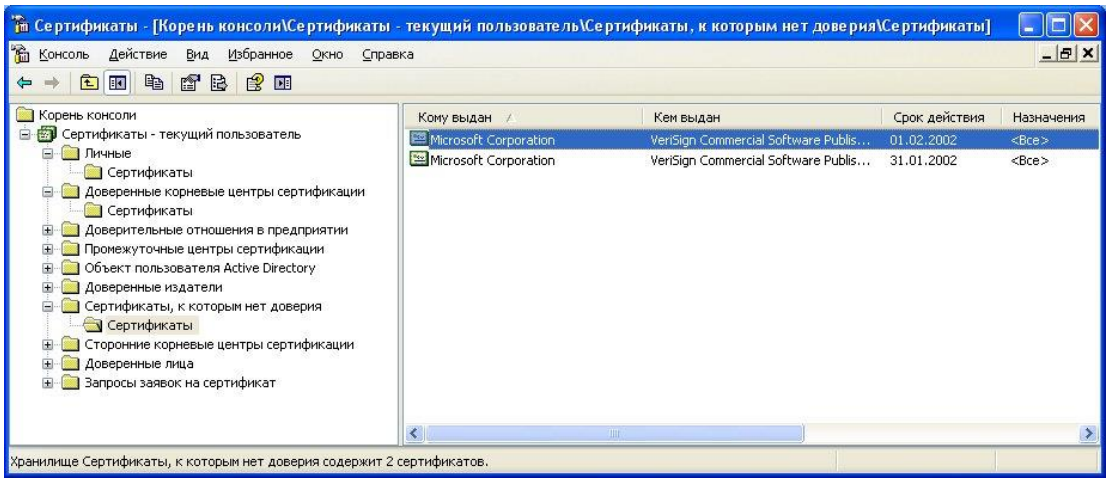


Рис. 4. Отозванные сертификаты

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).

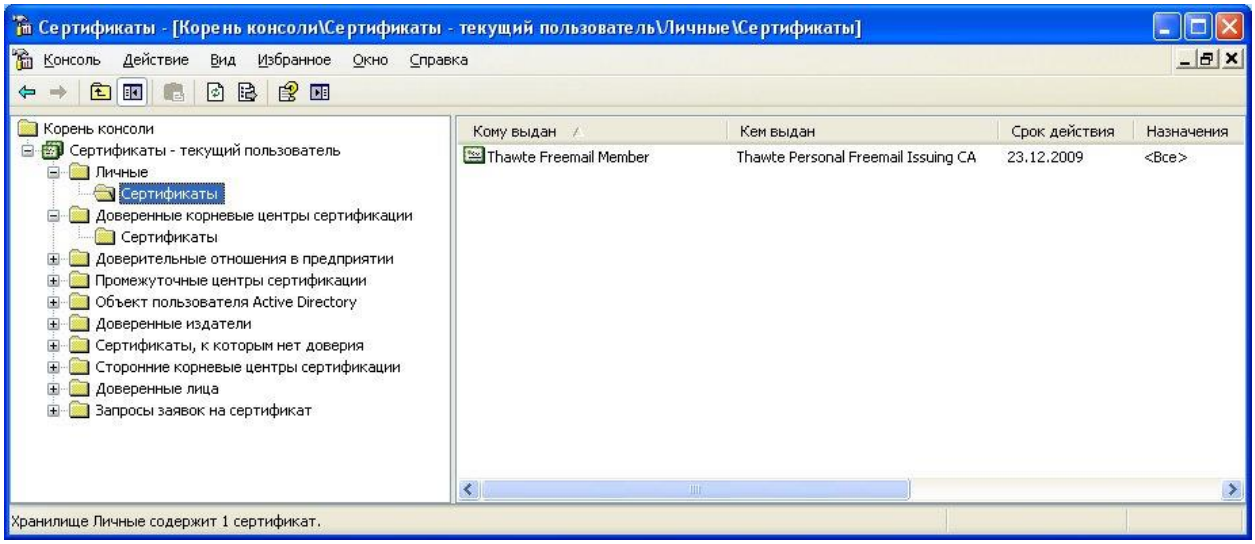


Рис. 5. Полученный сертификат

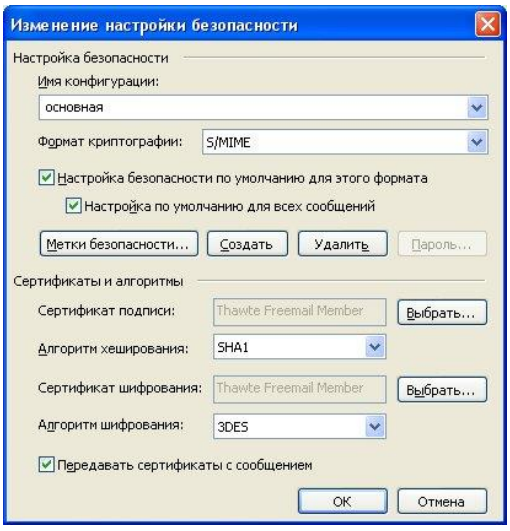


Рис. 6. Выбор сертификата для защиты почты с помощью S/MIME в Outlook.

Задание.

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 № 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.

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).

Рис. 1. В свойствах папки устанавливаем шифрование

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.

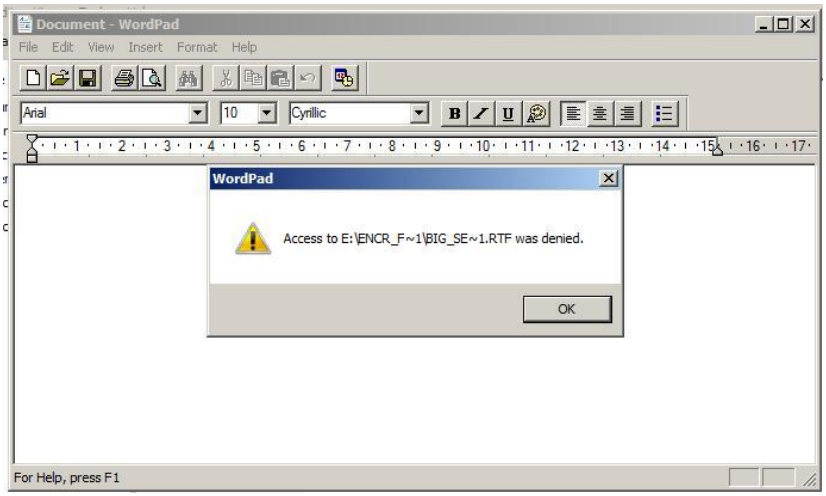


Рис. 2. Другой пользователь прочитать файл не сможет

Задание.

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).

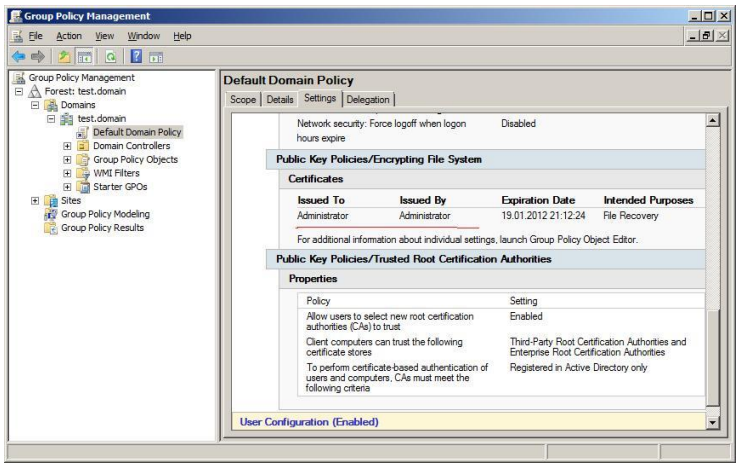


Рис. 3. Агент восстановления

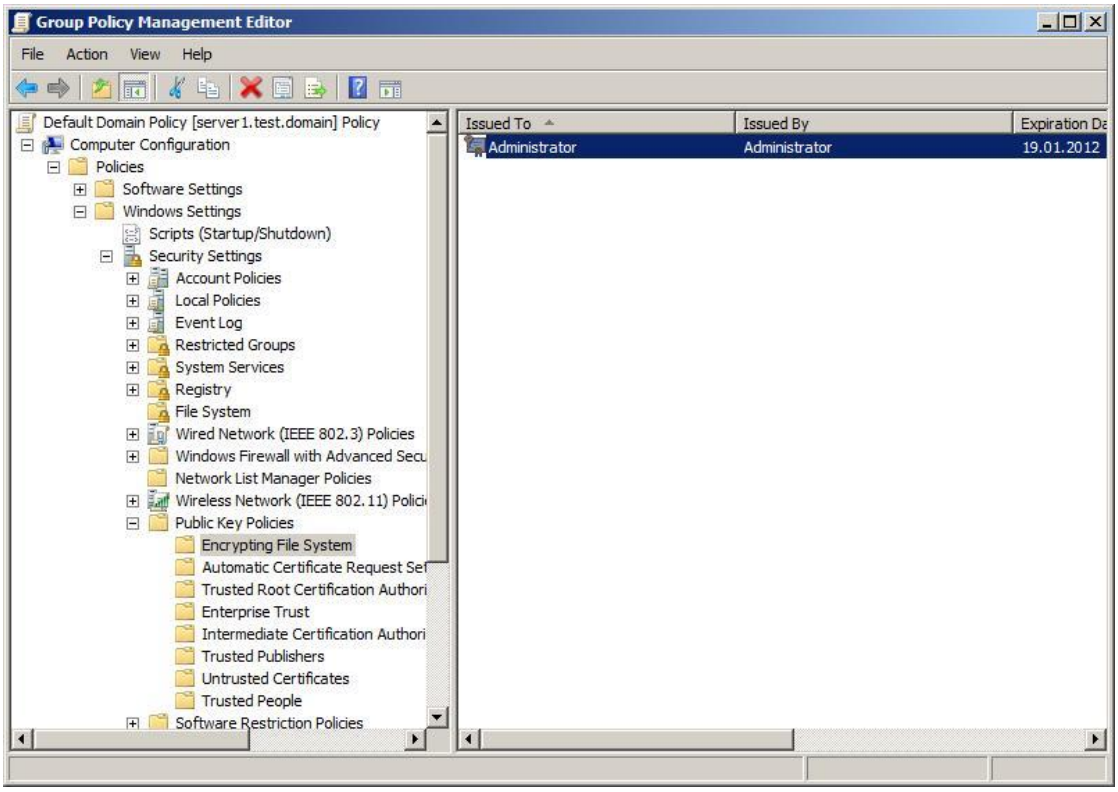


Рис. 4. Изменение агента восстановления

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 сертификаты других пользователей, которым предоставляется доступ к файлу.

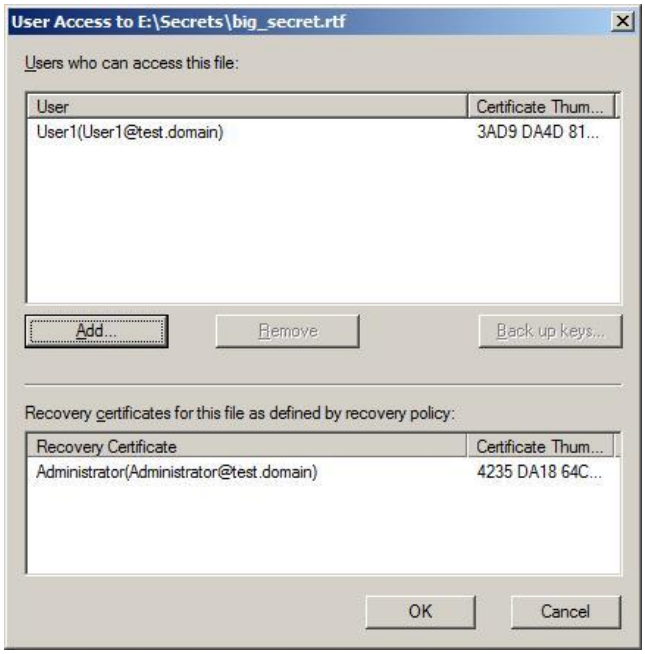


Рис. 5. Данные о пользователях, которые могут расшифровать файл

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).

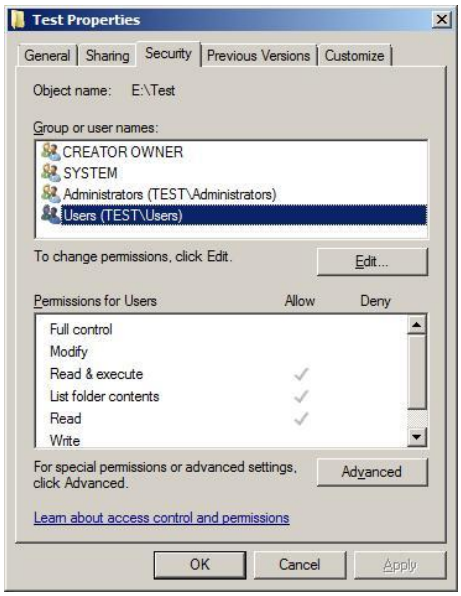


Рис. 1. Просмотр разрешений

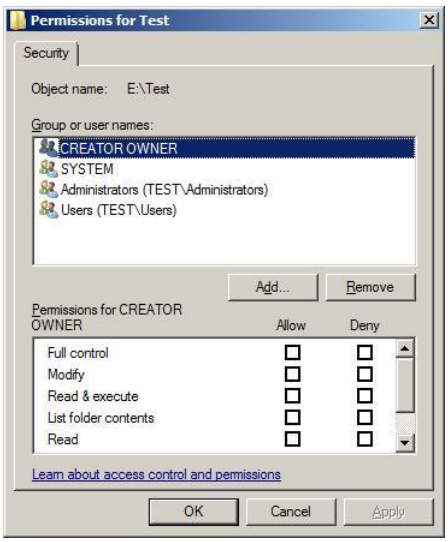


Рис. 2. Изменение разрешений

Задание

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

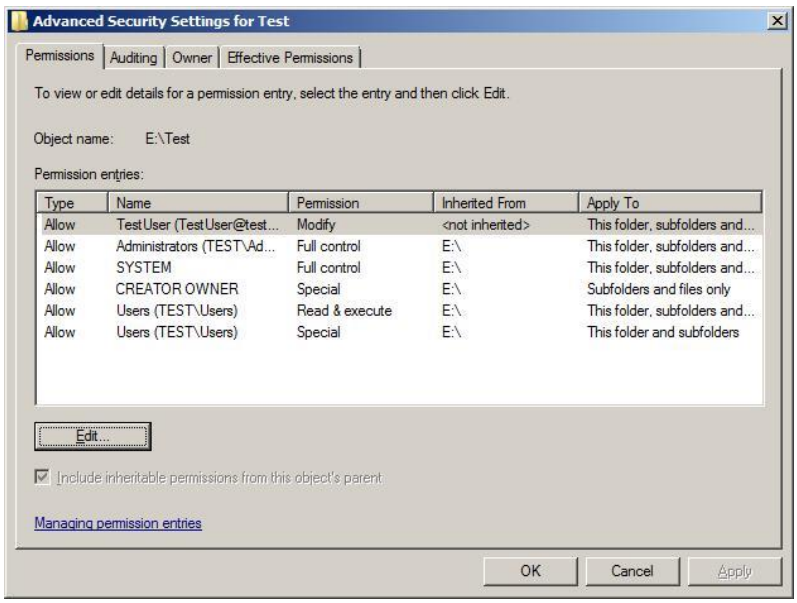


Рис. 4. Дополнительные параметры безопасности

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).

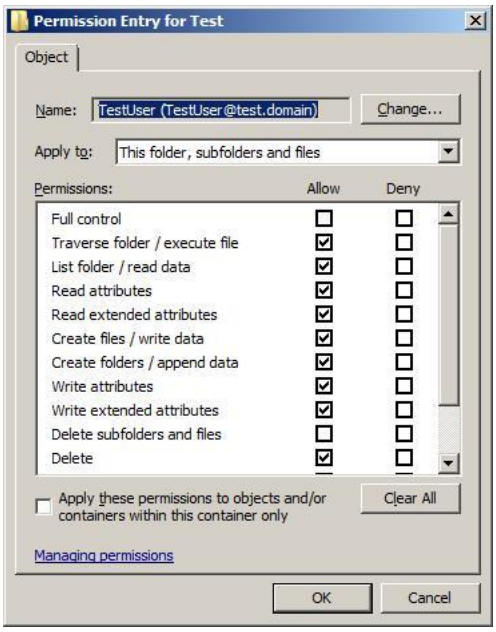


Рис.5. Специальные разрешения

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 пользователя, 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 (Administrators) – 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 операция рассматривается как привилегированная, и доступна не всякому пользователю, имеющему право на файл.

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

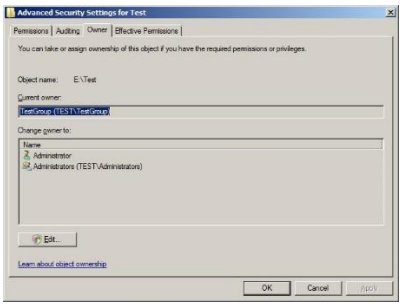


Рис.7. Смена владельца объекта

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.

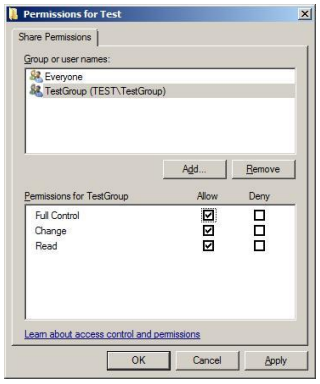


Рис.8. Разрешения на общую папку

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. Резервное копирование в Windows Server 2008/2012

Цель данной лабораторной работы – познакомиться со средствами организации резервного копирования в операционной системе Microsoft Windows Server 2008/2012.

С точки зрения управления рисками, важность процедуры резервного копирования очень высока. В тех случаях, когда реализация угрозы приводит к изменению или удалению данных, повреждению программных компонент системы, резервное копирование позволяет снизить причиненный ущерб и значительно ускорить восстановление системы.

При разработке политики резервного копирования нужно определить, как минимум, следующие параметры:

- частоту выполнения резервных копий;
- порядок восстановления данных из резервных копий;
- объем носителей информации, выделяемых для хранения резервных копий;
- количество хранимых копий;
- вопросы обеспечения безопасности носителей резервных копий.

Утилиты резервного копирования Windows Server 2008 существенно отличаются от того, что было в Windows Server 2003 (где эти задачи решались с помощью утилиты ntbackup). Чтобы их использовать, для начала требуется их установить (по умолчанию, они не устанавливаются). Делается это с помощью оснастки Server Manager, где надо выбрать пункт Add Feature в разделе Features (рис.1) и в появившемся списке выбрать пункт Windows Server Backup Features (рис.2.).

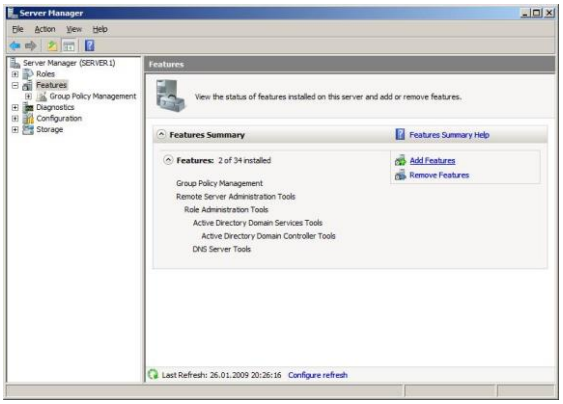


Рис. 1. Оснастка Server Manager позволяет добавить компоненты.

Как видно на рис. 2, предлагается выбрать следующие опции:

- Windows Server Backup;
- Command-line tools (утилиты командной строки).

Установка последних, позволяет управлять резервным копированием с помощью сценариев и требует установки Windows PowerShell. Но для выполнения лабораторной будет достаточно установить только Windows Server Backup.

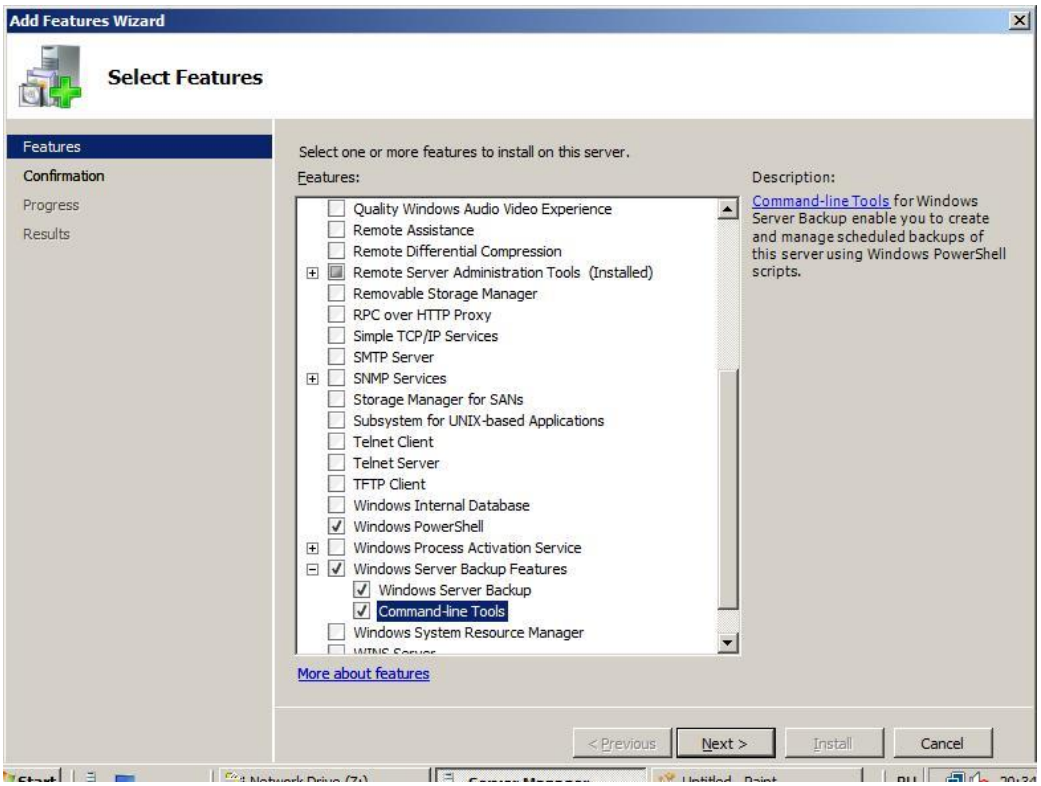


Рис. 2. Добавляем утилиты администрирования

После установки, в меню Administrative Tools становится доступной оснастка Windows Server Backup. С ее помощью можно проводить резервное копирование данных на локальном или удаленном компьютере (если это разрешено настройками).

Рассмотрим, как это происходит. Запустим утилиту. Резервное копирование может проводить пользователь, состоящий в группе Administrators (Администраторы) или Backup Operators (Операторы архива). При этом, у членов группы Backup Operators при запуске оснастки Windows Server Backup будет дополнительно запрашиваться пароль (в окне User Account Control), т.к. эти операции относятся к разряду потенциально опасных.

В окне оснастки в списке доступных действий (Actions), расположенном в правой части экрана, выберем опцию Backup Once … (т.е. однократная архивация). Запустившийся мастер резервного копирования предложит выбор между настройками для уже запланированного копирования (The same options that you used in the Backup Schedule Wizard for scheduled backups) и новыми

(Different options). Нужно выбрать второй вариант (если, как в нашем примере, утилита ранее не использовалась, то первый пункт списка будет неактивен).

Следующее окно мастера позволяет выбрать, производить ли полное резервное копирование или копирование отдельных разделов (рис.3). Здесь проявляется первое отличие новых инструментов – резервное копирование отдельных папок и файлов производить нельзя, только логический диск целиком.

Хотелось бы также обратить внимание на надпись в нижней части экрана, там дается ссылка на раздел справки, описывающий выполнение с помощью утилиты командной строки резервного копирования только состояния системы (System State).

Выберем вариант Custom.

Тогда на следующем экране появится список дисков (рис.4). Устанавливая или снимая отметки, можно указать, данные с каких дисков помещаются в резервную копию. Опция Enable System Recovery включает в архив разделы, где находятся компоненты операционной системы и файлы необходимые для загрузки (т.е. отметку напротив этих разделов будет не снять).

Предположим, нам нужно сделать резервную копию диска E:, на котором находятся пользовательские данные. Тогда отметки устанавливаем так, как это сделано на рис.4 и переходим к следующей стадии, на которой нужно определить, куда будет производиться копирование. Это может быть локальный диск (жесткий диск, пишущий DVD-привод и т.д.) или сетевая папка. Надо учитывать, что архивная копия не может сохраняться на диск, входящий в перечень архивируемых. Также нельзя сохранить архив на диск, где хранятся файлы операционной системы

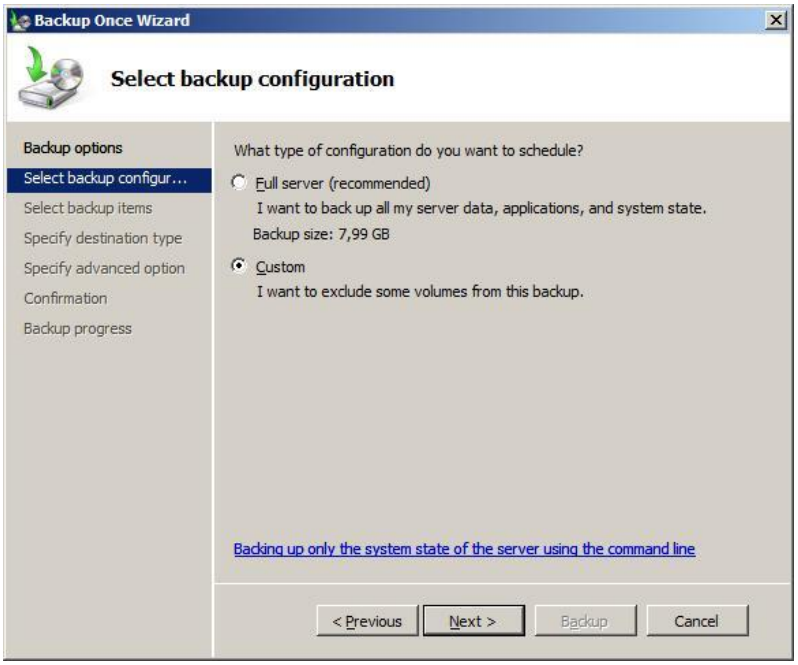


Рис. 3. Выбор между полным резервным копированием и копированием отдельных дисков

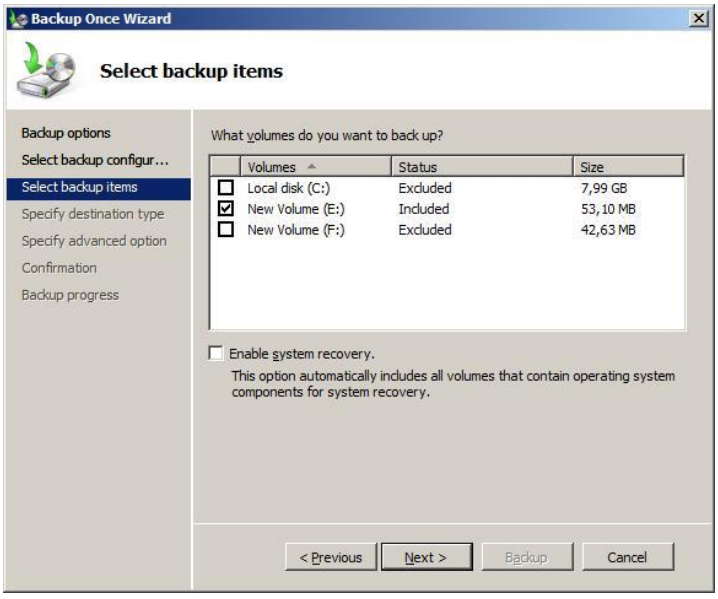


Рис. 4. Выбор дисков для резервного копирования

Учитывая все вышеизложенное, в рассматриваемом примере можно сделать резервную копию диска E: на диск F:, в сетевую папку или на DVD-диск. Выберем первый вариант, что и укажем в следующем окне мастера. После чего будет предложено выбрать тип резервного копирования (рис.5).

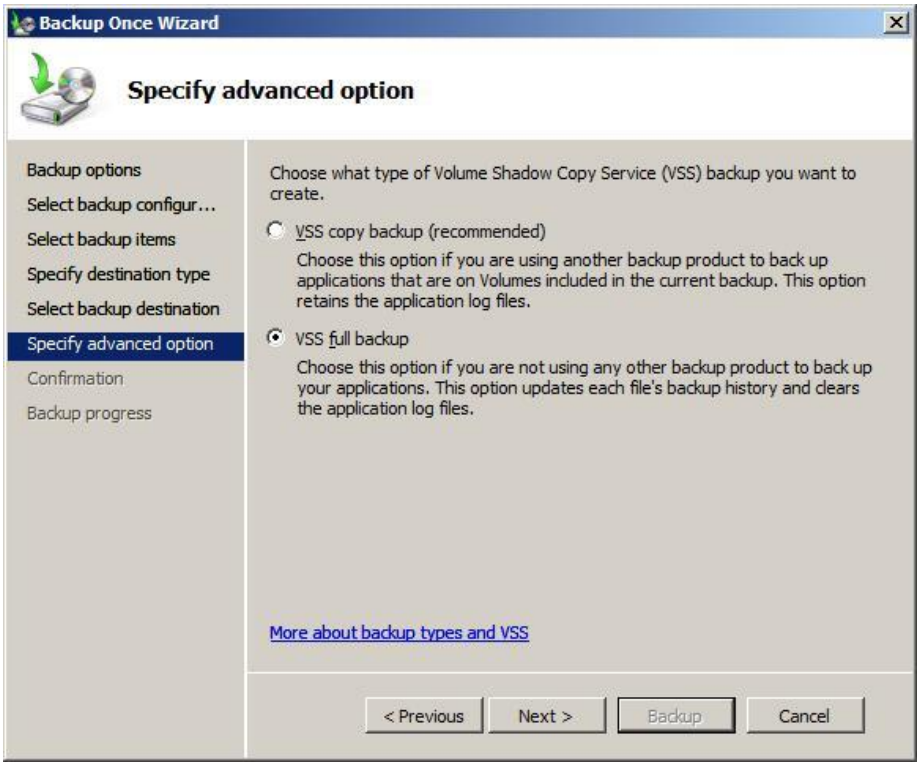


Рис. 5. Выбор типа копирования

Служба Volume Shadow Copy Service (VSS) может при резервном копировании отмечать файлы, как помещенные в архив, или не делать это. Если кроме средств Windows Server 2008 используются и другие продукты для

резервного копирования, рекомендуется выбрать вариант VSS copy backup. Если такого нет, можно смело выбирать вариант VSS full backup.

В следующем окне мастера будет запрошено подтверждение и, если оно получено, запустится резервное копирование.

В результате, в нашем примере на диске F: появится каталог WindowsImageBackup, в нем будет создан подкаталог, названный по имени архивируемого сервера, куда и попадет копия.

Задание

1.На учебном сервере (или виртуальной машине) выберите раздел для резервного копирования.

2.С учетом рассмотренных ограничений и объема копируемого раздела, выберите место для размещения копии. Определите, от имени какой учетной записи будет проводиться эта операция.

3.Выполните однократное резервное копирование выбранного раздела.

Теперь рассмотрим порядок восстановления данных из резервной копии.

В первой части лабораторной работы была сделана резервная копия раздела E:. Пусть понадобилось восстановить содержимое одной из папок из этого раздела. При этом требуется сравнить текущее содержимое папки с архивной копией, т.е. восстанавливать нужно в другую папку.

Запускаем оснастку Windows Server Backup и в списке Actions выбираем Recover (восстановление). Мастер восстановления уточняет, какой сервер будет восстанавливаться, после чего представит перечень имеющихся резервных копий (рис.6).

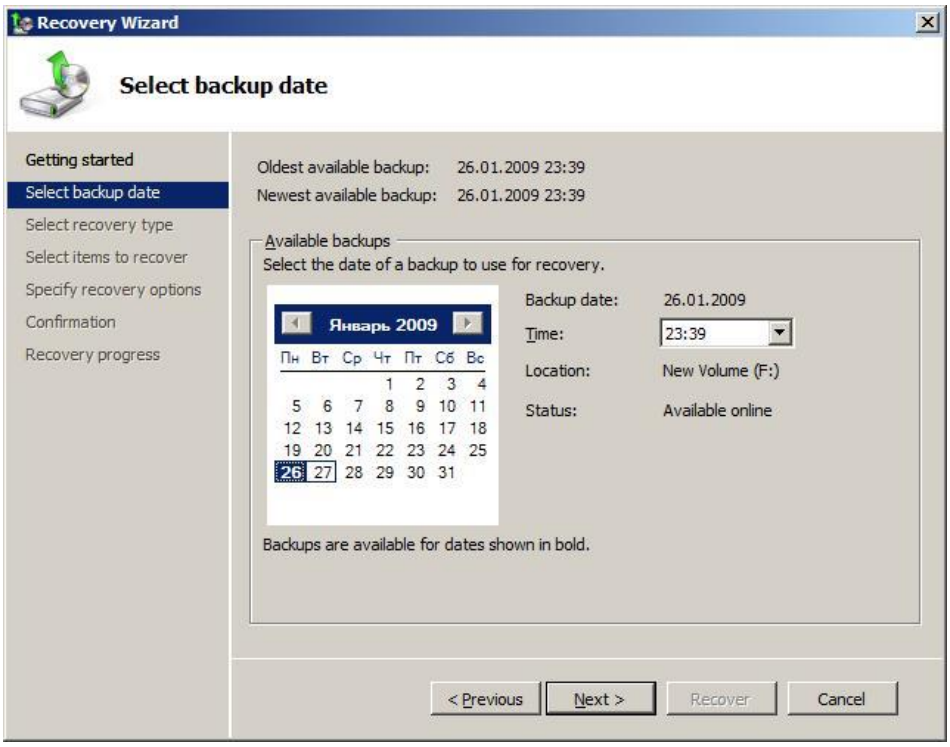


Рис. 6. Перечень доступных резервных копий для выбранного сервера

В следующем окне запрашивается, что именно восстанавливается. Нас интересует отдельная папка, потому выбираем вариант Files and folders (рис.7). Другие варианты – восстановление зарегистрированных приложений и восстановление раздела диска целиком.

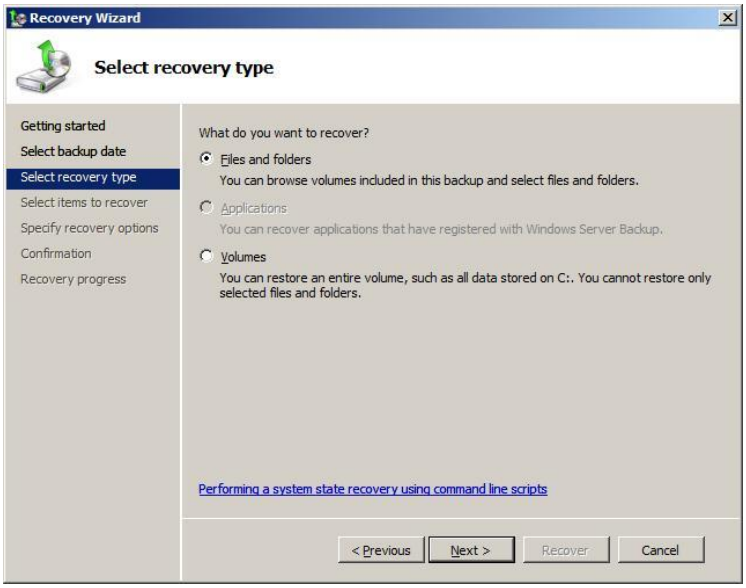


Рис. 7. Выбор типа восстановления

В следующем окне мастера в выпадающем списке нужно найти и выделить выбранную для восстановления папку. Если восстановить нужно несколько объектов, их выделяют совместно, удерживая клавишу Ctrl (или Shift для выделения диапазона). После этого выбирается путь для восстановления и задаются параметры. В нашем примере, мы хотим восстановить выбранную папку с файлами во вновь созданную папку restored (рис.8).

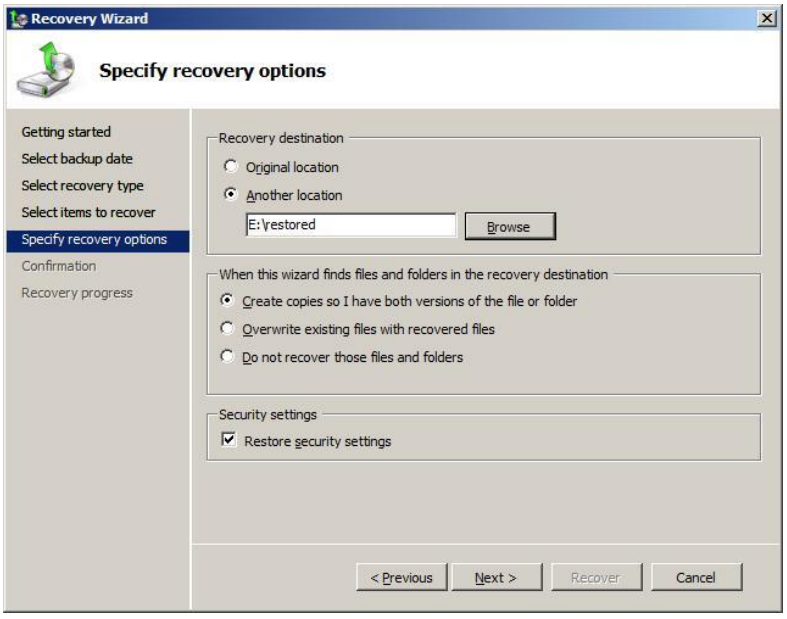


Рис. 8. Параметры восстановления

Кроме пути (исходный или альтернативный), выбирается вариант действий при совпадении имен файлов и папок. Это особенно актуально, если восстанавливать файлы в исходную папку. Вариантов три – создавать копии, перезаписывать имеющиеся объекты восстанавливаемыми, оставить имеющиеся объекты.

Последний из выбираемых в этом окне параметров указывает на то, восстанавливать ли настройки безопасности (т.е. списки доступа к файлам).

После выбора всех параметров будет запрошено подтверждение и начнется восстановление.

Задание

Выберите из архива, созданного в предыдущей части работы, группу файлов для восстановления. Восстановите их в первый раз по исходному пути с сохранением копий, во второй раз - по альтернативному пути. Опишите, в чем разница в полученных результатах.

Теперь рассмотрим организацию резервного копирования по расписанию. Для этого в Windows Server Backup выберем опцию Backup Schedule. Первое окно запустившегося мастера информирует, что прежде чем устанавливать резервное копирование по расписанию, нужно определить:

- что будет копироваться (полное резервное копирование сервера или отдельные диски);
- как часто надо проводить копирование;
- где размещать копии.

При этом надо учитывать:

1) даже при выборе резервного копирования отдельных разделов, в их список обязательно должен быть внесен раздел (-ы) с операционной системой;

2) копирование может выполняться один или несколько раз в день;

3) для хранения результатов резервного копирования должен выделяться отдельный диск, внутренний или внешний (например, подключаемый по USB). Перед началом использования, он будет отформатирован мастером архивации. Рекомендуется, чтобы он был не менее чем в 1,5 раза больше по объему, чем архивируемые диски.

Пусть требуется ежедневно делать резервное копирование диска раздела с операционной системой. В окне мастера аналогичном рис.3, выбираем вариант Custom, в окне аналогичном рис.4 – диск C (на котором расположена операционная система). Указываем расписание (рис.9).

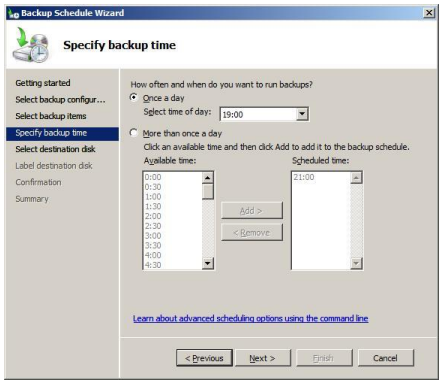


Рис. 9. Расписание резервного копирования

Дальше определяется диск (рис.10), он может быть не отформатирован. Диску будет назначена метка с названием сервера и датой определения резервного копирования, после чего будет проведено форматирование. Диску не назначается буква и он не будет доступен пользователям как обычный диск.

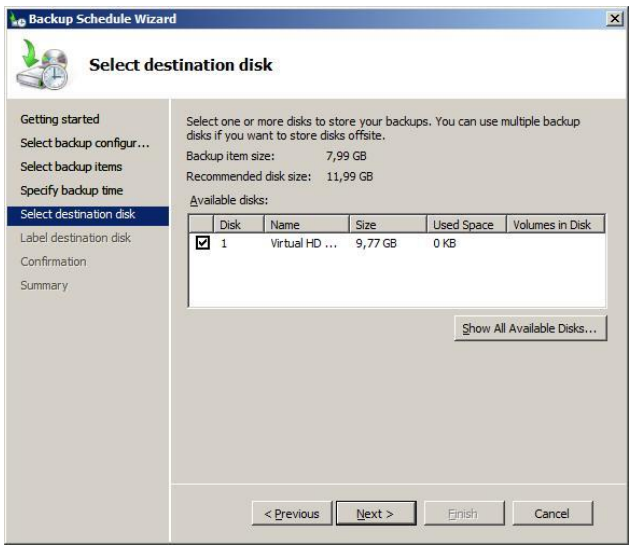


Рис. 10. Диск для хранения резервных копий

Когда работа по настройке автоматической архивации завершена, можно сделать дополнительные настройки, повышающие быстродействие для отдельных дисков. Для этого в списке Actions в оснастке Windows Server Backup выберите пункт Configure Performance Settings.

В открывшемся окне (рис.11) можно установить, какой тип резервного копирования производить для диска – полное (full) или добавочное (Incremental). По умолчанию используется полное. Добавочное помещает в архив только измененные с момента последнего архивирования файлы, это позволяет провести резервное копирование быстрее, но более существенно снижает производительность сервера в период копирования (т.к. надо проводить проверку).

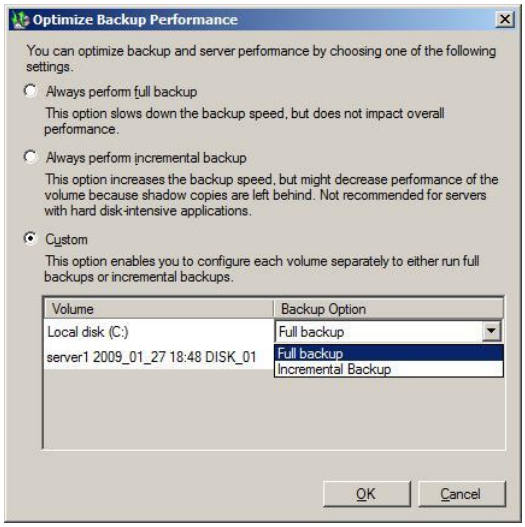


Рис.11. Выбор типа резервного копирования для диска

Порядок восстановления такой же, как и при однократном копировании.

Кстати, посмотреть параметры запланированного резервного копирования можно с помощью оснастки Task Scheduler (рис.12).

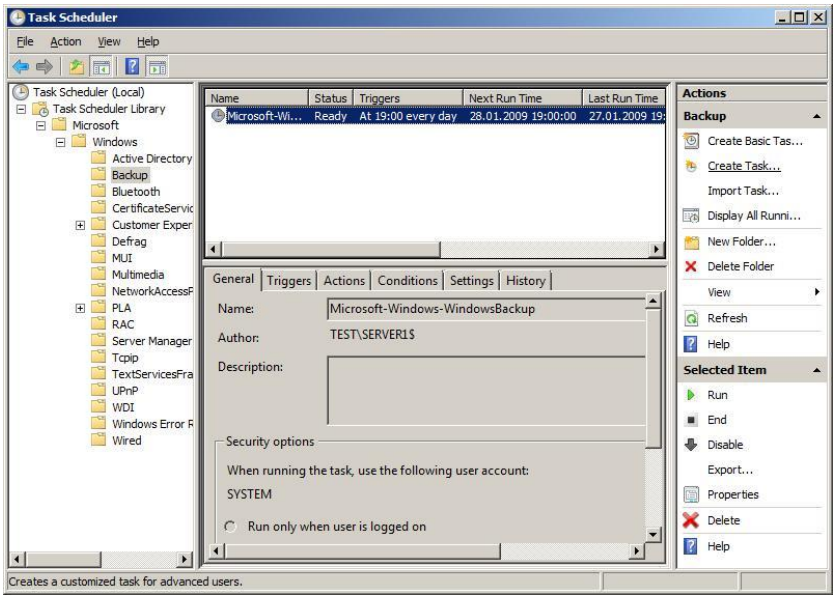


Рис. 12. Параметры созданного задания

Задание

Разработайте и реализуйте план ежедневного резервного копирования раздела с операционной системой.

При выполнении лабораторной работы на виртуальной машине для хранения резервных копий можно подключить дополнительный виртуальный диск (настройка делается в свойствах виртуальной машины, когда она не запущена). При выполнении работы на учебном севере, заранее определите физический диск, на который можно сохранить копии (диск не должен содержать полезных данных, т.к. он будет отформатирован!).

Выберите такое время создания копии, чтобы результат можно было увидеть в ходе выполнения лабораторной.

После создания копии, восстановите какой-либо из файлов.

Используя опцию Backup Schedule оснастки Windows Server Backup, удалите запланированное задание на резервное копирование.

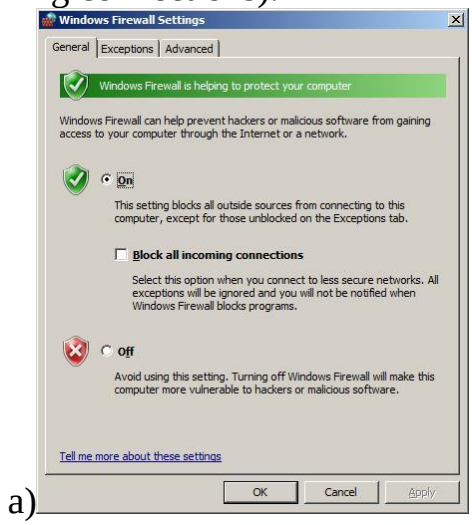
Лабораторная работа № 11. Встроенный межсетевой экран (firewall) Windows Server 2008/2012

Персональный межсетевой экран появился в операционных системах семейства Windows, начиная с Windows XP / Windows Server 2003. В Windows Server 2008/2012 возможности этого компонента существенно расширены, что позволяет более гибко производить настройки.

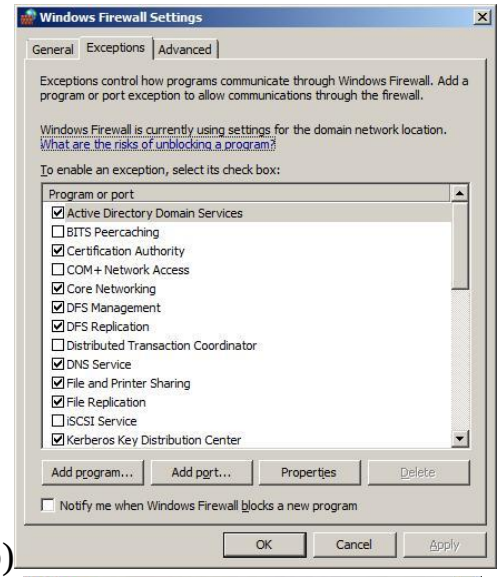
Текущие настройки можно посмотреть, запустив из Панели управления (Control Panel) Windows Firewall и выбрав в открывшемся окне ссылку

Change Settings. Появившееся окно управления параметрами межсетевого экрана содержит 3 вкладки (Рис.1 a), b), c).

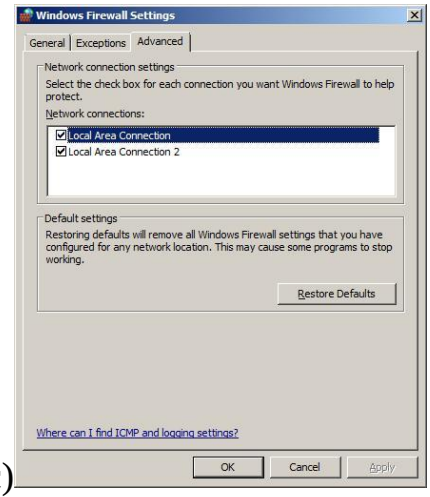
Первая из них позволяет включить или отключить межсетевой экран. Во включенном состоянии он может разрешать определенные входящие подключения или запрещать все входящие подключения (флажок Block all incoming connections).



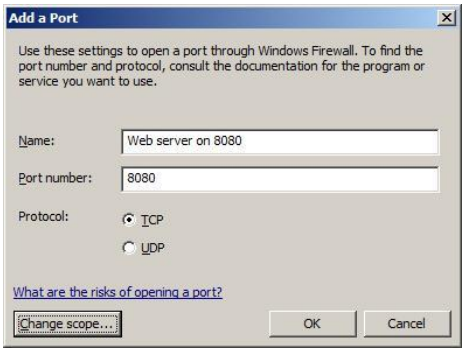
a)



b)



c)



d)

Рис. 1. Окно управления параметрами межсетевого экрана

Упомянутые исключения определяются на вкладке Exceptions. Там есть ряд предопределенных правил, а также пользователь может добавлять свои. Если нужно, чтобы какое-то приложение при включенном межсетевом экране обслуживало входящие подключения, для него должно быть описано правило. Сделать это можно либо указав программу (кнопка Add program), либо описав разрешаемый порт и протокол (кнопка Add Port). Пример формирования подобного правила представлен на рис. 1 d). Там дается разрешение для подключения на TCP-порт 8080. Если надо ограничить перечень ip-адресов, с которых производится подключение, это можно сделать, нажав кнопку Change Scope (по умолчанию, разрешены подключения с любого адреса).

Установка флажка Notify me when Windows Firewall blocks a new program приводит к тому, что при попытке нового приложения принимать входящие подключения, пользователю будет выдано сообщение. Если пользователь разрешит такой программе работать, для нее будет сформировано разрешающее правило.

Вкладка Advanced (рис.1 с)) позволяет включить или отключить межсетевой экран для отдельных сетевых интерфейсов.

Задание

Откройте окно управления межсетевым экраном.

Опишите действующие настройки.

Создайте новое разрешающее правило.

Пока что работа с межсетевым экраном практически не отличалась от того, что было в Windows Server 2003. Новые возможности мы увидим, если из меню Administrative Tools запустить оснастку Windows Firewall with Advanced Security. В окне оснастки можно увидеть настройки для разных профилей и выполнить более тонкую настройку правил фильтрации (рис.2).

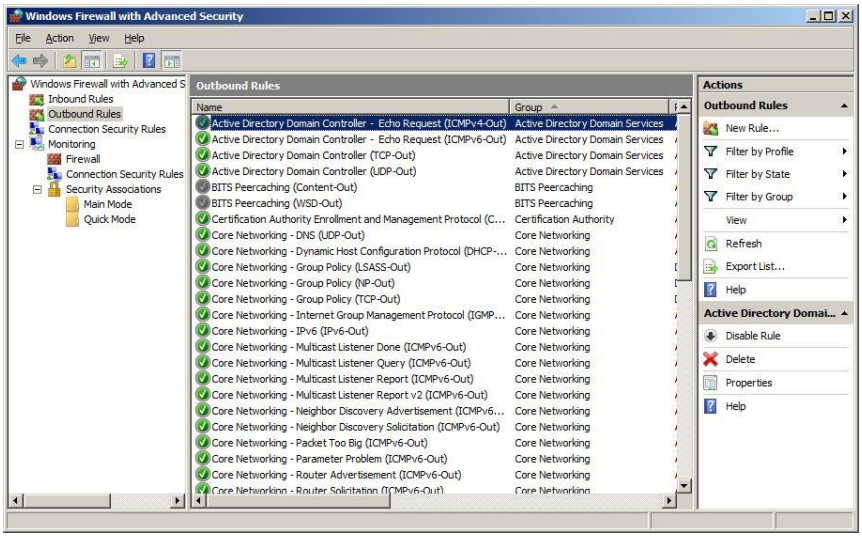


Рис. 2. Окно оснастки Windows Firewall with Advanced Security

Обратим внимание на правила фильтрации. Они разделены на две группы – входящие правила и исходящие правила. В нашем примере мы работаем на контроллере домена. И для контроллеров определено правило, разрешающее отправку icmp пакетов echo request (они, в частности, отправляются, если надо проверить доступность удаленного узла с помощью команды ping).

Задание

1). Найдите правило, разрешающее отсылку ICMP-пакетов echo reguest. Проверьте его работу для какого-нибудь узла из локальной или внешней сети, используя его ip-адрес (например, командой ping 192.168.0.10 можно проверить доступность компьютера с указным адресом). Если ответ пришел, можно переходить ко второй части задания. Если ответа нет, попробуйте найти такой узел, который пришлет ответ.

2). Выбрав кнопку New Rule создайте правило, запрещающее отсылку icmp-пакетов на данный узел. Проверьте его работу.

Теперь рассмотрим настройку, связанную с ведением журналов межсетевого экрана. По умолчанию журналирование отключено. Но если возникает подозрение, что межсетевой экран мешает установлению какого-то типа сетевых соединений, можно включить эту опцию и проанализировать журнал.

На рисунке 3 представлено главное окно оснастки. Выберем пункт Firewall Properties и активируем ведение журнала отброшенных пакетов (рис.4).

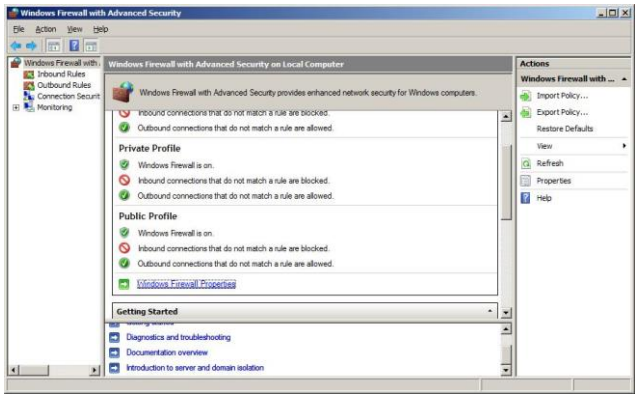


Рис. 3. Главное окно оснастки

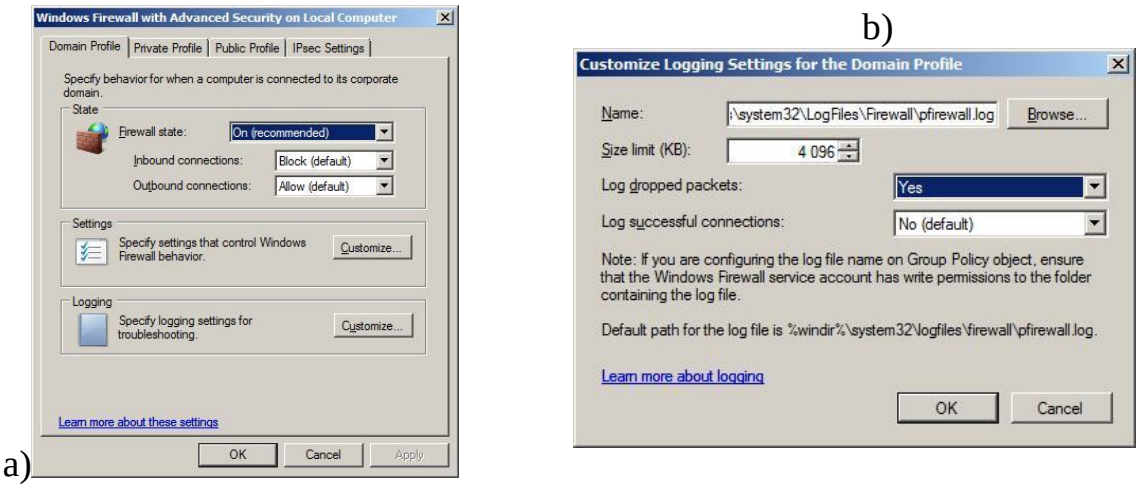


Рис. 4. Активируем ведение журнала

Для этого в группе Logging в окне рис.7 a) надо нажать кнопку Customize и выполнить настройку, представленную на рис. 7 b).

Задание

Активируйте ведение журнала.

Выполните команду ping для узла, для которого создавалось блокирующее правило.

Проверьте содержимое файла журнала (путь к нему описан в окне 7 b)).

Записи должны быть примерно следующего вида:

Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2009-01-31 22:43:02 DROP ICMP 192.168.131.65 195.242.2.2 - - 0 - - - - 80 - SEND
2009-01-31 22:43:03 DROP ICMP 192.168.131.65 195.242.2.2 - - 0 - - - - 80 - SEND
2009-01-31 22:43:04 DROP ICMP 192.168.131.65 195.242.2.2 - - 0 - - - - 80 - SEND
2009-01-31 22:43:05 DROP ICMP 192.168.131.65 195.242.2.2 - - 0 - - - - 80 - SEND

Лабораторная работа №12. Настройка протокола IPSec в Windows Server 2008/2012

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).

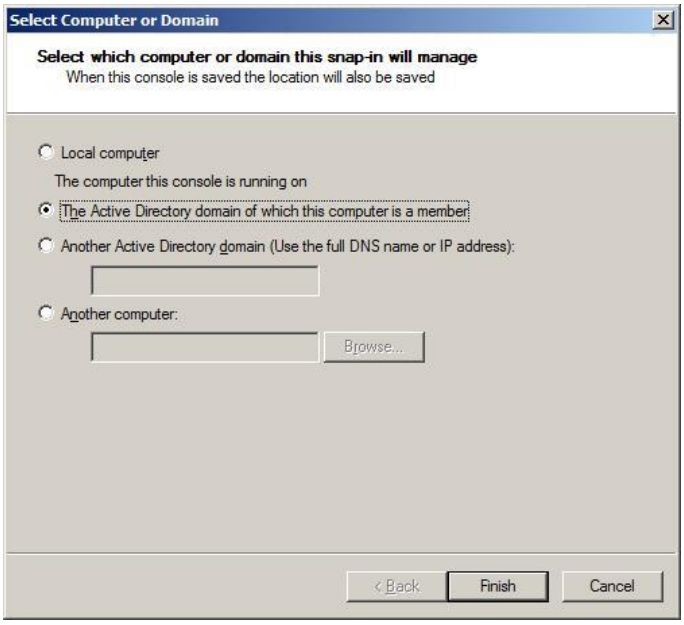


Рис. 1. Выбираем объект для работы

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.

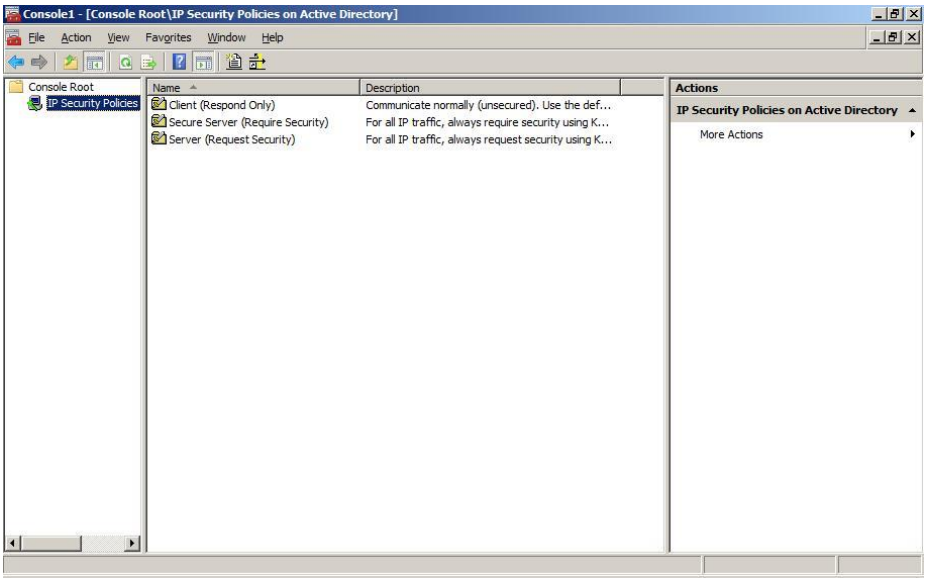


Рис. 2. Предопределенные политики IPSec

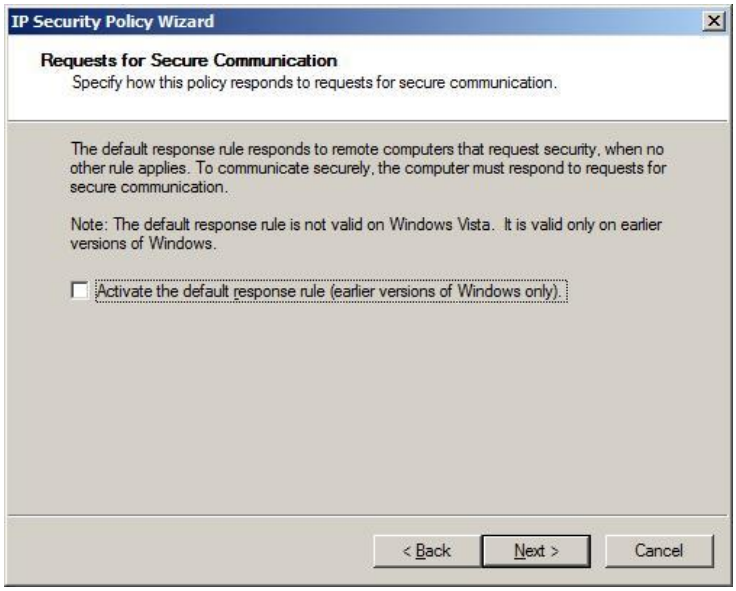


Рис. 3. Окно мастера IP Security Policy

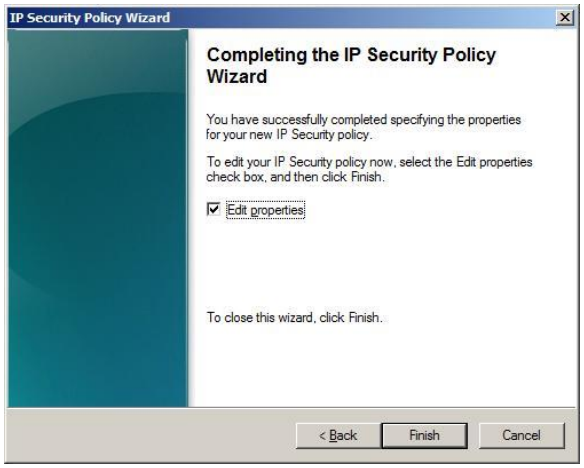


Рис. 4. Окно мастера IP Security Policy

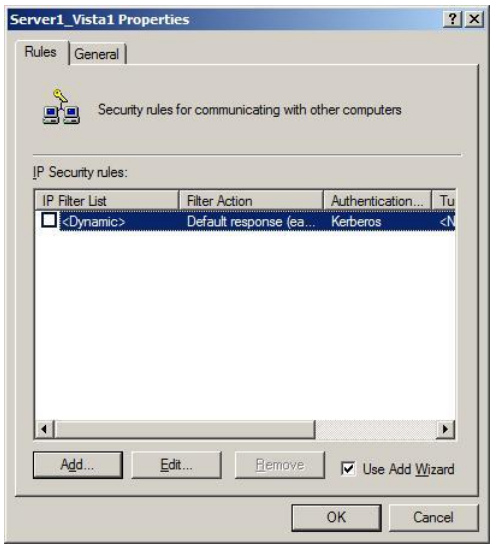


Рис. 5. Добавляем правило

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.

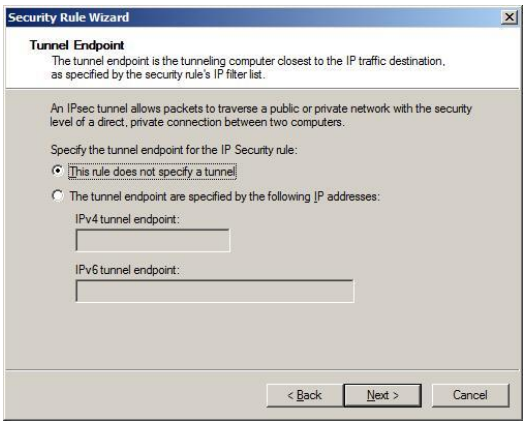


Рис. 6. Выбор типа соединения

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).

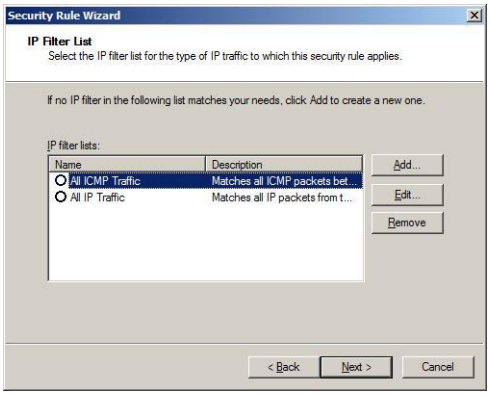


Рис.7. Фильтры позволяют определить, какие пакеты будут защищаться IPSec

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.

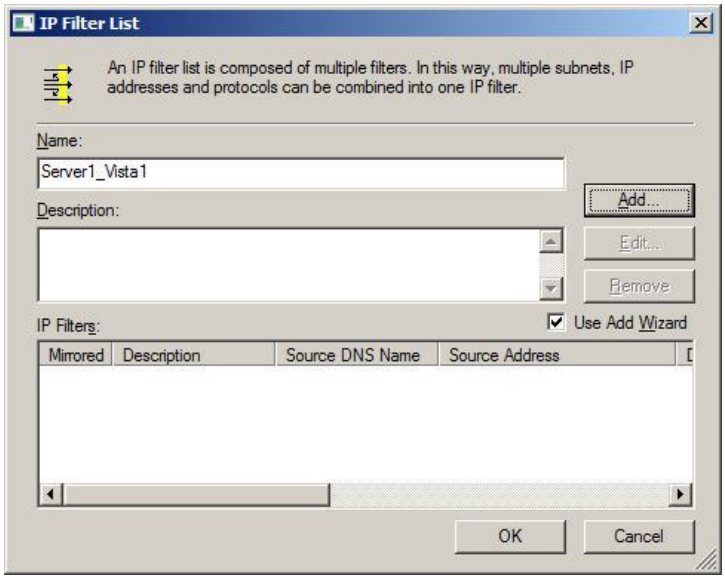


Рис. 8. Добавляем новый список фильтров

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).

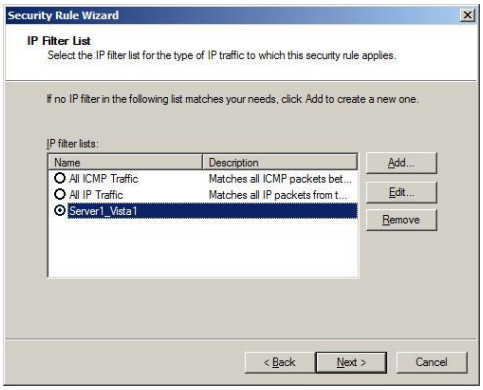


Рис. 9. Выбираем созданный фильтр

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.

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).

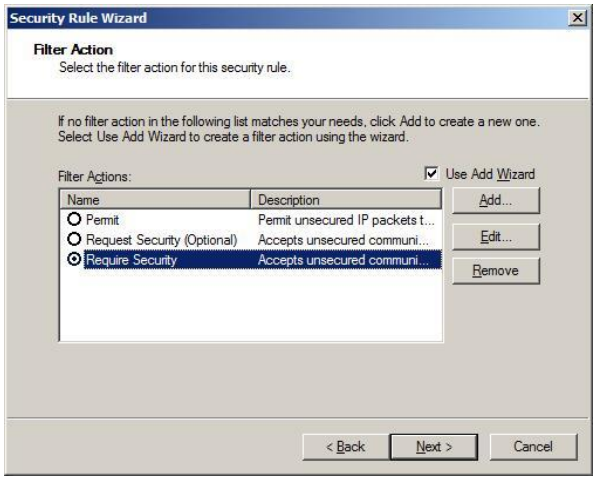


Рис. 10. Действия при получении незащищенного пакета

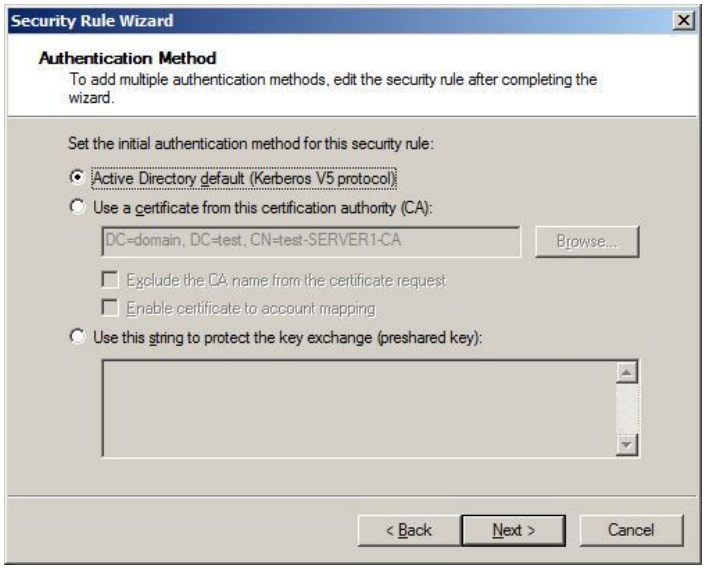


Рис. 11. Выбор метода аутентификации

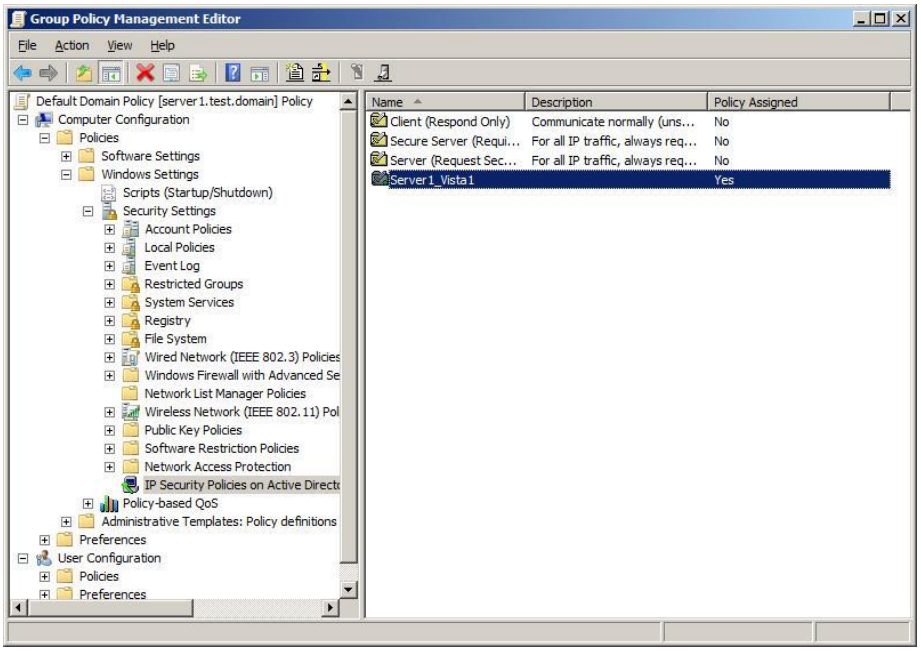


Рис. 12. Назначение политики

Задание

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).

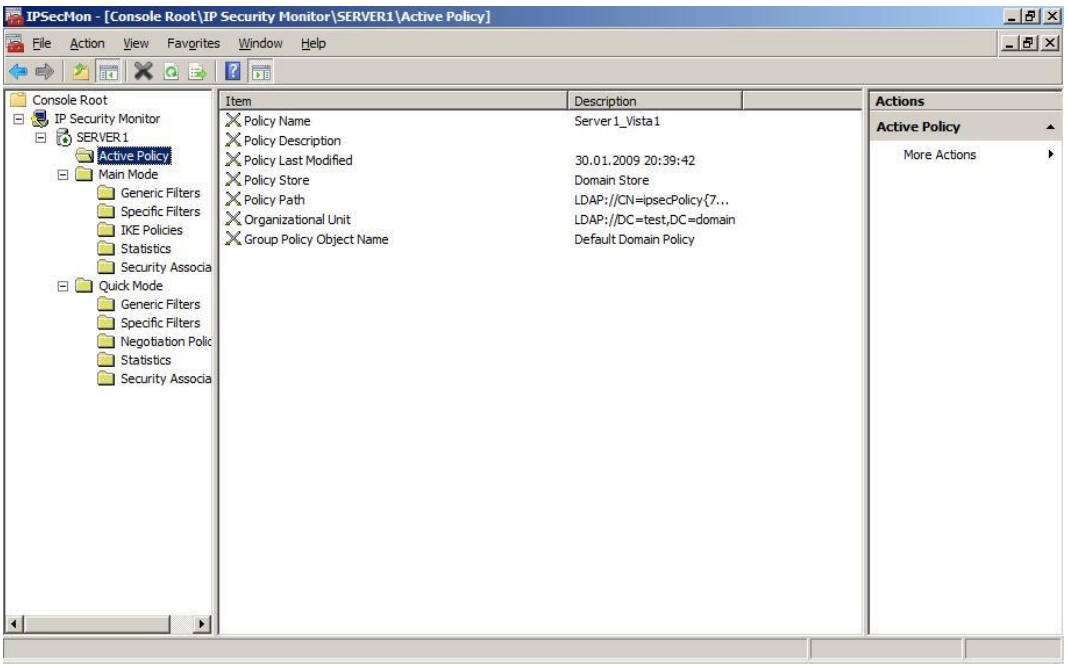


Рис. 13. Оснастка IPSec Monitor

Лабораторная работа № 13. Профилактика проникновения вредоносного программного обеспечения

Цель: практическое освоение студентами научно-теоретических положений дисциплины по вопросам защиты информации от воздействия вредоносного программного обеспечения на основе использования методов и средств профилактики вирусных атак, а также овладение ими техникой экспериментальных исследований и анализа полученных результатов, привитие навыков работы с вычислительной техникой.

Часть № 1

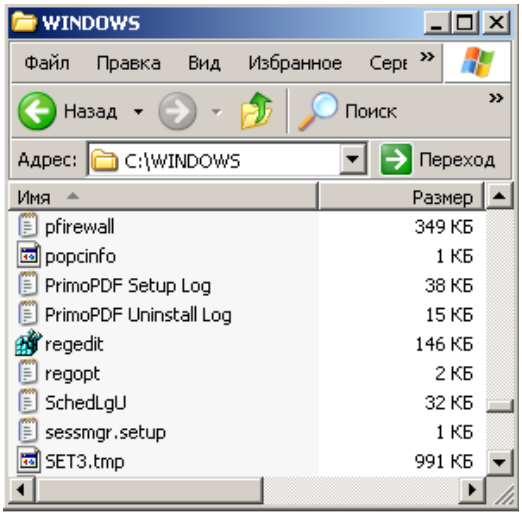
Профилактика проникновения вредоносного программного обеспечения посредством исследования Реестра ОС Windows

Краткие теоретические сведения

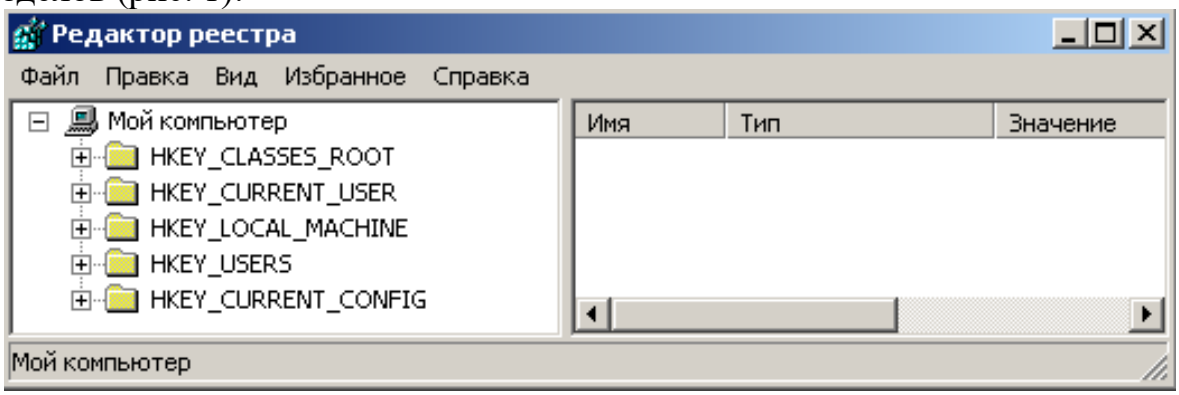
Реестр операционной системы Windows - это большая база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь копию реестра. Основным средством для' просмотра и редактирования записей реестра служит специализированная утилита **«Редактор реестра».**

Файл редактора реестра находится в папке Windows. Называется он

regedit.exe.

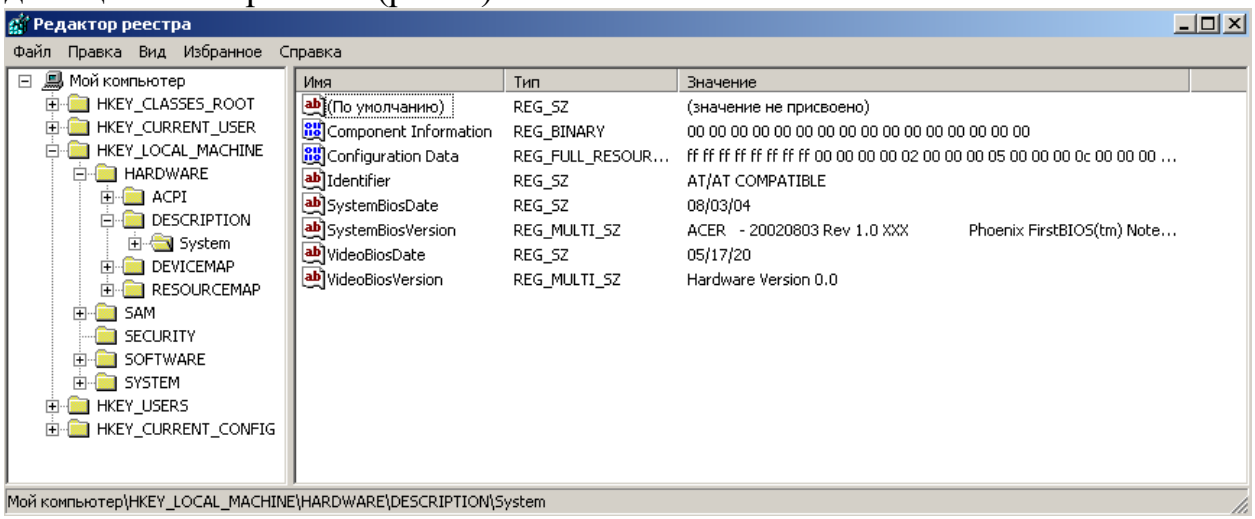


После запуска появится окно редактора реестра. Вы увидите список из 5 разделов (рис. 1):



HKEY_CLASSES_ROOT.
HKEY_CURRENT_USER.
HKEY_LOCAL_MACHINE.
HKEY_USERS.
HKEY_CURRENT_CONFIG.

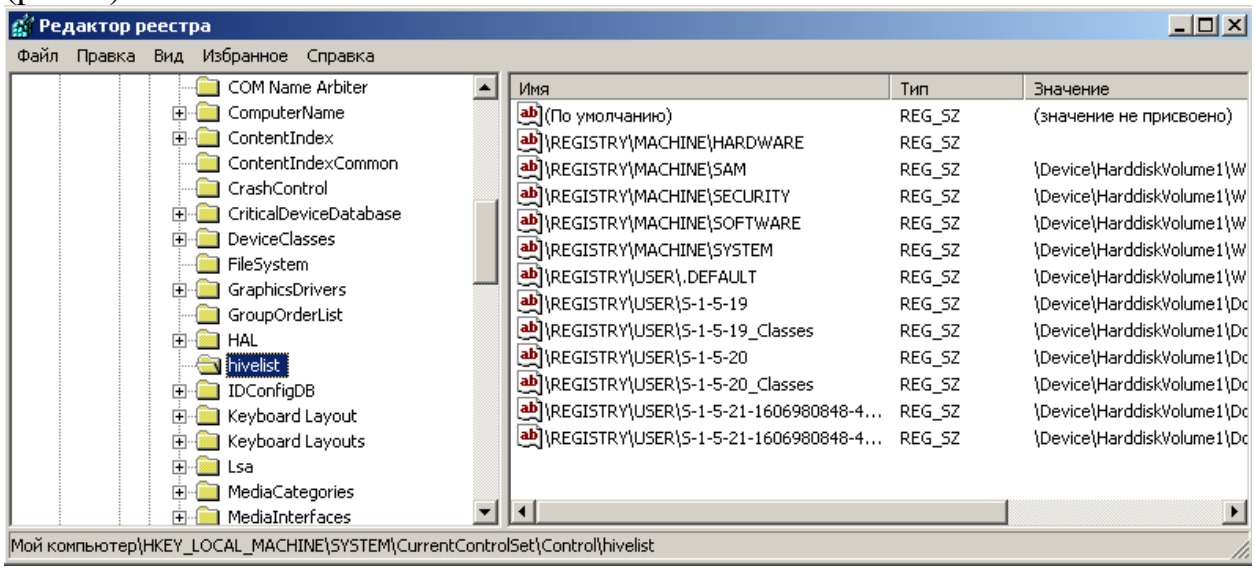
Работа с разделами реестра аналогична работе с папками в Проводнике. Конечным элементом дерева реестра являются ключи или параметры, делящиеся на три типа (рис. 2):



- строковые (напр. «C:\Windows»);

- двоичные (напр. 10 82 AO 8F);
- DWORD - этот тип ключа занимает 4 байта и отображается в шестнадцатеричном и в десятичном виде (например, 0x00000020 (32)).

В Windows системная информация разбита на так называемые ульи (***hive***). Это обусловлено принципиальным отличием концепции безопасности этих операционных систем. Имена файлов ульев и пути к каталогам, в которых они хранятся, расположены в разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Contro!\hivelist** (рис. 3).



В таблице 1 даны краткие описания ульев реестра и файлов, в которых хранятся параметры безопасности.

Таблица 1 Характеристика основных разделов системного Реестра

HKEY_LOCAL_MACHINE\SAM	Содержит информацию SAM (Security Access Manager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке \%System-root%\System32\Config
HKEY_LOCAL_MACH!NE\SECURITY	Содержит информацию безопасности в файлах SECURITY.SECURITY.LOG, SECURITY.SAV в папке \%Systemroot%\System32\Config
HKEY_LOCAL_MACHINE\SYSTEM	Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлахSYSTEM.SYSTEM.LOG, SYSTEM.SAV в папке \%Systemroot%\System32\Config
HKEY_CURRENT_CONFIG	Содержит информацию о подразделе System этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке \%Systemroot%\System32\Config
HKEY_USERS\.DEFAULT	Содержит информацию, которая будет использоваться для создания профиля нового пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке \%Systemroot%\System32\Config

HKEY_CURRENT_USER	Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT и - NTUSER.DAT.LOG, расположенных в каталоге \%Systemroot%\Profiles\User name, где User name — имя пользователя, зарегистрированного в системе на данный момент

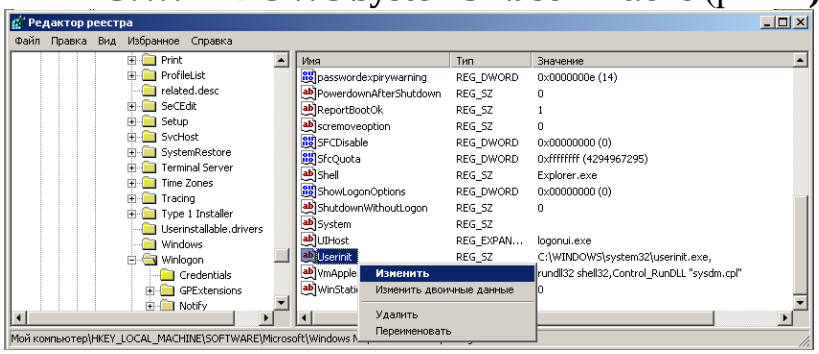
Задание

Проверить потенциальные места записей вредоносного программного обеспечения в системном реестре операционной системы Windows 2000 ***(XP).***

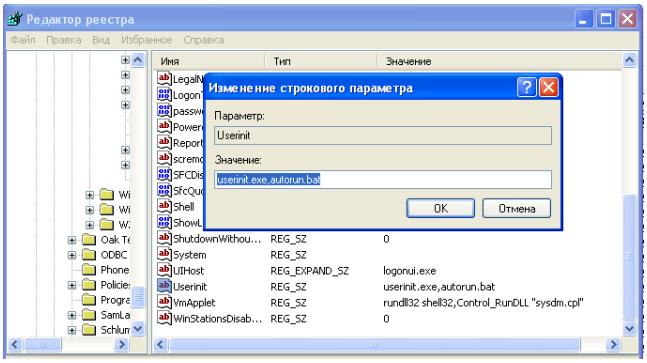
Алгоритм выполнения работы

Потенциальными местами записей «троянских программ» в системном реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.

1. Запустите программу **regedit.exe.**
2. В открывшемся окне выберите ветвь **HKEY_LOCAL_MACHINE** и далее **Software\ Microsoft\WindowsNT\CurrentVersion\Winlogon.**
3. В правой половине открытого окна программы **regedit.exe** появится список ключей.
4. Найдите ключ **Userinit (REG_SZ)** и проверьте его содержимое.
5. По умолчанию (исходное состояние) 151 этот ключ содержит следующую запись **C:\WINDOWS\system32\userinit.exe** (рис. **4).**



6. Если в указанном ключе содержатся дополнительные записи, то это могут быть «троянские программы».
7. В этом случае проанализируйте место расположения программы, обратите внимание на время создания файла и сопоставьте с Вашими действиями в это время.
8. Если время создания файла совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен «троянским конем».
9. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду **Изменить** из меню **Правка** программы **regedit.exe).**
10. **В** открывшемся окне в поле **Значение** (рисунок 5) удалите ссылку на подозрительный файл.



11. Закройте программу **regedit.exe**.

11. Перейдите в папку с подозрительным файлом и удалите его.

12. Перезагрузите операционную систему и выполните пункты задания 1-4.

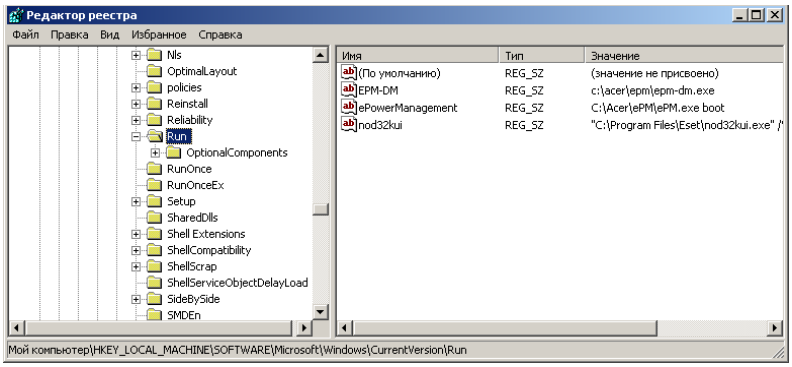
13. Если содержимое рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.

Еще одним потенциальным местом записей на запуск «троянских программ» является *раздел автозапуска* ***Run.***

Для его проверки выполните следующее.

1. Запустите программу **regedit.exe**.

2. В открывшемся окне выберите ветвь **HKEY_LOCAL_MACHINE** и далее **Software\Microsoft\Windows\CurrentVersion\Run\... (REG_SZ)** (рис. 6).



3. В рассматриваемом примере автоматически запускается резидентный антивирус (nod32kui), а также утилита, относящаяся к программе контроля состояния электропитания и заряда батареи (EPM-DM и ePowerManagement).

4. Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 6-14 предыдущего задания.

Часть № 2

Профилактика проникновения вредоносного программного обеспечения посредством исследования организации защиты от макровирусов средствами Microsoft Word.

Краткие теоретические сведения

Макрос - макрокоманда или набор макрокоманд, используемый для автоматического выполнения некоторых операций. Макросы записываются на языке программирования Visual Basic для приложений.

Макровирус – вредоносная программа, прописанная в макросе.

Цифровая подпись макроса. Специально созданный фрагмент макроса, подтверждающий его подлинность и безопасность. Наличие цифровой подписи подтверждает, что макрос или документ был получен от владельца подписи и не был изменен.

Цифровой сертификат - вложение в файл, проект макроса или сообщение электронной почты, подтверждающее его подлинность, обеспечивающее шифрование или предоставляющее поддающуюся проверке подпись. Для цифрового подписания проектов макросов необходимо установить цифровой сертификат.

Макровирусы используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).

Для существования вирусов в конкретной системе необходимо наличие встроенного в систему макроязыка со следующими возможностями:

1) привязка программы на макроязыке к конкретному файлу;
2) копирование макропрограмм (далее макросов) из одного файла в другой;
3) возможность получения управления макросом без вмешательства пользователя (автоматические или стандартные макросы).

Данным условиям удовлетворяют редакторы Microsoft Word и AmiPro, а также редактор электронных таблиц Excel. Эти системы содержат в себе макроязыки (Word - Word Basic, Excel - Visual Basic). В этих системах вирусы получают управление при открытии или закрытии зараженного файла, перехватывают стандартные файловые функции и затем заражают файлы, к которым каким-либо образом идет обращение.

Макровирусы активны не только в момент открытия/закрытия файла, но до тех пор, пока активен сам редактор.

В текстовом процессоре Microsoft Word определены, например, макросы, которые автоматически получают управление при вызове пользователем одной из стандартных команд — FileSave (Файл | Сохранить), FileSaveAs (Файл | Сохранить как), ToolsMacro (Сервис | Макрос | Макросы), ToolsCustomize (Сервис | Настройка) и т.д.

Документ Microsoft Office может также содержать макросы, автоматически получающие управление при нажатии пользователем определенной комбинации клавиш на клавиатуре или достижении некоторого момента времени (даты, времени суток).

Так как макровирусы распространяются под управлением прикладных программ, то этот факт делает их независимыми от операционной системы.

Наилучшим способом защиты от вредоносных макросов (макровирусов) в дополнение к административным мерам необходимо приобрести и установить специальное антивирусное программное обеспечение.

Задание

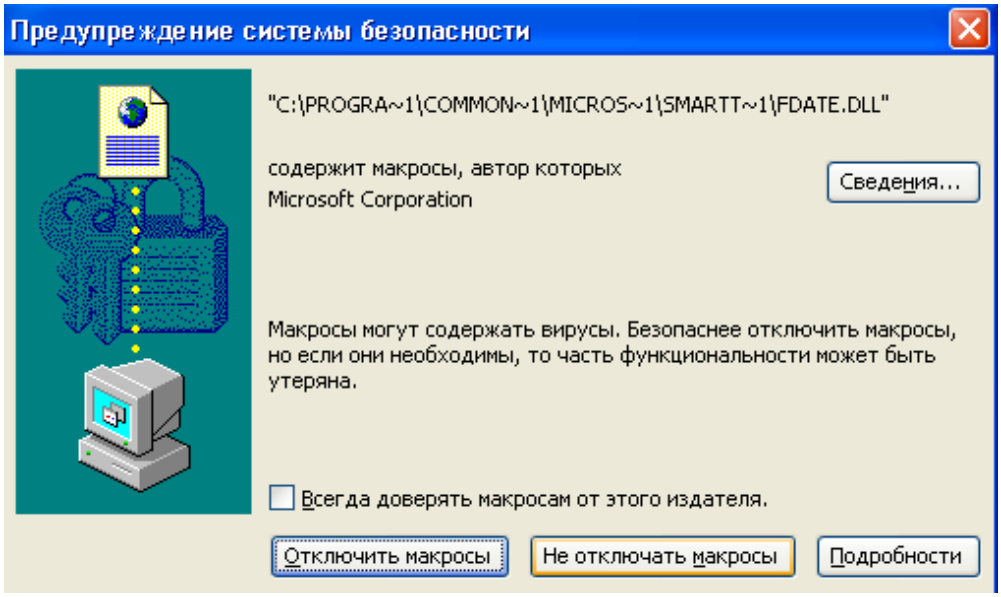
Исследовать порядок формирования политики защиты от макровирусов при использовании приложения Microsoft Word

Алгоритм выполнения работы

Запустите приложение Microsoft Word из пакета Office XP.
Произвести настройку **уровня безопасности при отработке макросов**

1. В меню **Сервис** выбрать команду **Параметры**.
2. Открыть вкладку **Безопасность**.
3. В группе **Защита от макросов** нажать кнопку **Защита от макросов**.
4. Открыть вкладку **Уровень безопасности**.
5. Выбрать нужный уровень безопасности.

В зависимости от настроек безопасности макросов, например, средний уровень, при открытии макросов выводится предупреждение [*Предупреждение об установленных шаблонах и надстройках, которые содержат макросы*] и предоставляется возможность запретить выполнение макросов для установленных шаблонов и настроек (в том числе для мастеров).



6. Откройте вкладку **Надежные источники**.
7. **Если снять флажок (5)** «*Доверять всем установленным надстройкам и шаблонам*», то при запуске приложения загрузка всех прописанных в приложении макросов будут сопровождаться предупреждением системы безопасности. Данный шаг может производиться опытными пользователями при анализе причин неустойчивой работы приложения.

В отчете отразить следующее:

1. Сформулировать определение реестра операционной системы. Какая утилита применяется для просмотра реестра.
2. Исследовать содержимое ключа ***Registered Organization*** **из каталога HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion**
3. Дать определение вируса, макровируса. Сформулировать условия существования вирусов в конкретной системе.
4. Исследовать порядок формирования политики защиты от макровирусов при использовании приложения Microsoft Excel (из пакета

Office XP) и описать маршрут действий пользователя при установке разрешения запуска только подписанных макросов из надежных источников при этом все неподписные макросы должны отключаться автоматически.

Отчет

о выполнении лабораторной работы № _____

Тема: Профилактика проникновения вредоносного программного обеспечения

Реестр *операционной системы Windows представляет собой*

Основным средством для просмотра и редактирования записей реестра является -

Исследовав содержимое ключа содержимое ключа ***RegisteredOrganization*** **из каталога HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion** мы открыли следующую запись в реестре:

Макросом называется -

Вирусом называется-

Существуют следующие условия существования вирусов в конкретной среде

Маршрут действий пользователя при установке разрешения запуска только подписанных макросов из надежных источников (при этом все неподписные макросы отключаться автоматически)

Студент (ка) группы _____ _____ (_____)

номер группы роспись фамилия

Отметка преподавателя о сдаче лабораторной работы: _____

роспись, дата

Список использованных источников

1. Об информации, информационных технологиях и о защите информации: федер. закон РФ № 149-ФЗ от 27.07.2006 г.
2. Доктрина информационной безопасности РФ № Пр-1895 от 06.09.2000 г.
3. О государственной тайне: федер. закон РФ № 5485-1 от 06.10.1997 г.
4. Указ Президента РФ «Перечень сведений конфиденциального характера» (№ 188 06.03.1997 г.).
5. Федеральный закон Российской Федерации «О персональных данных» (№ 152 от 27.07.2006 г.).
6. Федеральный закон Российской Федерации «Об электронной цифровой подписи» (№ 1-ФЗ от 26.12.2001 г.).
7. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 с.
8. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.
9. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.
10. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.
1. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт. Монография. Гриф УМЦ «Профессиональный учебник». Гриф НИИ образования и науки. / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ, 2016. — 239 с.
2. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г Милославская. — М.: ГЛТ, 2017. — 536 с.
3. Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.2 — Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. — М.: ГЛТ, 2018. — 558 с.
4. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 с.
5. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.
6. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016. — 296 с.
7. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 с.
8. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.

9. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. — 416 с.
10. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2017. — 702 с.
11. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. — М.: Акад. Проект, 2018. — 544 с.
12. Ярочкин, В.И. Информационная безопасность. 5-е изд. / В.И. Ярочкин. — М.: Академический проект, 2016. — 544 с.
13. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / под ред. Поляковой Т.А., Стрельцова А.А. – М.: Юрайт, 2017. – 325 с.
14. Кузнецов П.У. Информационное право [Электронный ресурс]: учебник для бакалавров. – М.: Издательство Юстиция, 2017. – 335 с. – URL: http://нэб.рф/catalog/000199_000009_009476417/ - ЭБС «НЭБ»
15. А. Пролетарский, Н. Руденков, Е. Смирнова, А. Суровов. Основные понятия в области информационной безопасности// Национальный Открытый Университет "ИНТУИТ": http://www.intuit.ru/studies/courses/16655/1300/print_lecture/25504
16. Ярочкин, В. Безопасность информационных систем / В. Ярочкин. - М.: Ось-89, 2016. - 320 с.
17. Введение в криптографию / Под. ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.
18. Барычев, С. Основы современной криптографии / С. Барычев, Р. Серов. – М.: 2001. – 152 с.
19. Бабаш, А.В. Криптография. Под. ред. В.П. Шерстюка, Э.А. Применко / А.В. Бабаш, Г.П. Шанкин – М.: СОЛОН-ПРЕСС, 2007. – 512 с.
20. CryptoBloG. Прикладные методы защиты информации. crypto-blog.ru
21. Галатенко В. А. Стандарты информационной безопасности. – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2005. - 264 с.
22. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с.
23. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с.
24. Галатенко В.А. Основы информационной безопасности: Курс лекций. – М.: ИНТУИТ. РУ, 2006. – 205 с.
25. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. – М.: Гелиос АРВ, 2006. – 528 с.
26. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.

27. Никулин В.В. Учебно-методическое пособие "Информационная безопасность" [Электронный ресурс] - URL: http://moodle.bgsha.com/course/view.php?id=25237
28. Никулин В.В. Учебно-методическое пособие «Безопасность и защита информации» [Электронный ресурс] - URL: http://moodle.bgsha.com/course/view.php?id=25340#section-7
29. Атака через Internet [Электронный ресурс] - URL: http://citforum.ru/internet/attack/c32.shtml
30. Антивирусная защита компьютерных систем: курс лекций для Интернет-университета информационных технологий от лаборатории Касперского – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2007. [Электронный ресурс]– URL: www.intuit.ru/department/security/antiviruskasp/
31. Вирусы и средства борьбы с ними: курс лекций для Интернет университета информационных технологий от лаборатории Касперского – М.: Интернет-университет информационных технологий - www.INTUIT.ru, 2007. [Электронный ресурс] – URL: www.intuit.ru/department/security/viruskasper/
32. Бейс Р. Введение в обнаружение атак и анализ защищенности // НИП «Информзащита» [Электронный ресурс] - URL: http://bugtraq.ru/library/books/icsa/

Учебное издание

Никулин Валерий Владимирович

Информационная безопасность

учебно-методическое пособие
Информационная безопасность. Лабораторный практикум для студентов направления подготовки 09.03.03 «Прикладная информатика»

Редактор Павлютина И.П.

Подписано к печати 10.11.2021. Формат 60х84. Бумага печатная.
Усл. п. л. 4,88. Тираж 100 экз. Изд. № 7061.

Издательство Брянского государственного аграрного университета

243365 Брянская область, Выгоничский район, с. Кокино, Брянский ГАУ