Министерство образования и науки Тамбовской области
Тамбовское областное государственное бюджетное профессиональное образовательное учреждение
«Котовский индустриальный техникум»

Рабочая программа профессионального модуля ПМ.03. Эксплуатация объектов сетевой инфраструктуры

09.02.06 Сетевое и системное администрирование

Котовск, 2023

Основная программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее СПО) 09.02.06 Сетевое и системное администрирование, входящих в укрупненную группу 09.00.00 Информатика и вычислительная техника, по направлению подготовки 230100 Информатика и вычислительная техника.

Организация-разработчик: Тамбовское областное государственное бюджетное профессиональное образовательное учреждение Котовский индустриальный техникум (ТОГБПОУ «Котовский индустриальный техникум»)

Разработчик:
Мухин А.С. преподаватель спецдисциплин

_____ А.С. Мухин

Рассмотрено на заседании ПЦК 09.02.06 Сетевое и системное администрирование и 09.02.07 Информационные системы и программирование 28 августа 2023 г. протокол №1, на заседании методического совета от 30 августа 2023 г., протокол № 1, утверждена зам. директора по УР И.В. Улуханова.

Председатель ПЦК _____ А.А. Забровский

Зам. директора _____ И.В. Улуханова

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1 Область применения программы

Программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование в части освоения основного вида профессиональной деятельности Эксплуатация объектов сетевой инфраструктуры и соответствующих профессиональных компетенций:

ПК3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно - аппаратные средства компьютерных сетей;

ПК3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях;

ПК 3.3. Эксплуатировать сетевые конфигурации;

ПК3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации;

ПК3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования;

ПК3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

Программа профессионального модуля может быть использована при разработке программ в дополнительном профессиональном образовании по повышению квалификации и переподготовке кадров в области информатики и вычислительной техники при наличии среднего (полного) общего образования.

Опыт работы: не требуется.

Уровень образования: основное общее, среднее (полное) общее, начальное профессиональное образование.

1.2. Цели и задачи профессионального 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:

- обслуживания сетевой инфраструктуры, восстановление работоспособности сети после сбоя;
- удалённого администрирования и восстановления работоспособности сетевой инфраструктуры;
- организации бесперебойной работы системы, резервного копирования и восстановления информации;

- поддержке пользователей сети, настройке 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;
- осуществлять диагностику и поиск неисправностей технических средств, выполнять действия по устранению неисправностей в части, касающейся полномочий техника;
- выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;
- правильно оформлять и техническую документацию;
- 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 понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных, основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем

1.3. Количество часов на освоение программы профессионального модуля:

Всего – 328 часа, в том числе:

- максимальная учебная нагрузка обучающегося – 328 часов, включая:
- учебная практика – 108;
- обязательную аудиторную учебную нагрузку обучающегося – 220 часов,

в том числе

- лабораторные и практические занятия – 60 часа;
- курсовая работа – 30.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися ВПД **Эксплуатация объектов сетевой инфраструктуры**, 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	Эксплуатировать 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 поступившего из ремонта оборудования.
ПК 3.6	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.
ОК 4.	Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, обеспечивать ее сплочение, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Быть готовым к смене технологий в профессиональной деятельности.
ОК 10.	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды ПК	Наименование разделов ПМ	**Всего**, часов (макс. учебная нагрузка и практики)	**Объем времени, отведённый на освоение МДК**					**Практика**	
			Обязательная аудиторная нагрузка обучающегося			**Самостоятельная работа обучающегося**			
			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	**Учебная,** часов	**Производственная,** часов (если предусмотрена рассредоточенная практика)
ПК 3.1., ПК 3.5.	**Раздел 1.** Установка, эксплуатация и обслуживание технических и программно аппаратных средств компьютерных сетей.	48	12	4				36	
ПК 3.2.	**Раздел 2.** Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях.	26	8	2				18	
ПК 3.3.	**Раздел 3.** Эксплуатация сетевых конфигураций.	90	66	14	30			24	
ПК 3.4.	**Раздел 4.** Составление схемы послеаварийного восстановления работоспособности компьютерной сети	34	16	6				18	
ПК 3.6.	**Раздел 5.** Замена расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой инфраструктуры	30	18	4				12	
	Производственная практика (по профилю специальности)								
ПК 3.1., ПК 3.5.	**Раздел 6.** Основные понятия	6	6						

ПК 3.2.	**Раздел 7.** Угрозы безопасности информации	24	24	12					
ПК 3.4.	**Раздел 8.** Построение систем защиты	50	50	12					
ПК 3.6.	**Раздел 9.** Службы компьютерной безопасности	20	20	6					
	Всего:	328	220	60	30			108	

3.2. Содержание обучения по профессиональному модулю

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)	Объем часов	Уровень усвоения
1	2	3	4
МДК.03.01. Эксплуатация объектов сетевой инфраструктуры			
Раздел 1.	**Установка, эксплуатация и обслуживание технических и программно - аппаратных средств компьютерных сетей**	**12**	
Введение	Цели и задачи, структура профессионального модуля. Последовательность освоения профессиональных компетенций по модулю. Требования к уровню предварительных знаний и умений. Краткая характеристика основных разделов модуля. Порядок и форма проведения занятий, использование основной и дополнительной литературы. Рекомендации по организации самостоятельной работы студентов при изучении модуля	**1**	**2**
Тема 1.1. Физические аспекты эксплуатации сети	Физическое вмешательство в инфраструктуру сети; активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.	**1**	**2**
Тема 1.2. Логические (информационные) аспекты эксплуатации сети	Несанкционированное ПО (в том числе сетевое); паразитная нагрузка.	**2**	**3**
	Лабораторная работа №1,2	**4**	
	Поддержка пользователей сети.		
	Настройка прав доступа.		
Тема 1.3. Расширяемость сети. Масштабируемость сети	Добавление отдельных элементов сети (пользователи, компьютеры, приложения, службы); наращивание длины сегментов сети; замена существующей аппаратуры на более мощную. Увеличение количества узлов сети; увеличение протяжённости связей между объектами сети.	**2**	**2**
Тема 1.4. Техническая и проектная документация	Паспорт технических устройств; руководство по эксплуатации. Физическая карта всей сети; логическая схема компьютерной сети. Оформление технической документации, правила оформления документов.	**2**	**2**
Раздел 2.	**Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях**	**8**	
Тема 2.1. Технические осмотры	Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры. Комплекс организационно-технических мероприятий; выявление и своевременная замена элементов инфраструктуры.	**2**	**2**
Тема 2.2. Профилактические работы	Проверка объектов сетевой инфраструктуры и профилактические работы Проверка физических компонентов, проверка документации и требований, проверка списка совместимого оборудования.	**2**	**2**
Тема 2.3. Резервирование	Проведение регулярного резервирования Обслуживание физических компонентов, контроль состояния аппаратного обеспечения, организация удалённого оповещения.	**2**	**3**

	Лабораторная работа №3	**2**	
	Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.		
Раздел 3.	**Эксплуатация сетевых конфигураций**	**66**	
Тема 3.1. Архитектура системы управления	Архитектура системы управления. Структура системы управления. Архитектура в концепции TMN; централизованное управление; децентрализованное управление.	**6**	**2**
Тема 3.2. Уровни управления	Уровни управления. Многоуровневая архитектура управления TMN: бизнесом, услугами, сетью, элементами сети, уровень элементов сети.	**6**	**2**
Тема 3.3. Протоколы управления	Области управления Области управления ошибками, конфигурацией, доступом, производительностью, безопасностью. Протоколы управления: SNMP, CMIP, TMN, LNMP, ANMP.	**4**	**2**
Тема 3.4. Управление отказами	Управление отказами. Выявление, определение и устранение последствий сбоев и отказов в работе сети.	**4**	**2**
Тема 3.5. Учет работы сети	Учёт работы сети. Управление конфигурацией. Регистрация, управление используемыми ресурсами и устройствами; конфигурирование компонентов сети, сетевые адреса и идентификаторы, управление параметрами сетевых операционных систем.	**6**	**2**
Тема 3.6. Безопасность сети	Управление безопасностью сети. Статистика работы сети в реальном времени, минимизация заторов и узких мест.	**6**	**2**
Тема 3.7. Контроль доступа	Контроль доступа, сохранение целостности данных и журналирование.	**4**	**2**
Тема 3.8. Анализ трафика сети	Анализ трафика сети. Выявление складывающихся тенденций и планирование ресурсов для будущих нужд.	**4**	**3**
	Лабораторная работа №4,5,6,7	**8**	
	Анализ сетевого трафика средствами сетевого монитора.		
	Запись данных средствами сетевого монитора.		
	Устранение неполадок с помощью Ping и PathPing.		
	Диагностика сети.		
Тема 3.9. Оборудование для диагностики сети.	Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	**4**	**2**
Тема 3.10. Экспертные системы	Экспертные системы. Выявление причин аномальной работы сетей, возможные способы приведения сети в работоспособное состояние. Встроенные системы диагностики и управления.	**4**	**2**
Тема 3.11. Сетевые мониторы	Сетевые мониторы. Средняя интенсивность общего трафика сети, средняя интенсивность потока пакетов с определённым типом ошибки. Программно-аппаратный модуль,	**4**	**3**

	установленный в коммуникационное оборудование; программный модуль, встроенный в операционные системы.		
	Лабораторная работа №8,9,10	**6**	
	Диспетчер задач. Сетевые утилиты.		
	Использование консоли. Оценка производительности.		
	Мониторинг сетевого трафика с помощью утилиты Netstat.		
Раздел 4.	**Схемы послеаварийного восстановления работоспособности компьютерной сети**	**16**	
Тема 4.1. Резервное копирование данных.	Резервное копирование данных.	**2**	**3**
	Лабораторная работа №11	**2**	
	Резервное копирование данных.		
Тема 4.2. Хранилища данных	Хранилищ данных. Принципы работы хранилищ данных.Принципы построения. Основные компоненты хранилища данных.	**2**	**2**
Тема 4.3. OLAP технология	Технологии управления информацией. OLAP технология.	**2**	**2**
Тема 4.4. Принцип работы СУБД	Понятие баз данных. Основные понятия, принцип работы СУБД.	**2**	**2**
Тема 4.5. Восстановление информации	Принципы планирования восстановления работоспособности сети при аварийной ситуации. План восстановления системы Порядок уведомления о чрезвычайных событиях . Активация. Возврат к нормальному функционированию системы.	**2**	**3**
	Лабораторная работа №12,13	**4**	
	Восстановление работоспособности сети после сбоя.		
	Утилита Acronis.		
Раздел 5.	**Замена расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой инфраструктуры**	**18**	
Тема 5.1. Принципы локализации неисправностей	Принципы локализации неисправностей.	**2**	**2**
Тема 5.2. Контрольно-измерительная аппаратура	Контрольно-измерительная аппаратура.	**2**	**2**
Тема 5.3. Сервисные платы и комплексы	Сервисные платы и комплексы.	**2**	**2**
Тема 5.4. Особенности	Программные средства диагностики. Номенклатура и особенности работы тест-программ.	**2**	**3**

работы тест-программ	Диагностика неисправностей средств сетевых коммуникаций. Контроль функционирования аппаратно-программных комплексов.		
	Лабораторная работа №14,15	**4**	
	Использование контрольно-измерительной аппаратуры.		
	Восстановление данных.		
Тема 5.5. Действия при не работающей сети	Действия при неработающей сети, при медленной сети. Действия при нестабильно работающей сети.	**2**	**2**
Тема 5.6. Замена расходных материалов и мелкий ремонт периферийного оборудования	Замена расходных материалов и мелкий ремонт периферийного оборудования.	**2**	**2**
Тема 5.7. Определение устаревшего оборудования и программных средств сетевой инфраструктуры	Определение устаревшего оборудования и программных средств сетевой инфраструктуры.	**2**	**2**
МДК.03.02. Безопасность функционирования информационных систем			
Раздел 1. Основные понятия		**6**	
Тема 6.1. Введение	Значение информации в современном мире. Важность вопроса обеспечения безопасного функционирования информационных систем. Предмет, задачи курса «Безопасность функционирования информационных систем». Взаимосвязь дисциплины с другими дисциплинами учебного плана.	**2**	**2**
Тема 6.2. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.	Понятие информации, информационного ресурса, информационной системы. Критичность информационного ресурса. Основные особенности информационной системы.	**4**	**2**
Раздел 2. Угрозы безопасности информации		**24**	
Тема 7.1. Угрозы безопасности информации	Основные причины реализации угроз информационной безопасности. Классификация угроз по используемым средствам. Классификация по характеру действий, используемых в атаке. Классификация по характеру уязвимостей. Классификация типовых удаленных атак по виду воздействия.	**2**	**2**
Тема 7.2. Классификация	Основная особенность эксплуатации средств и систем информационной безопасности.	**2**	**2**

угроз	Возрастание сложности ИС, новые угрозы безопасности, особенности ИС.		
Тема 7.3. Безопасность субъектов инфомационных отношений	Анализ бизнес-требований к защите информации в ИС, влияние общих бизнес-факторов на проект защиты. Снижение влияния несовместимости систем на их защиту. Угрозы безопасности ИС, возникающие из-за проблем с сопровождением. Разработка концептуального плана защиты. Принципы проектирования защиты информации. Рекомендации по проектированию защищенных элементов ИС. Укрепление защиты внутренней сети при помощи сегментирования. Планирование процедуры восстановления. Анализ технических ограничений, правила интеграции. Анализ ограничений по совместимости.	**2**	**2**
Тема 7.4. Классификация каналов проникновения в систему	Понятие грамотной эксплуатации системы. Мониторинг в режиме реального времени и анализ происходящих в ИС событий. Контроль безопасности системы. Преодоление нештатных ситуаций. Техническая поддержка средств и систем защиты. Анализ и контроль защищенности ресурсов.	**4**	**3**
	Лабораторная работа №1	**4**	
	«Конфигурирование службы каталога Active Directory»		
Тема 7.5 Неформальная модель нарушителя в информационной системе	Понятия уязвимости, угрозы. Определение сканера безопасности. Принципы работы сканера безопасности. Классы сканеров безопасности и их краткая характеристика. Недостатки сканеров безопасности.	**2**	**3**
	Лабораторная работа №2,3	**8**	
	«Сканеры безопасности сетевых сервисов и протоколов»		
	«Сканеры безопасности операционных систем»		
Раздел 3. Построение систем защиты		**50**	
Тема 8.1. Принцип построения системы защиты	Основные понятия. Домен. Контроллеры домена. Дерево. Лес.	**2**	**3**
	Лабораторная работа №4	**4**	
	«Межсетевые экраны и фильтры»		
Тема 8.2. Достоинства и недостатки различных мер защиты	Основные функции контроллеров домена. Контроллеры домена специального назначения. Серверы глобального каталога. Структурные объекты БД Active Directory. Разделы Active Directory .Домены. Деревья доменов. Леса. Доверительные отношения. Организационные единицы. Использование организационных единиц для управления группами объектов.	**4**	**2**
Тема 8.3. Основные предпринципы их построения	Проектирование структуры леса. Проектирование доменной структуры. Определение количества доменов. Проектирование инфраструктуры DNS. Проектирование структуры организационных единиц.	**4**	**3**
	Лабораторная работа №5	**4**	
	«Построение VPN»		
Тема 8.4. Основные	Основные методы обеспечения безопасности Active Directory. Участники безопасности.	**6**	**2**

принципы защиты от дезорганизации и НСД к информации	Списки управления доступом. Лексема доступа. Аутентификация и разрешение. Защита Active Directory с использованием протокола Kerberos. Управление объектами Active Directory. Использование групповых политик Active Directory.		
Тема 8.5. Модели управления доступом	Современные АСОИ. Нисходящий метод. Восходящий метод .Метод неформальной разработки и "security policy model".	**2**	**2**
Тема 8.6. Типы моделей управления доступом	Модель конечного автомата описывает систему как абстрактную математическую машину. Модель матрицы доступа (Harrison, Ruzo и Ullman 1976) меток безопасности управления доступом модель информационных потоков.	**2**	**2**
Тема 8.7. Описание модели управления доступом в системе как конечного автомата	Разработка модели управления доступом.Определение переменных состояния. Определение условий для безопасного состояния. Определение функций переходов из состояния в состояние назначение функции , функция элементарна, Определение начального состояния.	**4**	**2**
Тема 8.8. Модель безопасности Белл–Ла Падула	Чтение секретного файла несекретным процессом. Управление при помощи меток безопасности простая безопасность свойство ограничения SYSTEM HIGH и SYSTEM LOW многоуровневой безопасности.	**4**	**2**
Тема 8.9. Анализ информационных потоков	Информационный поток , скрытые каналы формальный анализ потока , уровня абстрактной модели и методы определения потенциальных потоков формальной спецификации метод формальной разработки.	**2**	**3**
	Лабораторная работа №6	**4**	
	«Системы обнаружения вторжений»		
Тема 8.10. Системы разграничения доступа	Диспетчер доступа , требование полноты контролируемых операций, требование изолированности, формальной проверки требование базой данных защиты (security database)	**4**	**2**
Тема 8.11. Криптографические методы защиты	Ключ, операция зашифрования/расшифрования , отправителем для зашифрования информации закрытие данных контроль целостности и аутентичности данных Прозрачное шифрование.	**4**	**2**
Раздел 4. Службы компьютерной безопасности		**20**	
Тема 9.1. Организационная структура, основные функции службы компьютерной безопасности	Служба компьютерной безопасности формирование требований к системе защиты планирование, организация наблюдение за функционированием системы состав службы штатный сотрудники службы защиты.	**4**	**2**
Тема 9.2. Организационные и организационно-	Разовые мероприятия мероприятия общесистемные определение порядка назначения организацию надежного пропускного режима. Мероприятия, проводимые по необходимости Периодически проводимые мероприятия. Постоянно проводимые мероприятия.	**4**	**3**

технические мероприятия по созданию и поддержанию функционирования системы защиты			
	Лабораторная работа №7	**4**	
	«Установка и настройка FTP-севера proftpd»		
Тема 9.3. Нормативные и организационно-распорядительные документы, необходимые для организации системы защиты информации от НСД	План защиты информации в системе цель защиты системы перечень значимых угроз безопасности основные правила. План обеспечения непрерывной работы обязанности и порядок действий различных категорий персонала. Договор о порядке организации обмена электронными документами	**4**	**3**
	Лабораторная работа №8	**2**	
	«Установка и настройка WEB-севера Apache»		
Тема 9.4. Заключительное занятие. Выводы по теории.	Острота проблемы защиты информационных технологий высокие темпы роста парка средств вычислительной техники повышение уровня доверия к автоматизированным системам концентрация больших объемов информации развитие рыночных отношений	**2**	**2**
Учебная практика (по профилю специальности)	**Виды работ:**	**108**	
	• Использование активного и пассивного оборудования сети;	**12**	
	• Составление карты локальной сети;	**12**	
	• Работа в домене;	**12**	
	• Регламенты ТО;	**12**	
	• Мониторы сети;	**12**	
	• Структура системы управления;	**12**	
	• Защита беспроводной сети;	**6**	
	• Настройка межсетевых экранов;	**6**	
	• Настройка коммутатора второго уровня;	**6**	
	• Требования безопасности;	**6**	
	• Разработка функциональных схем элементов автоматизированной системы защиты информации;	**6**	
	• Работа с кабельными сканерами и тестерами.	**6**	
Примерная тематика курсовых работ		**30**	

	• Настройка VPN соединения в Windows. • Настройка межсетевого экрана D-Link DFL-260E/860 E. • Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств. • Настройка защиты беспроводных сетей с помощью систем шифрования на примере точки доступа D-Link DIR 320. • Настройка коммутатора D-Link DES-3200 Series. • Установка и настройка системы обнаружения атак Snort. • Установка, настройка и использование программы InterNetView. • Использование утилиты Netstat. • Установка, настройка и использование программы VMware Workstation. • Использование утилиты Nmap. • Установка, настройка и использование программы VipNet Office. • Установка, настройка и использование программы WinPCap. • Установка, настройка и использование программы AdRem Netcrunch. • Установка, настройка и использование программы Nessus. • Настройка защиты беспроводных сетей с помощью систем шифрования на примере точки доступа D-Link DAP-2310. • Установка и настройка коммутаторов CISCO CATALYST серии 2900XL. • Настройка защиты беспроводных сетей с помощью систем шифрования на примере точки доступа TP-Link TL-WR 720 N. • Мелкий ремонт периферийного оборудования. • Использование утилиты Acronis. • Протоколы управления SNMP, CMIP, TMN, LNMP, ANMP. • Настройка ftp сервера средствами Windows 7. • Настройка удаленного доступа в Windows 7. • Установка и настройка IP камеры. • Схемы обжимки витой пары. • Настройка защиты беспроводных сетей с помощью систем шифрования на примере точки доступа D-Link DIR 620.		

	Всего:	**328**	

4.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация профессионального модуля предполагает наличие лабораторий «Эксплуатация объектов сетевой инфраструктуры» и «Программно-аппаратная защита объектов сетевой инфраструктуры», а также полигона «Технический контроль и диагностика сетевой инфраструктуры».

Лаборатория «Эксплуатация объектов сетевой инфраструктуры»

Оборудование лаборатории:

- рабочие места по количеству обучающихся;
- рабочее место преподавателя;
- типовой состав для монтажа и наладки компьютерной сети: кабели различного типа, обжимной инструмент, коннекторы RJ 45, тестеры для кабеля;
- пример проектной документации.

Оборудование и технологическое оснащение рабочих мест:

- компьютер обучающегося (аппаратное обеспечение:, 2-х ядерный процессор с частотой не менее 1,5 ГГц, оперативная память объёмом не менее 2 Гб; программное обеспечение: лицензионное, операционные системы Windows, Linux, MS Office, пакет САПР);
- компьютер преподавателя (аппаратное обеспечение: 2-х ядерный процессор с частотой не менее 2 ГГц, оперативная память объёмом не менее 2 Гб; программное обеспечение: лицензионное, операционные системы Windows, Linux, MS Office, пакет САПР);
- сервер в лаборатории (аппаратное обеспечение: не менее 2 сетевых плат, 2 ядерный процессор с частотой не менее 3 ГГц, оперативная память объёмом не менее 2 Гб; жёсткий диск объёмом не менее 1 Тб; программное обеспечение: Windows Server 2003, лицензионные антивирусные программы, лицензионные программы восстановления данных.

Технические средства обучения:

- необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения безопасности;
- интерактивная доска;
- проектор.

Лаборатория «Программно-аппаратная защита объектов сетевой инфраструктуры»

Оборудование лаборатории:

- рабочие места по количеству обучающихся;
- рабочее место преподавателя;
- пример проектной документации.

Технические средства обучения:

- сетевые маршрутизаторы;
- сетевые коммутаторы;
- сетевые хранилища;
- сетевые модули и трансиверы;
- шасси и блоки питания;
- шлюзы VPN;
- принт-серверы;
- IP-камеры;
- медиаконвертеры;
- сетевые адаптеры и карты;
- сетевые контроллеры;
- оборудование xDSL;
- аналоговые модемы;
- коммутационные панели;
- беспроводные маршрутизаторы;
- беспроводные принт-серверы;
- точки доступа Wi'Fi;
- Wi-Fi-адаптеры;
- Bluetooth-адаптеры;
- KVM-коммутаторы;
- KVM-адаптеры;
- VoIP-маршрутизаторы;
- VoIP-адаптеры;
- необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения её безопасности.

Оборудование и технологическое оснащение рабочих мест:

- компьютер обучающегося (аппаратное обеспечение:, 2-х ядерный процессор с частотой не менее 1,5 ГГц, оперативная память объёмом не менее 2 Гб; программное обеспечение: лицензионное, операционные системы Windows, Linux, MS Office, пакет САПР);
- компьютер преподавателя (аппаратное обеспечение: 2-х ядерный процессор с частотой не менее 2 ГГц, оперативная память объёмом не менее 2 Гб; программное обеспечение: лицензионное, операционные системы Windows, Linux, MS Office, пакет САПР);
- сервер в лаборатории (аппаратное обеспечение: не менее 2 сетевых плат, 2 ядерный процессор с частотой не менее 3 ГГц, оперативная память объёмом не менее 2 Гб; жёсткий диск объёмом не менее 1 Тб; программное обеспечение: Windows Server 2003, лицензионные антивирусные программы, лицензионные программы восстановления данных.

Перечень программного обеспечения:

- MS Windows 7.
- MS Office 2003.
- Ethereal, разработчик – Gerald Combs, источник – http://www.ethereal.com,
- InterNetView, разработчик – Evgene Ilchenko, источник – http://www.tsu.ru /~evgene/info/inv,
- Netcat, разработчик –Weld Pond <weld@l0pht.com>, источник – http://www. l0pht.com
- Nmap, разработчик–Insecure.Com, источник–http://www.insecure.com
- Snort, разработчик – Martin Roesch & The Snort Team. © Sourcefire Inc. et al., источник – http://www.snort.org,
- VipNet Office, разработчик – ОАО «Инфотекс», Москва, Россия, источник – http://www.infotecs.ru,
- VMware Workstation, разработчик–VMware Inc, источник – http://www. vmware.com,
- WinPCap, источник – http://winpcap.polito.it.
- AdRem Netcrunch, источник – http://www.adremsoft.com/netcrunch/
- Nessus, источник – http://www.nessus.org.

4.2. Информационное обеспечение обучения

Основные источники:

1. Компьютерные сети. Учебный курс: официальное пособие Microsoft для самостоятельной подготовки. – 2-е изд., испр. и доп. / Корпорация Майкорософт. – М.: Русская редакция, 2017.
2. Чекмарев Ю.В. Локальные вычислительные сети. – 2-е изд., испр. и доп. –М.: ДМК Пресс, 2017.
3. Биячуев Т.А. Безопасность корпоративных сетей / под ред. Л.Г. Осовецкого. – СПб: СПб ГУ ИТМО, 2016.
4. Брэгг Р. Безопасность сети на основе Microsoft Windows Server 2016. Учебный курс Microsoft. – СПб.: Питер, 2012.
5. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. – М.: Горячая линия-Телеком, 2016.
6. Закер К. Планирование и поддержка сетевой инфраструктуры Microsoft Windows Server 2008. Учебный курс MCSE. – М.: Издательско-торговый дом «Русская Редакция», 2012.
7. Закляков П. Обнаружение телекоммуникационных атак: теория и практика, Snort. / Системный администратор, №10(11), 2017.
8. Колисниченко Д.Н., Аллен П.В. LINUX: полное руководство. – СПб: Наука и техника, 2015.
9. Норткатт С, Новак Д. Обнаружение вторжений в сеть. Настольная книга специалиста по системному анализу. – М.: Лори, 2015.

10. Полянская О.Ю., Горбатов В.С. Инфраструктуры открытых ключей: Учебное пособие. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 20116.
11. Реймер С., Малкер М. Active Directory для Windows Server 2008. Справочник администратора. – М.: СП ЭКОМ, 2012.
12. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей. 2 изд. – М.: Cisco Systems 2016.
13. Стахнов А.А. Сетевое администрирование Linux. – СПб.: БХВ-Петербург, 2017.

Дополнительные источники:

1. Бигелоу С. Сети: поиск неисправностей, поддержка и восстановление. – СПб.: БХВ-Петербург, 2017.
2. Внедрение, управление и поддержка сетевой инфраструктуры Microsoft Windows Server 2008: учебный курс MCSA/MCSE / Пер. с англ. – М.: Русская Редакция, 2008.
3. Запечников С.В. Основы построения виртуальныхчастных сетей: учеб. пособие для вузов /С.В. Запечников, Н.Г. Милославская, А.И. Толстой. – М.: Горячая линия Телеком, 2015.
4. Корт С.С. Теоретические основы защиты информации: учеб. пособие для вузов. –М.: Гелиос АРВ, 2016.
5. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб.: Питер, 2017.
6. Лукацкий А.В. Обнаружение атак. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2015.
7. Мандиа К. Защита от вторжений. Расследование компьютерных преступлений / К.Мандиа, К. Просис. – М.: Лори, 2016.
8. Медведовский И.Д. Атака на Internet /И.Д. Медведовский, П.В. Семьянов, Д.Г. Леонов. – 2-е изд., перераб. и доп. – М.: ДМК, 2016.
9. Милославская Н.Г. Интрасети: доступ в Internet, защита: учеб. пособие для вузов / Н.Г. Милославская, А.И. Толстой. – М.: Юнити'Дана, 2017.
10. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях. Международный опыт: монография. – М.: Норма, 2017.
11. Рассел Ч. Microsoft Windows Server. Справочник администратора. – 2'е изд., испр. –М.: Эком, 2017.
12. Скрембрей Дж. Секреты хакеров. Безопасность Windows 7 – готовые решения. – М.: Вильямс, 2015.
13. Стивенс У.Р. Протоколы TCP/IP. Практическое руководство.–СПб.: БХВ-Петербург, 2015.
14. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. – М.: Лори, 2016.
15. Red HatEnterpriseLinux. Network Services and Security. – Red Hat, Inc., 2017.

16. Windows Server 2008 Security Guide. Microsoft Solutions for Security. – Microsoft Corporation, 2013.
17. Галкин В.А., Григорьев Ю.А. Телекоммуникации и сети: Учеб. пособие для вузов. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2016.
18. Ханикат Дж. Знакомство с Microsoft Windows Server 2016. – М.: Издательско-торговый дом «Русская Редакция», 2016.
19. Холме Д., Томас О. Управление и поддержка Microsoft Windows Server 2008. Учебный курс MCSA/MCSE. – М.: Издательско-торговый дом «Русская Редакция», 2012.

Интернет-ресурсы:

1. http://lanhelper.ru/seti
2. http://certsrv.ru/ru/tmg/html/cc3480db-6d59-40fc-8363-12f4c6e079aa.htm
3. http://www.pandia.ru/text/77/216/5595.php
4. http://www.ceae.ru/urids-komp-prestup.htm
5. http://ikt.rtk-ros.ru/p13aa1.html

4.3. Общие требования к организации образовательного процесса

Освоению данного профессионального модуля предшествует освоение программ общепрофессиональных дисциплин:

- ОП 01. Основы теории информации;
- ОП 02. Технологии физического уровня передачи данных;
- ОП 03. Архитектура аппаратных средств;
- ОП 04. Операционные системы;
- ОП 05. Основы программирования и баз данных;
- ОП 06. Электротехнические основы источников питания;
- ОП 07. Технические средства информатизации;
- ОП 08. Инженерная компьютерная графика
- ОП 09. Метрология, стандартизация, сертификация и техническое регулирование.

Учебная практика (по профилю специальности) проводится рассредоточено.

Освоение каждого междисциплинарного курса завершается экзаменом, а освоение программы профессионального модуля – проведением квалификационного экзамена.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): высшее профессиональное образование, соответствующее профилю модуля.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой:

Педагогический состав: дипломированные специалисты – преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин;

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результаты (освоенные ПК)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей	• настраивание сети с высокой скоростью и точностью; • составление рекомендаций по повышению работоспособности сети; • адекватный выбор технологическое оборудования для настройки сети;	Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы: • на практических занятиях; • при решении ситуационных задач; • при выполнении определённых видов работ учебной практики; • зачёт по разделу практики
ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях	• анализ свойства сети исходя из её служебного назначения; • составление рекомендации по повышению технологичности сети; • выполнение мониторинга и умение анализировать работу локальной сети с помощью программных средств;	Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы: • на практических занятиях; • при выполнении определённых видов работ учебной практики; • зачёт по разделу практики
ПК 3.3. Эксплуатация сетевых конфигураций	• обоснованный выбор способов настройки; • выявление, определение и устранение последствий сбоев и отказов в работе сети; • восстановление работоспособности сетевой инфраструктуры	Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы: • на практических занятиях; • при выполнении определённых видов работ учебной практики; • зачёт по разделу практики
ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации	• выбор и профессиональное использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов; • организация бесперебойной работы системы по резервному	Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы: • на практических занятиях; • при выполнении определённых видов работ учебной практики; • зачёт по разделу практики

	копированию; ● восстановление работоспособности сети после сбоя в соответствии с регламентом	
ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования	● выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов; ● грамотное оформление технической документации	Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы: ● на практических занятиях; ● зачёт по разделу практики
ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры	● работать с контрольно-измерительной аппаратурой в соответствии с условиями эксплуатации; ● осуществление обоснованной замены расходных материалов; ● произведение аппаратной и программной диагностики неисправностей;	Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы: ● на практических занятиях; ● при решении ситуационных задач; ● при выполнении определённых видов работ учебной практики; ● зачёт по разделу практики. Экзамен

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.

Результаты (освоенные ОК)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	• участие в работе студенческих научных обществ; • участие во внеурочной деятельности, связанной с будущей профессией/ специальностью (конкурсы профессионального мастерства, выставки и т. п.);	Экспертная оценка результатов деятельности обучающегося в процессе освоения образовательной программы: • на практических занятиях (при решении ситуационных задач, при участии в деловых играх : при подготовке и участии в семинарах, при подготовке рефератов, докладов и т. д.); • при выполнении и защите курсовой работы (проекта); • при выполнении работ на различных этапах учебной практики
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	• выбор и применение методов и способов решения профессиональных задач, оценка их эффективности и качества	
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	• анализ профессиональных ситуаций; • решение стандартных и нестандартных профессиональных задач	
ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	• эффективный поиск необходимой информации; • использование различных источников, включая электронные, при изучении теоретического материала и прохождении различных этапов производственной практики	
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности	• использование в учебной и профессиональной деятельности различных видов программного обеспечения, в том числе специального, при оформлении и презентации всех видов работ	
ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством,	взаимодействие: • с обучающимися при проведении деловых игр, выполнении коллективных	

потребителями	заданий (проектов); • с преподавателями, мастерами в ходе обучения; • с потребителями и коллегами в ходе практики	
ОК 7. Брать на себя ответственность за работу членов команды (подчинённых), за результат выполненных заданий	• самоанализ и коррекция результатов собственной деятельности при выполнении коллективных заданий (проектов); • ответственность за результат выполнения заданий	
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	• планирование и качественное выполнение заданий для самостоятельной работы при изучении теоретического материала и прохождении различных этапов практики; • определение этапов и содержания работы по реализации самообразования	
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности	• адаптация к изменяющимся условиям профессиональной деятельности; • проявление профессиональной маневренности при прохождении различных этапов практики	
ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)	• готовность к исполнению воинской обязанности с применением полученных профессиональных знаний (для юношей)	