Санкт-Петербургское государственное
бюджетное профессиональное образовательное учреждение
«Радиотехнический колледж»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

по программе подготовки специалистов среднего звена

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

Санкт-Петербург

2021г.

Одобрено на заседании
цикловой методической комиссии

Протокол №_1_ от «_27_» _08_ 20_21_ г.

Председатель _____

Утверждаю
заместитель директора по УМР

_____

«_27_» _08_ 20_21_ г.

Рекомендовано на заседании
Методического совета

Протокол №_1_ от «_27_» _08_ 20_21_ г.

Рабочая программа профессионального модуля ПМ.03 «Эксплуатация объектов сетевой инфраструктуры» разработана на основе требований Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование, утвержденного приказом Министерства образования и науки РФ 09.12.2016 №1548 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование» (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016г., регистрационный №44978).

Организация-разработчик:
Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Радиотехнический колледж»

Разработчик: Дубровин Виталий Александрович, преподаватель первой квалификационной категории

СОДЕРЖАНИЕ

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

1.1. Область применения программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.06 «Сетевое и системное администрирование» в части освоения основного вида профессиональной деятельности ВД 3 «Эксплуатация объектов сетевой инфра-структуры» и соответствующих профессиональных (ПК) компетенций:

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. Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации

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

ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.

ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

1.2. Цели и задачи модуля – требования к результатам освоения профессионального модуля

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

иметь практический опыт в:

- обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя;
- поддержке пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры;
- удаленном администрировании и восстановлении работоспособности сетевой инфраструктуры;

уметь:

– выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;

– осуществлять диагностику и поиск неисправностей всех компонентов сети;

– выполнять действия по устранению неисправностей

знать:

– архитектуру и функции систем управления сетями, стандарты систем управления;

– средства мониторинга и анализа локальных сетей;

– методы устранения неисправностей в технических средствах

Программа профессионального модуля разработана с учетом требований стандартов WorldSkills.

1.3. Количество часов на освоение программы профессионального модуля:

всего – 994 часа, в том числе:

– учебной нагрузки во взаимодействии с преподавателем – 480 час;

– самостоятельной работы обучающегося – 46 часов;

– учебной практики – 216 часов;

– производственной практики – 252 часов.

Часы вариативной части используются для изучения тем:

Тема 2.1. Основные понятия информационной безопасности

Тема 2.2. Принципы криптографической зашиты информации

Тема 2.4 Безопасность компьютерных сетей на основе стека протоколов TCP/IP.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВД) Эксплуатация объектов сетевой инфраструктуры, в том числе профессиональными (ПК) и общими (ОК) компетенциями.

Код	Наименование результатов 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.	Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации
ПК 3.5.	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта
ПК 3.6.	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

Перечень общих компетенций (ОК)

Код	Наименование общих компетенций
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 традиционных 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 И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля

Коды профессиональных компетенций	**Наименования МДК профессионального модуля**	**Всего часов** *(макс. учебная нагрузка и практики)*	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**		**Экзамен по модулю**
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная**	
			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**	**11**
ПК 3.1-ПК 3.6 ОК 01-11	МДК 03.01. Эксплуатация объектов сетевой инфраструктуры	**230**	**200**	**92**	**–**	**30**	**–**	**–**	**-**	**-**
ПК 3.1-ПК 3.6 ОК 01-11	МДК 03.02. Безопасность компьютерных сетей	**290**	**274**	**84**	**–**	**16**	**-**	**-**	**–**	**-**
ПК 3.1-ПК 3.6 ОК 01-11	Учебная практика	**216**						**216**	**-**	**-**
ПК 3.1-ПК 3.6 ОК 01-11	Производственная практика	**252**							**252**	**-**
Экзамен по модулю		**6**								**6**
		994	**474**	**176**	**–**	**46**	**–**	**216**	**252**	**6**

3.2 Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов
1	2	3
МДК.03.01. Эксплуатация объектов сетевой инфраструктуры		**230**
Раздел 1. Эксплуатация объектов сетевой инфраструктуры		**230**
Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры	**Содержание**	
	1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети.	78
	2. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.	
	3. Полоса пропускания, паразитная нагрузка.	
	4. Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).	
	5. Наращивание длины сегментов сети; замена существующей аппаратуры.	
	6. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.	
	7. Техническая и проектная документация. Паспорт технических устройств.	
	8. Физическая карта всей сети; логическая топология компьютерной сети.	
	9. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры.	
	10. Проверка объектов сетевой инфраструктуры и профилактические работы	
	11. Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.	
	12. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств.	
	13. Протокол SNMP, его характеристики, формат сообщений, набор услуг.	
	14. Задачи управления: анализ производительности и надежности сети.	
	15. Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	
	Практические работы	

	1. Оконцовка кабеля витая пара	46
	2. Заделка кабеля витая пара в розетку	
	3. Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену	
	4. Тестирование кабеля	
	5. Поддержка пользователей сети.	
	6. Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)	
	7. Выполнение действий по устранению неисправностей	
	8. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.	
	9. Оформление технической документации, правила оформления документов	
	10. Протокол управления SNMP	
	11. Основные характеристики протокола SNMP	
	12. Набор услуг (PDU) протокола SNMP	
	13. Формат сообщений SNMP	
	14. Задачи управления: анализ производительности сети	
	15. Задачи управления: анализ надежности сети	
	16. Управление безопасностью в сети.	
	17. Учет трафика в сети	
	18. Средства мониторинга компьютерных сетей	
	19. Средства анализа сети с помощью команд сетевой операционной системы	
	20. Финальная комплексная практическая работа по эксплуатации объектов сетевой инфраструктуры	
Тема 1.2. Эксплуатация систем IP-телефонии	**Содержание**	
	1. Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323. Установка и поддержка соединения H.323. Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper. Многопользовательские конференции. Обеспечение отказоустойчивости.	78
	2. Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты. Функциональные компоненты SIP. Сообщения SIP. Адресация SIP. Модель установления соединения. Планирование отказоустойчивости.	
	3. Установка и инсталляция программного коммутатора. Монтажные процедуры. Процедуры инсталляции. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248. Создание аналоговых абонентов. Внутристанционная маршрутизация.	
	4. Управление программным коммутатором. Маршрутизация. Группы соединительных линий. Подключение станций с TDM (абонентский доступ TDM). Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP -абоненты. Группы абонентов. Дополнительные абонентские услуги.	

	5. Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт.	
	6. Восстановление работы сети после аварии. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных.	
	Практические работы	
	1. Настройка аппаратных IP-телефонов	46
	2. Настройка программных IP-телефонов, факсов	
	3. Развертывание сети с использованием VLAN для IP-телефонии	
	4. Настройка шлюза	
	5. Установка, подключение и первоначальные настройки голосового маршрутизатора	
	6. Настройка таблицы пользователей в голосовом маршрутизаторе	
	7. Настройка групп в голосовом маршрутизаторе	
	8. Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе	
	9. Настройка голосовых сообщений в маршрутизаторе	
	10. Настройка программно-аппаратной IP-АТС	
	11. Установка и настройка программной IP-АТС (например, Asterisk)	
	12. Тестирование кодеков. Исследование параметров качества обслуживания	
	13. Мониторинг и анализ соединений по различным протоколам	
	14. Мониторинг вызовов в программном коммутаторе	
	15. Создание резервных копий баз данных	
	16. Диагностика и устранение неисправностей в системах IP-телефонии	
	17. Финальная комплексная практическая работа по эксплуатации систем IP-телефонии	
Самостоятельная работа обучающихся		**30**
МДК.03.02. Безопасность компьютерных сетей		**290**
Раздел 2. Безопасность компьютерных сетей		**290**
Тема 2.1. Основные понятия информационной безопасности	**Содержание**	
	Введение в информационную безопасность. Стандартизированные признаки и понятия. Определение информационной безопасности. Виды информационной безопасности. Существенные признаки понятия: конфиденциальность, целостность, доступность, апеллируемость, подотчётность, достоверность. Безопасность информации. Безопасность автоматизированных информационных систем. Ценность информации. Уровень секретности.	57

	Юридические аспекты информационной безопасности. Нормативные документы в области информационной безопасности. Органы и подразделения, обеспечивающие информационную безопасность. Исторические аспекты возникновения и развития информационной безопасности.	
	Модель управления безопасности. Определение модели управления безопасности. Описание модели. Цель создания модели обеспечения информационной безопасности. Структура системы обеспечения информационной безопасности: руководство организации, подразделение информационной безопасности, администраторы штатных и дополнительных средств защиты, ответственные за ОИБ в подразделениях, конечные пользователи. Подробное описание уровней модели управления безопасностью: уровень принятия решений, уровень подготовки информации для принятия решений, уровень организации и контроля исполнения решений, уровень поддержки исполнения политики информационной безопасности, уровень исполнения политики информационной безопасности.	
	Угрозы информационной безопасности. Определение угроз информационной безопасности. Классификации: по аспекту информационно безопасности (угрозы конфиденциальности, целостности, доступности), по расположению источника угроз (внутренние, внешние), по размерам наносимого ущерба (общие, локальные, частные), по степени воздействия на информационную систему (пассивные, активные), по природе возникновения (естественные, искусственные). Классификация источников угроз информационной безопасности: антропогенные источники, техногенные источники, стихийные источники.	
	Методы и категории атак. Виды категорий атак. Описание атаки доступа. Определение атаки модификации. Определение атаки на отказ в обслуживание. Определение атаки на отказ от обязательств. Определение цели и мотивации для взлома. Описание методов взлома: коллективный доступ, слабые пароли, дефекты программирования, социальный инжиниринг, переполнение буфера, отказ в обслуживание (централизованные и распределённые атаки).	
	Службы информационной безопасности. Нормативные документы в области информационной безопасности. Органы и подразделения, обеспечивающие информационную безопасность. Исторические аспекты возникновения и развития информационной безопасности	
	Обеспечение информационной безопасности. Средства защиты от несанкционированного доступа (НСД): средства авторизации, мандатное управление доступом, избирательное управление доступом, управление доступом на основе ролей, журналирование. Системы анализа и моделирования информационных потоков (CASE-системы). Системы мониторинга сети: системы обнаружения и предотвращения вторжений (IDS/IPS), системы предотвращения утечек конфиденциальной информации (DLP-системы). Анализаторы протоколов. Межсетевые экраны. Криптографические средства: шифрование, циф-ровая подпись. Системы резервного копирования. Системы бесперебойного питания: источники бесперебойного питания (UPS), резервирование нагрузки, генераторы напряжения	
Тема 2.2. Принципы криптографической зашиты информации	**Содержание**	
	Понятие криптографии. Виды категорий атак. Описание атаки доступа. Определение атаки модификации. Определение атаки на отказ в обслуживание. Определение атаки на отказ от обязательств.	57

	Понятие криптоанализа. Описание методов взлома: метод частотного анализа, коллективный доступ, слабые пароли, дефекты программирования, социальный инжиниринг, переполнение буфера, отказ в обслуживание (централизованные и распределённые атаки).	
	Понятия о симметричных и асимметричных криптографических системах. Открытый ключ, закрытый ключ. Основные понятия о симметричных криптосистемах. Алгоритм MD. Основные понятия о асимметричных криптосистемах. Алгоритм AES.	
	Алгоритм DES. Алгоритм DataEncryptionStandart (DES) описание, принцип работы. Тройной DES. Шифрование паролей.	
	Инфраструктура открытых ключей. Описание инфраструктуры открытых ключей PKI.Объекты PKI. Основные задачиPKI. Архитек-тура PKI. Алгоритм обмена ключами Диффи-Хеллмана.	
	Криптографическая системах шифрования данных RSA. Алгоритм RSA. Генерация ключей RSA. Алгоритм Эль-Гамаля. Алгоритм цифровой подписи.	
	Криптографические хэш-функции. Описание хеш-функций. Алгоритм SHA, описание, принцип работы. Алгоритм MD5, описание, принцип работы. Безопасность хеш-функций.	
	Атаки на криптосистемы. Типы атак. Общие: атака с использованием только шифрованного текста, атака с известным от-крытым текстом, атака с избранным открытым текстом, атака с избранным шифрованным тек-стом, атаки, в основе которых лежат парадокс задачи о днях рождения, двухсторонняя атака. Специфичные: атака со связанным ключом, атака с избранным ключом.	
	Практические работы	
	1 Шифрование информации с использованием стандарта DES.	10
	2. Шифрование информации с использованием стандарта RSA.	
Тема 2.3. Безопасность компьютерных сетей	**Содержание**	
	Фундаментальные принципы безопасной сети Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.	47
	Безопасность Сетевых устройств OSI Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности	
	Авторизация, аутентификация и учет доступа (AAA) Свойства AAA. Локальная AAA аутентификация. Server-based AAA	
	Реализация технологий брандмауэра	

	ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах.	
	Реализация технологий предотвращения вторжения IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS	
	Безопасность локальной сети Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN	
	Криптографические системы Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей.	
	Реализация технологий VPN VPN. GRE VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN с исполь-зованием CLI. Реализация Site-to-site IPSec VPN с использованием CCP. Реализация Remote-access VPN	
	Управление безопасной сетью Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварий-ных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик без-опасности.	
	Cisco ASA Введение в Адаптивное устройство безопасности ASA. Конфигурация фаирвола на базе ASA с использованием графического интерфейса ASDM. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM.	
	Практические работы	
	3. Социальная инженерия	64
	4. Исследование сетевых атак и инструментов проверки защиты сети	
	5. Настройка безопасного доступа к маршрутизатору	
	6. Обеспечение административного доступа AAA и сервера Radius	
	7. Настройка политики безопасности брандмауэров	
	8. Настройка системы предотвращения вторжений (IPS)	
	9. Настройка безопасности на втором уровне на коммутаторах	
	10. Исследование методов шифрования	
	11. Настройка Site-to-SiteVPN используя интерфейс командной строки	
	12. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки	
	13. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM	

	14. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM	
	15. НастройкаClientless Remote Access SSL VPNs используя ASDM	
	16. Настройка AnyConnect Remote Access SSL VPN используя ASDM	
	17. Финальная комплексная лабораторная работа по безопасности	
Тема 2.4 Безопасность компьютерных сетей на основе стека протоколов TCP/IP.	**Содержание**	
	Классы атак в сетях на основе TCP/IP. Атаки на сетевом и транспортном уровне: ping flood, IP spoofing, пассивное сканирование. MITM атаки. Способы предотвращение атак.	29
	DOS и DDOS атаки. Атаки отказа в обслуживании DDOS. Виды DDOS атак. Предотвращение DDOS атак.	
	Технологии аутентификация. Определение аутентификации. Элементы системы аутентификации: субъект, характеристика субъекта, хозяин системы аутентификации, механизм аутентификации, механизм управления доступом. Факторы аутентификации. Способы аутентификации: Аутентификация при помощи электронной подписи, Аутентификация по паролям, аутентификация при помощи SMS, биометрическая аутентификация, аутентификация через географическое местоположение, многофакторная аутентификация. Протоколы аутентификации.	
	Обеспечение безопасности канального уровня. MITM атаки канального уровня: ARP-spoofing, DHCP-spoofing, VLAN-hopping, MAC-flooding, атаки на протокол STP. Способы предотвращения атак на канальном уровне.	
	Протокол контроль доступа в сеть 802.1X. Стандарт для настройки аутентификации и авторизации пользователей и рабочих станций в сети предприятия. Исследование принципа работы стандарта IEEE 802.1x. Настройка стандарта IEEE 802.1x на сетевом оборудование	
	Протоколы SSL/TLS. Основные понятия протоколов SSL и TLS. Устройство, принцип работы протокола SSL. Цифровые сертификаты. Аутентификация и обмен ключами.	
	Безопасность веб-сервиса. Способы предотвращение угроз web-based.	
	Безопасность электронной почты. Способы предотвращение угроз e-mail.	
	Безопасность беспроводных соединений. Современные беспроводные технологии. Архитектуры беспроводных технологий. Безопасность передачи данных в беспроводных технологиях. Аутентификация рабочих станций. Алгоритм Wired Equivalent Privacy (WEP). Формат кадра, ключи, инкапсуляция и декапсуляция алгоритма WEP. Технология Wi-Fi Protected Access (WPA и WPA 2). Программная платформа аутентификации Extensible Authentication Protocol. Конфиденциальность рабочих станций. Механизм конфиденциальности Rivest cipher 4 (RC4). Целостность рабочих станций. Идентификатор набора служб. Обнаружение Wireless Local Area Network (WLAN). Прослушивание беспроводного сигнала	
	Атаки в компьютерных сетях Активные атаки на беспроводное соединение. Атаки на внутренние системы организации. Атаки на внешние системы организации. Реализация безопасности беспроводных сетей. Безопасность точек доступа. Безопасность передачи данных	
	Протокол Netflow. Принцип работы и применение протокола Netflow. Настройка протокола Netflow.	

	Практические работы	
	18. Безопасность компьютерных сетей	10
Самостоятельная работа обучающихся		**16**
Учебная практика Примерный перечень работ: 1. Настройка прав доступа. 2. Оформление технической документации, правила оформления документов. 3. Настройка аппаратного и программного обеспечения сети. 4. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain. 5. Программная диагностика неисправностей. 6. Аппаратная диагностика неисправностей. 7. Поиск неисправностей технических средств. 8. Выполнение действий по устранению неисправностей. 9. Использование активного, пассивного оборудования сети. 10. Устранение паразитирующей нагрузки в сети. 11. Построение физической карты локальной сети.		**216**
Производственная практика: Примерный перечень работ: 1. Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение. 2. Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях. 3. Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций. 4. Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли. 5. Установка прав доступа и контроль использования сетевых ресурсов. 6. Обеспечение своевременного копирования, архивирования и резервирования данных. 7. Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования. 8. Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению. 9. Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети. 10. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия. 11. Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций. 12. Документирование всех произведенных действий.		**252**
Тематика самостоятельной учебной работы: 1. Систематическая проработка конспектов занятий, учебной и специальной технической литературы.		

2. Конспектирование текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа при самом широком использовании Интернета и других IT-технологий. 3. Проектные формы работы, подготовка сообщений к выступлению на семинарах и конференциях; подготовка рефератов, докладов. 4. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчётов и подготовка к их защите.	
ПРАКТИЧЕСКАЯ ПОДГОТОВКА: МДК 03.01.: Тема 1.1 Практические работы №№ 6,7 Тема 1.2 Практические работы №№4,5 МДК 03.02.: Тема 2.3 Практические работы №№ 16,17	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Для реализации программы профессионального модуля должна быть предусмотрена лаборатория «Эксплуатации объектов сетевой инфраструктуры».

Оборудование лаборатории и рабочих мест лаборатории «Эксплуатации объектов сетевой инфраструктуры».

Для выполнения практических лабораторных занятий курса в группах (до 15 человек) требуются компьютеры и периферийное оборудование в приведенной ниже конфигурации:

- 12-15 компьютеров обучающихся и 1 компьютер преподавателя (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i3, оперативная память объемом не менее 8 Гб; HD 500 Gb или больше программное обеспечение: операционные системы Windows, UNIX, пакет офисных программ, пакет САПР);
- Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа, обжимной инструмент, коннекторы RJ-45, тестеры для кабеля, кросс-ножи, кросс-панели;
- Пример проектной документации;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности
- Сервер в лаборатории (аппаратное обеспечение: не менее 2 сетевых плат, 8-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 16 Гб, жесткие диски общим объемом не менее 2 Тб, программное обеспечение: Windows Server 2012 или более новая версия, лицензионные антивирусные программы, лицензионные программы восстановления данных, лицензионный программы по виртуализации.)
- Технические средства обучения:
- Компьютеры с лицензионным программным обеспечением
- Интерактивная доска
- Проектор

4.2 Информационное обеспечение обучения

Перечень используемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Груманова А.В.

Охрана труда и техники безопасности в сфере компьютерных технологий: учебник студ. учрежд. сред. проф. образования/Л.В. Груманова, В.О. Писарева. – М.: Издательский центр «Академия», 2018. – 160 с.

2. Эксплуатация объектов сетевой инфраструктуры: учебник для студ. учреждений сред. проф.образования; под ред. А.В. Назарова. – М.: Академия, 2018. – 368 с.
3. Остроух А.В.

Выполнение работ по монтажу, наладке, эксплуатации и обслуживанию локальных компьютерных сетей. – М.: Академия, 2018. – 160 с.

Дополнительный источники:

1. Берлин А.Н. Коммутация в системах и сетях связи. - М.: Эко-Тренд, 2006.

2. Ватаманюк А. Создание, обслуживание и администрирование сетей на 100%. СПб.: Питер, 2010.

3. Колисниченко Д. Linux. От новичка к профессионалу. – Спб.: БХВ-Петербург, 2011.

4. Кришнамурти Б., Рексфорд Дж. Web-протоколы. Теория и практика. – М.: Бином, 2010.

5. Курячий Г.В., Маслинский К.А. Операционная система Linux. Курс лекций: учеб. пособие. – 2-е изд. – М.: Интернет-университет информационных технологий, 2008.

6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учеб. для вузов. 4-е изд. – Спб.: Издательский дом «Питер», 2010.

7. Станек Уильям Р. Командная строка Microsoft Windows. Справочник администратора – Спб.: БХВ-петербург, 2009.

8. Хокинс С. Администрирование web-сервера APACHE и руководство по электронной коммерции. – М.: Вильями, 2001.

9. ГОСТ Р 34.11-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Функция хеширования.

10. ГОСТ Р. 50922-96. Защита информации. Основные термины и определения.

11. ГОСТ Р 52069.0-2003. Государственный стандарт Российской Федерации. Защита информации. Система стандартов. Основные положения. SAFETY OF INFORMATION. SYSTEM OF STANDARDS. BASIC PRINCIPLES.

12. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

Интернет-ресурсы:

1. Все о компьютерных сетях Режим доступа: http://www.sd-company.su/sd_base_xp/jurnals/other_network.php

4.3 Общие требования к организации образовательного процесса

Программа профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры обеспечивается учебно-методической документацией по всем междисциплинарным курсам.

Для освоения профессиональных компетенций в рамках профессионального модуля предусмотрены занятия в форме лекций, практических занятий, самостоятельная работа студентов.

Итоговой формой контроля и оценки результатов освоения профессионального модуля является сдача квалификационного экзамена.

Учебная практика проводиться концентрированно в лабораториях и полигонах колледжа согласно рабочей программы учебной практики.

Производственная практика проводится концентрированно после освоения всех разделов модуля в организациях, деятельность которых соответствует профилю подготовки обучающихся. Обязательным условием допуска к производственной практике в рамках профессионального модуля «Эксплуатация объектов сетевой инфраструктуры» является освоение междисциплинарных курсов «Эксплуатация объектов сетевой инфраструктуры» и «Безопасность компьютерных сетей». Аттестация по итогам производственной практики проводиться на основании отчетов и дневников по практике студентов и отзывов руководителей практики. Результаты прохождения производственной практики по модулю учитываются при проведении государственной аттестации.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу:

– наличие высшего образования, соответствующего профилю преподаваемого модуля «Эксплуатация объектов сетевой инфраструктуры»;

– опыт деятельности в организациях соответствующей профессиональной сферы;

– преподаватели должны проходить стажировку в профильных организациях не реже 1 раза в 3 года.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой:

– дипломированные специалисты – преподаватели междисциплинарных курсов;

– мастера, имеющие 5-6 квалификационный разряд с обязательной стажировкой в профильных организациях не реже 1-го раза в 3 года.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 3.3. Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам

	Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	
ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен по модулю
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и	- эффективно использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.;	

поддержание необходимого уровня физической подготовленности.		
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	
ОК. 11. Планировать предпринимательскую деятельность в профессиональной сфере	- эффективно планировать предпринимательскую деятельность в профессиональной сфере при проведении работ по конструированию сетевой инфраструктуры	

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
САНКТ-ПЕТЕРБУРГСКОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "РАДИОТЕХНИЧЕСКИЙ КОЛЛЕДЖ", Добрякова Марина Геннадьевна **04.03.24** 09:25 (MSK) Простая подпись