Автономная некоммерческая организация высшего образования
«Волгоградский институт бизнеса»

Рабочая программа учебной дисциплины

Сетевое администрирование

(Наименование дисциплины)

09.03.03 Прикладная информатика, направленность (профиль) «Менеджмент в области информационных технологий»

(Направление подготовки / Профиль)

Бакалавр

(Квалификация)

Кафедра разработчик Экономики и управления

Год набора **2023**

Вид учебной деятельности	Трудоемкость (объем) дисциплины					
	Очная форма	Очно-заочная форма		Заочная форма		
	д	в	св	з	сз	вв
Зачетные единицы	**6**			**6**	**6**	**6**
Общее количество часов	216			216	216	216
Аудиторные часы контактной работы обучающегося с преподавателями:	64			20	20	20
– Лекционные (Л)						
– Практические (ПЗ)	64			20	20	20
– *В том числе в форме практической подготовки*	*64*			*20*	*20*	*20*
– Лабораторные (ЛЗ)						
– Семинарские (СЗ)						
Самостоятельная работа обучающихся (СРО)	98			187	187	187
К (Р-Г) Р (П) (+;-)						
Тестирование (+;-)						
ДКР (+;-)						
Зачет (+;-)						
Зачет с оценкой (+;- (Кол-во часов))						
Экзамен (+;- (Кол-во часов))	+(54)			+(9)	+(9)	+(9)

Волгоград 2023

Содержание

Раздел 1. Организационно-методический раздел 3
Раздел 2. Тематический план 6
Раздел 3. Содержание дисциплины 8
Раздел 4. Организация самостоятельной работы обучающихся 12
Раздел 5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся 13
Раздел 6. Перечень учебной литературы, необходимой для освоения дисциплины 55
Раздел 7. Материально-техническая база и информационные технологии 55
Раздел 8. Методические указания для обучающихся по освоению дисциплины 57

Раздел 1. Организационно-методический раздел

1.1. Цели освоения дисциплины

Дисциплина **«Сетевое администрирование»** входит в **Часть, формируемую участниками образовательных отношений** дисциплин подготовки обучающихся по направлению подготовки **«09.03.03 Прикладная информатика», направленность (профиль) «Менеджмент в области информационных технологий».**

Целью дисциплины является формирование **компетенций** (*в соответствии с ФГОС ВО и требованиями к результатам освоения основной профессиональной образовательной программы высшего образования (ОПОП ВО)*):

Общепрофессиональных:

ОПК-9.1 Способен осуществлять непосредственное руководство этапами разработки и проверки работоспособности программного обеспечения

Профессиональных

ПК-5.1 Способен заказывать выполнение проектов по созданию, развитию, выводу на рынок и продажам программных продуктов

ПК-5.2 Способен контролировать выполнение проектов по созданию, развитию, выводу на рынок и продажам программных продуктов

ПК-7.1 Способен разрабатывать коммерческие предложения по приобретению и продаже технологических, продуктовых и прочих интеллектуальных активов

Перечисленные компетенции формируются в процессе достижения **индикаторов компетенций:**

Обобщенная трудовая функция/ трудовая функция	**Код и наименование дескриптора компетенций**	**Код и наименование индикатора достижения компетенций (из ПС)**
ПС 06.012 Менеджер продуктов в области информационных технологий **С Управление серией ИТ-продуктов и группой их менеджеров** **С/05.6** Командообразование и развитие персонала **С/07.6** Заказ разработки программы проектов по созданию, развитию, выводу на рынок и продажам ИТ-продуктов и контроль ее выполнения **С/09.6** Разработка предложений по приобретению и продаже технологических, продуктовых и прочих интеллектуальных активов и организаций	ОПК-9.1 Способен осуществлять непосредственное руководство этапами разработки и проверки работоспособности программного обеспечения	*Знает:* ИД-1 ОПК- 9.1 Основы менеджмента проектов С/05.6 *Умеет:* ИД-3 ОПК- 9.1 Планировать и управлять программами проектов С/07.6 *Имеет навыки и (или) опыт:* ИД-5 ОПК- 9.1 Консультирование руководства организации и служб, ответственных за оборот активов, по вопросу ценности интеллектуальных активов С/09.6

ПС 06.012 Менеджер продуктов в области информационных технологий **С Управление серией ИТ-продуктов и группой их менеджеров** **С/06.6** Продвижение ИТ-продуктов **С/07.6** Заказ разработки программы проектов по созданию, развитию, выводу на рынок и продажам ИТ-продуктов и контроль ее выполнения	ПК-5.1 Способен заказывать выполнение проектов по созданию, развитию, выводу на рынок и продажам программных продуктов	*Знает:* ИД-1 ПК- 5.1 Средства и методы разработки и проведения презентации ИТ-продуктов С/06.6 *Умеет:* ИД-3 ПК- 5.1 Организовывать рекламные кампании С/06.6 *Имеет навыки и (или) опыт:* ИД-5 ПК- 5.1 Формирование заказа программы проектов по созданию, развитию, выводу на рынок и продаже ИТ-продуктов С/07.6
ПС 06.012 Менеджер продуктов в области информационных технологий **С Управление серией ИТ-продуктов и группой их менеджеров** **С/05.6** Командообразование и развитие персонала **С/06.6** Продвижение ИТ-продуктов **С/07.6** Заказ разработки программы проектов по созданию, развитию, выводу на рынок и продажам ИТ-продуктов и контроль ее выполнения	ПК-5.2 Способен контролировать выполнение проектов по созданию, развитию, выводу на рынок и продажам программных продуктов	*Знает:* ИД-2 ПК- 5. 2 Основы менеджмента проектов С/05.6 *Умеет:* ИД-4 ПК- 5. 2 Аргументированно демонстрировать преимущества ИТ-продуктов С/06.6 *Имеет навыки и (или) опыт:* ИД-6 ПК- 5.2 Прием результатов отдельных этапов работ программы С/07.6
ПС 06.012 Менеджер продуктов в области информационных технологий **С Управление серией ИТ-продуктов и группой их менеджеров** **С/01.6** Заказ технологических исследований для серии ИТ-продуктов и анализ их результатов **С/09.6** Разработка предложений по приобретению и продаже технологических, продуктовых и прочих интеллектуальных активов и организаций	ПК-7.1 Способен разрабатывать коммерческие предложения по приобретению и продаже технологических, продуктовых и прочих интеллектуальных активов	*Знает:* ИД-1 ПК- 7.1 Основы управления интеллектуальными активами организации С/09.6 *Умеет:* ИД-3 ПК- 7.1 Разрабатывать технические задания на исследования С/01.6 *Имеет навыки и (или) опыт:* ИД-5 ПК- 7.1 Формирование предложений по приобретению привлекательных сторонних активов с целью развития серии ИТ-продуктов С/09.6

1.2. Место дисциплины в структуре ОПОП ВО
направления подготовки 09.03.03 Прикладная информатика, направленность (профиль) «Менеджмент в области информационных технологий»

№	Предшествующие дисциплины (дисциплины, изучаемые параллельно)	Последующие дисциплины
1	*2*	*3*
1	Правовые основы прикладной информатики	Операционные системы
2	Информационные системы и технологии	Проектирование информационных систем
3	Информационные технологии в менеджменте	Информационная безопасность
4	Управление проектами	Управление информационными системами
5	Информатика	
6	Проектный практикум	
7	Введение в направление подготовки	

Последовательность формирования компетенций в указанных дисциплинах может быть изменена в зависимости от формы и срока обучения, а также преподавания с использованием дистанционных технологий обучения.

1.3. Нормативная документация

Рабочая программа факультативной дисциплины составлена на основе:
- федерального государственного общего профессионального образовательного стандарта высшего образования по направлению **09.03.03 Прикладная информатика**;
- учебного плана направления подготовки **09.03.03 Прикладная информатика, направленность (профиль) «Менеджмент в области информационных технологий»** 2023 года набора;
- образца рабочей программы учебной дисциплины (приказ № 113-0 от 01.09.2021 г.).

Раздел 2. Тематический план

Очная форма обучения (полный срок)

№	Тема дисциплины	Трудоемкость					
		Всего	Аудиторные занятия			СРО	Код индикатора и дескриптора достижения компетенций
			Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Введение в сетевое администрирование	24		4	4	20	ИД-1 ОПК- 9.1 ИД-1 ПК- 5.1 ИД-2 ПК- 5. 2 ИД-1 ПК- 7.1
2	Администрирование пользователей сети	38		18	18	20	ИД-3 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-6 ПК- 5. 2 ИД-3 ПК- 7.1
3	Администрирование рабочей станции	36		16	16	20	ИД-5 ОПК- 9.1 ИД-3 ПК- 5.1 ИД-4 ПК- 5. 2 ИД-5 ПК- 7.1
4	Администрирование компьютерной сети	38		18	18	20	ИД-5 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-2 ПК- 5. 2 ИД-3 ПК- 7.1
5	Обеспечение безопасности в сети	26		8	8	18	ИД-3 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-6 ПК- 5. 2 ИД-5 ПК- 7.1
Вид промежуточной аттестации (Экзамен)		**+(54)**					
Итого		**216**		**64**	**64**	**98**	

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО, ВО)

№	Тема дисциплины	Трудоемкость					
		Всего	Аудиторные занятия			СРО	Код индикатора и дескриптора достижения компетенций
			Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Введение в сетевое администрирование	42		4	4	38	ИД-1 ОПК- 9.1 ИД-1 ПК- 5.1 ИД-2 ПК- 5. 2 ИД-1 ПК- 7.1
2	Администрирование пользователей сети	42		4	4	38	ИД-3 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-6 ПК- 5. 2 ИД-3 ПК- 7.1
3	Администрирование рабочей станции	40		4	4	38	ИД-5 ОПК- 9.1 ИД-3 ПК- 5.1 ИД-4 ПК- 5. 2 ИД-5 ПК- 7.1

4	Администрирование компьютерной сети	42		4	4	38	ИД-5 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-2 ПК- 5. 2 ИД-3 ПК- 7.1
5	Обеспечение безопасности в сети	39		4	4	35	ИД-3 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-6 ПК- 5. 2 ИД-5 ПК- 7.1
Вид промежуточной аттестации (Экзамен)		**+(9)**					
Итого		**216**		**20**	**20**	**187**	

Раздел 3. Содержание дисциплины

3.1. Содержание дисциплины

Тема 1. Введение в сетевое администрирование

Основные понятия и определения администрирования. Понятие сетевого и системного администрирования. Цели и задачи сетевого администрирования. Современные подходы к администрированию компьютерных сетей. Примеры программного обеспечения для администрирования. Администрирование в консоли и в графическом интерфейсе.

Тема 2. Администрирование пользователей сети

Понятие пользовательской учетной записи. Встроенные пользовательские учетные записи. Группы безопасности. Регистрация пользователей в системе. Права доступа пользователей к папкам и файлам. Домены и рабочие группы. Понятие профиля пользователя. Защита учетных записей. Использование групповой политики. Администрирование файлов и папок. Использование возможностей NTFS при администрировании. Методики, применяемые при работе с учетными записями. Утилиты администрирования.

Тема 3. Администрирование рабочей станции

Права доступа. Базовые и расширенные права доступа. Наследование прав доступа. Права доступа при копировании (перемещении) файлов. Владельцы файлов и папок. Утилиты администрирования рабочей станции. Понятие системных служб. Запуск, работа и остановка системных служб.

Тема 4. Администрирование компьютерной сети

Совместное использование файлов в сети. Совместное использование устройств в сети. Разбиение сети на подсети. Примеры использование сегментирования сетей. Передача данных в IP-сети. Использование масок при структуризации сети. Назначение IP-адресов узлам сети. Виды маршрутизации. Динамическая и статическая маршрутизация. Протокол динамической конфигурации клиентских машин. Пример расчета подсети. Утилиты администрирование компьютерной сети в консоли. Настройка сервера в сети.

Тема 5. Обеспечение безопасности в сети

Обеспечение безопасности системы при использовании TCP/IP. Брандмауэр. Задачи и функции брандмауэра. Встроенные и внешние брандмауэры. Организация IP-брандмауэра.

3.2. Содержание практического блока дисциплины

Очная форма обучения (полный срок)

№	Тема практического (семинарского, лабораторного) занятия - *В том числе в форме практической подготовки*
1	*2*
Тема 1. Введение в сетевое администрирование	
ПЗ 1	Основные утилиты Windows
ПЗ 2	Основные утилиты Windows
Тема 2. Администрирование пользователей сети	
ПЗ 3	Администрирование учетных записей
ПЗ 4	Администрирование учетных записей
ПЗ 5	Администрирование учетных записей
ПЗ 6	Администрирование файлов и папок
ПЗ 7	Администрирование файлов и папок
ПЗ 8	Администрирование файлов и папок
ПЗ 9	Администрирование пользователей сети
ПЗ 10	Администрирование пользователей сети
ПЗ 11	Администрирование пользователей сети
Тема 3. Администрирование рабочей станции	
ПЗ 12	Управление правами доступа
ПЗ 13	Управление правами доступа
ПЗ 14	Управление правами доступа
ПЗ 15	Управление правами доступа
ПЗ 16	Обслуживание и контроль над системой
ПЗ 17	Обслуживание и контроль над системой
ПЗ 18	Обслуживание и контроль над системой
ПЗ 19	Обслуживание и контроль над системой
Тема 4. Администрирование компьютерной сети	
ПЗ 20	Администрирование локальной сети
ПЗ 21	Администрирование локальной сети
ПЗ 22	Администрирование локальной сети
ПЗ 23	Настройка сервиса DHCP
ПЗ 24	Настройка сервиса DHCP
ПЗ 25	Администрирование с применением консоли
ПЗ 26	Администрирование с применением консоли
ПЗ 27	Администрирование Web-сервера
ПЗ 28	Администрирование Web-сервера
Тема 5. Обеспечение безопасности в сети	
ПЗ 29	Обеспечение безопасности системы при использовании TCP/IP
ПЗ 30	Обеспечение безопасности системы при использовании TCP/IP
ПЗ 31	Настройка брандмауэра
ПЗ 32	Настройка брандмауэра

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО, на базе ВО)

№	Тема практического (семинарского, лабораторного) занятия - *В том числе в форме практической подготовки*
1	*2*
Тема 1. Введение в сетевое администрирование	
ПЗ 1	Основные утилиты Windows
ПЗ 2	Основные утилиты Windows

Тема 2. Администрирование пользователей сети	
ПЗ 3	Администрирование учетных записей
ПЗ 4	Администрирование файлов и папок
Тема 3. Администрирование рабочей станции	
ПЗ 5	Управление правами доступа
ПЗ 6	Обслуживание и контроль над системой
Тема 4. Администрирование компьютерной сети	
ПЗ 7	Администрирование локальной сети
ПЗ 8	Администрирование с применением консоли
Тема 5. Обеспечение безопасности в сети	
ПЗ 9	Обеспечение безопасности системы при использовании TCP/IP
ПЗ 10	Настройка брандмауэра

3.3. Образовательные технологии

Очная форма обучения (полный срок)

№	Тема занятия	Вид учебного занятия	Форма / Методы интерактивного обучения	% учебного времени
1	*2*	*3*	*4*	*5*
1	Введение в сетевое администрирование	ПЗ	Дискуссия	25
2	Администрирование пользователей сети	ПЗ	Дискуссия	25
3	Администрирование пользователей сети	ПЗ	Дискуссия	25
4	Администрирование пользователей сети	ПЗ	Дискуссия	25
5	Администрирование пользователей сети	ПЗ	Мозговой штурм	25
6	Администрирование пользователей сети	ПЗ	Мозговой штурм	25
7	Администрирование рабочей станции	ПЗ	Дискуссия	25
8	Администрирование рабочей станции	ПЗ	Дискуссия	25
9	Администрирование рабочей станции	ПЗ	Дискуссия	25
10	Администрирование рабочей станции	ПЗ	Деловая игра	50
11	Администрирование компьютерной сети	ПЗ	Дискуссия	25
12	Администрирование компьютерной сети	ПЗ	Деловая игра	50
13	Администрирование компьютерной сети	ПЗ	Дискуссия	25
14	Администрирование компьютерной сети	ПЗ	Дискуссия	25
Итого %				**25%**

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО, на базе ВО)

№	Тема занятия	Вид учебного занятия	Форма / Методы интерактивного обучения	% учебного времени
1	*2*	*3*	*4*	*5*
1	Введение в сетевое администрирование	ПЗ	Дискуссия	25
2	Администрирование пользователей сети	ПЗ	Дискуссия	25
3	Администрирование пользователей сети	ПЗ	Дискуссия	25
4	Администрирование рабочей станции	ПЗ	Дискуссия	25
5	Администрирование рабочей станции	ПЗ	Дискуссия	25
6	Администрирование компьютерной сети	ПЗ	Дискуссия	25
7	Администрирование компьютерной сети	ПЗ	Деловая игра	50
Итого %				**25%**

Раздел 4. Организация самостоятельной работы обучающихся

4.1. Организация самостоятельной работы обучающихся

№	Тема дисциплины	№ вопросов	№ рекомендуемой литературы
1	*2*	*3*	*4*
1	Введение в сетевое администрирование	1-3	1, 2, 5
2	Администрирование пользователей сети	4-8	2-6
3	Администрирование рабочей станции	9, 10	2, 5, 6
4	Администрирование компьютерной сети	11-22	2, 5
5	Обеспечение безопасности в сети	23- 25	4, 5, 6

Перечень вопросов, выносимых на самостоятельную работу обучающихся

1. Понятие сетевого и системного администрирования.
2. Цели и задачи сетевого администрирования.
3. Современные подходы к администрированию компьютерных сетей.
4. Встроенные пользовательские учетные записи.
5. Группы безопасности.
6. Регистрация пользователей в системе.
7. Права доступа пользователей к папкам и файлам.
8. Домены и рабочие группы.
9. Понятие профиля пользователя.
10. Организация сети TCP/IP. Преимущества и недостатки.
11. Межсетевой обмен в сетях TCP/IP. Инкапсуляция протоколов.
12. Протоколы SLIP, PPP и ARP.
13. Протоколы ICMP, UDP.
14. Протокол TCP (Transfer Control Protocol – базовый транспортный протокол). Установка соединения TCP.
15. Логическая организация компьютерных сетей.
16. Разбиение сети на подсети. Маска подсети.
17. Использование масок при структуризации сети
18. Назначение IP-адресов узлам сети.
19. Принципы передачи данных в IP-сетях. Порты и сокеты.
20. Концепция квитирования.
21. Виды маршрутизации. Простая маршрутизация. Адаптивная маршрутизация.
22. Администрирование серверов. Система Доменных имен
23. Основные подходы к планированию корпоративной сети.
24. Построения транспортной системы корпоративной сети.
25. Создание корпоративной сети на основе Active Directory.

4.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся

Самостоятельная работа обучающихся обеспечивается следующими учебно-методическими материалами:

1. Указаниями в рабочей программе по дисциплине (п.4.1.)
2. Лекционные материалы в составе учебно-методического комплекса по дисциплине
3. Заданиями и методическими рекомендациями по организации самостоятельной работы обучающихся в составе учебно-методического комплекса по дисциплине.
4. Глоссарием по дисциплине в составе учебно-методического комплекса по дисциплине.

Раздел 5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся

Фонд оценочных средств по дисциплине представляет собой совокупность контролирующих материалов, предназначенных для измерения уровня достижения обучающимися установленных результатов образовательной программы. ФОС по дисциплине используется при проведении оперативного контроля и промежуточной аттестации обучающихся. Требования к структуре и содержанию ФОС дисциплины регламентируются Положением о фонде оценочных материалов по программам высшего образования – программам бакалавриата, магистратуры.

5.1. Паспорт фонда оценочных средств

Очная форма обучения (полный срок)

№	Контролируемые разделы (темы) дисциплины	Оценочные средства				
		Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.	СРО	Код индикатора и дескриптора достижения компетенций
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Введение в сетевое администрирование		УО, Д	УО, Д	ПРВ	ИД-1 ОПК- 9.1 ИД-1 ПК- 5.1 ИД-2 ПК- 5. 2 ИД-1 ПК- 7.1
2	Администрирование пользователей сети		УО, Д, МШ	УО, Д, МШ	ПРВ	ИД-3 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-6 ПК- 5. 2 ИД-3 ПК- 7.1
3	Администрирование рабочей станции		УО, Д	УО, Д	ПРВ	ИД-5 ОПК- 9.1 ИД-3 ПК- 5.1 ИД-4 ПК- 5. 2 ИД-5 ПК- 7.1
4	Администрирование компьютерной сети		Д, ДИ	Д, ДИ	ПРВ	ИД-5 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-2 ПК- 5. 2 ИД-3 ПК- 7.1
5	Обеспечение безопасности в сети		УО	УО	ПРВ	ИД-3 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-6 ПК- 5. 2 ИД-5 ПК- 7.1

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО, на базе ВО)

№	Контролируемые разделы (темы) дисциплины	Оценочные средства				
		Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.	СРО	Код индикатора и дескриптора достижения компетенций
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Введение в сетевое администрирование		УО, Д		ПРВ	ИД-1 ОПК- 9.1 ИД-1 ПК- 5.1 ИД-2 ПК- 5. 2 ИД-1 ПК- 7.1
2	Администрирование пользователей		УО, Д,		ПРВ	ИД-3 ОПК- 9.1

	сети		МШ			ИД-5 ПК- 5.1 ИД-6 ПК- 5. 2 ИД-3 ПК- 7.1
3	Администрирование рабочей станции		УО, Д		ПРВ	ИД-5 ОПК- 9.1 ИД-3 ПК- 5.1 ИД-4 ПК- 5. 2 ИД-5 ПК- 7.1
4	Администрирование компьютерной сети		Д, ДИ		ПРВ	ИД-5 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-2 ПК- 5. 2 ИД-3 ПК- 7.1
5	Обеспечение безопасности в сети		УО		ПРВ	ИД-3 ОПК- 9.1 ИД-5 ПК- 5.1 ИД-6 ПК- 5. 2 ИД-5 ПК- 7.1

Условные обозначения оценочных средств (Столбцы 3, 4, 5):

УО – Устный (фронтальный, индивидуальный, комбинированный) опрос

ПРВ – Проверка рефератов, отчетов, рецензий, аннотаций, конспектов, графического материала, эссе, переводов, решений заданий, выполненных заданий в электронном виде и т.д.

ДИ – Деловая игра

МШ – Метод мозгового штурма

Д – Дискуссия, полемика, диспут, дебаты

5.2. Оценочные средства текущего контроля
Перечень практических (семинарских) заданий

Тема № 1: «Введение в сетевое администрирование»

Практическое занятие.
Основные утилиты Windows XP

Цель работы:

- изучить основные положения системы Windows;
- изучить основные утилиты системы Windows;
- изучить настройку с помощью утилит системы Windows.

Результат обучения. После обучения студент должен:

- знать основные положения системы Windows;
- знать основные утилиты системы Windows;
- уметь использовать внутренние утилиты системы Windows.

1. Работа с консолью (командной строкой)

Для работы в системе Windows (для примера указана Windows XP, но задания можно выполнять для любой версии Windows) можно использовать как графический интерфейс, так и интерфейс командной строки. Причем все системные операции, выполненные в графическом интерфейсе или в интерфейсе командной строки, равноправны между собой. Для работы с командной строкой необходимо запустить, так называемую, **консоль**.

Консоль запускает следующим образом:

- Нажмите кнопку **Пуск**.
- Выберите команду **Выполнить**.
- Вводите команду **cmd** и жмите **Enter**.

Внешний вид командной строки можно изменять. Для этого:

1. Щелкните правой кнопкой мыши по строке заголовка окна и выберите пункт **Свойства** (Properties).
2. Откроется окно с четырьмя вкладками, на которых будут доступны опции изменения настроек программы.
3. Откройте закладку **Цвет** (Color) и выберите любой цвет экрана и текста из 16 стандартных цветов, для которых имеется соответствующие образцы.
4. Откройте вкладку **Расположение** (Layout). Здесь настраивается размер окна и экранного буфера. Если в ранних ОС MS-DOS и Windows размер экрана оставался неизменным — 25 строк в высоту и 80 символов в длину, то в системах NT и более поздних можно просто задать достаточно большой размер буфера экрана и пользоваться полосой прокрутки, что гораздо удобнее.

Самостоятельно увеличьте размер окна консоли.

2. Утилиты командной строки

2.1. Утилита Systeminfo

Утилита Systeminfo предоставляет детальную информацию о конфигурации компьютера и его операционной системе.

1. Введите в командной строке команду

systeminfo

2. Внимательно ознакомьтесь с выведенной на экран информацией.
3. Введите в командной строке команду

systeminfo /?

4. Внимательно ознакомьтесь со справочной информацией утилиты systeminfo.
5. Введите в командной строке команду

systeminfo>info.doc

При этом вся справочная информация будет записана в текстовый файл **info.doc**

6. Запустите программу Microsoft Word и откройте в ней файл **info.doc**.
7. **Выпишите в отчет** (или сделайте экранную копию) следующую системную информацию:

- имя компьютера (узла),
- название и версия операционной системы,
- процессор и его тактовая частота,
- тип материнской платы,
- версия BIOS,
- объем оперативной (физической) памяти;
- объем доступной физической памяти;
- объем виртуальной памяти,
- объем доступной виртуальной памяти;
- время работы операционной системы без перезагрузки.

2.2. Утилита Shutdown

Утилита Shutdown выключает или перезагружает локальный или удаленный компьютер. Ее параметры позволяют задать время, через которое произойдет действие, пользователь получит сообщение, а также объяснение причины завершения работы.

1. Внимательно ознакомьтесь со справочной информацией утилиты **Shutdown.**
2. Запустите утилиту **Shutdown**.
3. Установите время отключения компьютера **30 секунд**.
4. **Выпишите в отчет** используемую команду.
5. Проверьте выполнение данной команды.

2.3. Утилита Tasklist

Утилита Tasklist позволяет выводить на экран список всех задач.

1. Внимательно ознакомьтесь со справочной информацией утилиты **Tasklist**.
2. Введите в командной строке команду

tasklist

3. Внимательно ознакомьтесь с выведенной на экран информацией.
4. **Выпишите в отчет** все основные задачи, запущенные на компьютере.

5. Выведите на экран список всех задач, которые используют модули **DLL**.
6. **Выпишите в отчет** используемую при этом команду.

2.4. Утилита Taskkill

Утилита Taskkill завершает выполняющиеся процессы.

1. Внимательно ознакомьтесь со справочной информацией утилиты Taskkill.
2. Самостоятельно завершите работу любой задачи командой

   tskill <имя процесса>

   или **tskill <id процесса>**
3. Введите команду

   taskkill /f /fi "username eq Guest"

4. При этом будут завершены все задания, запущенные пользователем Guest. Если вы вошли в систему под другим именем, то используйте это имя.

2.5 Утилита Bootcfg

Утилита Bootcfg обеспечивает конфигурирование файла настроек boot.ini.

1. Самостоятельно изучите действие этой утилиты.
2. Установите интервал времени в секундах, после истечения которого, загружается ОС по умолчанию, равным **60 сек**.
3. Запишите в **отчет** команду, которой вы изменили значение таймаута.
4. Проверьте изменение данного параметра путем перезагрузки системы.
5. Верните исходное значение таймаута.

2.7. Утилита Openfiles

Утилита **Openfiles** показывает все открытые файлы на компьютере и процессы, которые с ними работают.

1. Внимательно ознакомьтесь со справочной информацией данной утилиты.
2. Включите опцию построения списка объектов.
3. Запишите **в отчет**, какую команду вы при этом использовали.
4. Для того чтобы просмотреть все открытые в системе файлы введите команду

   openfiles /query

5. В результате вы определите все файлы, открытые как локально, так и удаленно, а также узнаете имена процессов, использующих их. **Выпишите эту информацию в отчет**.

3. Создание виртуальных дубликатов файлов

Для создания дубликатов файлов в системе Windows XP используется команда **Fsutil hardlink**. Она принимает всего один параметр — **create**. Эта команда позволяет создавать жесткие ссылки на файлы. Жесткие ссылки позволяют одному файлу иметь несколько разных имен (т.е. виртуальных копий). Один и тот же файл может появляться в разных директориях или даже в одной директории с различными именами. И данные этого файла не могут быть удалены, пока счетчик всех дубликатов файлов не будет равен нулю.

Так как все ссылки указывают на один и тот же файл, программы могут открывать любую из них и изменять исходный файл. Приведем пример использования этой команды. Допустим, имеется файл d:\1.avi, занимающий 600 Мб. Воспользовавшись командой

fsutil hardlink create d:\2.avi d:\1.avi

вы создаете жесткую ссылку на этот файл. В результате вы получите два файла, но объем занимаемого дискового пространства не изменится. Хотя если Вы выделите эти два файла, Вам будет показано, что они занимают 1200 мегабайт. Таким образом, Вы можете создать неограниченное число копий какого-либо файла, но на занятом пространстве диска это никак не отразится. Причем если удалить один из таких клонов, все остальные останутся без изменений.

Для того чтобы уничтожить исходный файл необходимо удалить все жесткие ссылки на него. Но у этой команды есть **ограничения**: все файлы должны быть в пределах одного тома, и файловая система — только NTFS (NT File System).

4. Практическое задание

Самостоятельно проделайте следующие действия:

1. Запустите консоль системы Windows XP.

2. Выведите на экран детальную информацию о конфигурации компьютера.
3. Выведите в файл детальную информацию о конфигурации компьютера.
4. Выведите на экран список всех основных задач, запущенных на компьютере.
5. Запустите программу Блокнот.
6. Используя консоль, завершите работу этой программы.
7. Установите интервал времени в секундах, после истечения которого, загружается ОС по умолчанию, равным 40 сек.
8. Просмотрите все открытые в системе файлы с удаленных компьютеров.
9. Создайте три виртуальные копии для любого текстового файла.
10. Покажите результат работы преподавателю.
11. Удалите все копии виртуального файла.

5. Создание отчета

После выполнение практического задания студент должен составить отчет в формате DOCX, в котором должны быть отражены следующие положения:

– номер и название практической работы;
– цель и план занятия;
– экранные копии выполнения практического задания.

Ответьте в отчете письменно на следующие вопросы:

1. Какие интерфейсы используются в системе Windows XP? Укажите их достоинства и недостатки.
2. Для чего нужна утилита **Openfiles**?
3. Для чего нужна утилита **Schtask**?
4. Для чего нужна утилита **Bootcfg**?
5. Для чего нужна утилита **Taskkill**?
6. Для чего нужна утилита **Tasklist**?
7. Для чего нужна утилита **Shutdown**?
8. Для чего нужна утилита **Systeminfo**?

Тема № 2: «Администрирование пользователей сети»

Практическое занятие.
Задание № 1. Администрирование учетных записей

Цель работы:
– изучить основные возможности администрирования пользователей Windows XP;
– изучить основные работы учетных записей;
– получить навыки администрирования Windows XP.

Результат обучения. После обучения студент должен:
– знать основные возможности администрирования пользователей Windows XP;
– уметь работать с учетными записями;
– уметь выполнять администрирование Windows XP.

1. Основные положения

Понятие пользовательской учетной записи

Для каждого пользователя, получающего доступ к компьютеру, определяется защищенная паролем **учетная запись**. Благодаря этому можно блокировать доступ к компьютеру для незнакомых пользователей и ограничивать доступ к файлам, содержащим секретную информацию. Несмотря на то, что понятие учетной записи достаточно простое, его реализация в Windows имеет некоторые особенности.

Каждый пользователь, приступающий к работе на компьютере с установленной Windows 2000/XP, должен зарегистрироваться, т.е. подтвердить свою **идентичность**. Процесс подтверждения реализован путем проверки имени пользователя и пароля. После успешной

регистрации пользователя Windows обращается к защищенной информации из учетной записи, определяющей перечень доступных/запрещенных ресурсов. При этом используются разрешения, определяющие доступ к совместно используемым файлам, папкам и сетевым ресурсам.

Информация о пользовательских учетных записях хранится в защищенной базе данных Security Accounts Manager (**SAM**). С целью отслеживания каждой записи и связанных с нею прав и разрешений применяется значение переменной длины, называемое **идентификатором безопасности** (SID). В момент создания пользовательской учетной записи ей присваивается уникальный идентификатор SID. В Windows 2000/XP все значения SID начинаются с сокращения S-1. Затем следует ряд чисел, уникальным образом идентифицирующих каждую учетную запись. Доступ к этим идентификаторам осуществляется с помощью системного реестра.

Если пользователь работает в корпоративной сети, то могут использоваться доменные учетные записи. **Доменные учетные записи** хранятся на центральном компьютере, который называется доменным контроллером. При этом в процессе регистрации в поле Log On To (Регистрация) в окне Log On To Windows (Регистрация в Windows) указывается имя компьютера (при регистрации с применением локальной учетной записи) или название домена (в случае регистрации с использованием доменной учетной записи).

Каждая доменная пользовательская учетная запись имеет собственный уникальный идентификатор SID. Эта запись хранится в каталоге домена, который управляется доменным контроллером. Каждый участник домена может связываться с этой базой данных и использовать находящийся там список учетных записей. Поэтому пользователь индивидуального компьютера, указав название доменной группы безопасности, может передавать право доступа к ресурсам общего пользования.

Встроенные пользовательские учетные записи

После завершения установки Windows 2000/XP создаются несколько встроенных пользовательских учетных записей, которым назначены определенные привилегии и ограничения:

– **Администратор** (Administrator). Данная учетная запись предоставляет полный набор прав доступа для всего компьютера. Являясь постоянным членом группы Administrators, эта учетная запись позволяет реализовать неограниченный доступ ко всем файлам и ключам системного реестра. Учетная запись Administrator **может** создавать другие учетные записи пользователей.

– **Гость** (Guest). Учетная запись Guest предназначена для случайных пользователей или же тех, кто обращается к данной системе однократно. Заданные по умолчанию привилегии для этой учетной записи довольно ограниченны. Пользователи-гости могут только выполнять программы и сохранять документы, управлять ресурсами ЭВМ они не имеют права.

В Windows XP учетная запись Administrator (и другие) обычно не отображается на экране Welcome при регистрации. Если необходимо зарегистрироваться с помощью учетной записи Administrator (или любой другой учетной записи, которая не отображается на экране Welcome), нажмите два раза комбинацию клавиш Ctrl + Alt + Delete для отображения диалогового окна Log On To Windows, где можно указать любое пользовательское имя.

– **HelpAssistant**. Учетная запись HelpAssistant, используемая для сеансов Remote Assistance, по умолчанию отключена (и защищена строгим паролем). Она устанавливается на компьютере начинающего пользователя и предназначена для регистрации удаленного эксперта.

– **SUPPORT_xxxxxxxx. Windows XP** может содержать одну или несколько учетных записей, которые предназначены для реализации интерактивной поддержки и обслуживания поставщиками, например компанией Microsoft либо производителем вашего компьютера. Здесь xxxxxxxxx представляет номер, определяемый поставщиком.

Группы безопасности.

Для облегчения администрирования несколько учетных записей можно объединить в одну группу и назначать унифицированные права доступа всем ее членам, а не каждому пользователю в отдельности. Такая группа будет называться ***группой безопасности***.

Группы безопасности позволяют организовать пользовательские учетные записи в соответствии с требованиями к уровню безопасности. Можно создать группу безопасности дома, в офисе, можно сформировать группу, объединяющую всех бухгалтеров и т.д. При этом разрешения, определяющие уровень безопасности, можно присваивать всей группе или отдельным

пользователям. Пользовательская учетная запись может относиться к одной группе, к нескольким группам либо вообще не быть связанной ни с одной из групп.

Несмотря на то, что привилегии можно передавать каждой пользовательской учетной записи, этот путь достаточно утомителен и часто приводит к ошибкам. Передача привилегий отдельным пользовательским учетным записям свидетельствует о **недостаточной практической подготовке администратора**. Лучше присваивать разрешения и права доступа группам, а затем добавлять пользовательские учетные записи в группу, имеющую соответствующие привилегии.

Типы учетных записей.

Для Windows XP характерен термин **тип учетной записи**. Обычно этот термин имеет значение при обращении к инструменту User Accounts (Пользовательские учетные записи) в панели управления. Тип учетной записи обеспечивает простейший метод, позволяющий описать членство в группе безопасности. И хотя допускается произвольное количество групп безопасности, Windows XP относит каждую пользовательскую учетную запись к одному из четырех указанных типов:

– Computer administrator (администраторы компьютера). Члены указанной группы Administrators (Администраторы) классифицируются в качестве учетных записей администраторов компьютера.

– Limited (ограничения). Члены группы Users (Пользователи) классифицируются с помощью учетных записей с ограничениями.

– Guest (Гости). Члены группы Guests (Гости) ассоциируются с гостевыми учетными записями.

– Unknown (неизвестные). Учетная пользовательская запись, не включенная в группы Administrators, Users или Guests, относится к категории неизвестных учетных записей. Поскольку учетные записи, создаваемые с помощью утилиты User Accounts из панели управления, присваиваются группе Administrators или группе Users, неизвестные учетные записи встречаются только при обновлении ранних версий Windows, а также при обращении к, консоли Local Users And Groups или к команде Net Localgroup при контроле членства в группах.

Встроенные группы безопасности

В состав Windows входит несколько встроенных групп безопасности. Каждая из них имеет заранее определенный набор прав доступа, разрешений и ограничений. Ниже приводится краткое описание этих групп.

Администраторы - Наиболее мощная группа, обеспечивающая полный контроль над системой. Администратор имеет право выполнять следующие операции:

– установка операционной системы и ее компонентов;

– установка пакетов обновления;

– обновление операционной системы;

– восстановление операционной системы;

– настройка главных параметров операционной системы (политики паролей, управления доступом, политики аудита, настройки драйверов в режиме ядра и так далее);

– вступление во владение файлами, ставшими недоступными;

– управление журналами безопасности и аудита;

– архивирование и восстановление системы.

Опытные пользователи (Power Users) - Включает многие, но не все привилегии, присущие группе администраторов. Опытный пользователь имеет право выполнять следующие операции:

– выполнять приложения, сертифицированные для Windows 2000 и Windows XP Professional, а также устаревшие приложения;

– устанавливать программы, не изменяющие файлы операционной системы, и системные службы;

– настраивать ресурсы на уровне системы, включая принтеры, дату и время, параметры электропитания и другие ресурсы панели управления;

– создавать и управлять локальными учетными записями пользователей и групп;

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

Пользователи (Users) - Ограниченный набор привилегий для пользователей, которые не нуждаются в администрировании системы. Пользователь имеет право выполнять следующие операции:

– запускать только сертифицированные для Windows приложения;
– создавать локальные группы и управлять ими;
– создавать и изменять свои файлы.

Гости (Guests) - Поддержка ограниченного доступа для случайных пользователей и гостей.

Операторы архива (Backup Operators) - Предоставление привилегий, требуемых для восстановления файлов и папок. Члены этой группы могут архивировать и восстанавливать файлы на компьютере независимо от всех разрешений, которыми защищены эти файлы.

Репликаторы (Replicator) - Обеспечение возможности управления репликацией, присущей доменным сетям.

Операторы настройки сети (Network) - Члены этой группы допускаются к установке, конфигурированию сетевых компонентов.

Пользователи удаленного рабочего стола (Remote) - Обеспечение доступа к компьютеру посредством удаленного рабочего стола (Remote Desktop). Позволяет специалистам в удаленном режиме просматривать действия, происходящие на экране компьютера или брать на себя управление рабочей станцией в случае возникновения проблем.

HelpServices - Предоставление возможности техническому персоналу подключаться к вашему компьютеру.

Для обеспечения высокой степени безопасности в процессе текущей работы рекомендуется не регистрироваться сотрудникам (даже самим администраторам) с правами доступа администратора. Вместо этого при ежедневной работе надо воспользоваться учетной записью с несколько меньшими системными привилегиями. Регистрироваться в роли администратора следует только в тех случаях, когда требуется выполнять именно административные задания. Подобный подход позволит избежать нарушений в системной конфигурации, инфицирования операционной системы вирусом, а также создаст заслоны для внедрения «троянских коней». В Windows 2000 свои ежедневные обязанности можно выполнять в рамках группы Power Users.

Управление регистрацией и процессом аутентификации.

Существует три метода регистрации:
– метод интерактивной регистрации;
– метод безопасной регистрации;
– метод автоматической регистрации.

Метод интерактивной регистрации заключается в том, что после загрузки ОС появляется экран, на котором приводятся имена пользователей. Данный метод обеспечивает простой способ регистрации в сети, но позволяет многим программам перехватывать вводимые пароли.

Метод безопасной регистрации заключается в том, что сотруднику требуется ввести свое имя и пароль. Из-за технических особенностей данный способ не позволяет «троянским коням» перехватывать пароли.

Метод автоматической регистрации заключается в том, что когда включается компьютер, Windows автоматически вводит заданные по умолчанию имя пользователя и пароль.

2. Практическое задание

1. Перезагрузите Windows XP.
2. В окне приветствия дважды нажмите клавиши **Ctrl + Alt + Delete**.
3. Введите свое имя и пароль.
4. Откройте панель управления.
5. Откройте папку **Учетные записи пользователей**.
6. Выберите ссылку **Изменение входа пользователей в систему**.
7. Снимите флажок **Использовать страницу приветствия**.
8. Нажмите кнопку **Применение параметров**.
9. Перезагрузите Windows XP.
10. Введите свое имя и пароль входа в систему.
11. Верните исходные установки.
12. Перезагрузите Windows XP.
13. Проверьте восстановления способа входа в систему.
14. Создайте учетную запись **user1** с возможностями администратора.

15. Назначьте ей пароль **qwerty**.
16. С помощью команды **Выполнить** запустите **Панель управления** с дополнительной опцией командой **control userpasswords2**.
17. В открывшемся окне выделите учетную запись **user** и нажмите кнопку **Свойства**.
18. Откройте закладку **Членство в группах**.
19. Включите параметр **Обычный доступ**, что приравняет учетную запись user к опытным пользователям.
20. Примените сделанные изменения.
21. Вернитесь в исходное окно.
22. Выберите закладку дополнительно.
23. В параметре **Безопасный вход в систему** включите опцию **Требовать нажатие Ctrl + Alt + Delete**. Этим вы уменьшите вероятность подбора пароля к системе.
24. Примените сделанные изменения.
25. Перезагрузите компьютер.
26. Создайте учетную запись **user2** с возможностями администратора.
27. Назначьте ей пароль **asdfgh**.
28. С помощью команды **Выполнить** запустите **Панель управления** с дополнительной опцией командой **control userpasswords2**.
29. В открывшемся окне выделите учетную запись **user** и нажмите кнопку **Свойства**.
30. Внесите эту запись в группу **Операторы архива**. Для этого:
31. С помощью команды **Выполнить** запустите **Панель управления** с дополнительной опцией командой **control userpasswords2**.
32. В открывшемся окне выделите учетную запись **user** и нажмите кнопку **Свойства**.
33. Откройте закладку **Членство в группах**.
34. Включите опцию **Другой** и из списка выберите группу **Операторы архива**.
35. Перезагрузите компьютер.
36. Войдите в систему под своим именем.
37. Удалите учетную запись **user1**.
38. Удалите учетную запись **user2**.

Задание № 2.
Администрирование файлов и папок

Цель работы:
- изучить основные возможности администрирования файлов и папок Windows XP;
- изучить основные положения групповой политики;
- получить навыки администрирования Windows XP.

Результат обучения. После обучения студент должен:
- знать основные возможности администрирования файлов и папок в Windows XP;
- уметь работать с учетными записями;
- уметь выполнять администрирование Windows XP.

План занятия:
1. Изучение теоретических вопросов темы;
2. Выполнение практического задания;
3. Выполнение отчета.

1. Основные положения

Защита учетных записей.

Для защиты информации от злоумышленников в Windows XP используется утилита Syskey. Эта утилита, используя несколько уровней кодирования, **защищает информацию учетной записи**, сохраняемую в базе данных SAM. (То есть пароли учетных записей кодируется с помощью ключа шифрования, предназначенного именно для учетной записи каждого

пользователя. В свою очередь, ключ шифрования кодируется с помощью основного защитного ключа, а последний ключ шифруется с помощью ключа запуска). Отключить шифрование паролей учетных записей в системе невозможно, т.е. данная защита включена всегда.

По умолчанию ключ запуска случайным образом генерируется компьютером. Этот ключ хранится на локальном компьютере. Обычно именно такой подход позволяет успешно защищать парольную информацию в системном реестре. Рекомендуется периодически изменять ключ шифрования. Для этого проделайте следующее:

1. Выберите пункты меню **Пуск – Выполнить**.
2. Введите команду **syskey** и нажмите **ОК**.
3. В появившемся окне нажмите кнопку **Обновить**.
4. Далее нажмите ОК. В результате вы обновили ключ базы данных учетных записей.

Использование групповой политики.

Администратору, для определения настроек безопасности на локальном компьютере, можно воспользоваться специально предназначенным инструментом Group Policy. Благодаря этому можно контролировать более 450 аспектов поведения операционной системы, автоматизировать события, происходящие в момент запуска и прекращения работы, а также при регистрации пользователей и в момент завершения регистрации.

Для открытия консоли Group Policy выполните следующее:

1. Выберите пункты меню **Пуск – Выполнить**.
2. Введите команду **gpedit.msc** и нажмите **ОК**.

Пункты в категории **Конфигурация компьютера** (Computer Configuration) содержат настройки, регулирующие доступ для пользователей и групп.

Выполните следующие действия:

1. Найдите раздел **Политика паролей** (Password Policy) в категории Конфигурация компьютера.
2. Установите следующие параметры:
   - Максимальный срок действия паролей – **100 дней**.
   - Минимальная длина паролей – **3 символа**.
   - Хранить в памяти **три последних пароля**, для неповторяемости паролей.
3. Найдите раздел Назначение прав пользователей.
4. Установите следующие параметры:
   - Доступ к компьютеру из сети – только администраторы и пользователи.
   - Завершение работы системы – все.
   - Изменение системного времени - только администраторы.
5. Найдите раздел Параметры безопасности.
6. Установите следующие параметры:
   - Интерактивный вход в систему: текст сообщения для пользователей – «Внимание! За работой в сети ведется наблюдение со стороны администратора».
   - Устройства: разрешено форматировать и извлекать съемные носители – Администраторы и опытные пользователи.
7. Перезагрузите компьютер.
8. Войдите в систему под именем Гость (если этой учетной записи нет, то создайте ее).
9. Попытайтесь изменить время на компьютере.
10. В случае неудачи перезагрузите систему и войдите под своим именем.
11. Верните все исходные параметры.

Администрирование файлов и папок.

К числу универсальных возможностей Windows 2000/XP относятся и такие, которые позволяют как на уровне локального компьютера, так и при использовании общедоступных сетевых ресурсов ограничивать доступ к файлам и папкам.

Управлением доступом к папкам можно осуществлять двумя способами:

1. управлять доступом, используя стандартный режим "**Общий доступ**" (в окне "Свойства" выбрать закладку "Доступ", а потом в появившемся окне нажать кнопку "Разрешение"),
2. управлять доступом, используя возможности файловой системы NTFS.

Каждый из методов имеет свои преимущества и недостатки.

Первый вариант удобен тем, что, используя его, можно ограничить в сети доступ к папкам на дисках, отформатированных под файловую систему FAT16 (FAT32). А к недостаткам этого способа относятся:

- доступ к папкам проверяется только для сетевых пользователей (т.е. локальные пользователи будут иметь полный доступ к папкам);
- все разрешения задаются только для папки целиком, а не для отдельных файлов;
- предоставляется небольшой набор параметров для конфигурирования (только полный доступ, изменение и чтение).

Использование разрешений NTFS.

Для каждого объекта, который хранится в томе, отформатированном с помощью файловой системы NTFS, Windows поддерживает контрольный список доступа (access control list, **ACL**). Как следует из названия, этим списком определяется перечень пользователей, которым разрешен доступ к данному объекту (обычно идет речь о файле или папке), а также тех пользователей, доступ которых исключается. Индивидуальные пункты в ACL называются записями, контролирующими доступ (access control entries, ACE), и содержат следующую информацию:

- идентификатор SID пользователи или группы;
- список разрешений, формирующих право доступа, создаваемое на основе большого списка основных и специальных разрешений — Full Control, Read и Write,
- информация о наследовании, которая определяет, будет ли Windows использовать разрешения из родительской папки, и если будет, то каким образом;
- флаг, указывающий на разрешение/запрет доступа.

Для использования второго способа управления доступом к папкам нужно открыть у соответствующего объекта окно свойств и выбрать вкладку "**Безопасность**" (Security), на которой установить флажки для нужных параметров доступа.

Данный способ имеет следующие преимущества:

- Доступ к папкам проверяется абсолютно для всех пользователей.
- Предоставляется широкий набор параметров для конфигурирования. Запретить и разрешить можно следующую функции: смена владельца, смена и чтение разрешений, удаление, чтение и изменение атрибутов, запись и дозапись данных, чтение данных, обзор папок и выполнение файлов и т.д.
- Для папок можно указывать, как применяются настройки: только внутри этой папки, для дочерних папок, для файлов и так далее.
- Если пользователь является владельцем файла, он может распоряжаться им по своему усмотрению, предоставляя права доступа другим пользователям.

В качестве недостатка, однако, можно отметить, что управлением доступом становится значительно сложнее. Все разрешения носят аддитивный характер, то есть, права складываются из прав группы, в которую входит пользователь, и прав, которыми наделен лично он. При этом нужно помнить, что запрещающие директивы всегда имеют больший приоритет, чем разрешающие, и использовать их надо с осторожностью. Так, если у пользователя есть, например, право на чтение некоторого файла, но он входит в группу, которой это делать запрещено, то он не сможет читать файл.

2. Практическое задание:

1. Создайте учетную запись **Клиент**.
2. Установите тип учетной записи – **ограниченная**.
3. Пароль для входа создавать не надо.
4. На диске D создайте папку с именем **Рабочая папка**.
5. Выделите эту папку и выполните команду **Сервис – Свойства папки**.
6. Откройте закладку **Вид**.
7. Снимите опцию **Использовать простой общий доступ к файлам**.
8. Примените сделанные изменения.
9. Щелкните правой кнопкой мышки на созданной папке и выберите пункт **Свойства**.
10. Откройте закладку **Общий доступ и безопасность**.

11. Включите опцию **Открыть общий доступ к этой папке**.
12. Установите предельное число пользователей – 2.
13. Нажмите кнопку **Разрешения**.
14. В открывшемся окне удалите группу **Все**.
15. Нажмите кнопку **Добавить**.
16. Нажмите кнопку **Дополнительно**.
17. Нажмите кнопку **Поиск**. При этом откроются все учетные записи.
18. Найдите учетную запись **Клиент** и нажмите **ОК**.
19. В исходном окне еще раз нажмите **ОК**.
20. Разрешите учетной записи **Клиент** только **чтение** данных.
21. Примените сделанные изменения.
22. Перезагрузите компьютер.
23. Войдите в систему под именем **Клиент**.
24. Попытайтесь создать новую папку внутри рабочей папки.
25. В случае неудачи перезагрузите систему и войдите под своим именем.
26. Удалите рабочую папку.
27. Удалите учетную запись **Клиент**.
28. Создайте папку на диске **C** и настройте к ней доступ так, чтобы посторонний пользователь мог изменять в ней файлы, но удалять не мог.
29. Покажите результат работы преподавателю.

Задание № 3.
Администрирование пользователей сети

Цель работы:

- изучить основные возможности администрирования пользователей в Windows XP;
- изучить основные положения назначения учетных записей и паролей;
- получить навыки администрирования Windows XP.

Результат обучения. После обучения студент должен:

- знать основные возможности администрирования пользователей в Windows XP;
- уметь работать с учетными записями и паролями;
- уметь выполнять администрирование Windows XP.

План занятия:

1. Изучение теоретических вопросов темы;
2. Выполнение практического задания;
3. Выполнение отчета.

1. Методики, применяемые при работе с учетными записями

Как уже говорилось, при работе с системой желательно регистрироваться под учетной записью, которая не относится к группе администраторов. Однако возникают ситуации, при которой многие программы не устанавливаются, если работа в системе идет от имени пользователя. Если возникает такая ситуация, то Windows 2000 предоставляет в этом случае механизм, который позволяет запускать приложения в другом контексте безопасности, не перезагружая при этом систему. Эта возможность обеспечивается благодаря автоматически запускающейся в начале работы системы службе Secondary Logon Service (***запуск от имени***). Чтобы воспользоваться этим механизмом, нужно то выполнить следующее:

1. Правой кнопкой мыши щелкнуть на программе установки нового приложения и выбрать команду **Запуск от имени** (Run As). В версии Windows 2000 с целью обеспечения доступа к команде Run As потребуется нажать клавишу Shift.
2. Указать разрешение для административной учетной записи.

Если после установки программы и при попытке ее запуска пользователем, не обладающим административными полномочиями, она не выполняется, может потребоваться выбор режима совместимости. Для этого необходимо зарегистрироваться с административными правами доступа (или воспользоваться командой Run As) и выполнить следующие шаги:

1. Если программа выполняется с компакт-диска или сетевого диска, откройте меню кнопки **Пуск** (Start) и выполните команду **Программы - Служебные - Программа - Мастер совместимости** (All Programs - Accessories - Program - Compatibility Wizard).
2. Если программа установлена на локальном жестком диске, щелкните правой кнопкой мыши на ее ярлыке, выберите опции **Свойства** (Properties), а затем щелкните на вкладке **Совместимость** (Compatibility).

Примечание:

Если Windows 2000 с Service Pack 2 или сервисный пакет более поздней версии, то доступна вкладка Compatibility, напоминающая аналогичную вкладку для Windows XP. Если указать в командной строке regsvr32 %systemroot%\apppatch\slayerui.dll, можно подключить требуемое свойство (Эту операцию следует выполнить единожды). В результате щелчка правой кнопкой мыши на ярлыке программы и выбора опции Properties (Свойства) отображается диалоговое окно, содержащее вкладку Compatibuility.

Если Windows 2000 без SR2 и вы заранее не установили утилиты Support Tools и Application Compatibility, воспользуйтесь компакт-диском Windows 2000 Professional, перейдите в папку \Support\Tools и запустите программу установки. Для запуска на выполнение Application Compatibility откройте меню кнопки Start (Пуск) и выберите команду Programs > Windows 2000 Support Tools * Application Compatibility Tool (Программы > Средства поддержки Windows 2000 > Совместимость приложений)(либо просто в командной строке укажите apcompat).

3. Если выбор режима совместимости не приводит к устранению проблем, воспользуйтесь опцией Run As для запуска программы на выполнение.

Можно также **настроить ярлык программы** таким образом, чтобы при щелчке на нем отображался запрос на ввод перечня разрешений для используемой учетной записи; благодаря этой опции можно запускать программу обычным способом, а не путем выбора в контекстном меню опции Run As. Пользовательское имя и пароль вводит сам оператор. Проделайте следующее:

1. С целью конфигурирования ярлыка щелкните на нем правой кнопкой мыши (этот прием применим исключительно по отношению к ярлыкам для программ, но не для исполняемых файлов программ).
2. Выберите опцию Свойства (Properties), затем выделите вкладку **Ярлык** (Shortcut).
3. В среде Windows XP щелкните на кнопке **Дополнительно** (Advanced). Затем выберите опцию Выполнить с другим набором разрешений (Run With Different Credentials).
4. В среде Windows 2000 на вкладке **Ярлык** (Shortcut) установите флажок Run With Different Credentials (Выполнять с другими разрешениями);

Если изложенные технические приемы не позволяют решить проблему, то придется работать с программой от имени администратора.

Практическое задание:

1. Создайте ограниченную учетную запись **Студент**.
2. Войдите в систему под именем **Студент**.
3. Из папки Program на Server от имени **администратора** (своей учетной записи, т.к. вы администраторы) установите программу DHCP Turbo – файл **dhcpt.exe**
4. После установки перезагрузите компьютер и войдите в систему под именем **Студент**.
5. Запустите программу DHCP Turbo (файл **dhcptui.exe**) от имени администратора.
6. Установите для файла **dhcptui.exe** режим совместимости с системой Windows 98.
7. Создайте на рабочем столе ярлык программы.
8. Настройте ярлык программы таким образом, чтобы при щелчке на нем отображался запрос на ввод перечня разрешений
9. Покажите результат преподавателю.

10. Удалите программу DHCP Turbo.

2. Назначение пароля для пользовательской учетной записи

Один из важных этапов конфигурирования пользовательских учетных записей заключается в назначении для каждой из них регистрационного пароля.

Примечание:

При работе в Windows XP ни в коем случае не удаляйте (изменяйте) пароль другого пользователя. Исключение составляют моменты, когда пароль был забыт и не существует другого метода доступа к учетной записи. Если все же проделать эту операцию, то пользователь утеряет свои персональные сертификаты и пароли, предназначенные для обеспечения доступа к web-узлам и сетевым ресурсам! При отсутствии персональных сертификатов блокируется доступ к зашифрованным файлам пользователей, а также к электронным сообщениям, закодированным с помощью частных пользовательских ключей!

В случае изменения пользовательского пароля невозможно получить доступ к сертификатам и закодированной информации путем возврата к старым паролям или с помощью средства Passwords Reset Disk!

Рассмотрим **три способа изменения паролей**.

1. Утилита Users And Passwords обеспечивает установку паролей для всех локальных учетных записей, за исключением текущей записи. (С целью изменения пользовательского пароля нажмите комбинацию клавиш Ctrl + Alt + Delete, затем щелкните на кнопке Change Password (Изменить пароль).) На вкладке Users (Пользователи) выберите имя пользователя, затем щелкните на кнопке Set Password (Установить пароль) (Windows 2000) или Reset Password (Переустановить пароль) (Windows XP).

2. При работе с утилитой Local Users And Groups назначение паролей производится путем щелчка на пункте Users в дереве консоли, затем щелчка правой кнопкой мыши на имени пользователя с последующим выбором опции Set Password.

3. При работе с утилитой User Accounts назначение пароля производится путем щелчка на имени учетной записи и на ссылке Create A Password (Создать пароль). Формирование подсказки для пароля — исключительная прерогатива именно этой утилиты. (Отображение подсказки на экране происходит после щелчка на пиктограмме со знаком вопроса или в результате щелчка на имени пользователя, отображенном на экране регистрации.)

Практическое задание:

1. Для учетной записи **Студент** выполните назначение паролей тремя разными способами.
2. Удалите учетную запись **Студент**.

3. Обеспечение безопасности учетной записи администратора

(практическое освоение этого раздела выполните дома)

Учетная запись администратора является целью различного рода атак. Поэтому для обеспечения безопасности данной учетной записи необходимо изменить ее имя. Для этого:

1. Откройте окно утилиты Users And Passwords. (Если выполняется Windows XP и компьютер не включен в состав домена, в командной строке введите команду control userpasswords2).
2. На вкладке Users дважды щелкните на учетной записи **Администратор** (Administrator).
3. В поле **Имя пользователя** (User Name) введите новое имя для учетной записи администратора.

Примечание.

После завершения переименования учетной записи администратора можно создать новую учетную запись, называемую Администратор (Administrator). Поместите вновь созданную учетную запись в группу безопасности Гости (Guests) и защитите ее с помощью сложного пароля. Эта учетная запись выполняет две функции: пускает возможных вредителей по ложному следу и облегчает определение попыток взлома системы.

Если вы располагаете альтернативной учетной записью (то есть иной пользовательской учетной записью, которая входит в группу Administrators), можете отключить встроенную учетную запись администратора, благодаря чему предотвращается возможность регистрации посторонних пользователей.

В Windows 2000 невозможно отключить встроенные учетные записи, но можно назначать такие права доступа пользователей, благодаря которым предотвращается возможность регистрации для данной учетной записи. Запустите консоль Local Security Settings (Локальные настройки безопасности) (просто в командной строке укажите **secpol.msc**), затем откройте окно Security Settings\Local Policies\ User Rights Assignment (Настройки безопасности\Локальные политики\Назначение прав доступа пользователей). Находясь в панели подробностей, дважды щелкните на праве доступа Deny Logon Locally (Запретить локальную регистрацию). Щелкните на кнопке Add (Добавить), выберите опцию Administrator, затем щелкните на кнопках Add и OK.

Аналогично можно отключить или переименовать **гостевую учетную запись**. Так как этот тип учетной записи не предполагает использования паролей, следует убедиться в том, что она недоступна для случайных пользователей.

Примечание.

Если применяется политика блокирования учетных записей, то даже в случае отключения учетной записи, указывается количество неудачных попыток подбора пароля, после чего происходит блокирование учетной записи. Запустите на выполнение утилиту Local Users And Groups, откройте гостевую учетную запись (Guest) и проверьте, выбрана ли опция Account Is Locked Out (Учетная запись заблокирована). Если все обстоит именно так, значит, кто-то пытался зарегистрироваться в качестве гостя.

3. Создание отчета

После выполнение практического задания студент должен составить отчет, в котором должны быть отражены следующие положения:

1. Номер и название практической работы.
2. Цель и план занятия.
3. Экранные копии выполнения практического задания.
4. Ответы на следующие вопросы:

– Как подтверждается **идентичность** на компьютере с установленной ОС Windows 2000/XP?
– Зачем нужны учетные записи?
– Что такое SID?
– Какие встроенные пользовательские учетные записи создаются после установки Windows 2000/XP? Чем они отличаются?
– Что такое группы безопасности? Зачем они нужны?
– Какие типы учетных записей есть в Windows XP?
– Почему для текущей работы рекомендуется не регистрироваться с правами доступа администратора?
– Какие методы регистрации в системе вам известны?
– Какой утилитой защищаются учетные записи на компьютере?
– Какой файл используется для запуска консоли Group Policy?
– Какие способы управления доступом к папкам вам известны? Какие достоинства и недостатки им присущи?
– Что такое ACL? Что в нем хранится?
– Как вы считаете, для диска С можно было установить ограничения на работу с папками?
– Какой инструмент используется для определения настроек безопасности в Windows XP?
– Что делать, если программа не устанавливается при использовании вашей учетной записи?
– Что делать, если программа не запускается при использовании вашей учетной записи?
– Что делать, если программа написана для более ранней версии ОС Windows и не работает в Windows XP?
– Почему нельзя изменять пароль другого пользователя в системе Windows XP?
– Какая утилита обеспечивает формирование подсказки для пароля пользователя?
– Как обеспечить безопасность учетной записи администратора?
– Какую еще учетную запись желательно обезопасить?

После составления отчета студент сдает его преподавателю и защищает. После успешной защиты отчета студент переходит к выполнению следующей практической работы. Не

допускается выполнение и отчет следующих лабораторных работ, без успешной защиты предыдущей работы.

Тема № 3: «Администрирование рабочей станции»

Практические занятия.
Задание № 1. Управление правами доступа

Цель работы:
- изучить основные возможности администрирования локальной сети;
- изучить основные положения администрирования сетей;
- получить навыки администрирования Windows XP.

Результат обучения. После обучения студент должен:
- знать основные возможности администрирования локальной сети;
- уметь выполнять администрирование локальной сети;
- уметь выполнять администрирование системы Windows XP.

1. Права доступа

В системе NTFS для каждого файла (и папки) ведется список управления доступом **ACE** (Access control entry). Администраторы и владельцы файла могут модифицировать ACE, предоставляя или отказывая в правах доступа другим пользователям.

Если пользователь создает новую папку, то Windows присваивает права доступа **Full Control** пользователю, создавшему эту папку, встроенной группе **Администраторы** и учетной записи **System**. Пользователи с ограниченными учетными записями имеют полномочия **Read & Execute**.

Права доступа к папкам делятся на
- базовые
- расширенные.

К **базовым правам доступа** относятся следующие:

1. **Полный контроль** – позволяет просматривать содержимое папки, создавать новые файлы и папки, удалять файлы и папки, читать и открывать файлы, изменять права доступа к файлам и внутренним папкам.
2. **Изменение** – позволяет читать, редактировать, создавать и удалять файлы, но не позволяет изменять права доступа к внутренним папкам и файлам.
3. **Чтение и выполнение** – позволяет просматривать содержимое файлов и вызывать программы на выполнение.
4. **Просмотр содержимого папки** – аналогично предыдущим правам, но это право доступа наследуется внутренними папками, но не файлами в этих папках.
5. **Чтение –** позволяет просматривать содержимое папки, атрибуты файлов, обеспечивает возможность чтения и синхронизации файлов.
6. **Запись** – позволяет создавать файлы, записывать данные, считывать значения атрибутов и права доступа, а также выполнять синхронизацию файлов.

Для просмотра расширенных прав доступа необходимо:

1. Щелкнуть правой кнопкой мышки на любой папке и выбрать команду **Свойства**.
2. В открывшемся окне выбрать закладку **Безопасность**.
3. Выделить нужного пользователя (или группу).
4. Нажать кнопку **Дополнительно**.
5. В новом окне также выделить нужного пользователя (или группу).
6. Нажать кнопку **Изменить**.

2. Наследование прав доступа

Кроме прав доступа, устанавливаемых пользователем или программой, файлы и папки могут наследовать права доступа от родительских папок. По умолчанию, заданные права доступа для

текущей папки передаются создаваемым внутренним папкам. Для просмотра (изменения) опций наследования необходимо выполнить те же действия, которые указаны выше, т.е.:

1. Щелкнуть правой кнопкой мышки на любой папке и выбрать команду **Свойства**.
2. В открывшемся окне выбрать закладку **Безопасность**.
3. Выделить нужного пользователя (или группу).
4. Нажать кнопку **Дополнительно**.
5. Включить или отключить опцию **Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне.**

3. Права доступа при копировании (перемещении) файлов.

При копировании или перемещении файлов происходит изменение прав доступа, т.е. файлы получают новые права доступа и прежний пользователь может уже не получить доступ к файлам, с которым работал прежде.

Когда происходит копирование или перемещение файлов (папок), вновь созданный объект получает права доступа так, словно объект создается с самого начала. При этом:

1. Когда копируется или перемещается файл (папка), вновь созданный объект получает права доступа той папки, в которой теперь будет располагаться.
2. Пользователь, который осуществляет перемещение или копирование объекта, становится создателем и владельцем этого объекта.

С этим и связано возможное изменение прав доступа.

4. Владельцы файлов и папок

При администрировании важно еще учитывать следующий момент. Каждый файл или папка в разделе NTFS имеют владельца. **Владелец** файла (папки) имеет право предоставлять или отказывать в правах доступа к файлам или папкам другим пользователям.

В качестве владельца пользователь может заблокировать доступ всех остальных пользователей, включая и членов группы **Администраторы**. Таким образом, доступ к файлу (папке) может быть закрыт, даже если администратор установил полный доступ к объекту.

5. Практическое задание

Задание №1. Совместная работа в сети.

1. Договоритесь с соседом о выполнении данного задания и разделитесь на первый и второй номер.
2. Первый номер загружает ПК под именем **ПИ4**.
3. Второй номер загружает ПК под именем **ПИ2**.
4. Первый номер создает на диске **С** папку **WORK**. и предоставляет к ней полный доступ для своего коллеги (**ПИ2**).
5. Второй номер в это время создает любой текстовый файл.
6. Этот файл второй номер сохраняет в папке **WORK** своего соседа под именем **Proba1.doc** и закрывает файл.
7. После чего второй номер открывает созданный файл **Proba1.doc** и вносит в него любые изменения. После чего изменения необходимо сохранить и файл закрыть.
8. Первый номер меняет права доступа к папке, а второй номер создает новый текстовый файл и сохраняет его на ПК первого номера под именем **Proba2.doc**.
9. Файл изменяется и сохраняется.
10. Данные действия повторяются для всех базовых прав доступа (т.е. всего должно быть 6 файлов).

Задание №2. Смена владельцев объектов.

1. Создайте учетную запись **Клиент** с правами администратора.
2. Войдите в систему под именем **Клиент**.
3. Создайте папку на диске **С**.
4. Используя контекстное меню, вызовите свойства созданной папки.
5. Откройте закладку **Безопасность**.
6. Установите полный доступ к папке только для пользователей **ПИ2**.

7. Нажмите кнопку **Дополнительно**.
8. Откройте закладку **Владелец**.
9. В разделе **Текущий владелец** этого элемента вы увидите свою учетную запись.
10. Внизу в поле **Изменить владельца на** выберите учетную запись **ПИ4** (ПИ2, ПИ3).
11. Нажмите кнопку **Применить**.
12. Перезагрузите систему и войдите под именем **Клиент**.
13. Попытайтесь теперь открыть созданную вами папку.
14. Если доступа нет, то покажите результат работы преподавателю.
15. Восстановите доступ к своей папке.
16. Удалите эту папку.

Задание №3. Работа с сетевыми дисками.

1. В сетевом окружении откройте список доступных ресурсов любого компьютера в классе.
2. Щелкните правой кнопкой мыши на ресурсе **Рисунки** и выберите команду **Подключить сетевой диск**.
3. Нажмите **ОК** (Готово).
4. Закройте все окна.
5. На **Рабочем столе** откройте папку **Мой компьютер**.
6. В открывшемся окне выберите подключенный диск **Рисунки**.
7. Откройте на этом диске любой файл и просмотрите его.
8. Закройте программу с открытым файлом.
9. Самостоятельно подключите сетевой диск – папку **User** с любого компьютера в классе.
10. **Создайте** на этом диске папку под своим именем.
11. **Отключить** сетевой диск **User**.
12. Отключите сетевой диск **Рисунки**.
13. Отмените доступ к папкам **User, WinCom32**, **Рисунки** на своем компьютере.

Задание № 2.
Обслуживание и контроль над системой

Цель работы:

- изучить основные возможности по обслуживанию системы Windows XP;
- изучить основные положения контроля над системой;
- получить навыки администрирования Windows XP.

Результат обучения. После обучения студент должен:

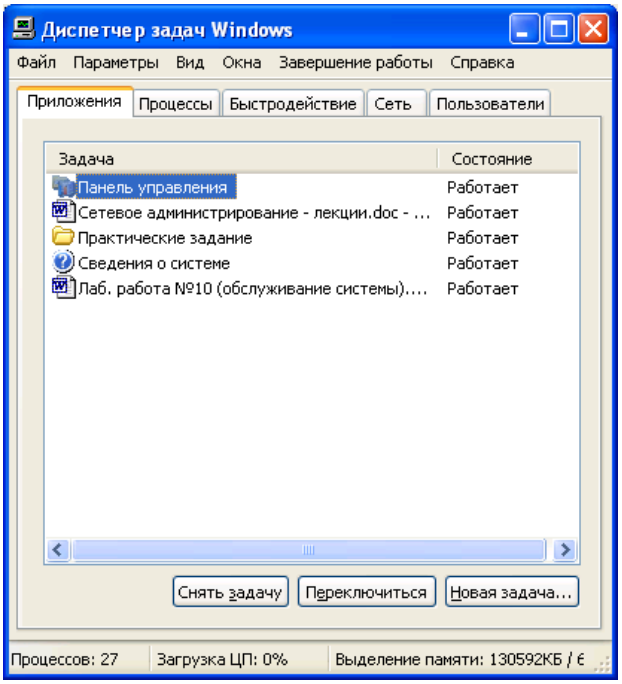
- знать основные возможности обслуживания системы Windows XP;
- уметь выполнять операции контроля над системой Windows XP;
- уметь выполнять администрирование системы Windows XP.

План занятия:

1. Изучение теоретических вопросов темы;
2. Выполнение практического задания;
3. Выполнение отчета.

1. Диспетчер задач

Для контроля за текущей ситуацией в системе имеется несколько различных средств. Одним из них является **Диспетчер задач**. Чтобы долго не искать файл запуска Диспетчера задач, просто для вызова программы нажмите **Ctrl + Alt + Delete** (или Ctrl + Shift + Esc). В результате откроется следующее окно:



Используя Диспетчера задач, выполните следующие действия:

1. **Выпишите** в отчет текущие задачи, выполняемые на вашем ПК.
2. **Выпишите** в отчет процессы, занимающие самый большой объем памяти (укажите какой).
3. **Выпишите** в отчет объем файла подкачки.
4. **Выпишите** в отчет, сколько байт отправлено по сети.
5. **Выпишите** в отчет, сколько байт получено по сети.
6. Запустите приложения **Калькулятор**, **Блокнот**, **Paint**.
7. Сверните все эти приложения.
8. Используя Диспетчера задач, переключитесь в **Paint**.
9. Используя Диспетчера задач, закройте приложения (снимите задачи) **Калькулятор** и **Блокнот**.
10. Запустите **консоль**, используя Диспетчера задач. Для этого нажмите кнопку **Новая задача** и в открывшемся окне введите команду **cmd**, после чего нажмите **ОК**.
11. Закройте консоль, используя Диспетчера задач.
12. Запустите приложения **Калькулятор**, **Блокнот**, **Paint**.
13. Откройте в Диспетчере программ закладку **Процессы**.
14. Найдите процессы, соответствующие приложениям Калькулятор, Блокнот, Paint.
15. **Завершите процессы**, соответствующие приложениям Калькулятор, Блокнот, Paint.

2. Производительность и обслуживание

Для выбора указанного раздела администрирования системы необходимо открыть в панели управления папку **Производительность и обслуживание**. Если вы не увидите этой папки, то необходимо переключиться **к виду по категориям**.

В этой папке содержаться программы по оперативному контролю за системой. Изучите их работу по отдельности.

Для этого выполните следующие действия:

1. Откройте папку Администрирование.
2. Откройте папку Управление компьютером.
3. Выберите раздел Дефрагментация диска.
4. Проведите анализ дисков C и D.
5. Выпишите в отчет количество фрагментированных файлов и процентное их отношение.
6. Если анализ показывает, что требуется дефрагментация, то проведите ее.
7. Просмотрите самостоятельно другие разделы в папке Управление компьютером.
8. Откройте папку Просмотр событий.

9. Просмотрите, какие особые события, касающиеся приложений, произошли за последний день. Выпишите в отчет эти события.

Понятие системных служб (Services).

Системные службы предназначены для того, чтобы другие программы и оборудование работали корректно, и загружаются либо на старте системы, либо при обращении других программ к их функциям. Однако Windows не знает, какие программы и какое оборудование вы используете постоянно, а что вам не понадобится ни при каких условиях. Поэтому в памяти могут оказаться абсолютно ненужные службы, что крайне негативно скажется на производительности системы в целом.

Поэтому необходимо при настройке системы выполнить инвентаризацию списка из почти 80 служб, чтобы максимально разгрузить и процессор, и оперативную память. В колонке "Startup Type" списка служб отражен текущий способ их загрузки - именно его надо изменить.

Посмотрите на колонку "Status" - запущенные службы будут сопровождаться комментарием "Started", и таких изначально немало. Ваша задача, как администратора, сократить их число. При установке режима запуска службы в диалоговом окне ее свойств возможны три варианта:

– **Автоматически** (Automatic) - служба стартует во время загрузки ОС. Это слегка увеличивает время загрузки, но некоторые службы обязательно должны инициализироваться непосредственно на старте Windows.

– **Вручную** (Manual) - служба стартует не при загрузке ОС, а только в случае необходимости. Время загрузки системы при этом немного сокращается, но во время работы в Windows периодически возможна потеря производительности системы, так как на инициализацию службы нужно некоторое время.

– **Отключена** (Disabled) - служба не стартует, даже если будет затребована каким-то приложением.

Можно сказать, что оптимальным будет режим **Вручную** (Manual), при котором любая служба может автоматически запуститься при первом обращении к ней (в редких случаях, правда, способ этот не подходит, так как некоторые программы требуют для своей работы уже запущенную службу). В принципе, допустимо вообще для всех служб выставить режим **Вручную** - тогда загруженным окажется только то, что нужно системе. Но лучше будет после этого перевести обратно в режим **Автоматически** те службы, которые оказались запущены сразу после входа в Windows. Это повысить скорость загрузки системы.

Изучите настройку системных служб на следующем примере.

1. Откройте папку **Службы компонентов**.
2. Откройте папку **Службы** (локальные).
3. **Выпишите в отчет** несколько служб (известных вам), которые:

– запускаются автоматически;

– запускаются вручную;

– отключены.

4. Найдите в конце списка службу **Фоновая интеллектуальная служба передачи**.
5. Настройте ее таким образом, чтобы она автоматически запускалась при запуске ПК.
6. Перезагрузите ПК и проверьте режим запуска Фоновой интеллектуальной службы передачи.
7. Отключите автоматический запуск Фоновой интеллектуальной службы передачи.

3. Настройка системы

Утилита Настройка системы используется для оптимизации работы Windows XP. Для запуска программы **Настройка системы** используется файл **msconfig.exe**.

Самостоятельно изучите возможности утилиты **Настройка системы**.

4. Практическое задание

1. Отключите службу **Беспроводная настройка**.
2. Отключите службу **Диспетчер очереди печати**.
3. Отключите службу **Планировщик заданий**.
4. Перезагрузите ПК, проверьте режим запуска указанных служб.

5. Создание отчета

После выполнение практического задания студент должен составить отчет, в котором должны быть отражены следующие положения:

1. Номер и название практической работы.
2. Цель и план занятия.
3. Экранные копии выполненных заданий.
4. Письменные ответы на следующие вопросы:

– Кому предоставляется полный доступ к папке при ее создании?
– Что включают в себя базовые права доступа?
– Что позволяет выполнять право доступа «Содержание папки/Чтение данных»?
– Что позволяет выполнять право доступа «Создание папок/Дозапись данных»?
– Как ограничить доступ к своим ресурсам (не дать удалить файлы, не дать изменить файлы и т.д.)?
– Как подключить сетевой диск к компьютеру? Что представляет собой сетевой диск?
– Какая особенность имеется в Windows 2000/XP при копировании или перемещении файла?
– Сколько способов можно использовать в Диспетчере задач для закрытия зависшего приложения?
– Какие типы сообщений используются в утилите Просмотр событий?
– Какие операции по настройке системы можно выполнять с помощью утилиты Настройка системы?
– Выпишите все параметры загрузки для файла **boot.ini** и укажите, что они означают.
– Какой с точки зрения производительности системы режим запуска системных служб является оптимальным?
– Какие системные службы можно безболезненно отключить на вашем учебном ПК?

Тема № 4: «Администрирование компьютерной сети»

Практические занятия.
Задание № 1. Администрирование локальной сети

Цель работы:

- изучить основные возможности администрирования локальной сети;
- изучить основные положения администрирования сетей;
- получить навыки администрирования Windows.

Результат обучения. После обучения студент должен:

- знать основные возможности администрирования локальной сети;
- уметь выполнять администрирование локальной сети;
- уметь выполнять администрирование системы Windows.

План занятия:

1. Изучение теоретических вопросов темы;
2. Выполнение практического задания;
3. Выполнение отчета.

1. Совместное использование файлов в сети

В Windows XP каждый пользователь, входящий в группу **Опытные пользователи** (Power Users) или **Администраторы** (Administrators), может указать папку для общего доступа. (Пользователи, обладающие учетными записями с ограничениями, не могут создавать обще-доступных папок).

При этом следует использовать следующие аспекты:

– Если папка используется совместно, **все** содержащиеся в ней файлы доступны для пользователей сети, имеющих соответствующие разрешения (невозможно сделать общедоступными только отдельные файлы из подобной папки).

– Для общедоступной папки **невозможно** присвоить пароль (как в Windows 98). Однако можно указать режим «только чтение» или «полный доступ» для отдельных папок.

– Если файлы общедоступных папок защищены с применением NTFS-разрешений, эти разрешения будут справедливы по отношению к каждому пользователю, получающему доступ к файлам в сети.

При совместном использовании файлов в сети возрастает вероятность их заражения вирусом. Одним из способов борьбы с этим является включение отображения расширений всех файловых имен при общем доступе к файлам. Так некоторые вирусы и программы-трояны используют трюк, позволяющий «пробить брешь» в защите пользовательской информации в среде Windows. Суть этого трюка заключается в добавлении второго расширения имени файла, которое выглядит совершенно безопасным и на экран не выводится. В результате маскируется исполняемый файл. Например, файл **Letter.doc.vbs** отобразится в виде **Letter.doc**. Менее подготовленные или более невнимательные пользователи могут запустить опасный файл и заразить сетевой компьютер вирусом.

Чтобы защитить себя от этого явления выполните следующее:

1. Откройте Проводник (Windows Explorer) и выполните команду **Сервис – Свойства папки** (Tools - Folder Options)
2. На вкладке **Вид** (View) отмените установку флажка **Скрыть расширения для известных типов файлов** (Hide Extensions For Known File Types).
3. Закройте окно настроек

2. Совместное использование принтера в сети

Windows XP/2000 полностью поддерживает удаленную печать. Когда рабочие станции соединяются с сервером, к которому физически подключен принтер, драйвер принтера автоматически устанавливается на рабочей станции.

Приведем краткий обзор операций, производимых с документом, посланным на принтер с клиента, для которого Windows XP/2000 используется как сервер печати.

1. Пользователь на компьютере-клиенте запрашивает печать документа из приложения.
2. Приложение обращается к графическому интерфейсу устройства (GDI), который вызывает драйвер принтера, связанный с целевым принтером. На основе информации о документе GDI и драйвер принтера формируют задание на печать, а затем передают его клиентскому диспетчеру очереди печати.
3. Клиентский компьютер поставляет задание по выводу на печать серверу печати.
4. На сервер печати задания от клиентов поступают в формате *расширенный метафайл* (extended metafile). Сервер передает задание на печать локальному «провайдеру» печати, который помещает его в очередь.
5. Локальный провайдер печати вызывает монитор печати, который опознает тип данных задания и принимает задание на печать, преобразуя его согласно типу данных.
6. Монитор печати может состоять из *монитора языка* (language monitor) и *монитора порта* (port monitor). Для двунаправленных принтеров монитор языка обеспечивает двустороннюю связь между компьютером и принтером, а затем передает задание на печать на монитор порта. Если принтер не является двунаправленным, задание на печать идет непосредственно на монитор порта, который посылает его на принтер.
7. Принтер принимает задание на печать, преобразует каждую страницу в растровый формат и печатает ее.

3. Практическое задание

Задание №1. Предоставление доступа к папкам компьютера.

1. Создайте на диске **C (**или на другом диске) папку **USER**.
2. Щелкните правой кнопкой мыши на папке **User**.
3. В открывшемся списке выберите команду **Общий доступ и безопасность**.

4. Откройте закладку **Доступ** и включите опцию **Открыть общий доступ к этой папке**.
5. Введите имя общего ресурса - **User**. В поле "Комментарий" наберите – **Рабочая папка**.
6. Установите предельное число пользователей – не более 10.
7. Нажмите кнопку **Разрешения**.
8. В новом окне в разделе **Группы и пользователи** выделите строку **Все** и удалите данную группу.
9. Нажмите кнопку **Добавить**.
10. В новом окне нажмите кнопку **Дополнительно**.
11. Нажмите кнопку **Поиск**, в результате отобразится список всех пользователей и групп в сети.
12. Найдите и выделите **свою группу**. После чего нажмите **ОК**.
13. В исходном окне еще раз нажмите **ОК**.
14. Установите для своей группы **полный доступ**.
15. Аналогично для любой другой группы установите доступ только на **чтение**.
16. Нажмите кнопки **Применить** и **ОК**.
17. Запустите программу графический редактор **Paint**.
18. Нарисуйте произвольный рисунок.
19. Сохраните этот рисунок на диске **C** в папке **User** под своим именем (например, Рисунок Петрова).
20. Закройте **Paint**.

Задание №2. Работа в сети.

1. Установите общий доступ для созданной папки со следующими данными:
   - сетевое имя – **Общая папка**;
   - комментарий – **практика по Windows**;
   - доступ – **все, только чтение**.
2. На своем ПК выберите созданную папку на диске **C**.
3. Установите общий доступ для папки со следующими данными:

– сетевое имя - **Рисунки**;
– комментарий – **Рисунки с других компьютеров**;
– доступ – **все пользователи, полный**.

Задание № 2.
Настройка сервиса DHCP

Цель работы:

– изучить основные положения сервиса DHCP;
– изучить основные принципы работы сервиса DHCP;
– изучить настройку сервера DHCP;
– познакомится с программой DHCP Turbo.

Результат обучения. После обучения студент должен:

– знать основные положения сервиса DHCP;
– знать основные правила настройки сервиса DHCP.

План занятия:

1. Изучение теоретических вопросов темы;
2. Выполнение практического задания;
3. Выполнение отчета.

1. Основные положения

DHCP обозначает Dynamic Host Configuration Protocol - то есть протокол динамической конфигурации клиентских машин. Это один из наиболее важных и полезных протоколов семейства TCP/IP, помогающий автоматически конфигурировать десятки и сотни машин одновременно. Многие технологии напрямую зависят от этого протокола: например, протокол

удаленной загрузки PXE ищет сервер DHCP для получения дальнейших указаний по получению загрузочного образа.

В принципе DHCP относится к числу "безпроблемных" протоколов, то есть все операционные системы корректно поддерживают его функции.

DHCP обладает следующими преимуществами:

1. При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами. Динамическое разделение адресов позволяет строить IP-сеть, количество узлов в которой намного превышает количество имеющихся в распоряжении администратора IP-адресов.
2. DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением.

Рассмотрим DHCP на примере реализации **DHCP Turbo** фирмы **Weird Solutions**. При необходимости получить IP-адрес хост посылает запрос на резервацию IP-адреса, на который серверы отвечают на протяжении некоторого времени. На этом этапе сервер может проверить наличие свободного IP-адреса, пропинговать его на предмет отсутствия конфликтов или проверить MAC-адрес данного хоста.

Первое, что нужно сделать при настройке DHCP, это определить диапазон раздаваемых адресов и маску подсети. Часто используются подсети категории "C" Первый адрес в подсети всегда обозначает саму подсеть, последний - адрес групповой рассылки (broadcasting). Количество компьютеров в подсети определяется количеством нулей в конце маски. Возведите двойку в эту степень, вычтите два - и получите потенциальное количество доступных вам адресов.

Пример расчета подсети

Для примера возьмем произвольную подсеть: адрес сервера 10.0.0.97, маска 255.255.255.224, в бинарном виде - 11111111.1111111.1111111.11100000.

Число нулей в конце маски - пять, то есть два в пятой степени дает 32. Следовательно, возможность наших подсетей категории C - 32 адреса. Можно представить, что первая подсеть начинается с адреса 10.0.0.0, вторая - 10.0.0.32, третья - 10.0.0.64, четвертая - 10.0.0.96.

Будем работать в адресном пространстве от 10.0.0.96 до 10.0.0.127 и, если требуется, чтобы наши компьютеры после запуска попали в одну подсеть с сервером, то выделять адреса следует только из этого диапазона. Как уже было сказано, первый адрес - это адрес подсети как целого, последний - броадкастинг, так что они исключаются. Пусть будет три компьютера, которые будем конфигурировать через данный сервер, так что достаточно только трех адресов. Возьмем адреса в диапазоне от 10.0.0.124 до 10.0.0.126. Диапазон адресов и подмаска сети называется scope (видимость) и является одним из основных понятий DHCP, с которым связаны все остальные настройки. То есть любая настройка относится к той или иной области.

2. Практическое задание

1. Запустите программу инсталляции **dhcpt.exe**
2. После установки перезагрузите компьютер и запустите программу DHCP Turbo.
3. Необходимо сначала остановить локальный сервер. Для этого выполните команду **Tools – Control Service**.
4. В открывшемся окне нажмите кнопку **Stop,** а затем **Stop**.
5. В программе выполните команду **File – New – Server** и создайте новый сервер с произвольным именем.
6. Выделите в окне созданный сервер.
7. Запустите сервер, для этого выполните команду **File – Connect**. В открывшемся окне нажмите кнопку **Login** без ввода пароля. Если компьютер не позволяет выполнить данную команду для вашего сервера то используйте локальный сервер **Localhost**.
8. Выделите закладку **Option Types**. В результате откроются все опции программы.
9. Для изменения нужной опции необходимо дважды щелкнуть на имени опции и выбрать команду **New Option Type**. (Без необходимости не меняйте их)

Опции

Все параметры, передаваемые от сервера клиенту, называются опциями. Опции делятся на категории. Существуют **обязательные опции**, такие как IP-адрес и маска подсети. Некоторые опции используются только в служебных целях, например, определяют начало и конец списка опций, - вы не сможете настроить их значения, хоть и увидите их в списке. Остальные же опции необходимы в специальных ситуациях, например при сетевой загрузке.

10. Выделите раздел **Scopes**.
11. Выполните команду **File – New scope**.
12. В открывшемся окне задайте произвольные имя и описание.
13. Справа задайте начальный и конечный адрес, который будет задаваться компьютерам сети 10.0.0.124 - 10.0.0.126.
14. Задайте также маску подсети - 255.255.255.224.
15. Дважды щелкните мышкой на разделе **Scopes**, при этом откроется список.
16. В этом списке выделите созданный раздел. В результате справа откроются все параметры сервера DHCP.

Основные параметры для Windows-клиентов

Следующее, что интересует после создания области (дополнительно можно задать еще несколько параметров), это именно параметры, которые раздаем хосту, помимо его IP и маски. Как правило, три из них имеют важное значение: маршрутизатор по умолчанию, DNS-сервер и WINS-сервер. Эти параметры, как уже было сказано, задаются опциями. Опции - это хорошо документированные переменные, имеющие номер и имя. Номера могут быть как положительными, так и отрицательными. Опции, помимо прочего, - типизованные значения, то есть они могут быть как числами и строками, так и специальными типами, вроде IP- или MAC-адреса.

Итак, главные опции: 3 (Gateways), 6 (Domain Name Servers), 44 (NBT Name Servers), 46 (NBT Node Type). Несколько пояснений - во-первых, как вы видите, все параметры групповые, то есть подразумевают несколько значений, чем вы можете воспользоваться. WINS настраивается через параметры NBT - опция 44 указывает на сервер, а опция 46 должна быть равна 8 (hybrid). Все указанные опции вы добавляете на закладке Policies.

Хотя это вовсе и не обязательно, но вы можете получить у DHCP-сервера любые дополнительные параметры для загружаемой машины, например суффикс доменного имени (опция 15), имя DHCP-сервера (опция 20), сетевое имя хоста (опция 12) и так далее.

17. Самостоятельно просмотрите где находятся данные опции и как можно изменить их.

Важный вопрос - как отказаться от чужих сетевых MAC-адресов и обслуживать лишь несколько подопечных хостов? Ведь, как правило, не стоит устанавливать мост и отрезать подопечные компьютеры от остальной сети - это потребует дополнительного сервера с двумя интерфейсами, а также настройки маршрутизации и т.д. Этого и не нужно делать - достаточно определить ваш сервер как приватный. Сделать это можно на закладке **Свойства сервера**, доступной по правой кнопке мыши над именем сервера.

После определения вашего сервера как приватного он будет отказывать в обслуживании всем хостам, кроме тех, сетевые MAC-адреса которых указаны в появляющейся папке Registrations.

18. Закройте программу.
19. **Деинсталлируйте** программу DHCP Turbo.

Задание № 3.
Администрирование с применением консоли

Цель работы:

- изучить основные возможности администрирования системы Windows XP с консоли;
- изучить основные возможности утилит консоли;
- получить навыки администрирования Windows XP.

Результат обучения. После обучения студент должен:

- знать основные возможности администрирования системы Windows XP с консоли;
- уметь работать с основными утилитами консоли;
- уметь выполнять администрирование Windows XP.

План занятия:

1. Изучение теоретических вопросов темы;
2. Выполнение практического задания;
3. Выполнение отчета.

1. Утилита командной строки Net User

Net User – утилита, которая создает и изменяет учетные записи пользователей на компьютере. Когда используется без параметров, выводит список учетных записей пользователей для данного компьютера. Информация об учетных записях пользователей хранится в базе данных учетных записей.

Общий вид записи команды выглядит следующим образом:

Net User имя_пользователя пароль [*] /[параметры]

Основные параметры указаны в таблице:

Параметры и ключи	**Описание**
/Add	Создание новой учетной записи. Имя пользователя может содержать максимум 20 символов и не допускает применения следующих знаков: »/\[]:;)=,+*?<>
пароль * или /Random	Установка пароля. Если указать звездочку (*), отобразится запрос на ввод пользовательского пароля. После выбора переключателя /Random случайным образом система генерируется пароль, состоящий из восьми символов
/Domain	Выполняет операцию на контроллере домена в указанном домене.
/active:no или /active:yes	Отключение или включение учетной записи.
/Delete	Удаляет учетную запись пользователя из базы данных учетных записей.
/Fullname: "имя"	Указание полного имени пользователя
/Comment:«текст»	Указание описательного комментария (максимум до 40 символов).
/Passwordchg:yes или /Passwordchg:no	Определяет возможность изменения пароля пользователем
/Active:no или /Active:yes	Активизация/блокирование учетной записи. (Если учетная запись заблокирована, пользователь не может регистрироваться или получать доступ к компьютеру.)
/Expires:дата или /Expires:never	Установка даты устаревания учетной записи. Срок действия учетной записи завершается в начале указанного дня; после наступления этого события пользователь не может зарегистрироваться либо получить доступ к ресурсам на компьютере до тех пор, пока администратор не установит новую дату устаревания.

Освойте работу утилиты Net user на практическом примере:

1. Просмотрите список учетных записей на компьютере. Для этого введите в командной строке команду:

net user

2. Ознакомьтесь со справочной информацией утилиты командной строки Net User. Для этого введите в командной строке команду:

net help user

3. Чтобы в дальнейшем просматривать только доступные опции утилиты можете вводить традиционный запрос:

net user /?

4. Создайте пользовательскую учетную запись **Клиент**. Для этого введите следующую команду:

net user клиент /add

5. Запустите утилиту **Учетные записи пользователей** и проверьте создание учетной записи **Клиент**.
6. **Закройте утилиту** Учетные записи пользователей**.**
7. Отключите учетную запись **Клиент**. Для этого введите команду:

net user клиент /active:no

8. Проверьте отключение учетной записи **Клиент**.
9. Включите учетную запись **Клиент**. Для этого введите команду:

net user клиент /active:yes

10. Удалите учетную запись **Клиент**. Для этого введите команду:

net user клиент /delete

11. Запустите утилиту **Учетные записи пользователей** и проверьте удаление учетной записи **Клиент**.
12. **Закройте утилиту** Учетные записи пользователей**.**
13. Создайте пользовательскую учетную запись **User** с паролем 12345678. Для этого введите следующую команду:

net user user 12345678 /add

14. Перезагрузите компьютер и войдите в систему под именем **user** с паролем 12345678.
15. Перезагрузите компьютер и войдите в систему под своим именем.
16. Удалите учетную запись User.

2. Настройка прав доступа с консоли

Для настройки прав доступа с консоли используется утилита **Cacls**. Для просмотра и изменения текущих прав для папки используется следующий вид команды:

Cacls имя_папки /T /E /C /G имя:доступ /R имя [...] /P имя:доступ [...] /C имя [...]

Параметры и ключи:

/T - замена таблиц управления доступом для указанных файлов в текущем каталоге и всех подкаталогах.

/E - изменение таблицы управления доступом вместо ее замены.

/C - продолжение при ошибках отказа в доступе.

/G имя:доступ - определение разрешений для указанных пользователей.

где "доступ" может принимать следующие значения:

R - Чтение

W – Запись

C - Изменение (запись)

F - Полный доступ

/R имя - отзыв разрешений для пользователя (только вместе с /E).

/P имя:доступ - замена разрешений для указанного пользователя.

где "доступ" может принимать следующие значения:

N – Отсутствует

R – Чтение (read).

W – Запись (write);

C – Изменение (change);

F - Полный доступ (full control);

/C имя - запрет на доступ для указанного пользователя.

На примере просмотрим работу эту утилиту:

1. Создайте пользователя **User** с ограниченными возможностями.
2. Создайте на диске **C** папку **Work**.
3. Запустите консоль.
4. Перейдите в корневой каталог диска **C**.

5. Для просмотра текущих прав для папки User введите команду:

Cacls work

6. Установите пользователю **User** для папки **Work** права только чтения. Для этого введите команду:

Cacls work /g user:r

7. Проверьте изменение прав доступа.
8. Самостоятельно установите пользователю **User** для папки **Work** права на запись.
9. Проверьте изменение прав доступа.
10. Удалите папку Work.

3. Практическое задание

Задание №1.

1. Используя утилиту Net user, создайте учетную запись **Student1** со следующими параметрами:

– пароль – 555555;
– полное имя – «студент ПИЭ»;
– комментарий - «студент специальности ПИЭ»

2. Используя утилиту Net user, создайте учетную запись **Student2** со следующими параметрами:

– пароль 111111 – задается пользователем при создании учетной записи;
– полное имя – «студент 3ПИЭ»

3. Используя утилиту Net user, создайте учетную запись **Student3** со следующими параметрами:

– пароль – генерируется системой автоматически
– полное имя – «студент ПИЭ»

4. Запустите утилиту **Учетные записи пользователей** и проверьте создание учетных записей.
5. Используя утилиту Net user, **отключите** учетную запись **Student3**.
6. **Выпишите в отчет** последовательно все команды, с помощью которых вы выполнили это задание.

Задание №2.

1. Используя утилиту Net user, **включите** учетную запись **Student3**.
2. Создайте на диске **C** папку **ZADANIE**.
3. Установите пользователю **Student1** для папки **ZADANIE** права только чтения.
4. Установите пользователю **Student2** для папки **ZADANIE** полный доступ.
5. Установите пользователю **Student3** для папки **ZADANIE** запрет на доступ.
6. Замените пользователю **Student1** для папки **ZADANIE** право только чтения на право **запись**.
7. Замените пользователю **Student2** для папки **ZADANIE** право полный доступ на право **только чтение**.
8. Проверьте выполнение сделанных установок.
9. Используя утилиту Net user, удалите учетные записи **Student1 – Student3**.
10. **Выпишите в отчет** последовательно все команды, с помощью которых вы выполнили это задание.

Задание № 4.
Администрирование Web-сервера

Цель работы:

– изучить основные возможности администрирования Web-сервера;
– получить навыки администрирования Web-сервера.

Результат обучения. После обучения студент должен:

- знать основные возможности администрирования Web-сервера;
- уметь выполнять администрирование Web-сервера.

План занятия:

1. Изучение теоретических вопросов темы;
2. Выполнение практического задания;
3. Выполнение отчета.

1. Web-сервер

Web-сервер – это программа, которая работает на компьютере. **Основная задача** Web-сервера - поиск html-документов по запросу от клиента (т.е. браузера) или динамическое их создание (с помощью CGI, Perl, Java и т.д.). Однако поиском или динамической генерацией html-документов функции web-серверов не исчерпываются. Web-сервер также может осуществлять следующие **функции**:

- генерация запросов к базе данных;
- обработка данных, полученных из базы данных;
- аутентификация пользователя;
- разграничение доступа пользователей;
- статистический анализ (подсчет общего числа посещений, числа уникальных клиентов, частоты использования различных версий браузера, отслеживание адресов, с которых пользователей попал на данный документ и т.д.)
- поддержка гостевых книг, форумов, чатов.

Взаимодействие между клиентом и Web-сервером происходит по принципу "запрос-ответ". Запрос указывается в адресной строке браузера.

Web-сервер работает таким образом, что при появлении запроса с его именем, автоматически инициализируется файл index.htm (поэтому он и не указывается в адресной строке). Этот файл считается домашней страницей сайта. Также в качестве домашней страницы может выступать файл default.htm.

Для доступа к любому файлу нужно указывать его явно в строке адреса, например:

http://www.master.ru/mypage.htm

Расширение htm (html) говорит о том, что вызываемый файл не содержит серверных сценариев (файлы, содержащие серверные сценарии, должны иметь расширения cgi, pl, asp или другие - в зависимости от языка сценария). Серверному сценарию могут передаваться параметры. В этом случае обращение к документу выглядит так:

протокол://имя сервера/путь и имя документа?параметры

Например:

http://www.master.ru/student/spis.cgi?nom_stud=17

Однако пользователю, как правило, не приходится вводить их в адресной строке. Потому что пользователь вводит данные, подлежащие отправке на сервер, посредством форм. А адрес серверного сценария, принимающего данные, введенные пользователем при помощи формы, указывается в атрибуте **action** тэга **<form**...

В настоящее время для серверов, функционирующих под ОС UNIX, обычно используют Web-сервер Apache, для серверов под Windows 2000 - Internet Information Server (IIS).

Компанией Microsoft разработана технология написания серверных сценариев, рассчитанная на применение Web-сервера IIS. Она называется ASP (Active Server Pages - Активные серверные страницы). ASP-сценарии могут быть написаны на языках JScript и VBScript.

2. Практическое задание

1. Установите Internet Information Server (IIS). Его следует установить через Пуск - Настройка - Панель управления - Установка и удаление программ - Установка компонент Windows. Если IIS установлен, то этот пункт пропустите.
2. Перезагрузите компьютер.
3. Откройте Internet Information Server (Пуск – Администрирование).

4. Ознакомьтесь с интерфейсом программы.
5. Скопируйте свои html-файлы в папку **C:\InetPub\Wwwroot**, которая является корневым каталогом **Web-сервера**.
6. Проверьте работу вашего Web-сервера с другого компьютера.
7. Нарисуйте произвольный рисунок.
8. Сохраните его в папке **C:\Inetpub\ftproot**.
9. На другом компьютере подключитесь к своему серверу, используя протокол **FTP**.
10. Используя протокол FTP, скопируйте рисунок со своего сервера на другой компьютер.
11. Покажите результат работы преподавателю.
12. Удалите все свои файлы.
13. Удалите Internet Information Server.

3. Создание отчета

После выполнение практического задания студент должен составить отчет, в котором должны быть отражены следующие положения:

1. Номер и название лабораторной работы.
2. Цель и план занятия.
3. Экранные копии выполненных заданий.
4. Ответы на следующие вопросы:

– Кто может предоставить в общий доступ папку на ПК?
– Как организовать общий доступ к папке?
– Можно ли для доступа к папке назначить пароль?
– Почему при совместном использовании файлов в сети желательно включать режим отображения всех расширений?
– Какое сетевое имя носит ваш компьютер?
– Какие ресурсы компьютера можно предоставить в общий доступ?
– Какая утилита используется для администрирования учетных записей в консоли?
– Какая утилита используется для администрирования файлов и папок в консоли?
– Какие преимущества предоставляет консоль по сравнению с утилитами графической оболочки?
– Можно ли сделать так, чтобы пользователь не мог изменить свой пароль в системе?
– Что такое Web-сервер?
– Что такое FTP-сервер?
– Что такое MAC-адрес? (самостоятельно найдите ответ на этот вопрос или воспользуйтесь Интернет).
– Что такое IP-адрес компьютера?
– Зачем нужен сервер DHCP?
– Сколько способов выделения IP–адресов для сетевых компьютеров вы знаете.
– Какие в целом этапы нужно выполнить при организации сети TCP/IP?
– Что такое стек протоколов?
– Что такое инкапсуляция протоколов?
– Каким недостатком на ваш взгляд обладает технология DHCP?
– Сколько компьютеров может быть в подсети, если ее маска 255.255.255.100
– Какие имена html-файлов могут быть у домашней страницы Web-сервера?
– Как выглядит адрес файла в WWW при использовании серверного сценария?
– В какой папке хранятся html-файлы сервера Internet Information Server?
– В какой папке хранятся файлы сервера Internet Information Server для доступа по FTP?

После составления отчета студент сдает его преподавателю и защищает. После успешной защиты отчета студент переходит к выполнению следующей лабораторной работы. Не допускается выполнение и отчет следующих лабораторных работ, без успешной защиты предыдущей работы.

Тема № 5: «Обеспечение безопасности в сети»

Практические занятия.
Задание № 1. Обеспечение безопасности системы при использовании TCP/IP

Цель работы:
- изучить основные возможности обеспечения безопасности в системах с TCP/IP;
- изучить основы безопасности сетей TCP/IP;
- получить навыки администрирования Windows XP.

Результат обучения. После обучения студент должен:
- знать основные возможности обеспечения безопасности в системах с TCP/IP;
- уметь выполнять проверку безопасности локальной сети;
- уметь выполнять администрирование системы Windows XP.

План занятия:
1. Изучение теоретических вопросов темы;
2. Выполнение практического задания;
3. Выполнение отчета.

1. Проверка состояния безопасности с помощью MBSA

Для проверки безопасности системы, в которой в качестве основы установлен стек протоколов TCP/IP, используется программа **Microsoft Baseline Security Analyzer** (MBSA).

MBSA проверяет компьютер на наличие общеизвестных уязвимых мест (как правило, это ошибки неправильного администрирования и конфигурирования системы). Выполните данную проверку своего компьютера и компьютеров в сети. Для этого:

1. Установите на своем компьютере программу MBSA.
2. Запустите программу MBSA.
3. В открывшемся окне выберите опцию **Scan more than one computer** (Проверить несколько компьютеров).
4. В новом окне укажите имя вашего компьютера для проверки в поле **Computer name**.
5. Установите все опции для проверки.

В качестве опций проверки можно выбрать следующие:

- **Check for Windows vulnerabilities** (Проверка уязвимых мест Windows). Выбор этой опции позволит MBSA проверить систему на наличие небезопасных настроек. Например, программа может проверить, все ли жесткие диски отформатированы с применением файловой системы NTFS, определить статус гостевой учетной записи и проверить права доступа к сетевым папкам.
- **Check for weak passwords** (Проверка на наличие слабых паролей). Проверяются пароли для каждой учетной записи и в случае, если пароль пустой или не отвечает требованиям безопасности, выдается предупреждение.
- **Check for IIS vulnerabilities** (Проверка уязвимых мест IIS). При выборе этого пункта MBSA проверяет настройки Internet Information Services на предмет выявления небезопасных установок.
- **Check for SQL vulnerabilities** (Проверка уязвимых мест SQL). При выборе этой опции программа ищет небезопасные настройки в SQL Server. Если на компьютере не установлен SQL Server, программа укажет на этот факт.
- **Check for hotfixes** (Проверка последних исправлений). При выборе этой опции программа проверит компьютеры на наличие критических обновлений.

6. Нажмите ссылку **Start scan**.
7. После выполнения тестов обратите на красные крестики, которые свидетельствуют об уязвимом месте. Желтые крестики показывают на наличие некритических ошибок. Зеленая галочка означает, что все в порядке.
8. Выпишите в отчет все уязвимые места системы с расшифровкой полученных результатов.

2. Практическое задание

1. Выполните проверку соседнего компьютера в сети.
2. Покажите результат работы преподавателю.

Задание № 2.
Настройка брандмауэра

Цель работы:

- изучить основные возможности администрирования брандмауэра;
- изучить основные положения администрирования сетей;
- получить навыки администрирования Windows XP.

Результат обучения. После обучения студент должен:

- знать основные возможности администрирования брандмауэра;
- уметь выполнять администрирование брандмауэра;
- уметь выполнять администрирование системы Windows XP.

План занятия:

1. Изучение теоретических вопросов темы;
2. Выполнение практического задания;
3. Выполнение отчета.

1. Брандмауэр

Брандмауэр – это специальная программа, которая создает защитный барьер между компьютером и окружающими компьютерами в сети. Брандмауэр может использоваться как для обеспечения защиты компьютера от внешних атак из сети Интернет, так и для изоляции компьютера в ЛВС.

Сущность работы брандмауэра заключается в предотвращении прохождения пакетов в систему, которые не соответствуют заданным критериям. Правила фильтрации пакетов могут быть сконфигурированы таким образом, чтобы блокировать или позволять передачу пакета между определенными IP-адресами или портами. Брандмауэр проверяет атрибуты каждого пакета и может пропустить этот пакет или блокировать его.

Например, брандмауэры часто проверяют в пакетах флаги **SYN** и **ACK**. Рассмотрим их назначение. Пакеты, которые передаются по сети с помощью протокола TCP, имеют в заголовке флаги **SYN** и **ACK**, которые играют важную роль при настройке безопасности. Флаги SYN и ACK вообще играют следующую роль:

1. При организации соединения между двумя компьютерами один из них посылает пакет с флагом **SYN** (cynchronize – синхронизировать). Т.е. компьютер сообщает о намерении открыть канал связи.
2. Принимающий компьютер отвечает пакетом, в котором установлены оба флага **SYN** и **ACK** (acknowledge - подтверждать). Т.е. компьютер подтверждает о возможности открыть канал связи.
3. Первый компьютер посылает пакет, где установлен только флаг **ACK**.

Данная технология называется **трехсторонним квитированием** связи TCP.

2. Брандмауэр Internet Connection Firewall

В операционной системе Windows XP имеется встроенный брандмауэр Internet Connection Firewall (ICF). При настройке исходящего подключения ICF позволяет принимать только такие ответы, информация о которых соответствует состояниям, перечисленным в специальной таблице. Т.е. брандмауэр отбрасывает любой пакет, который не ассоциируется с предыдущими исходящими флагами SYN и ACK.

ICF не блокирует пакеты, которые удовлетворяют следующим условиям:

– пакет адресован порту, которому разрешено принимать входящие данные;
– для пакета установлен только флаг SYN.

Для запуска и настройки Internet Connection Firewall выполните следующие действия:

1. Откройте **Панель управления**.
2. Откройте папку **Сеть и подключения к Интернету**.
3. Откройте папку **Сетевые подключения**.
4. В правой части окна выберите раздел «**Изменить параметры брандмауэра Windows**».
5. В открывшемся окне установите опцию **Включить**.
6. Откройте закладку **Исключения**.
7. Добавьте программу **Интернет-Червы** в список исключений.
8. Используя кнопки **Изменить** и **Изменить область**, установите чтобы к этой программе был свободный доступ только с компьютеров ЛВС.
9. Откройте закладку **Дополнительно**.
10. Выберите текущее соединение.
11. Нажмите кнопку **Параметры**.
12. Выделите службу **FTP-сервер**.
13. Ознакомьтесь с описанием службы **FTP-сервер**. Нажмите **ОК**.
14. Выделите службу **Telnet-сервер**.
15. Ознакомьтесь с описанием службы **Telnet-сервер**. Нажмите **ОК**. Таким образом, был предоставлен доступ по сети к службам, минуя брандмауэра.
16. **Покажите результат работы преподавателю**.
17. **Отмените** все сделанные изменения.
18. Выключите брандмауэр.

3. Организация IP-брандмауэра встроенными средствами Windows XP

Основной протокол для стека TCP/IP – это протокол **IP** (Internet Protocol). Он работает на сетевом уровне и занимается доставкой пакетов. У отправителя и получателя должны существовать уникальные IP-адреса компьютеров, которые указываются в заголовках пакетов. Таким образом, **первый способ фильтрации** – фильтрация данных по IP-адресу отправителя.

Помимо протокола IP в сети одновременно работают несколько других протоколов. Каждый из них добавляет в пакет свой заголовок, то есть в момент передачи по сети пакет представляет собой «слоеный пирог», где помимо данных помещены заголовки различных протоколов. Например, это протоколы транспортного уровня – **TCP** (Transmission Control Protocol) и **UDP** (User Datagram Protocol). Данные протоколы непосредственно работают с сетевыми службами. Причем адресация сетевых служб происходит по адресу службы – номеру порта. Отсюда вытекает **второй способ фильтрации** данных – ограничение доступа по номеру порта.

Можно комбинировать эти два способа. Так номер порта можно комбинировать с IP адресом – к примеру, разрешать доступ к серверу (стандартно TCP порт 80) только с определенных IP адресов. Комбинация «IP адрес» + «номер порта» называется ***сокетом***. Сокет позволяет уникально адресовать любую службу в сети Интернете.

Когда вы обращаетесь к удаленному серверу по протоколу TCP, то происходит процесс установления связи. К примеру, вы обратились к веб-серверу узла 192.168.1.1 (стандартно – на TCP порт 80). При этом ваш компьютер (клиент) тоже должен выделить порт, чтобы сервер знал, куда отправлять ответ. Порт клиента выделяется случайным образом – к примеру, TCP 29334.

Номера портов большинства служб стандартизированы, и вы можете посмотреть их в файле "services", который размещается в служебной папке **%systemroot%\system32\drivers\etc**. Папка %Systemroot% находится в папке Windows.

Создание IP-брандмауэра встроенными средствами Windows XP состоит из следующих этапов:

1-й этап – создается новая политика безопасности IP в системе.

2-й этап – в новой политике безопасности создаются фильтры, которые будут обеспечивать фильтрацию данных.

3-й этап – выполняется настройка фильтров.

Теперь рассмотрим на практическом примере, как организовывается брандмауэр средствами ОС Windows XP.

4. Практическое задание

1. Откройте **Панель управления**.
2. Далее выберите **Администрирование – Локальная политика безопасности**. В результате откроется следующее окно (Рисунок 1).

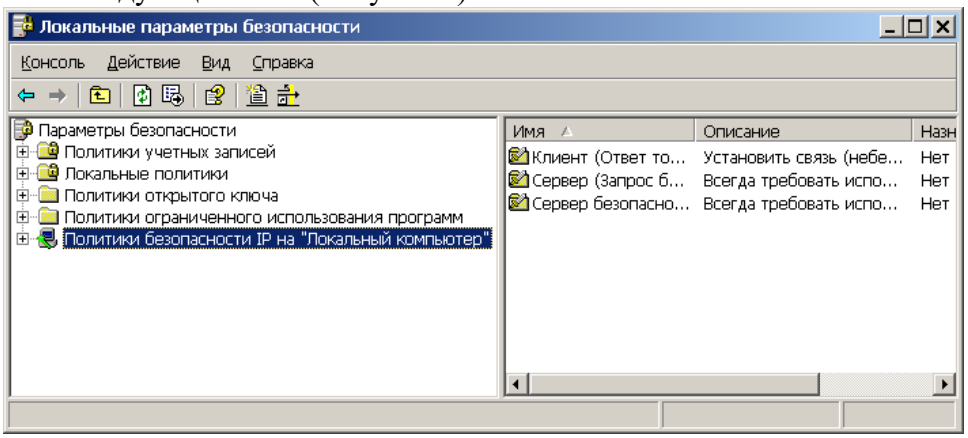


Рисунок – Установка политики безопасности

3. Выделите раздел **Политики безопасности IP на «Локальный компьютер»**.
4. Нажмите правую клавишу мыши на данном разделе и выберите **Создать политику безопасности IP**. В результате запустится мастер установки IP политики.
5. Нажмите кнопку **Далее** в появившемся окне.
6. В следующем окне оставьте имя политики безопасности без изменения - **Новая политика безопасности IP**. Нажмите кнопку **Далее**.
7. В следующем оставьте галочку в позиции **Использовать правило по умолчанию**. Нажмите кнопку **Далее**.
8. В следующем окне также оставьте включенным **Стандарт службы каталогов**. Нажмите кнопку **Далее**. Если появиться сообщение, что компьютер не является членом домена, то ответьте на вопрос в окне - **Да**.
9. В новом окне снимите галочку **Изменить свойства**. Свойства политики безопасности мы отредактируем позже.
10. Нажмите кнопку **Готово**. В результате в окне появилась новая политика безопасности (Рисунок 2).

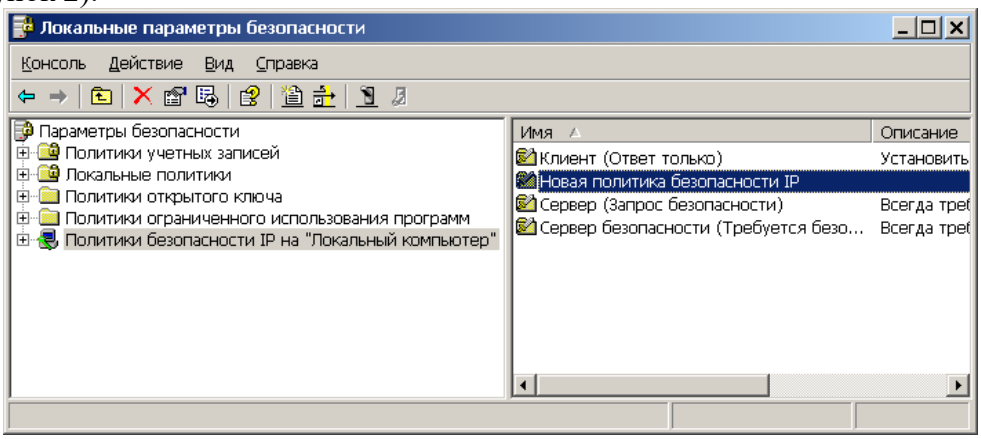


Рисунок 2 – Новая политика безопасности

11. Выделите раздел **Политики безопасности IP на «Локальный компьютер»**.
12. Щелкните на данном разделе правой кнопкой мыши и выберите команду **Управление списками IP-фильтра…** (Рисунок 3)

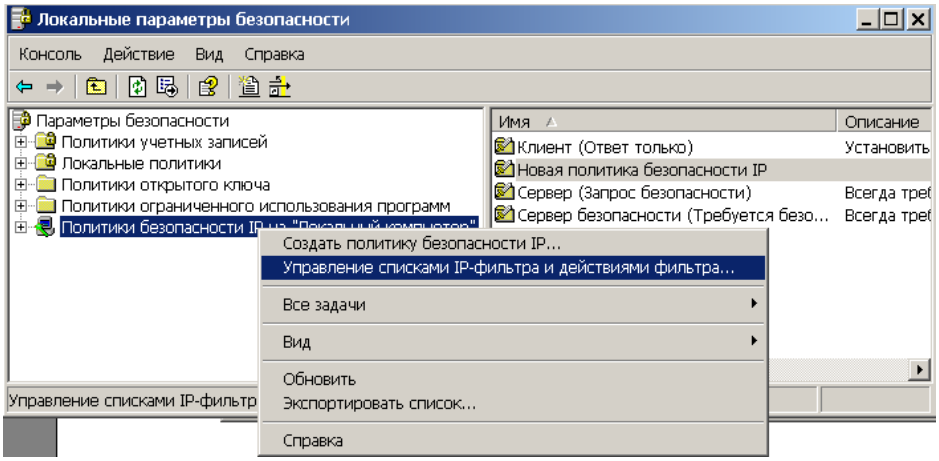


Рисунок 3 – Настройка новой политики

13. В появившемся окне выберите закладку **Управление действиями фильтра**.
14. В данном окне нажмите кнопку **Добавить**. Запуститься мастер настройки фильтра. В первом окне нажмите **Далее**.
15. Во втором окне введите имя - **Запрет связи**. И наберите небольшое описание фильтра (Рисунок 4)

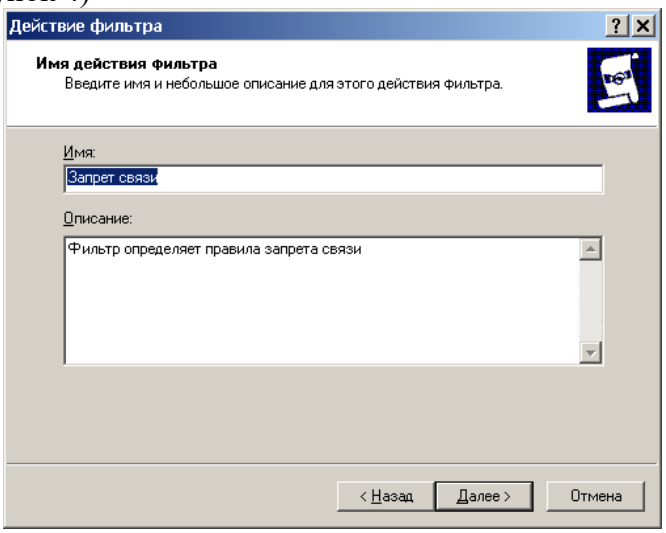


Рисунок 4 – Создание фильтра

16. Нажмите кнопку **Далее**.
17. В следующем окне выберите пункт **Блокировать**. Будет настраивать связь по следующему принципу – запретим связь со всеми узлами, а потом будем потихоньку открывать то, что нам нужно.
18. Нажмите кнопку **Далее**.
19. В последнем окне нажмите кнопку **Готово**. В результате в окне действий появилось действие **Запрет связи** (Рисунок 5).

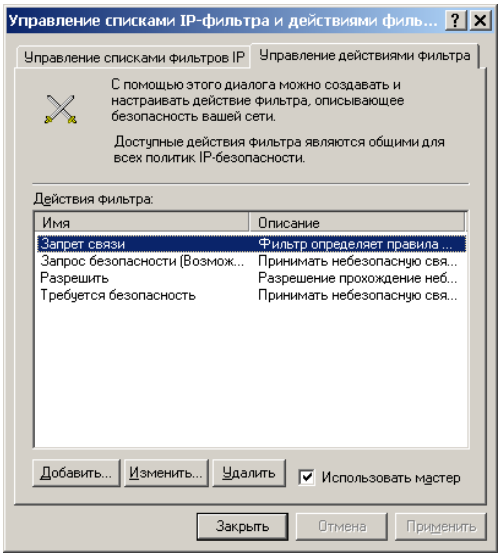


Рисунок 5 – Создание действия фильтра

20. Нажмите кнопку **Закрыть**.
21. Перейдите к редактированию созданной политики (для этого достаточно нажать два раза левой клавишей мыши на ее название).
22. В открывшемся окне нажмите кнопку **Добавить**. В результате запустится очередной мастер правил безопасности.
23. В первом окне нажмите **Далее**.
24. Так как туннель мы задавать не будем, то в следующем окне нажмите кнопку **Далее**, без изменения текущих настроек.
25. В следующем окне включите опцию **Подключение удаленного доступа**. Нажмите **Далее**.

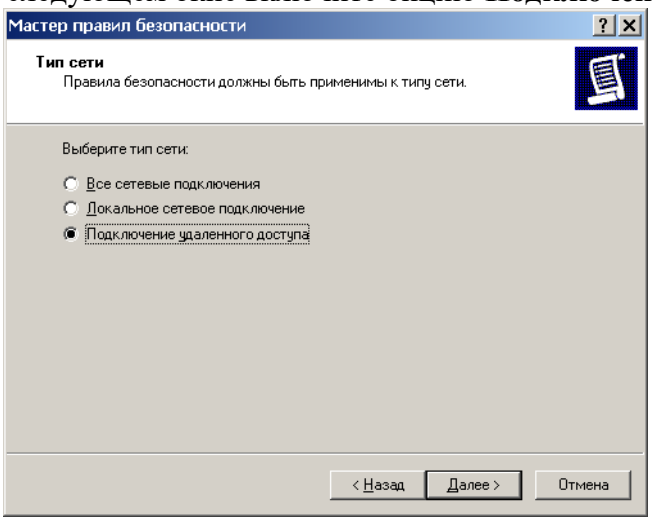


Рисунок 6 – Выбор типа сети

26. В следующем окне оставьте все без изменений и нажмите **Далее**.
27. Мы должны запретить все для всех. Поэтому в новом окне включаете опцию **Полный IP-трафик** и нажимаете кнопку **Добавить**.

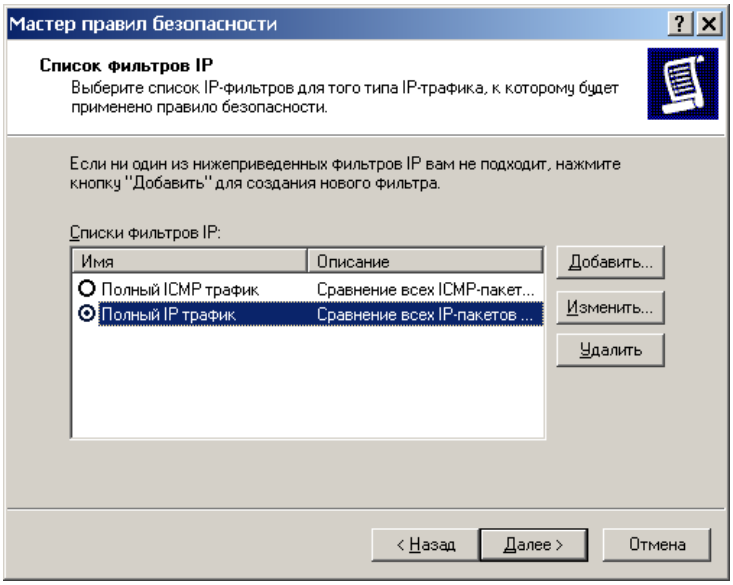


Рисунок 7 – Создание IP-фильтра

28. Назовите фильтр «**Новый IP-фильтр**».
29. Нажмите кнопку **Добавить**. Вновь запускается мастер (они вам еще не надоели?).
30. Здесь указывается источник пакета. Поскольку нужно запретить пакеты от всех источников, то задайте в этом окне **Любой IP-адрес**.

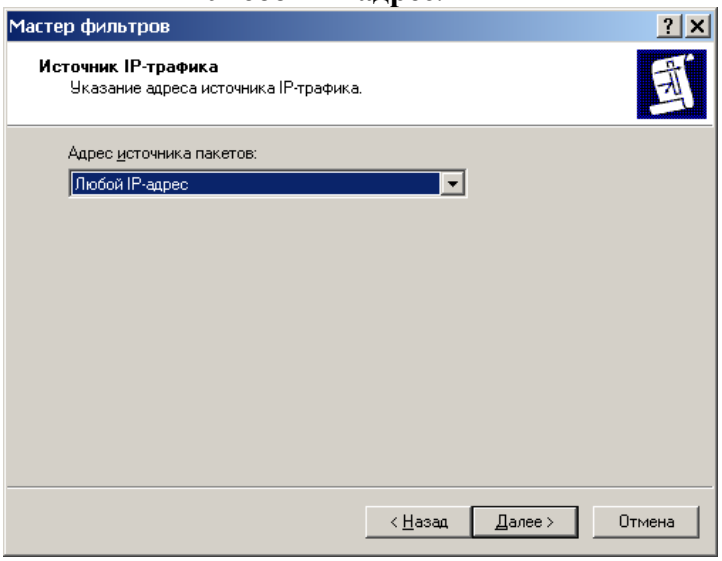


Рисунок 8 – Задание источника пакетов

31. Нажмите кнопку **Далее**.
32. Здесь указывается адрес получателя пакета. Требуется запретить пакеты от всех IP источников для нашего компьютера, поэтому выберите Мой IP-адрес.

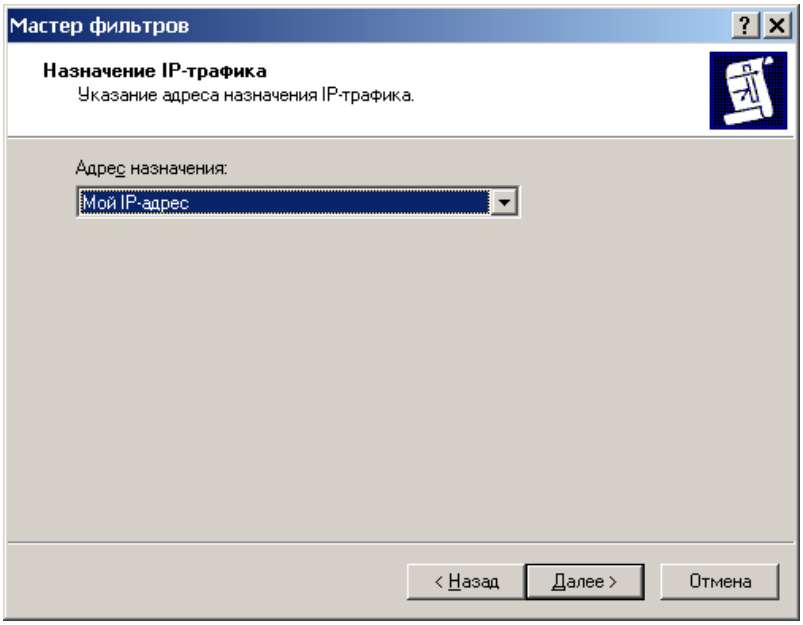


Рисунок 9 – Задание адреса назначения

33. Нажмите кнопку **Далее**.
34. Мы запрещаем все протоколы. Поэтому в следующем окне выбираем "**Любой**". Нажмите кнопку **Далее**.
35. В последнем окне нажмите **Готово**.
36. Мы создали новый IP-фильтр. Нажмите кнопку **ОК**.
37. Появится список фильтров. Выберите созданный фильтр и нажмите **Далее**.
38. В следующем окне выберите созданное действие – **Запрет связи** и нажмите **Далее**.

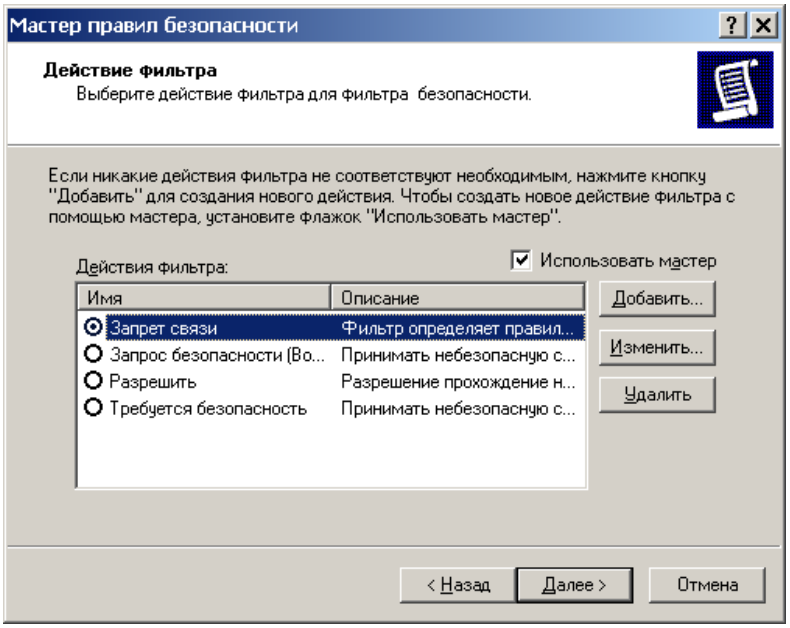


Рисунок 10 – Выбор действия

39. В политике появилось новое правило – запрещение всего от всех и для всех. Т.е. ваш компьютер теперь полностью защищен при удаленном подключении.

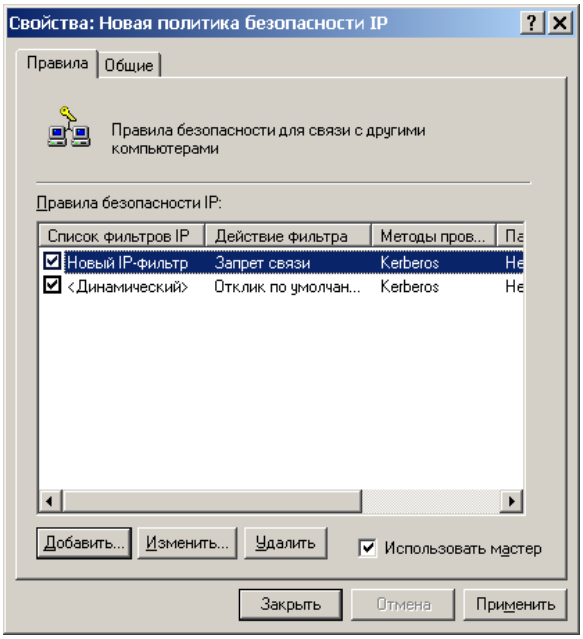


Рисунок 11 – Созданный фильтр

Теперь будем постепенно вводить разрешения. Первоначально следует разрешить ICMP трафик от всех пользователей на вашу машину.

1. Нажмите кнопку **Добавить** в исходном окне (Рисунок 11).
2. Пройдите уже известные вам шаги мастера до шага выбора фильтра IP.
3. Выберите фильтр **Полный ICMP-трафик**. Нажмите кнопку **Далее**.

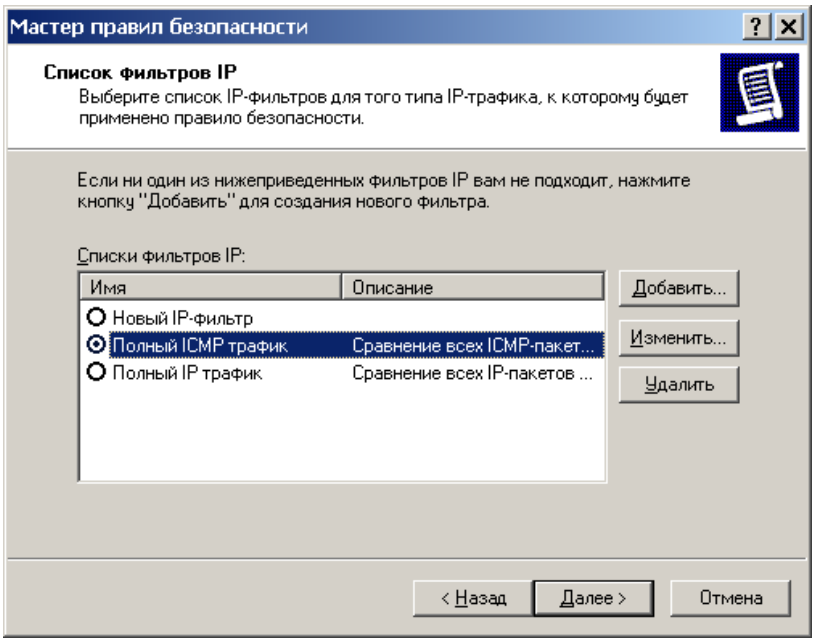


Рисунок 12 – Выбор фильтра для ICMP

4. В следующем окне выберите действие **Разрешить**. Нажмите кнопку **Далее** и самостоятельно завершите мастер.
5. В результате у вас появился новый фильтр с разрешением.

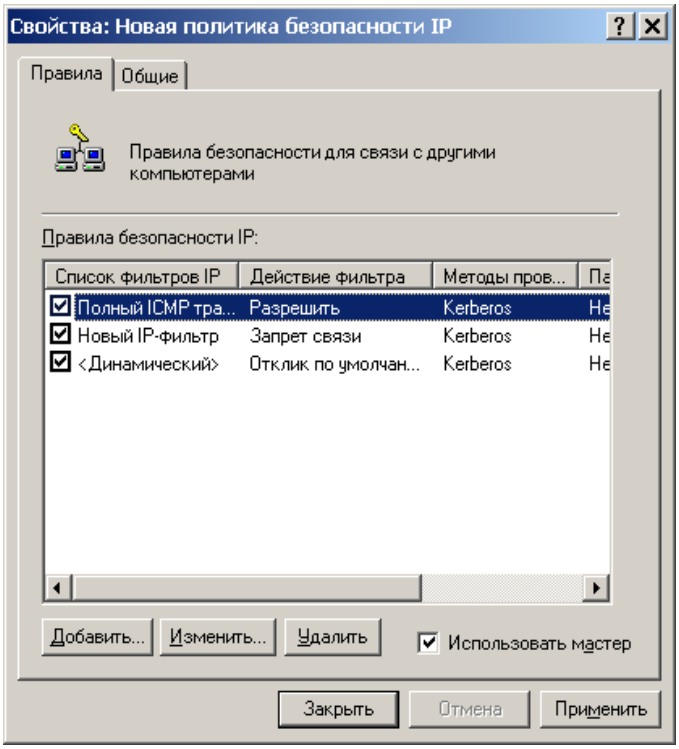


Рисунок 13 – Создание фильтра с разрешением

Теперь у нас не будет работать ничего, кроме ICMP протокола. Сейчас осталось выделить те службы, которые нам нужны, и прописать для них доступ. Лучше всего создать еще один список фильтров, например, "Службы Интернет", и добавить в него несколько строчек фильтров с правом "**Разрешить**".

Ниже приведены строчки для самых распространенных служб. Следует отметить, что по умолчанию каждая служба добавляется зеркально – то есть если мы разрешаем связь от нашего компьютера к любым веб-серверам (порт 80), то будет реализовываться и обратная связь для передачи ответа веб-сервера. Можете самостоятельно выполнить предлагаемые настройки.

1. Запросы DNS сервера. Разрешить 53 порт получателя (destination port address) протокола UDP от нашего компьютера к любому компьютеру. Вместо любого компьютера можно указать DNS сервер провайдера.
2. Веб-трафик. Открыть порт TCP 80 получателя от нашего компьютера к любому компьютеру.
3. FTP-трафик. Открыть порты TCP 20 и TCP 21 получателя от нашего компьютера к любому компьютеру.
4. SMTP трафик (для отправки писем). Открыть порт TCP 25 получателя от нашего компьютера к любому компьютеру (можно вместо любого компьютера указать SMTP сервер провайдера).
5. POP3 трафик (для приема писем). Открываем порт TCP 110 получателя от нашего компьютера к любому компьютеру (или к POP3 серверу провайдера).
6. IMAP трафик (для приема писем). Открываем порт TCP 143 получателя от нашего компьютера к любому компьютеру (или к IMAP серверу провайдера).
7. ICQ трафик. Зависит от сервера ICQ, обычно TCP порт 5190 получателя от нашего компьютера к любому компьютеру (или к серверу ICQ).

5. Создание отчета

После выполнение практического задания студент должен составить отчет, в котором должны быть отражены следующие положения:

1. Номер и название практической работы.
2. Цель и план занятия.
3. Экранные копии выполненных заданий.
4. Ответы на следующие вопросы:

– Что такое безопасность системы?
– Что такое уязвимость системы?

– Что такое атака?
– Какие виды сетевых атак вам известны?
– Что считается ошибками при неправильном администрировании системы?
– Почему возникают уязвимые места в системе?
– Какие способы обеспечения безопасности системы вы знаете?
– Что такое брандмауэр?
– В чем заключается сущность его работы?
– Что такое флаги **SYN** и **ASK**? Какую роль они играют при настройке безопасности в системе?
– Что такое порт?
– Что такое сокет?
– Что такое протокол?
– Сколько способов фильтрации данных в сетях TCP/IP вы знаете?
– Как организовать брандмауэр встроенными средствами ОС Windows XP?
– Как предоставить доступ по сети к программе, минуя брандмауэра?
– Как предоставить доступ по сети к службе, минуя брандмауэра?

5.3. Тематика письменных работ обучающихся

В течение изучения дисциплины «Сетевое администрирование» обучающиеся должны сдать и отчитать реферат по одной из предложенных ниже тем:

1. Понятие сетевого и системного администрирования. Основные различия.
2. Цели и задачи сетевого администрирования.
3. Современные подходы к администрированию компьютерных сетей.
4. Встроенные пользовательские учетные записи. Назначение. Примеры использования.
5. Группы безопасности. Назначение, примеры использования.
6. Регистрация пользователей в системе.
7. Права доступа пользователей к папкам и файлам.
8. Домены и рабочие группы. Назначение. Примеры использования.
9. Понятие профиля пользователя. Назначение. Примеры использования.
10. Организация сети TCP/IP. Преимущества и недостатки.
11. Межсетевой обмен в сетях TCP/IP. Инкапсуляция протоколов.
12. Протоколы SLIP, PPP и ARP. Назначение. Примеры использования.
13. Протоколы ICMP, UDP. Назначение. Примеры использования.
14. Протокол TCP (Transfer Control Protocol – базовый транспортный протокол). Установка соединения TCP.
15. Логическая организация компьютерных сетей.
16. Разбиение сети на подсети. Маска подсети.
17. Использование масок при структуризации сети
18. Назначение IP-адресов узлам сети.
19. Принципы передачи данных в IP-сетях. Порты и сокеты.
20. Концепция квитирования.
21. Виды маршрутизации. Простая маршрутизация. Адаптивная маршрутизация.
22. Администрирование серверов. Система Доменных имен
23. Электронная почта в IP-сетях.
24. Взаимодействие ЭВМ с помощью протокола Telnet.
25. Обмен файлами. Служба FTP.
26. Основные подходы к планированию корпоративной сети.
27. Построения транспортной системы корпоративной сети.
28. Создание корпоративной сети на основе Active Directory.
29. Контроллеры домена. Назначение. Примеры использования.

5.4. Перечень вопросов к итоговому контролю знаний по дисциплине

Вопросы к экзамену:

1. Основные утилиты Windows.

2. Создание виртуальных дубликатов файлов.
3. Этапы загрузки Windows.
4. Встроенная оптимизация Windows.
5. Понятие пользовательской учетной записи. Типы учетных записей.
6. Группы безопасности. Встроенные группы безопасности.
7. Защита учетных записей в Windows.
8. Использование групповой политики.
9. Администрирование файлов и папок.
10. Утилиты администрирования. Примеры.
11. Имена пользователей и полные имена.
12. Запуск программ в системе Windows. Совместимость версий.
13. Обеспечение безопасности учетной записи администратора.
14. Совместное использование файлов в сети.
15. Совместное использование устройств в сети.
16. Права доступа. Наследование прав доступа.
17. Обслуживание системы и контроль над ней. Управление компьютером.
18. Присвоение (назначение) IP-адресов.
19. Администрирование с применением консоли. Утилиты.
20. Утилита командной строки Net User.
21. Настройка прав доступа с консоли.
22. Администрирование Web-сервера.
23. Настройка брандмауэра в системе.
24. Организация IP-брандмауэра встроенными средствами Windows.
25. Проверка безопасности с помощью программы MBSA.
26. Active Directory. Назначение, возможности, примеры использования. Создание корпоративной сети на основе Active Directory.
27. Контроллеры домена. Назначение. Примеры использования.
28. Обеспечение безопасности учетной записи администратора. Примеры.

Раздел 6. Перечень учебной литературы, необходимой для освоения дисциплины

6.1. Основная литература

1. Власов, Ю. В. Администрирование сетей на платформе MS Windows Server : учебное пособие / Ю. В. Власов, Т. И. Рицкова. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 622 c. — ISBN 978-5-4497-0649-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/97536.html.

2. Сысоев, Э. В. Администрирование компьютерных сетей : учебное пособие / Э. В. Сысоев, А. В. Терехов, Е. В. Бурцева. — Тамбов : Тамбовский государственный технический университет, ЭБС АСВ, 2017. — 79 c. — ISBN 978-5-8265-1802-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/85916.html.

3. Гончарук, С. В. Администрирование ОС Linux : учебное пособие / С. В. Гончарук. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 163 c. — ISBN 978-5-4497-0299-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89414.html.

6.2. Дополнительная литература

4. Костюк, А. И. Администрирование баз данных и компьютерных сетей : учебное пособие / А. И. Костюк, Д. А. Беспалов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 127 c. — ISBN 978-5-9275-3577-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/107941.html.

5. Сергеев, А. Н. Администрирование сетей на основе Windows : лабораторный практикум / А. Н. Сергеев, Е. В. Татьянич. — Волгоград : Волгоградский государственный социально-педагогический университет, 2017. — 48 c. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/62772.html.

6.3. Другие источники информации и средства обеспечения освоения дисциплины

6. Журнал «Бизнес. Образование. Право. Вестник Волгоградского института бизнеса» [Электронный ресурс] // URL: http://vestnik.volbi.ru/

7. Журнал «Сети» [Электронный ресурс] // URL: http://www.osp.ru/nets.

8. Издательство “Открытые системы” [Электронный ресурс] // URL: http://www.osp.ru.

9. Официальный сайт компании Microsoft [Электронный ресурс] // URL: http://www.microsoft.com.

10. ПО для организации конференций

11. СПС «КонсультантПлюс», URL: http://www.consultant.ru/document/cons_doc

12. СПС «ГАРАНТ», URL: http://base.garant.ru/

13. ЦИТ Форум [Электронный ресурс] // URL: http://citforum.ru.

Раздел 7. Материально-техническая база и информационные технологии

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

Материально-техническое обеспечение дисциплины включает в себя учебные аудитории для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы обучающихся.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения. Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети Интернет.

Дисциплина может реализовываться с применением дистанционных технологий обучения. Специфика реализации дисциплины с применением дистанционных технологий обучения

устанавливается дополнением к рабочей программе. В части не противоречащей специфике, изложенной в дополнении к программе, применяется настоящая рабочая программа.

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине с применением дистанционных образовательных технологий включает в себя:

Компьютерная техника, расположенная в учебном корпусе Института (ул. Качинцев, 63, кабинет Центра дистанционного обучения):

1. Intel i 3 3.4Ghz\ОЗУ 4Gb\500GB\RadeonHD5450
2. Intel PENTIUM 2.9GHz\ОЗУ 4GB\500GB

3 личные электронные устройства (компьютеры, ноутбуки, планшеты и иное), а также средства связи преподавателей и студентов.

Информационные технологии, необходимые для осуществления образовательного процесса по дисциплине с применением дистанционных образовательных технологий включают в себя:

- система дистанционного обучения (СДО) (Learning Management System) (LMS) Moodle (Modular Object-Oriented Dynamic Learning Environment);
- электронная почта;
- система компьютерного тестирования;
- электронная библиотека IPRbooks;
- система интернет-связи skype;
- телефонная связь;
- ПО для проведения конференции

Обучение обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья осуществляется посредством применения специальных технических средств в зависимости от вида нозологии.

При проведении учебных занятий по дисциплине используются мультимедийные комплексы, электронные учебники и учебные пособия, адаптированные к ограничениям здоровья обучающихся.

Лекционные аудитории оборудованы мультимедийными кафедрами, подключенными к звуковым колонкам, позволяющими усилить звук для категории слабослышащих обучающихся, а также проекционными экранами, которые увеличивают изображение в несколько раз и позволяют воспринимать учебную информацию обучающимся с нарушениями зрения.

При обучении лиц с нарушениями слуха используется усилитель слуха для слабослышащих людей Cyber Ear модель HAP-40, помогающий обучаемым лучше воспринимать учебную информацию.

Обучающиеся с ограниченными возможностями здоровья, обеспечены печатными и электронными образовательными ресурсами (программы, учебники, учебные пособия, материалы для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

для лиц с нарушениями зрения:

- в форме электронного документа;
- в форме аудиофайла;

для лиц с нарушениями слуха:

- в печатной форме;
- в форме электронного документа;

для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Раздел 8. Методические указания для обучающихся по освоению дисциплины

Для успешного усвоения материала курса требуются значительное время, концентрация внимания и усилия: посещение лекционных занятий и конспектирование преподаваемого материала, работа с ним дома, самостоятельная проработка материала рекомендуемых учебников и учебных пособий при самостоятельной подготовке. Особое внимание следует обратить на выполнение практических работ, практических задач по СРО, тестовых вопросов.

При самостоятельной работе с учебниками и учебными пособиями полезно иметь под рукой справочную литературу (энциклопедии) или доступ к сети Интернет, так как могут встречаться новые термины, понятия, которые раньше обучающиеся не знали.

Цель практических занятий по дисциплине «Сетевое администрирование» - закрепление знаний по определенной теме, приобретенных в результате прослушивания лекций, получения консультаций и самостоятельного изучения различных источников литературы. При выполнении данных работ обучающиеся должны будут глубоко изучить принцип работы и настройку сетевого программного обеспечения. Получить навыки его настройки и обслуживания.

Перед практическим занятием обучающийся должен детально изучить теоретические материалы вопросов практики в учебниках, конспектах лекций, периодических журналах и прочее. Если при выполнении практического задания у обучающегося остаются неясности, то ему необходимо оперативно обратиться к преподавателю за уточнением.

После выполнения практического работы обучающиеся должны выполнить самостоятельную работу. Самостоятельная работа включает в себя индивидуальное задание по пройденной теме. Таким образом, каждый обучающийся выполняет только свой вариант задания. Выполнение практических заданий сопровождается выполнением письменного отчета в тетради. Отчет должен выполняться аккуратно, быть легко читаемым подчерком, при этом допускаются общепринятые сокращения.

При дистанционном выполнении практических работ обучающийся может самостоятельно приобрести операционные системы Windows XP, Windows 7, Windows 8, Windows 10, Windows 2008 Server, Windows 2012 Server. Ответственность за установку и настройку программного обеспечения в данном случае ложится на самого обучающегося. Следует воспользоваться методическими указаниями по установке данных программных систем.

Результаты выполненных заданий оцениваются с учетом теоретических знаний по соответствующим разделам дисциплины, техники выполнения работы, объективности и обоснованности принимаемых решений в процессе работы с данными, качества оформления. Переход к выполнению следующей практического работы допускается только после отчета выполненной работы.

Учебно-методическое издание

Рабочая программа учебной дисциплины

Сетевое администрирование

(Наименование дисциплины в соответствии с учебным планом)

Филиппов Михаил Владимирович

(Фамилия, Имя, Отчество составителя)