РОСЖЕЛДОР
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Ростовский государственный университет путей сообщения»
(ФГБОУ ВО РГУПС)
Филиал РГУПС в г. Воронеж

Утверждаю:
Заместитель директора по УПР филиала
РГУПС в г. Воронеж
_____ Гуленко П.И
«01» сентября 2023 г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 56e04e82f2d91c396292d43d4b4c48071
Владелец: Гуленко Петр Игоревич
Действителен: с 06.06.2023 по 29.08.2024

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

по МДК 05.03. Защита информации в компьютерных сетях

Специальность: 09.02.01. Компьютерные системы и комплексы

Профиль: технический

Квалификация выпускника: техник по компьютерным системам

Форма обучения: очная

Воронеж 2023 г.

Авторы-составители преподаватели высшей категории
Толубаева Л.А., Русинова Е.С.
предлагают методические указания по выполнению практических работ
по МДК 05.03. Защита информации в компьютерных сетях

Протокол № 04 от 01.09.2023 г.
Председатель цикловой комиссии_____ Русинова Е.С.
(подпись) (Ф.И.О.)

СОДЕРЖАНИЕ

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания для проведения практических занятий составлены в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы, учебным планом и рабочей программой ПМ.05 Компьютерные и телекоммуникационные сети. Методические указания предназначены для студентов и преподавателей средних профессиональных учебных заведений, изучающих МДК 05.03 Защита информации в компьютерных сетях.

Данные указания содержат необходимый теоретический материал, задания, необходимые для выполнения практических работ.

Целью изучения МДК 05.03 Защита информации в компьютерных сетях является освоение следующих компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 5.1. Проектировать и администрировать локально-вычислительные сети.

ПК 5.2. Проводить контроль, диагностику и восстановление работоспособности компьютерных и вычислительных сетей.

ПК 5.3. Определять методы и основные принципы защиты информации от несанкционированного доступа.

ПК 5.4. Настраивать виды соединений в IP - телефонии и взаимодействие с компьютерной сетью.

В результате выполнения практических работ обучающийся должен

уметь:

– участвовать в проектировании, монтаже и эксплуатации и диагностике компьютерных сетей;

– правильно выявлять и оценивать угрозы безопасности информации;

– категорировать информацию в соответствии с действующим законодательством;

– определять сферу действия и использовать законодательство в области инфор-

мационной безопасности;

– реализовывать технологии VPN и VLAN;

– правильно выбирать программные и/или аппаратные средства защиты информации от всех видов угроз по различным критериям;

– использовать оснастки политик безопасности различных операционных систем;

знать:

– типы сетей, серверов, сетевую топологию;

– типы передачи данных, стандартные стеки коммуникационных протоколов;

– установку и конфигурирование сетевого оборудования;

– принципы построения телекоммуникационных вычислительных сетей (ТВС);

– принципы построения беспроводного соединения;

– основы технологии IP – телефонии;

– технологию виртуальных частных сетей VPN;

– технологию виртуальных сетей;

– методы и средства обеспечения информационной безопасности;

– защиту от несанкционированного доступа, основные принципы защиты информации;

– технические методы и средства защиты информации.

2 ТЕМАТИЧЕСКИЙ ПЛАН

№№ п/п	Наименование темы	Количество часов
1	2	**3**
1.	Сети Microsoft Windows. Принципы построения. Работа с сетью в графическом режиме	2
2.	Сети Microsoft Windows. Работа в режиме консоли. Работа в режиме консоли.	2
3.	Сети Microsoft Windows. Настройка подключения рабочей станции к сети	2
4.	Разграничение доступа и управление сетевыми ресурсами сети Microsoft Windows Управление учетными записями пользователей, групп и сетевых ресурсов	2
5.	Групповые политики Microsoft Windows	2
6.	Межсетевой экран Microsoft Windows	2
7.	Протокол сетевой безопасности IPSec	2
8.	Настройка параметров подключения к сети во FreeBSD	2
9.	Разграничение доступа и управление сетевыми ресурсами во FreeBSD. Настройка межсетевого экрана	2
10.	Безопасность сетей на прикладном уровне. Использование Центра Сертификации Microsoft Windows.	2
11.	Основные угрозы информации в компьютерных системах	2
12.	Специфика возникновения угроз в открытых сетях	2
13.	Специфика возникновения угроз в открытых сетях	2
14.	Особенности защиты информации на узлах компьютерной сети с использованием криптографических методов	2
15.	Особенности защиты информации на узлах компьютерной сети с использованием криптографических методов	2
16.	Администрирование серверных систем и приложений	2
17.	Администрирование серверных систем и приложений	2
18.	Использование межсетевых экранов для защиты информационных процессов	2
19.	Использование межсетевых экранов для защиты информационных процессов	2
20.	Использование межсетевых экранов для защиты информационных процессов	2
21.	Требования к защите автоматизированных систем от НСД	2
22.	Требования к защите автоматизированных систем от НСД	2
	Итого:	**44**

Практическая работа №1 Сети Microsoft Windows. Принципы построения. Работа с сетью в графическом режиме

Цель работы

Цель работы состоит в изучении принципов организации сети на базе операционных систем семейства Microsoft Windows. А так же в приобретении навыков работы с этими сетями в графическом режиме.

Задание на работу

1. Изучить принципы построения сетей на базе операционных систем семейства Microsoft Windows.

2. Просмотреть список рабочих групп (доменов), компьютеров, сетевых ресурсов компьютера.

3. Подключить сетевую папку с сервера сети. Подключить скрытую сетевую папку с компьютера сети. Скопировать файл на сетевой диск и с сетевого диска. Отключить сетевой диск.

4. Подключить сетевой принтер с сервера сети. Просмотреть очередь печати подключенного принтера. Распечатать любой текстовый файл на этом принтере. Приостановить и восстановить задание в очереди печати. Удалить задание из очереди печати. Отключить сетевой принтер.

5. Найти компьютер с заданным именем в сети. Найти файлы или папки по заданному шаблону на указанном компьютере.

6. Предоставить общий доступ к одной из папок своего компьютера. Разрешить всем пользователям сети только просмотр содержимого папки, а членам своей группы разрешить полный доступ.

7. Создать скрытую сетевую папку на вашем компьютере.

8. Предоставить общий доступ к принтеру своего компьютера. Разрешить всем пользователям печать на сетевом принтере, а членам своей группы разрешить управление очередью печати принтера.

9. Ознакомиться с работой программы NetMeeting. Начать встречу или подключиться к уже существующей встрече, дождаться подключения дополнительных пользователей, обменяться короткими сообщениями с участниками встречи с помощью команды «Разговор». Принять участие в совместном рисовании рисунка с помощью команды «Доска». Разослать всем участникам встречи какой-нибудь текстовый файл.

10. Составить отчет о проделанной работе.

Практическая работа №2 Сети Microsoft Windows. Работа в режиме консоли. Работа в режиме консоли.

Цель работы

Целью работы является изучение возможностей выполнения различных операций при работе с сетью Microsoft в режиме командной строки. Необходимо изучить консольные команды и научиться их использовать.

Задание на работу

1. Ознакомиться с принципами работы с сетью в режиме командной строки

2. Ознакомиться с возможностями команды net

а. Просмотреть список компьютеров в сети, в заданной рабочей группе или домене. Просмотреть список сетевых ресурсов сервера. Определить тип этих ресурсов.

b. Подключить сетевой диск с сервера сети. Попробовать скопировать какой-нибудь файл с подключенного сетевого диска и на него.

c. Подключить сетевой принтер с сервера сети. Просмотреть список заданий в очереди печати принтера. Отправить на принтер любой текстовый файл. Приостановить печать всех заданий. Удалить свое задание из очереди печати.

d. Отключить сетевой диск и сетевой принтер.

e. Предоставить общий доступ к одной из папок своего компьютера.

f. Вывести список запущенных на компьютере сетевых служб. Остановить работу одной из служб. Запустить остановленную службу.

3. Выяснить текущие параметры подключения рабочей станции к сети с помощью команды ipconfig

4. Выяснить возможность соединения с соседним компьютером (ping)

5. Выяснить маршрут передачи пакетов до некоторых узлов сети Интернет (tracert) 6. Выяснить физический адрес сетевого адаптера соседнего компьютера (arp)

7. Написать отчет о проделанной работе

Практическая работа №3 Сети Microsoft Windows. Настройка подключения рабочей станции к сети

Цель работы

Целью данной работы является изучение принципов настройки сетевого окружения рабочей станции для работы с сетью Microsoft Windows в различных режимах, а так же настройка сетевого окружения для работы сетями других типов (Novell NetWware).

Задание на работу

1. Изучить принципы настройки сетевого окружения

2. Усвоить состав программных компонентов, минимально необходимых для работы в сети. А так же усвоить состав программных компонентов для работы с различными типами сетей.

3. Выяснить назначение различных параметров драйвера сетевого адаптера.

4. Выяснить назначение различных параметров протокола IPX/SPX

5. Выяснить назначение различных параметров протокола Интернета TCP/IP.

6. Изучить параметры Клиента сети Microsoft Windows и Клиента сети Novell NewWare.

7. Изучить особенности настройки сетевого окружения при наличии нескольких подключений к различным сетям

8. Написать отчет о проделанной работе

Практическая работа №4 Разграничение доступа и управление сетевыми ресурсами сети Microsoft Windows Управление учетными записями пользователей, групп и сетевых ресурсов

Цель работы

Целью данной работы является изучение возможностей сервера по созданию и управлению учетными записями подразделений, пользователей и групп пользователей, регистрации компьютеров в домене, созданию общих папок и принтеров, управлению доступом пользователей к ресурсам контроллера домена и сетевым ресурсам.

Задание на работу

В данной работе необходимо: 1. Подключиться к контроллеру домена с помощью клиента службы терминалов.

2. В оснастке «Active Directory. Пользователи и компьютеры» создать новое подразделение, указать пользователя, которому делегируются права управления этим подразделением.

3. В подразделении создать учетную запись нового пользователя. Настроить параметры этой учетной записи.

4. Создать учетную запись группы пользователей. Настроить параметры.

5. Зарегистрировать в домене новый компьютер.

6. Зарегистрировать общую папку в домене.

7. Зарегистрировать принтер в домене.

8. Предоставить локальный и сетевой доступ пользователю и группе к папке C:\TEMP на сервере.

9. На рабочей станции, подключенной к домену, зарегистрироваться в домене под именем нового пользователя. Осуществить подключение ранее созданных общей папки и принтера.

10. Проверить итоговые права доступа пользователя к папке C:\TEMP на сервере в случае подключения локально или по сети.

11. Написать отчет о проделанной работе

Практическая работа №5 Групповые политики Microsoft Windows

Цель работы

Целью данной работы является получения навыков управления пользователями и компьютерами домена с помощью политики безопасности домена. Уяснение различий между локальной политикой, политикой безопасности контроллера домена и политикой безопасности домена.

Задание на работу

В данной работе необходимо:

1. Создать подразделение, создать учетную запись нового пользователя, включить в подразделение новый компьютер.

2. Для подразделения создать политику безопасности

3. Для компьютера подразделения в политике безопасности:

a. ограничить минимальную длину пароля пользователя 8 символами

b. задать периодичность смены пароля 30 дней

c. задать блокирование учетной записи после 5 попыток ввода неправильного пароля

d. запретить смену системного времени e. задать другие ограничения

4. Для пользователя подразделения в политике безопасности:

a. Задать настройки прокси-сервера по умолчанию

b. Установить перенаправление папки «Мои документы» всех пользователей на заранее заданную сетевую папку на сервере

c. Задать автоматическое удаление папок пользователя из главного меню

d. Скрыть из главного меню папки «Избранное» и «Настройки»

e. Установить фоновый рисунок рабочего стола по умолчанию

f. Задать другие ограничения

5. Зарегистрироваться в сети под именем созданного пользователя и проверить действие ограничений, введенных политикой безопасности.

6. Написать отчет о проделанной работе

Практическая работа № 6 Межсетевой экран Microsoft Windows

Цель работы

Целью данной работы является закрепление на практике теоретического материала по межсетевым экранам и практическое ознакомление с возможностями и настройкой межсетевого экрана, встроенного в операционную систему Windows XP SP2.

Задание на работу

1. Изучить теоретический материал по межсетевым экранам

2. Изучить возможности межсетевого экрана, встроенного в операционную систему Windows XP SP2.

3. Включить межсетевой экран на рабочей станции

4. Заблокировать Общий доступ к файлам и принтера на рабочей станции средствами Межсетевого экрана Windows

5. Разблокировать Общий доступ к файлам и принтерам, разрешить сетевой доступ только для рабочих станций локальной сети

6. Отключить межсетевой экран на одном из интерфейсов. Проверить результат

7. Задать параметры журнала безопасности. Просмотреть журнал безопасности, найти в журнале безопасности записи о попытках подключения к рабочей станции 8. Заблокировать возможность работы программы FAR Manager с ресурсами сети

9. Разблокировать возможность работы с сетью ранее заблокированной программы

10. Написать отчет о проделанной работе

Практическая работа № 7 Протокол сетевой безопасности IPSec

Цель работы

Целью данной работы является изучение принципов защиты сетевых взаимодействия с помощью протокола безопасности IPSec, встроенного в операционные системы семейства Microsoft Windows.

Задание на работу Необходимо создать несколько политик безопасности IP для решения следующих задач:

1. Политика для клиента сети, разрешающая только защищенное (шифрование и поддержка целостности) обращение к любому http серверу.

2. Политика для клиента сети, разрешающая защищенное (шифрование) обращение к локальному http серверу с адресом 192.168.24.1 и не защищенные обращения к другим http и ftp серверам.

3. Политика для сервера сети, разрешающая только защищенные (поддержка целостности) обращения из локальной сети и незащищенные обращения от остальных станций по любому протоколу.

4. Политика для сервера сети, разрешающая только защищенные (шифрование и поддержка целостности) обращения по протоколам POP3 и SMPT с любой станции. 5. Политика безопасного (шифрование и поддержка целостности) соединения двух серверов. Остальные соединения не защищенные.

6. Написать отчет о проделанной работе

Практическая работа № 8 Настройка параметров подключения к сети во FreeBSD

Цель работы

Целью данной работы является изучение принципов настройка подключения к сети компьютеров с установленной операционной системой FreeBSD. Задание на работу В данной работе необходимо:

1. Освоить принципы настройки подключения к сети компьютера с установленной операционной системой FreeBSD

2. Изучить настройку подключения к сети с помощью утилиты sysinstall

3. Изучить работу утилиты ifconfig.

a. Просмотреть список доступных сетевых интерфейсов

b. Выключить/включить/добавить/удалить сетевой интерфейс

c. Назначить одному из сетевых интерфейсов IP-адрес и маску подсети

4. Настроить постоянный IP-адрес для одного из сетевых интерфейсов

5. Настроить динамический IP-адрес для одного из сетевых интерфейсов (настройка с помощью DHCP-протокола)

6. Настроить параметры маршрутизации. Настроить маршрут по умолчанию. Настроить маршрут для широковещательных пакетов

7. Настроить параметры системы разрешения имен. Указать DNScерверы.

8. Написать отчет о проделанной работе

Практическая работа № 9 Разграничение доступа и управление сетевыми ресурсами во FreeBSD. Настройка межсетевого экрана

Цель работы

Целью данной работы является изучение принципов разграничения доступа в операционной системе FreeBSD, а так же изучение принципов настройки межсетевого экрана в данной операционной системе.

Задание на работу В данной работе необходимо выполнить:

1. Изучить принципы разграничения доступа пользователей к файлам в операционной системе FreeBSD

2. Зарегистрировать двух пользователей в операционной системе. Зарегистрировать новую группу пользователей. Включить новых пользователей в созданную группу. 3. Изменить права доступа, назначенные на рабочие папки пользователей по умолчанию, так чтобы один из пользователей мог входить в рабочую папку другого пользователя и выполнять некоторые действия с файлами, а второй пользователь не мог входить в рабочую папку первого пользователя

4. Изучить принципы настройки межсетевого экрана ipfw, встроенного в операционную систему FreeBSD

5. Настроить параметры межсетевого экрана таким образом, чтобы к данному компьютеру можно было подключаться только из локальной сети

6. Настроить параметры межсетевого экрана таким образом, чтобы к данному компьютеру можно было подключаться по протоколам HTTP, SMTP и POP3 из любой точки Интернета

7. Настроить межсетевой экран таким образом, чтобы запросы, пришедшие на определенный сетевой интерфейс передавались другому компьютеру в локальной сети

8. Настроить параметры межсетевого экрана таким образом, чтобы с данного компьютера можно было подключаться только по протоколам HTTP и SSH к другим компьютерам сети Интернет

9. Написать отчет о проделанной работе

Практическая работа №10 Безопасность сетей на прикладном уровне. Использование Центра Сертификации Microsoft Windows.

Цель работы

Целью данной работы является изучение принципов защиты сетевых взаимодействия на прикладном уровне с помощью Службы сертификации Microsoft Windows.

Задание на работу. В данной работе необходимо:

1. Изучить принципы защиты сетевых взаимодействий на прикладном уровне

2. Установить и настроить Центр сертификации Microsoft Windows

3. Изготовить ключи и выпустить сертификат открытого ключа для двух пользователей

4. Настроить программу Outlook Express (или другую почтовую программу) на использование ключей защиты

5. Осуществить обмен электронными письмами, защищенными с помощью электронно-цифровой подписи и шифрования. Проверить правильность подписи у каждого пользователя

6. Изготовить ключи и выдать сертификаты, необходимые для защищенного взаимодействия с веб-сервером сети

7. В программе Диспетчер IIS на сервере настроить веб-сервер, который поддерживает защищенное взаимодействие с клиентами Интернета

8. На рабочей станции настроить программу Internet Exploror для защищенного взаимодействия с веб-вервером. Осуществить подключение к защищенному веб-серверу и просмотреть доступные на нем страницы.

9. Написать отчет о проделанной работе

Практическая работа №11 Основные угрозы информации в компьютерных системах

Цель работы:

Изучить основные угрозы информации в компьютерных системах.

Ход работы:

1) По согласованию с преподавателем определить исходные данные: ∗ Вид предприятия, краткое описание структуры предприятия, видов продукции и процессов. ∗ Краткое описание инфраструктуры и ресурсов. ∗ Описание информационной инфраструктуры предприятия.

2) Определить основные виды объектов защиты для данного предприятия. Для каждого вида объектов привести конкретные примеры. Объекты защиты выбирать в составе оборудования, инфраструктуры, персонала предприятия.

3) Определить основные виды угроз и способов их реализации для основных объектов защиты для заданного предприятия.

4) Для каждого вида угроз определить основные способы и средства предотвращения угроз.

5) Сформулировать основные элементы системы инженерно-технической защиты информации для заданного предприятия.

Рекомендуется изложить информацию в табличной форме, например

№п/п	Элемент орг-структуры или инфраструктуры	Вид угрозы	Методы защиты	Средства инженерно-технической защиты
1	2	3	4	5

Практическая работа №12-13 Специфика возникновения угроз в открытых сетях

Сетевые сканеры безопасности – программные средства, позволяющие проверить уровень уязвимости сетей. Они имитируют различные обращения к сетевым узлам, выявляя операционные системы компьютеров, запущенные сервисы, имеющиеся уязвимости. В неко торых случаях сканеры безопасности также имитируют реализацию различных атак, чтобы проверить уровень подверженности им компьютеров защищаемой сети. При проведении анализа рисков сканеры безопасности могут использоваться как в процессе инвентаризации ресурсов, так и для оценки уровня уязвимости узлов сети. В данной лабораторной работе используется ПО Shadow Security Scanner разработки компании Safety-Lab, ознакомительная версия которого бесплатно доступна на сайте www.safety-lab.ru или www.safety-lab.com После запуска сканера надо начать новую сессию (нажав соответствующую кнопку на панели инструментов). Затем следует выбрать тип проводимых проверок, описываемый правилом (рис.1). К определению проверяемых параметров надо относиться достаточно внимательно. Например, проведение на работающей в штатном режиме информационной системе имитации атак на отказ в обслуживании (DoS tests) может привести к сбою в работе системы, что зачастую недопустимо. Другой пример - сканирование всех TCP и UDP портов (а не только «стандартных») приведет к большим затратам времени, но позволит выявить запущенные службы, использующие нестандартные порты (подробнее об этом см. ниже).

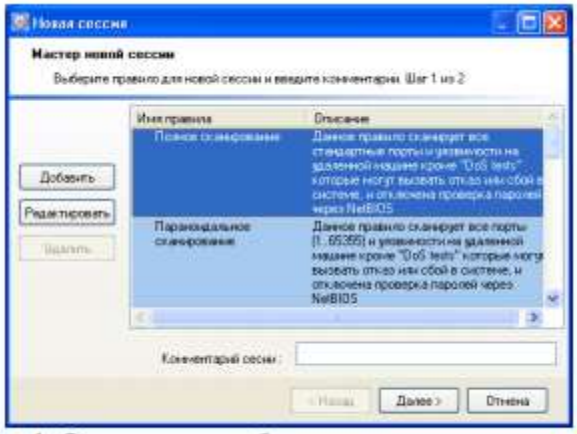


Рис.1. Определение набора проводимых проверок.

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

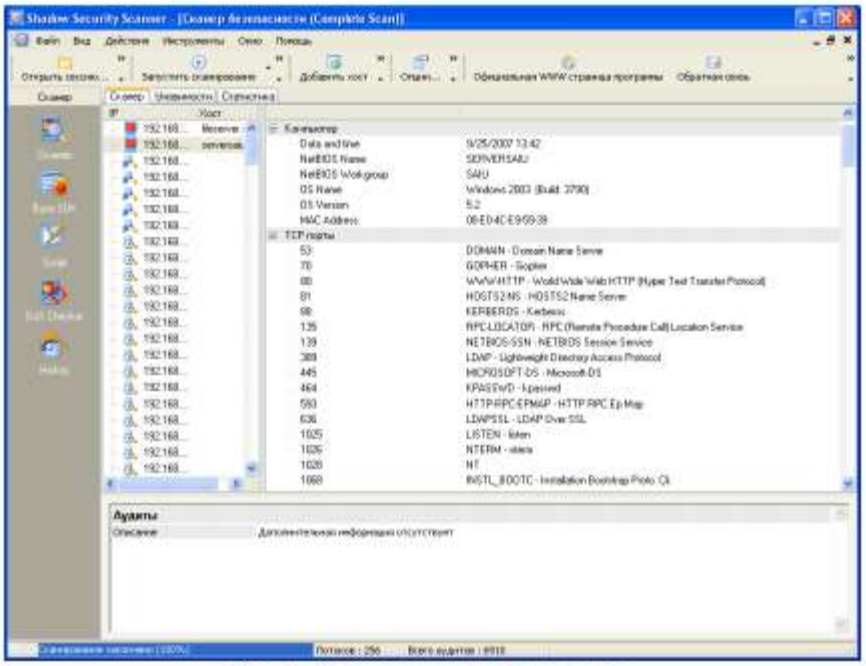


Рис. 3. Результаты сканирования.

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). 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.

Ход работы:

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.

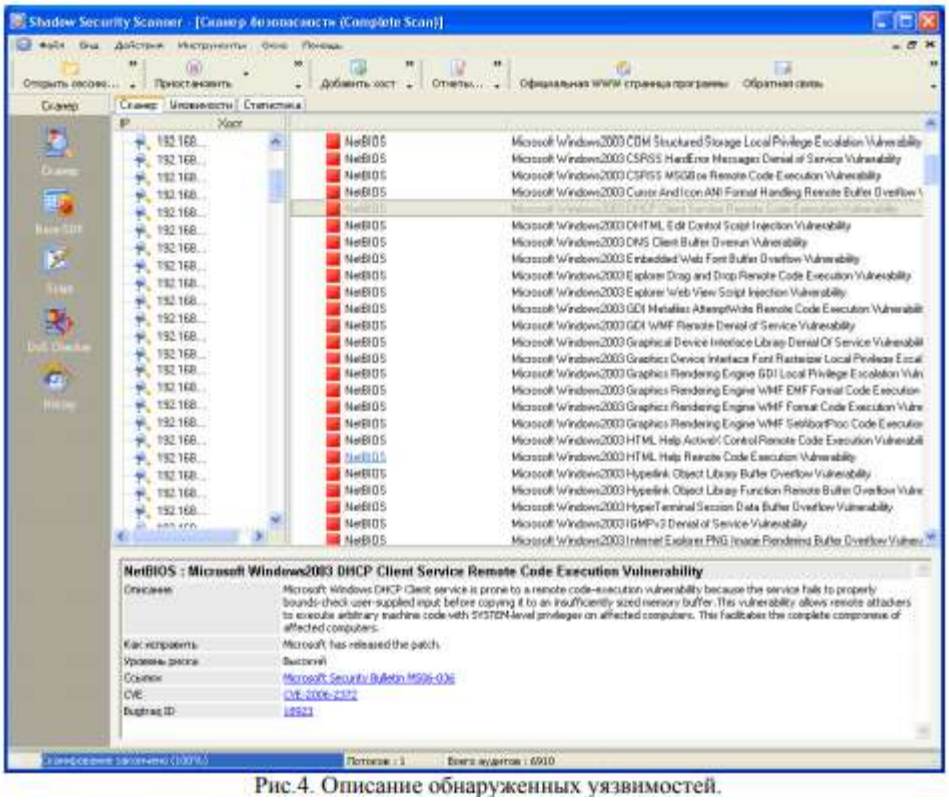


Рис.4. Описание обнаруженных уязвимостей.

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

Практическая работа № 14-15 Особенности защиты информации на узлах компьютерной сети с использованием криптографических методов

Цель работы: Изучить особенности защиты информации на узлах компьютерной сети с использованием криптографических методов.

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 конфи денциальных данных (предприятий или личных) оказывается на дисках ноутбуков, на съемных носителях и т.д. Вероятность того,

что подобное устройство будет украдено или временно попадет в чужие руки, существенно выше чем, например, для жесткого диска корпоративного персонального компьютера (хотя и в этом случае, возможны кражи или копирование содержимого накопителей). Если данные хранить в зашифрованном виде, то даже если носитель украден, конфиденциальность данных нарушена не будет. В этом и заключается цель использования EFS. Следует учитывать, что для передачи по сети, зашифрованный EFS файл будет расшифрован, и для защиты данных в этих случаях надо использовать дополнительные механизмы. Рассмотрим работу EFS. Пусть, у нас имеется сервер Windows Server 2008, входящий в домен, и три учетные записи, обладающие административными правами на сервере (одна из них - встроенная административная запись Administrator). Пользователь User1 хочет защитить конфиденциальные файлы. Тут надо отметить, что хотя шифровать с помощью EFS можно и отдельные файлы, рекомендуется применять шифрование целиком к папке. User1 с помощью оснастки Certificates запрашивает сертификат (можно выбрать шаблон User или Basic EFS). Теперь у него появляется ключевая пара и сертификат открытого ключа, и можно приступать к шифрованию. Чтобы зашифровать папку, в ее свойствах на вкладке General нажимаем кнопку Advanced и получаем доступ к атрибуту, указывающему на шифрование файла.

Рис.1. В свойствах папки устанавливаем шифрование.

Работа EFS организована так, что одновременно сжатие и шифрование файлов и папок осуществляться не может. Поэтому нельзя разом установить атрибуты Compress contents to save disk и Encrypt contents to secure data (рис.1). При настройках по умолчанию, зашифрованная папка выделяется в проводнике зеленым цветом. Для зашифровавшего файл пользователя порядок работы с ним не изменится. Теперь выполним «переключение пользователей» и зайдем в систему под другой учетной записью, обладающей административными правами, но не являющейся встроенной административной записью. Пусть это будет User2. Несмотря на то, что User2 имеет такие же разрешения на доступ к файлу, что и User1, прочитать он его не сможет (рис.2). Также он не сможет его скопировать, т.к. для этого надо расшифровать файл. Но надо учитывать, что User2 может удалить или переименовать файл или папку.

Рис.2. Другой пользователь прочитать файл не сможет.

Ход работы:

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).

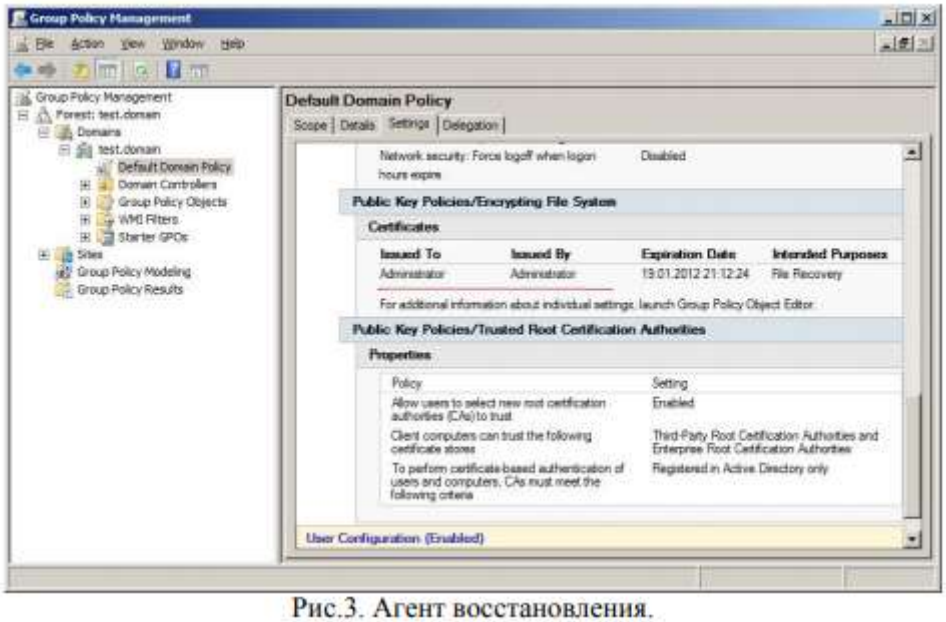


Рис.3. Агент восстановления.

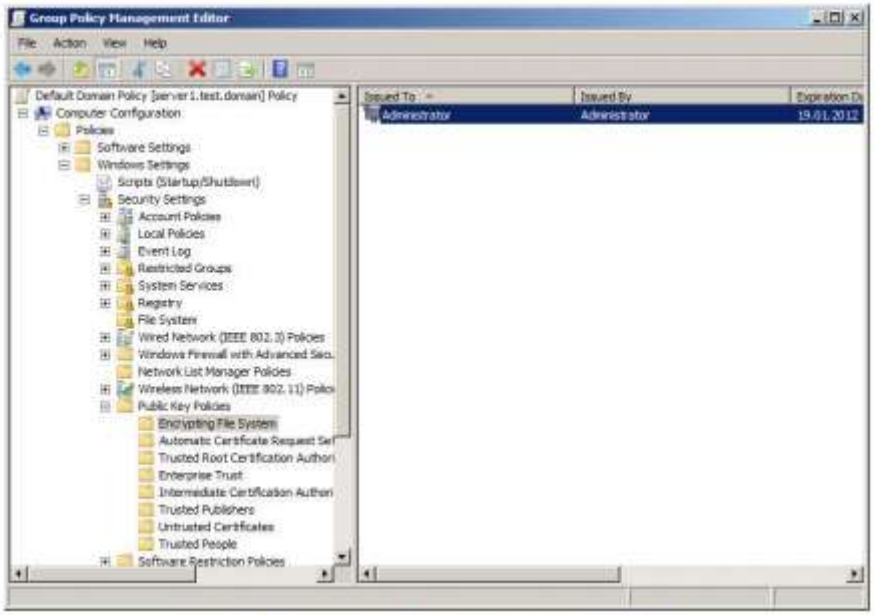


Рис.4. Изменение агента восстановления.

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 пользова тель 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.

Практическая работа № 16-17 Администрирование серверных систем и приложений

Цель работы: Изучить методы администрирования серверных систем и приложений.

Сбор данных об информационной системе с помощью средств администрирования Windows (оснасток MMC). Для проведения оценки рисков необходимо провести инвентаризацию активов информационной системы (ИС). Если в ИС используются домены Windows, для получения данных о системе можно использовать средства администрирования, реализованные в виде оснасток консоли администрирования (Microsoft management console – mmc). Используемые в данной работе инструменты могут быть запущены из раздела «Администрирование» меню «Пуск» или через «Панель управления» (Пуск -> Панель управления -> Администрирование).

Целью данной лабораторной работы является сбор данных об имеющихся компьютерах, установленных на них операционных системах, предоставляемых в общий доступ файловых ресурсах. Из раздела «Администрирование» запустите Active Directory Users and Computers. В раскрывающемся списке объектов выберите Ваш домен, там откройте перечень компьютеров (папка Computers – рис.1).

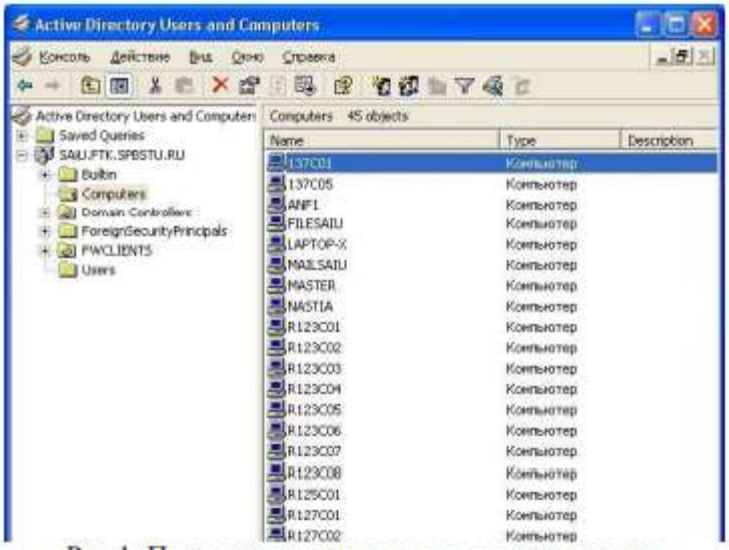


Рис.1. Получение перечня компьютеров домена.

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

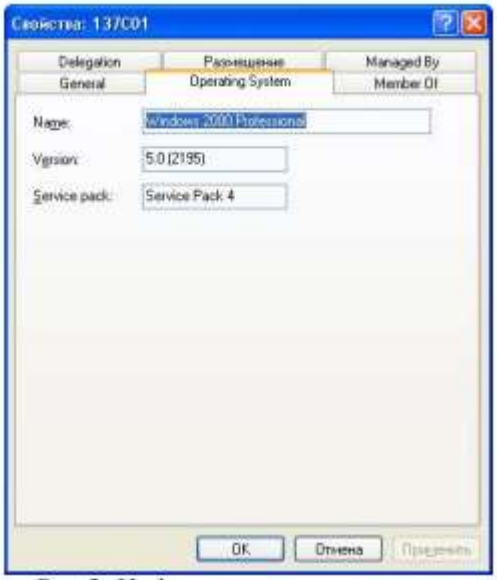


Рис.2. Информация о компьютере.

Информацию о соответствии имен компьютеров IP-адресам можно получить, используя утилиту командной строки nslookup или административную оснастку «DNS». Например, узнать IP-адрес компьютера comp1.mcompany.ru можно с помощью команды nslookup comp1.mcompany.ru Часто действующие настройки в сети таковы, что ip-адреса компьютерам выделяются динамически, с использованием службы dhcp, и могут периодически меняться. Как правило, у серверов ip-адреса постоянны. Теперь перейдем к этапу сбора данных об информационных ресурсах, поддерживаемых на компьютере. Перечень предоставляемых

в общий доступ папок можно получить с помощью оснастки «Управление компьютером». На рис.3 представлен пример перечня ресурсов рабочей станции, предоставляемых в общий доступ в служебных целях. Этот список можно также экспортировать в текстовый файл.

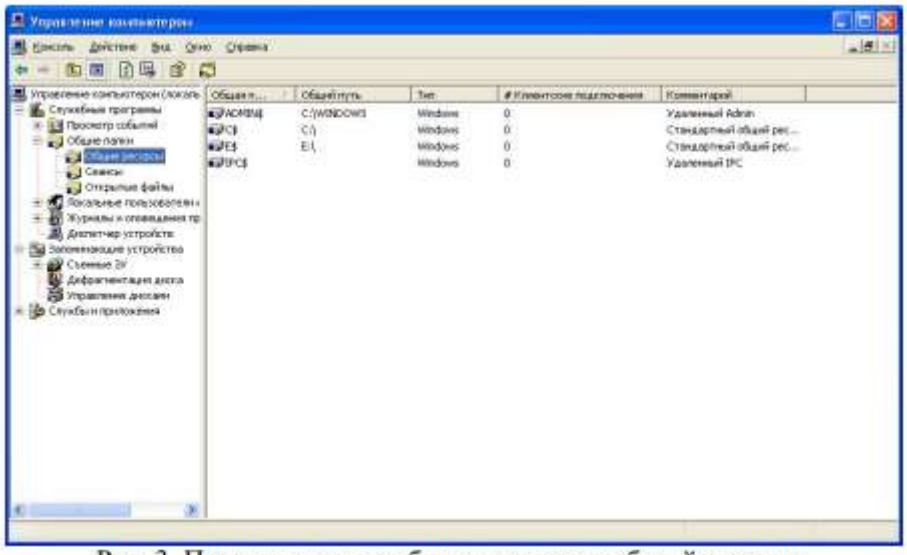


Рис. 3. Пример перечня общих ресурсов рабочей станции.

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

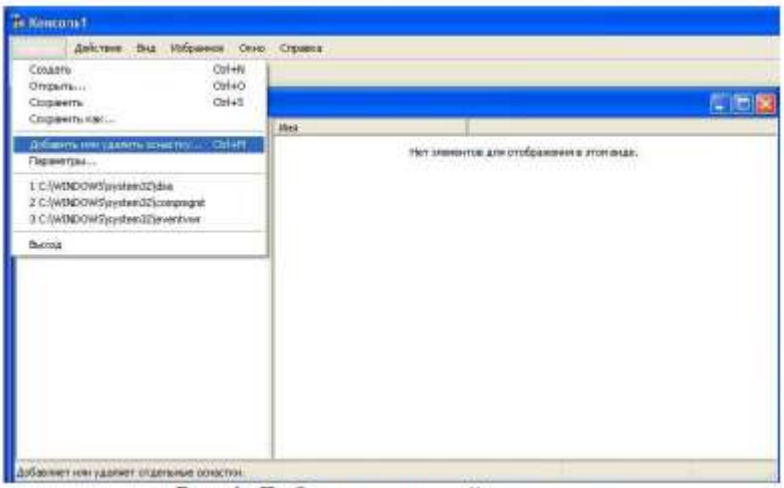


Рис.4. Добавление новой оснастки.

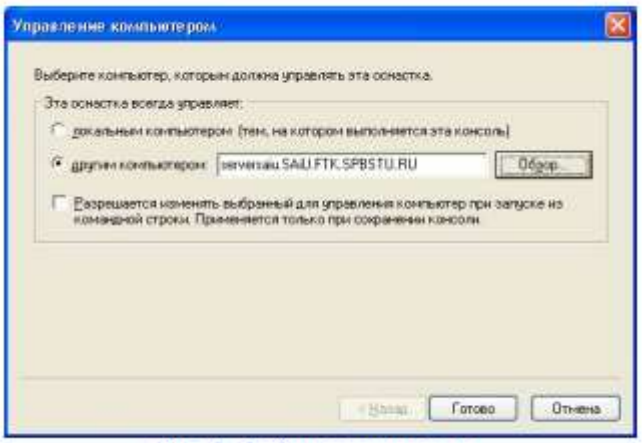


Рис.5. Выбор компьютера.

В остальном для пользователя все будет происходить так же, как и при работе с локальным компьютером. В свойствах ресурса можно узнать о разрешениях, которые установлены на него как для разделяемого ресурса (рис. 6), а на вкладке «Безопасность» - разрешениях файловой системы NTFS (если папка расположена на разделе с этой файловой системой, а не с FAT).

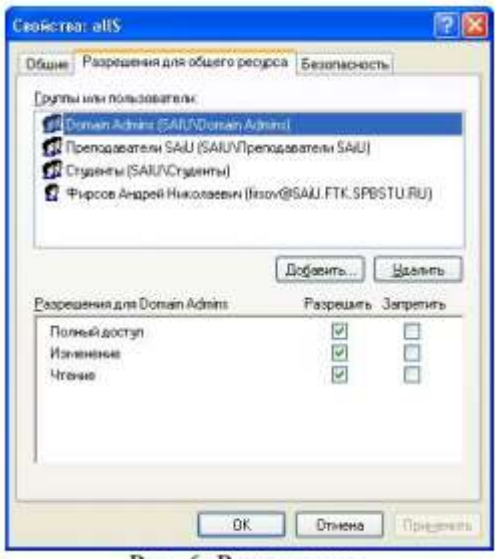


Рис. 6. Разрешения.

Ход работы:

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 до-

менных группах можно получить через оснастку Active Directory Users and Computers, о локальных группах – через «Управление компьютером».

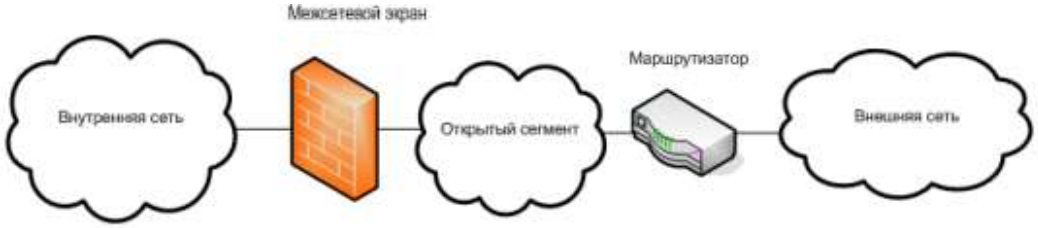
Практическая работа № 18-20 Использование межсетевых экранов для защиты информационных процессов

Цель работы:

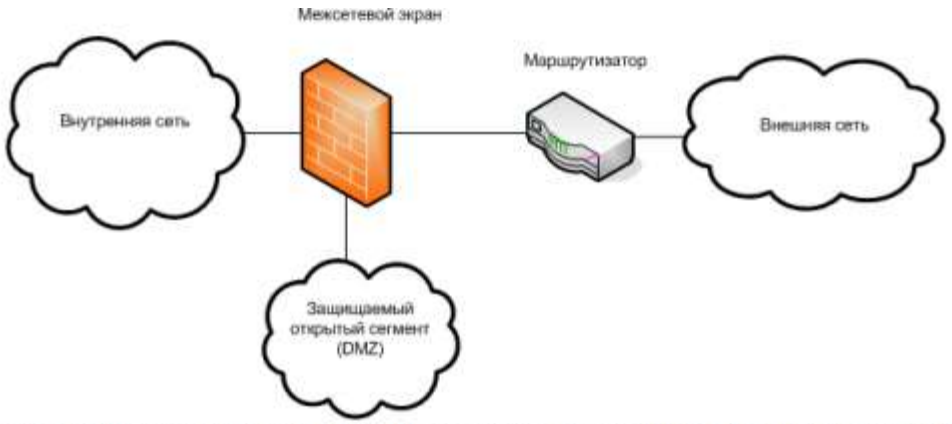
Изучить методы использования межсетевых экранов для защиты информационных процессов Общие сведения Межсетевой экран (МЭ) – это средство защиты информации, осуществляющее анализ и фильтрацию проходящих через него сетевых пакетов. В зависимости от установленных правил, МЭ пропускает или уничтожает пакеты, разрешая или запрещая таким образом сетевые соединения. МЭ является классическим средством защиты периметра компьютерной се ти: он устанавливается на границе между внутренней (защищаемой) и внешней (потенциально опасной) сетями и контролирует соединения между узлами этих сетей. Но бывают и другие схемы подключения, которые будут рассмотрены ниже. Английский термин, используемый для обозначения МЭ – firewall. Поэтому в литературе межсетевые экраны иногда также называют файервол или брандмауэр (немецкий термин, аналог firewall). Как уже было отмечено, фильтрация производится на основании правил. Наиболее безопасным при формировании правил для МЭ считается подход «запрещено все, что явно не разрешено». В этом случае, сетевой пакет проверяется на соответствие разрешающим правилам, а если таковых не найдется – отбрасывается. Но в некоторых случаях применяется и обратный принцип: «разрешено все, что явно не запрещено». Тогда проверка производится на соответствие запрещающим правилам и, если таких не будет найдено, пакет будет пропущен. Фильтрацию можно производить на разных уровнях эталонной модели сетевого взаимодействия OSI. По этому признаку МЭ делятся на следующие классы [20,22]: - экранирующий маршрутизатор; - экранирующий транспорт (шлюз сеансового уровня); - экранирующий шлюз (шлюз прикладного уровня). Экранирующий маршрутизатор (или пакетный фильтр) функционирует на сетевом уровне модели OSI, но для выполнения проверок может использовать информацию и из заголовков протоколов транспортного уровня. Соответственно, фильтрация может производиться по ip-адресам отправителя и получателя и по TCP и UDP портам. Такие МЭ отличает высокая производительность и относительная простота – функциональностью пакетных фильтров обладают сейчас даже наиболее простые и недорогие аппаратные маршрутизаторы. В то же время, они не защищают от многих атак, например, связанных с подменой участников соединений. Шлюз сеансового уровня работает на сеансовом уровне модели OSI и также может контролировать информацию сетевого и транспортного уровней. Соответственно, в дополнение к перечисленным выше возможностям, подобный МЭ может контролировать процесс установки соединения и проводить проверку проходящих пакетов на принадлежность разрешенным соединениям. Шлюз прикладного уровня может анализировать пакеты на всех уровнях модели OSI от сетевого до прикладного, что обеспечивает наиболее высокий уровень защиты. В дополнение к ранее перечисленным, появляются такие возможности, как аутентификация пользователей, анализ команд протоколов прикладного уровня, проверка передаваемых данных (на наличие компьютерных вирусов, соответствие политике безопасности) и т.д. Рассмотрим теперь вопросы, связанные с установкой МЭ. На рис. 48 представлены типовые схемы подключения МЭ. В первом случае (рис.48 а), МЭ устанавливается после маршрутизатора и защищает всю внутреннюю сеть. Такая схема применяется, если требования в области защиты от несанкционированного межсетевого доступа примерно одинаковы для всех узлов внутренней сети. Например, «разре-

шать соединения, устанавливаемые из внутренней сети во внешнюю, и пресекать попытки подключения из внешней сети во внутреннюю». В том случае, если требования для разных узлов различны (например, нужно разместить почтовый сервер, к которому могут подключаться «извне»), подобная схема установки межсетевого экрана не является достаточно безопасной. Если в нашем примере нарушитель, в результате реализации сетевой атаки, получит контроль над указанным почтовым сервером, через него он может получить доступ и к другим узлам внутренней сети. В подобных случаях иногда перед МЭ создается открытый сегмент сети предприятия (рис. 48 b), а МЭ защищает остальную внутреннюю сеть. Недостаток данной схемы заключается в том, что подключения к узлам открытого сегмента МЭ не контролирует. Более предпочтительным в данном случае является использование МЭ с тремя сетевыми интерфейсами (рис.48 c). В этом случае, МЭ конфигурируется таким образом, чтобы пра вила доступа во внутреннюю сеть были более строгими, чем в открытый сегмент. В то же время, и те, и другие соединения могут контролироваться МЭ. Открытый сегмент в этом случае иногда называется «демилитаризованной зоной» – DMZ. Еще более надежной считается схема, в которой для защиты сети с DMZ задействуются два независимо конфигурируемых МЭ (рис.48 d). В этом случае, МЭ 2 реализует более жесткий набор правил фильтрации по сравнению с МЭ1. И даже успешная атака на первый МЭ не сделает внутреннюю сеть беззащитной. В последнее время стал широко использоваться вариант установки программного МЭ непосредственно на защищаемый компьютер. Иногда такой МЭ называют «персональным». Подобная схема позволяет защититься от угроз исходящих не только из внешней сети, но из внутренней.

a) подключение межсетевого экрана с двумя сетевыми интерфейсами для «единообразной» защиты локальной сети



b) подключение межсетевого экрана с двумя сетевыми интерфейсами при выделении открытого сегмента внутренней сети



c) подключение межсетевого экрана с тремя сетевыми интерфейсами для защиты внутренней сети и ее открытого сегмента

d) подключение двух межсетевых экранов для защиты внутренней сети и ее открытого сегмента

Рис. 2.1. Типовые схемы подключения межсетевых экранов.

Встроенный межсетевой экран (firewall) Windows Server 2008. Персональный межсетевой экран появился в операционных системах семейства Windows, начиная с Windows XP / Windows Server 2003. В Windows Server 2008 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). Упомянутые исключения определяются на вкладке Exceptions. Там есть ряд предопределенных правил, а также пользователь может добавлять свои. Если нужно, чтобы какоето 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 c)) позволяет включить или отключить межсетевой экран для отдельных сетевых интерфейсов.

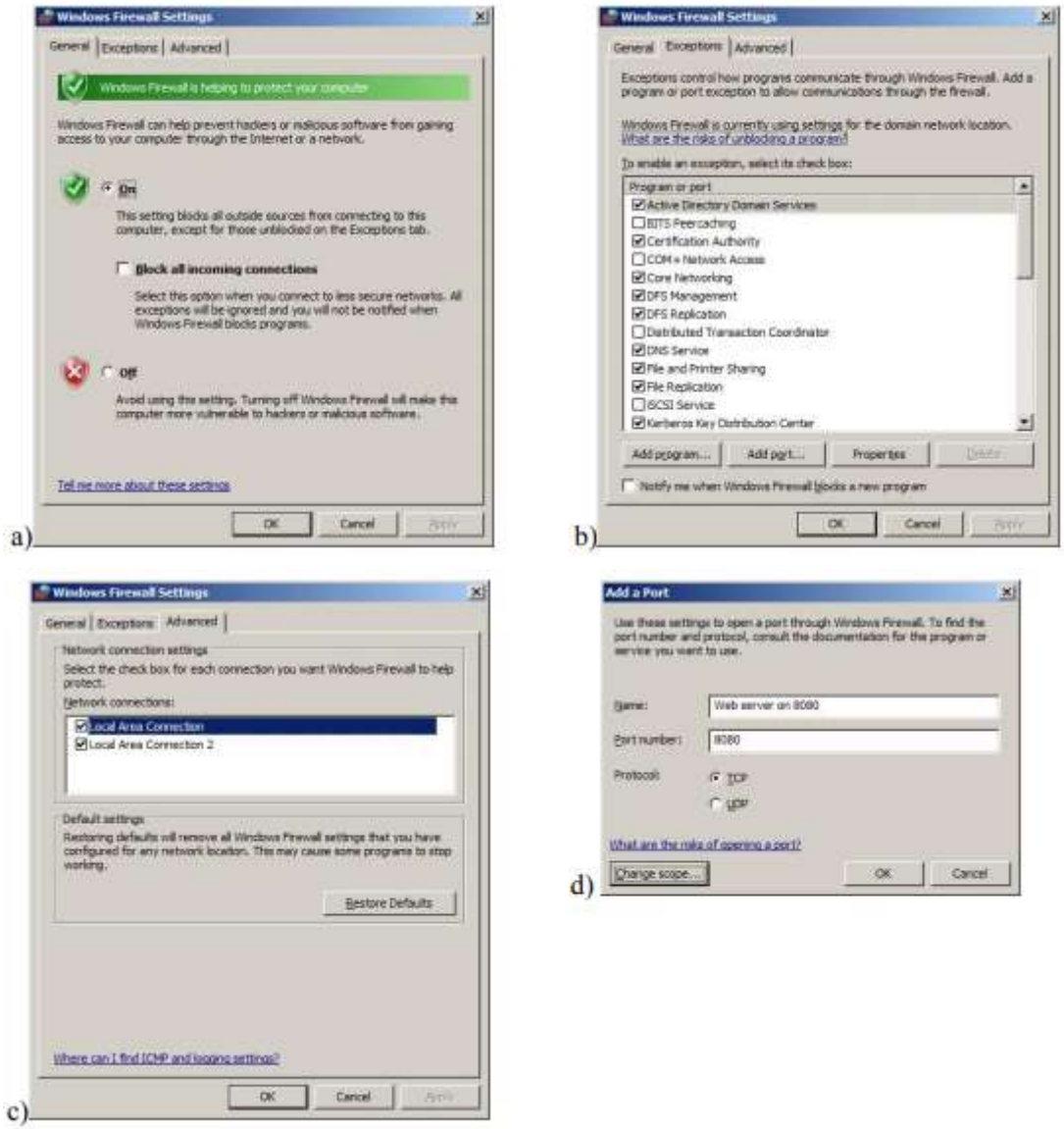


Рис.1. Окно управления параметрами межсетевого экрана

Ход работы: 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).

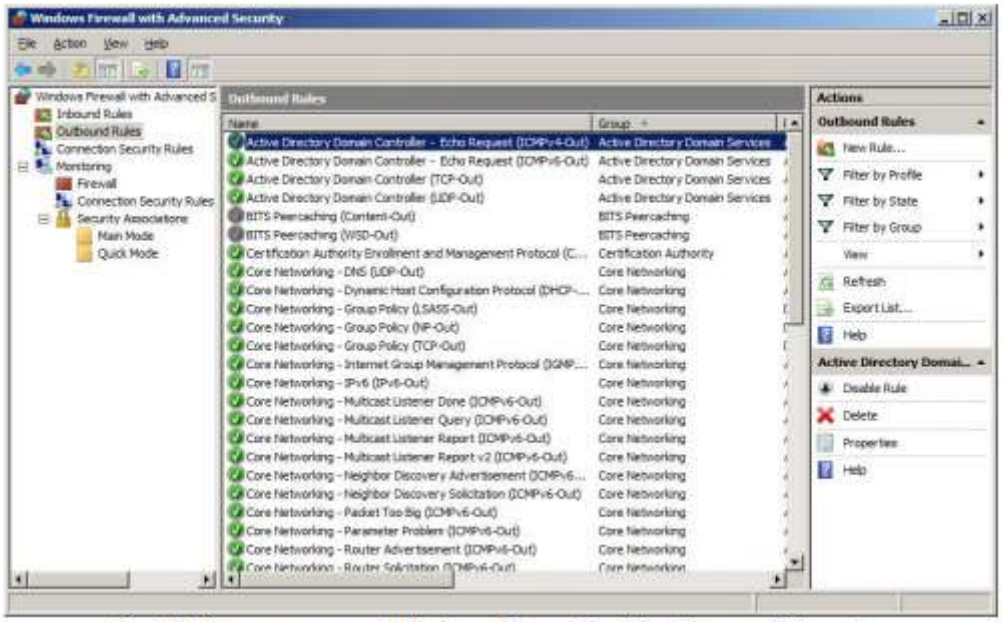


Рис.2. Окно оснастки Windows Firewall with Advanced Security.

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 рис.2.2 представлено главное окно оснастки. Выберем пункт Firewall Properties и активируем ведение журнала отброшенных пакетов (рис.2.3).

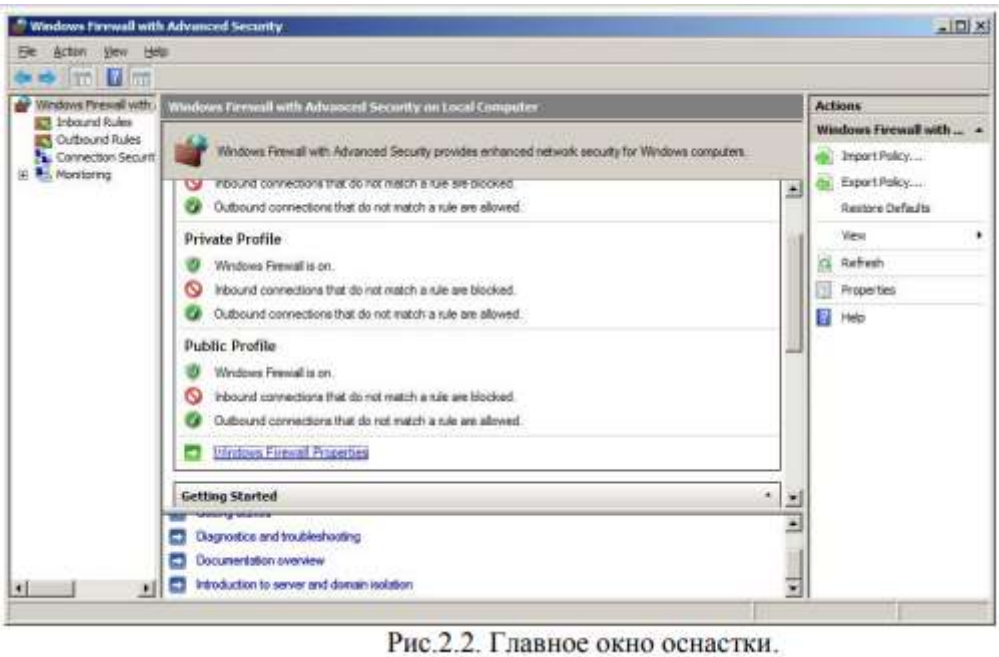


Рис.2.2. Главное окно оснастки.

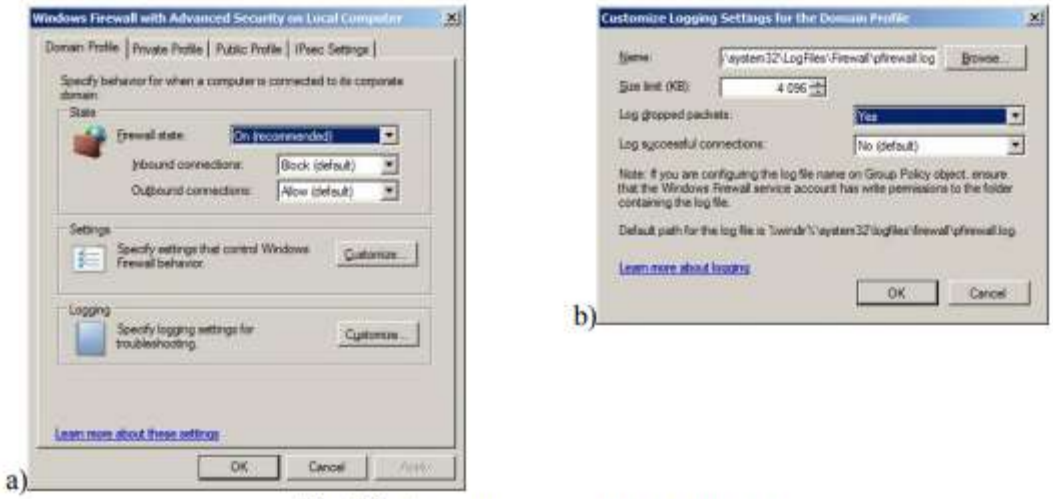


Рис.2.3. Активируем ведение журнала.

Для этого в группе Logging в окне рис.2.3 a) надо нажать кнопку Customize и выполнить настройку, представленную на рис. 2.3 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 2.3 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 - - - - 8 0 - SEND 2009-01-31 22:43:03 DROP ICMP 192.168.131.65 195.242.2.2 - - 0 - - - - 8 0 – SEND

2009-01-31 22:43:04 DROP ICMP 192.168.131.65 195.242.2.2 - - 0 - - - - 8 0 - SEND 2009-01-31 22:43:05 DROP ICMP 192.168.131.65 195.242.2.2 - - 0 - - - - 8 0 - SEND

Практическая работа № 21-22 Требования к защите автоматизированных систем от НСД

Цель работы: Изучить программные методы защиты автоматизированных систем от НСД. 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.2.4). 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.2.5).

Рис.2.4. Просмотр разрешений.

Рис.2.5 Изменение разрешений.

Ход работы: 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.2.6) о том, что эти разрешения наследуются от родительского объекта. Для того, чтобы отменить наследование надо на вкладке Security (рис.2.3) нажать кнопку Advanced. В появившемся окне (рис.2.7) 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.

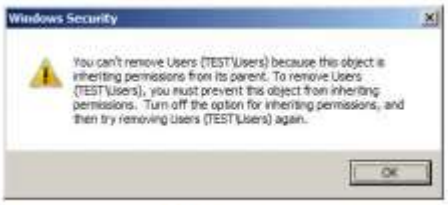


Рис.2.6. Предупреждение.

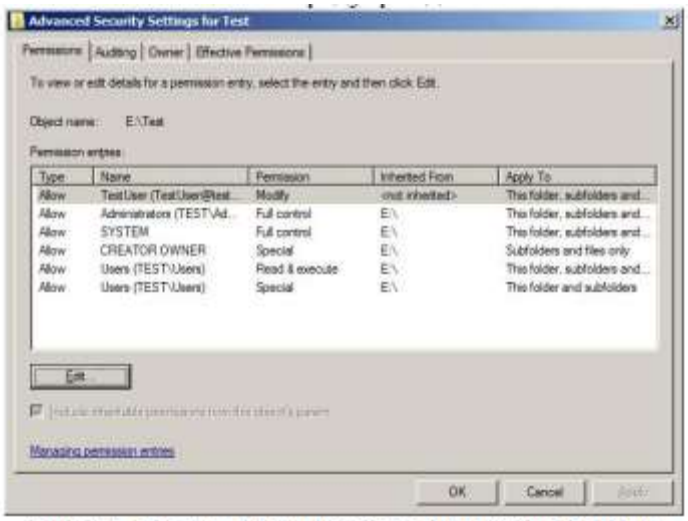


Рис.2.7. Дополнительные параметры безопасности.

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.2.8).

Рис.2.8. 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.2.9 (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.2.9. 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.2.7). Там, нажав кнопку Select, можно выбрать пользователя или группу, для которой будет показано эффективное разрешение.

Задание. Проверьте, чтобы у пользователя TestUser на папку, с которой работаем, было разрешение modify. Проверьте действующее эффективное разрешение. Не заканчивая сеанса пользователя, переключитесь в сеанс пользователя Administrator. Добавьте в список разрешений на папку запрещение для группы TestGroup всех видов доступа (выберите Deny для разрешения Full Control). Внесите пользователя TestUser в группу TestGroup. Посмотрите эффективное разрешение для пользователя TestUser. Переключитесь в сеанс пользователя TestUser. Попробуйте открыть папку и создать документ. Завершите сеанс TestUser (выполните выход из системы) и снова войдите в систему. Повторно попробуйте открыть папку и создать документ. Как можно объяснить полученный результат (подсказка есть в начале описания лабораторной)? Теперь рассмотрим вопросы, связанные с владением папкой или файлом. Пользователь, создавший папку или файл, становится ее владельцем. Текущего владельца объекта можно узнать, если в окне дополнительных параметров безопасности (рис.4) выбрать вкладку Owner. Владелец файла может изменять разрешения на доступ к этому файлу, даже в том случае, если ему самому доступ запрещен. Порядок смены владельца файла в Windows Server 2008 отличается от того, что было в предыдущих версиях ОС. Ранее, администратор или пользователь, имеющий на файл (папку) право Take Ownership могли стать владельцами файла. Причем, владельцем мог быть или конкретный пользователь, или группа Администраторы (Adminisrators) – другую группу владельцем было не назначить. В Windows Server 2008 администратор (или член группы администраторов) может не только сам стать владельцем, но и передать право владения произвольному пользователю или группе. Но эта операция рассматривается как привилегированная, и доступна не всякому пользователю, имеющему право на файл. На рис. 2.10 показано, что Администратор сделал владельцем папки Test группу TestGroup.

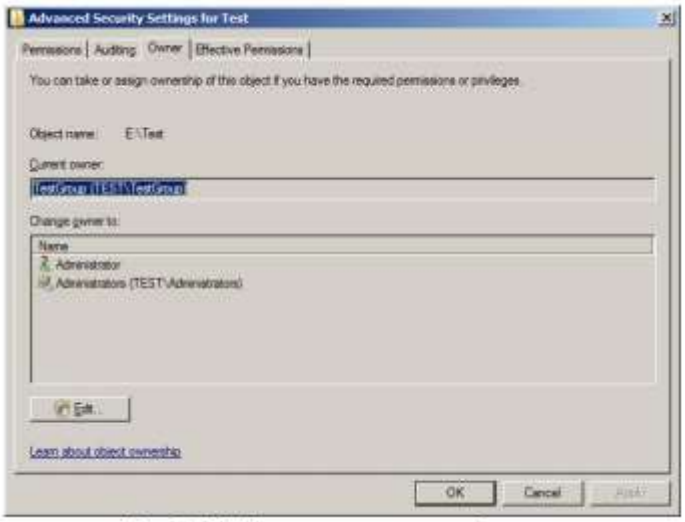


Рис.2.10. Смена владельца объекта.

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.2.11. 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.2.11). 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).

СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ

1. Нестеров С. А. Информационная безопасность: учебник и практикум для среднего профессионального образования — Москва : Издательство Юрайт, 2019. — 321 с. — (Профессиональное образование). — ISBN 978-5-534-07979-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/

2. Партыка Т. Л., Попов, И.И. Информационная безопасность: учебное пособие – 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2019. - 432 с.: 60x90 1/16. - (Профессиональное образование) - Текст : электронный. - URL: https://new.znanium.com/

3. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2019. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). - Текст: электронный. - URL: https://new.znanium.com/