МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное
образовательное учреждение Московской области
«Шатурский энергетический техникум»
(ГБПОУ МО «ШЭТ»)

УТВЕРЖДАЮ
зам. директора по УМР
_____С.А. Косова
«02» 06 2023 г.

РАБОЧАЯ ПРОГРАММА

ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Эксплуатация объектов сетевой инфраструктуры

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

г. Шатура
2023 г.

Рабочая программа учебной дисциплины разработана в соответствии Федеральным государственным образовательным стандартом (далее - ФГОС) по специальности программы подготовки специалистов среднего звена (далее ППССЗ) 09.02.06 Сетевое и системное администрирование (базовой подготовки).

Организация-разработчик: ГБПОУ МО «ШЭТ»

Разработчики:

Аверьянов Алексей Станиславович, преподаватель специальных дисциплин

Еремина Елена Алексеевна, преподаватель специальных дисциплин

ОДОБРЕНО

цикловой комиссией преподавателей специальности УГС Информатика и вычислительная техника и Информационная безопасность (09.02.06, 10.02.04)

Протокол № 11 от «01» 06 2023 г.

Председатель ЦК: _____ Е.А. Еремина

Внутренний рецензент: _____ Е.В. Лялина, методист ГБПОУ МО «ШЭТ»

СОДЕРЖАНИЕ

1. **ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** **4**
2. **РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** **5**
3. **СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** **6**
4. **УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** **21**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

1.1.Область применения программы

Программа МДК 03.02 Безопасность компьютерных сетей профессионального модуля является частью основной профессиональной образовательной программы базовой подготовки в соответствии с ФГОС по специальности СПО: 09.02.06 Сетевое и системное администрирование в части освоения основного вида профессиональной деятельности (ВПД): Эксплуатация объектов сетевой инфраструктуры и соответствующих профессиональных компетенций (ПК):

ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.

ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.

ПК 3.3. Использовать инструментальные средства для эксплуатации сетевых конфигураций.

ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.

1.2 Цели и задачи модуля - требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;
- удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;
- организации бесперебойной работы системы по резервному копированию и восстановлению информации;
- поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры;

уметь:

- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- использовать схемы послеаварийного восстановления работоспособности сети эксплуатировать технические средства сетевой инфраструктуры;
- наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;
- устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;

знать:

- архитектуру и функции систем управления сетями, стандарты систем управления;
- задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;

- средства мониторинга и анализа локальных сетей;
- классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;
- правила эксплуатации технических средств сетевой инфраструктуры;
- расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;
- методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;
- основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности, в том числе профессиональными и общими компетенциями:

Код	Наименование результата обучения
ПК 3.1	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
ПК 3.2	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
ПК 3.3.	Эксплуатация сетевых конфигураций.
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.
ОК 11.	Планировать предпринимательскую деятельность в профессиональной сфере

3. Структура профессионального модуля

Код профессиональных компетенций	***Наименования междисциплинарных курсов профессионального модуля***	***Всего часов*** *(макс. учебная нагрузка и практики)*	***Объем времени, отведенный на освоение междисциплинарного курса (курсов)***					***Практика***	
			Обязательная аудиторная учебная нагрузка обучающегося			***Самостоятельная работа обучающегося***		***Учебная,*** *часов*	***Производственная (по профилю специальности),*** *часов (если предусмотрена рассредоточенная практика)*
			Всего, *часов*	***в т.ч. лабораторные работы и практические занятия,*** *часов*	***в т.ч., курсовая работа (проект),*** *часов*	***Всего,*** *часов*	***в т.ч., курсовая работа (проект),*** *часов*		
1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
ПК 3.1-3.4	**МДК.03.01.** Эксплуатация объектов сетевой инфраструктуры	***180***	***90***	***88***	*	***2***	*	*****	*****
ПК 3.1-3.4	**МДК.03.02.** Безопасность функционирования информационных систем	***21***	***108***	***106***	*	***4***	*	*****	*****
УП.03Учебная практика		***108***						***108***	
ПП.03 Производственная практика		***144***							***144***
Консультации		***14***							
Экзамен по модулю		***16***							
Всего:		***680***	***198***	***194***		***6***			

Основные образовательные технологии: Информационно-коммуникационные, игровые технологии, применение деятельностного подхода в организации обучения, технологии модульного, разноуровневого, проблемного обучения, задачное обучение, кейс-технологии, технология учебного портфолио.

3.2. Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
МДК 03.01 Эксплуатация объектов сетевой инфраструктуры		**180**	
Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры	**Содержание**	**52**	
	1. Архитектура системы управления.		1
	2. Структура системы управления.		1
	3. Уровни управления.		1
	4. Области управления.		1
	5. Протоколы управления.		1
	6. Управление отказами.		2
	7. Учет работы сети.		1
	8. Резервное копирование данных. Хранилища данных		2
	9. Аудит сетевой инфраструктуры.		2
	10. Технология IP-телефонии.		2
	11. Взаимодействие протокола VoIP.		1
	12. Протокол H323.		2
	13. Принципы построения протокола SIP.		2
	14. QoS.		1
	15. Интегрирование обслуживание IntServ.		1
	16. Протокол резервирования ресурсов.		2
	17. Технология MPLS.		2
	18. Сравнение технологий обеспечения QoS.		2
	19. Методы резервного копирования.		3
	20. Виртуализация сервера		1
	21. Несанкционированное ПО, паразитная нагрузка		2
	22. Техническая и проектная документация		3

	23. Физическая карта сети		3
	24. Логическая схема компьютерной сети		2
	25. Проверка объектов сетевой инфраструктуры и профилактические работы		2
	26. Управление конфигурацией. Изучение базовых команд настройки сетевой ОС		1
	27. Учет трафика в сети		2
	28. Архитектура системы управления.		1
	Практические занятия	**42**	
	1. Анализ сетевого трафика средствами Сетевого монитора		
	2. Запись данных средствами Сетевого монитора		
	3. Управление конфигурацией. Управление производительностью, безопасностью сети		
	4. Устранение неполадок с помощью сетевых утилит		
	5. Диагностика сети и Netdiag		
	6. Удаленное администрирование		
Тема 1.2. Схема послеаварийного восстановления	**Содержание**	**38**	
	1. Принципы планирования восстановления работоспособности сети при аварийной ситуации		2
	2. Допущения при разработке схемы послеаварийного восстановления.		2
	3. Организация работ по восстановлению функционирования системы		2
	4. План восстановления системы		3
	5. Принципы локализации неисправностей.		3
	6. Контрольно-измерительная аппаратура.		3
	7. Сервисные платы и комплексы.		2
	8. Программные средства диагностики.		3
	9. Номенклатура и особенности работы тест-программ.		2
	10. Диагностика неисправностей средств сетевых коммуникаций.		3
	11. Контроль функционирования аппаратно-программных комплексов.		3
	12. Действия при не работающей сети, при медленной сети.		3
	13. Действия при не стабильно работающей сети.		3
	14. Допущения при разработке схемы послеаварийного восстановления.		3
	15. Организация работ по восстановлению функционирования системы.		3
	16. План восстановления системы.		2
	Практические занятия	**46**	
	1. Эксплуатация технических средств сетевой инфраструктуры		

	2. Восстановление работоспособности сети после сбоя		
	3. Настройка конфигурации коммутатора		
	4. Разработка плана восстановления		
	5. Использование схемы послеаварийного восстановления сети		
	6. Возврат к нормальному функционированию системы		
	7. Работа контрольно-измерительной аппаратуры		
	8. Программная диагностика неисправностей		
	Самостоятельная работа	2	
	Создать сообщение на тему «Виртуальные частные сети» Создать презентацию на тему «Адресация в IP –сетях» Создать презентацию на тему «Взаимодействие между разнородными сетями» Создать сообщение «Сети на основе сервера. Кластеризация сервера» Подготовить инструкцию на тему «Настройка сети в Windows Vista» Подготовить презентацию на тему «Операционная система UNIX» Подготовить презентацию на тему «Операционная система Apple Talk» Подготовить сообщение на тему «Операционная система Banyan VINES» Составить кроссворд на тему «Доменная система имен (DNS)» Подготовить сообщение на тему «Топология коммутации пакетов и ретрансляция кадра (Frame Relay)» Подготовить презентацию на тему «Современные проблемы управления ИТ-инфраструктурой» Подготовить реферат на тему «Средства продуктов Unicenter для управления ИТ-инфраструкту- рой» Подготовить сравнительную таблицу по теме «Комплекс программных продуктов Hewlet – Packard ориентированных на управление корпоративными ИТ любого масштаба» Подготовить сообщение на тему «Основные назначения средств Microsoft Systems Management Server» Подготовить презентацию на тему «Основные назначения средств Microsoft Operations Manager» Составить инструкцию по использованию утилиты Acronis для изучения безопасной зоны Acronis, Составить инструкцию по теме «Создание контрольной точки восстановления с помощью Acronis» Создать базу данных на примере учебной группы;		

	Разработать план восстановления работоспособности сети на примере одной взятой организации (техникума, офиса) Разработать инструкцию по теме «Поиск неисправностей по принципу локализации неисправностей конкретного оборудования» Составить сообщение на тему «Принцип работы новых контрольно-измерительных аппаратов»		

МДК 03.02. Безопасность функционирования информационных систем				**218**	
Тема 2.1. Основы информационной безопасности	Содержание учебного материала:			**28**	2
	1	Понятие угрозы информационной безопасности. Виды противников или «нарушителей».			
	2	Виды возможных нарушений информационной системы.			
	3	Анализ угроз информационной безопасности.			
	4	Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).			
	5	Свойства информации: конфиденциальность, доступность, целостность.			
	6	Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб.			
	7	Примеры реализации угроз информационной безопасности.			
	8	Защита информации. Основные принципы обеспечения информационной безопасности.			
	9	Причины, виды и каналы утечки информации.			
	10	Использование защищенных компьютерных систем.			
	11	Общие принципы построения защищенных систем			
	12	Иерархический метод разработки защищенных систем. Структурный принцип.			
	13	Профили защиты. Базовые и полные функциональные профили.			

	14	Исследование корректности реализации и верификации автоматизированных систем.		
	15	Спецификация требований, предъявляемых к системе.		
	Практические занятия		**20**	2
	1	Подготовка предварительного варианта концепции информационной безопасности компании.		
	2	Построение структуры нормативно-правовых документов деятельности компании на базе российского законодательства в сфере информационного права.		
	3	Подготовка описания охраняемой информации, «портрета» нарушителя, модели угроз, построение модели информационной безопасности.		
	4	Разработка параметров защищенности программных и информационных систем компании и программы ИБ		
	5	Разработка модели общей и частных политик информационной безопасности компании. Подготовка нормативного документа для введения в действия политики ИБ.		
	6	Описание структуры информационных рисков, построение модели процесса оценки рисков, составление списка мероприятий для уменьшения рисков. Обзор программных продуктов для оценки информационных рисков.		
	7	Формирование опорной системы стандартов для реализации информационной безопасности предприятия.		
Тема 2.2. Программно-технические методы защиты сетей	Содержание учебного материала		**32**	2
	1	Общее представление о структуре защищенной информационной системы.		
	2	Особенности современных информационных систем.		
	3	Факторы, влияющие на безопасность информационной системы.		
	4	Понятие информационного сервиса безопасности. Виды сервисов безопасности.		

	5	Сервисы управления доступом. Механизмы доступа данных в сетевых операционных системах.		
	6	Ролевая модель управления доступом. Примеры реализации моделей управления доступом.		
	7	Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.		
	8	Анализ событий, средства выявления уязвимостей в информационной системе.		
	9	Обеспечение защиты корпоративной информационной сети от атак на информационные сервисы.		
	10	Организационная структура, система обеспечения информационной безопасности.		
	11	Общие угрозы и уязвимости на уровне пользователей.		
	12	Общие угрозы и уязвимости на уровне устройств.		
	13	Общие угрозы и уязвимости на уровне локальной сети.		
	14	Общие угрозы частичного «облака»		
	15	Распространенные угрозы общедоступного «облака»		
	16	Обязанности ОИБ в подразделениях		
	Практические занятия		**24**	2
	1	Установка информационных систем, согласно технической документации.		
	2	Установка и тестирование информационных систем.		
	3	Эксплуатация информационных систем, обеспечение антивирусной защиты.		
	4	Выявление и описание каналов утечки информации на конкретном примере.		
	5	Описание сопровождения технологических процессов в системах защиты информационных сетей на конкретном примере.		
	6	Определение угроз безопасности, каналов утечки информации, построение модели нарушителя.		
	7	Построение модели нарушителя.		
	8	Описание универсальных механизмов защиты информации вычислительных систем и сетей.		

	9	Описание формирования назначения ролей пользователям информационной системы.		
	10	Установка программных средств защиты (программные прокси-серверы, диагностические программы или т.п.).		
Тема 2.3. Инфраструктура открытых ключей. Защищенные протоколы, межсетевые экраны	Содержание учебного материала		**24**	2
	1	Защита Интернет-подключений, функции и назначение межсетевых экранов.		
	2	Понятие демилитаризованной зоны.		
	3	Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах.		
	4	Протокол IPSec, его особенности. Использование протокола IPSec для обеспечения аутентификации и защиты передачи данных.		
	5	Протоколы AH, ESP. Обмен ключами Интернет (IKE). Безопасные ассоциации.		
	6	Туннельные протоколы. Протоколы PPTP, L2TP/IPSec.		
	7	Использование службы RRAS в операционной системе MS Windows Server для организации VPN - подключений		
	8	Защита передачи данных. Протокол SSL, его функции и назначение.		
	9	Организация защиты несанкционированных подключений к веб-ресурсам.		
	10	Центры сертификации. Выдача и использование цифровых сертификатов.		
	11	Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы.		
	12	Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.		
	Практические занятия		**22**	2
	1	Установка программных средств защиты (программные прокси-серверы, диагностические программы или т.п.)		
	2	Обнаружение программных закладок.		

	3	Обнаружение троянского коня.		
	4	Выполнение работы по обезвреживанию разрушающего программного воздействия		
	5	Использование встроенных средств ОС.		
	6	Описание механизмов и принципов работы систем шифрования с открытым ключом.		
	7	Составление описания основных классов вирусов.		
	8	Проведение анализа сравнительных характеристик у каналов утечки информации.		
Тема 2.4. Организационные меры защиты	Содержание учебного материала		**24**	2
	1	Состав и организационная структура системы обеспечения информационной безопасности.		
	2	Регламентация процессов и действий персонала.		
	3	Соглашение-обязательство сотрудника.		
	4	Регламентация процесса авторизации.		
	5	Регламентация процесса внесения изменений в аппаратно-программную конфигурацию подсистем.		
	6	Регламентация процесса информационного обмена со сторонними организациями. Инструкция по обеспечению информационной безопасности при работе в Internet.		
	7	Регламентация применения средств защиты информации.		
	8	Регламентация действий в нештатных ситуациях.		
	9	Определение требований к защищенности ресурсов.		
	10	Иерархический метод разработки защищенных систем.		
	11	Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований, предъявляемых к системе.		
	12	Теория безопасных систем.		
	Практические занятия		**40**	2

	1	Исследование проблем обеспечения информационной безопасности национальных платежных систем на базе российских интеллектуальных карт.		
	2	Исследование проблем создания и развития национальной системы управления цифровыми сертификатами.		
	3	Исследование проблем безопасности общероссийской информационной инфраструктуры в условиях ее вхождения в глобальные инфраструктуры.		
	4	Исследование проблем информационной безопасности корпоративных сетей.		
	5	Проблемы лицензирования деятельности в области информационно-телекоммуникационных систем.		
	6	Анализ тенденций в развитии глобальной информационной сети и состояния участия в ней России.		3
	7	Исследование фундаментальных проблем теоретической криптографии и смежных с ней областей математики.		
	8	Исследование криптографических проблем.		
	9	Исследование методов криптографического анализа современных шифрсистем.		
	Самостоятельная работа при изучении раздела 2 ПМ 03: Систематическая проработка конспектов занятий, учебной и специальной литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите.		**4**	
	Учебная практика		**108**	
	Производственная практика.		**144**	
	Консультации		**14**	
	Экзамен по МДК 03.01		**8**	
	Экзамен по ПМ.03		**8**	
		всего:	680	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Оборудование кабинета и рабочих мест лаборатории «Компьютерных сетей»:
- автоматизированные рабочие места на 12-15 обучающихся;
- автоматизированное рабочее место преподавателя;
- специализированная мебель;
- комплект нормативных документов;
- комплект учебно-методической документации.
- проектор;
- сканер;
- принтер;
- программное обеспечение общего и профессионального назначения.

Оборудование лаборатории и рабочих мест лаборатории **«Организация и принципы построения компьютерных систем»**:
Для выполнения практических лабораторных занятий курса в группах (до 15 человек) требуются компьютеры и периферийное оборудование в приведенной ниже конфигурации

- Компьютер обучающегося (аппаратное обеспечение: не менее 2 сетевых плат, процессор Процессор не ниже Core i3, оперативная память объемом не менее 8 Гб; HD 500 Gb или больше программное обеспечение: лицензионное ПО-CryptoAPI операционные системы Windows, UNIX, MS Office, пакет САПР).
- Компьютер преподавателя (аппаратное обеспечение: не менее 2 сетевых плат, процессор Процессор не ниже Core i3, оперативная память объемом не менее 8 Гб; HD 500 Gb или больше программное обеспечение: лицензионное ПО-CryptoAPI операционные системы Windows, UNIX, MS Office, пакет САПР).
- Сервер в лаборатории (аппаратное обеспечение: не менее 2 сетевых плат, 8-х ядерный процессор с частотой не менее трех ГГц, оперативная память объемом не менее 16 Гб, жесткие диски общим объемом не менее 2 Тб, программное обеспечение: Windows Server 2012 или более новая, лицензионные антивирусные программы, лицензионные программы восстановления данных, лицензионный программы по виртуализации.)
- 6 маршрутизаторов обладающими следующими характеристиками:

  ОЗУ не менее 256 Мб с возможностью расширения
  ПЗУ не менее 128 Мб с возможностью расширения
  USB порт: не менее одного стандарта USB 1.1
  Встроенные сетевые порты: не менее 2-х Ethernet скоростью не менее 100Мб/с.
  Внутренние разъёмы для установки дополнительных модулей расширения: не менее двух для модулей AIM.
  Разъёмы для подключения дополнительных интерфейсов: не менее 4; 2 из них для модулей типа HWIC, WIC, VIC, VWIC; 1для модулей типа WIC, VIC, VWIC; 1 для модулей VIC или VWIC.
  Наличие слота для установки аппаратного модуля шифрования и ускорения обработки трафика в VPN соединениях, поддерживающего стандарты DES, 3DES, AES 128, AES 192, AES 256
  Консольный порт для управления маршрутизатором через порт стандарта RS232: не менее одного с максимальной скоростью 115.2 кб/с.
  Встроенное программное обеспечение должно поддерживать статическую и динамическую маршрутизацию, поддерживать протоколы динамической маршрутизации RIP, RIP v2, IGRP, EIGRP, OSPF.

Маршрутизатор должен поддерживать управление через локальный последовательный порт и удалённо по протоколу telnet.
Оборудование должно поддерживать протокол обнаружения соседей CDP.
Иметь сертификаты безопасности и электромагнитной совместимости:
UL 60950, CAN/CSA C22.2 No. 60950, IEC 60950, EN 60950-1, AS/NZS 60950, EN300386, EN55024/CISPR24, EN50082-1, EN61000-6-2, FCC Part 15, ICES-003 Class A, EN55022 Class A, CISPR22 Class A, AS/NZS 3548 Class A, VCCI Class A, EN 300386, EN61000-3-3, EN61000-3-2, FIPS 140-2 Certification

– 6 коммутаторов обладающих следующими характеристиками:

Коммутатор с 24 портами Ethernet со скоростью не менее 100 Мб/с и 2 портами Ethernet со скоростью не менее 1000Мб/с
В коммутаторе должен присутствовать разъём для связи с ПК по интерфейсу RS-232. При использовании нестандартного разъёма в комплекте должен быть соответствующий кабель или переходник для COM разъёма.
Скорость коммутации не менее 16Gbps
ПЗУ не менее 32 Мб
ОЗУ не менее 64Мб
максимальное количество VLAN 255
Доступные номера VLAN 4000
Поддержка протокола VTP (VLAN trunking protocol) для совместного использования единого набора VLAN на группе коммутаторов.
Размер MTU 9000б
Скорость коммутации для 64 байтных пакетов 6.5*106 пакетов/с
Размер таблицы мак адресов: не менее 8000 записей
Количество групп для IGMP трафика для протокола IPv4 255
Количество мак адресов в записях для службы QoS: 128 в обычном режиме и 384 в режиме QoS.
Количество мак адресов в записях контроля доступа: 384 в обычном режиме и 128 в режиме QoS.
Коммутатор должен поддерживать управление через локальный последовательный порт, удалённое управление по протоколу telnet.
Коммутатор должен поддерживать протокол обнаружения соседей CDP.
Оборудование должно поддерживать следующие стандарты:
В области протоколов передачи
IEEE 802.1D Spanning Tree Protocol, IEEE 802.1p CoS Prioritization, IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab (LLDP), IEEE 802.3ad, IEEE 802.3af, IEEE 802.3ah (100BASE-X single/multimode fiber only), IEEE 802.3x full duplex on, 10BASE-T, 100BASE-TX, and 1000BASE-T, IEEE 802.3 10BASE-T specification, IEEE 802.3u 100BASE-TX specification, IEEE 802.3ab 1000BASE-T specification, IEEE 802.3z 1000BASE-X specification, RMON I and II standards, SNMP v1, v2c, and v3
В области взаимодействия с другими сетевыми устройствами, диагностики и удалённого управления
RFC 768 — UDP, RFC 783 — TFTP, RFC 791 — IP, RFC 792 — ICMP, RFC 793 — TCP, RFC 826 — ARP, RFC 854 — Telnet, RFC 951 - Bootstrap Protocol (BOOTP), RFC 959 — FTP, RFC 1112 - IP Multicast and IGMP, RFC 1157 - SNMP v1, RFC 1166 - IP Addresses, RFC 1256 - Internet Control Message Protocol (ICMP) Router Discovery, RFC 1305 — NTP, RFC 1492 — TACACS+, RFC 1493 - Bridge MIB, RFC 1542 - BOOTP extensions, RFC 1643 - Ethernet Interface MIB, RFC 1757 — RMON, RFC 1901 - SNMP v2C, RFC 1902-1907 - SNMP v2, RFC 1981 - Maximum Transmission Unit (MTU) Path Discovery IPv6, FRC 2068 — HTTP, RFC 2131 — DHCP, RFC 2138 — RADIUS, RFC 2233 - IF MIB v3, RFC 2373 - IPv6

Aggregatable Addrs, RFC 2460 — IPv6, RFC 2461 - IPv6 Neighbor Discovery, RFC 2462 - IPv6 Autoconfiguration, RFC 2463 - ICMP IPv6, RFC 2474 - Differentiated Services (DiffServ) Precedence, RFC 2597 - Assured Forwarding, RFC 2598 - Expedited Forwarding, RFC 2571 - SNMP Management, RFC 3046 - DHCP Relay Agent Information Option
RFC 3376 - IGMP v3, RFC 3580 - 802.1X RADIUS.
Иметь сертификаты безопасности и электромагнитной совместимости:
UL 60950-1, Second Edition, CAN/CSA 22.2 No. 60950-1, Second Edition, TUV/GS to EN 60950-1, Second Edition, CB to IEC 60950-1 Second Edition with all country deviations, CE Marking, NOM (through partners and distributors), FCC Part 15 Class A, EN 55022 Class A (CISPR22), EN 55024 (CISPR24), AS/NZS CISPR22 Class A, CE, CNS13438 Class A, MIC, GOST, China EMC Certifications.

- Набор последовательных кабелей (входит в комплект поставки оборудования для сетевой академии Cisco) со следующими характеристиками:
  Кабель для соединения разъёмов Smart Serial с V.35 (Winchester) female разъёмом. -6 шт.
  Кабель для соединения разъёмов Smart Serial с V.35 (Winchester) male разъёмом. – 6шт.
- Модули для последовательных соединений в количестве 6 шт., подходящие для маршрутизаторов со следующими характеристиками:
  Модуль для последовательных соединений HWIC-2A/S должен содержать два порта типа Smart Serial с поддержкой скоростей до 128кб/с для синхронных линий и 115.2кб/с для асинхронных. Модуль должен поддерживать стандарты соединения с DTE/DCE оборудованием V.35, RS-232, RS-449, RS-530, RS-530A, X.21.
- 2 беспроводных маршрутизатора Linksys (предпочтительно серии EA 2700, 3500, 4500) или аналогичные устройства SOHO
- IP телефоны от 3 шт.
- Программно-аппаратные шлюзы безопасности от 2 шт.
- 1 компьютер для лабораторных занятий с ОС Microsoft Windows Server, Linux и системами виртуализации
- 12-15 компьютеров или ноутбуков для лабораторных занятий (Microsoft Windows) и Linux

Реализация профессионального модуля предполагает учебную и производственную практики, которые можно проводить как сосредоточенно, т.е. после изучения МДК, так и распределено.