Топанов Александр Павлович
Подписано цифровой подписью: Топанов Александр Павлович

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

АРХАНГЕЛЬСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ
ИМ. Б.Л. РОЗИНГА (ФИЛИАЛ) СПбГУТ
(АКТ (ф) СПбГУТ)

УТВЕРЖДАЮ
И.о. зам. директора по учебной работе
_____ М.А. Цыганкова
20 05 2022 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МНОГОКАНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ ЭЛЕКТРОСВЯЗИ

по специальности:

11.02.09 – Многоканальные телекоммуникационные системы

г. Архангельск
2022

Рабочая программа профессионального модуля составлена на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.09 – Многоканальные телекоммуникационные системы, примерной программы профессионального модуля и в соответствии с учебным планом по специальности 11.02.09 – Многоканальные телекоммуникационные системы.

Рабочая программа рассмотрена и одобрена цикловой комиссией Сетей и систем связи

Протокол №__9__ от __20.05.__ 2022 г.

Председатель_____ М.П. Рыжков

Составитель:

М.В. Куницына, преподаватель высшей квалификационной категории АКТ (ф) СПбГУТ.

П.М. Рыжков, преподаватель высшей квалификационной категории АКТ (ф) СПбГУТ.

СОДЕРЖАНИЕ

1 ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МНОГОКАНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ ЭЛЕКТРОСВЯЗИ

1.1 Область применения программы

Рабочая программа профессионального модуля – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 11.02.09 Многоканальные телекоммуникационные системы, базовой подготовки в части освоения основного вида деятельности (ВД): **Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи** и соответствующих профессиональных компетенций (ПК):

ПК 3.1. Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи.

ПК 3.2. Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.

ПК 3.3. Обеспечивать безопасное администрирование многоканальных телекоммуникационных систем и информационно-коммуникационных сетей связи.

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:

- выявления каналов утечки информации;
- определения необходимых средств защиты;
- проведения аттестации объекта защиты (проверки уровня защищенности);
- разработки политики безопасности для объекта защиты;
- установки, настройки специализированного оборудования по защите информации;
- выявления возможных атак на автоматизированные системы;
- установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;
- конфигурирования автоматизированных систем и информационно - коммуникационных сетей;
- проверки защищенности автоматизированных систем и информационно - коммуникационных сетей;

- защиты баз данных;
- организации защиты в различных операционных системах и средах;
- шифрования информации;

уметь:

- классифицировать угрозы информационной безопасности;
- проводить выбор средств защиты в соответствии с выявленными угрозами;
- определять возможные виды атак;
- осуществлять мероприятия по проведению аттестационных работ;
- разрабатывать политику безопасности объекта;
- использовать программные продукты, выявляющие недостатки систем защиты;
- выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
- производить установку и настройку средств защиты;
- конфигурировать автоматизированные системы и информационно - коммуникационные сети в соответствии с политикой информационной безопасности;
- выполнять тестирование систем с целью определения уровня защищенности;
- использовать программные продукты для защиты баз данных;
- применять криптографические методы защиты информации;

знать:

- каналы утечки информации;
- назначение, классификацию и принципы работы специализированного оборудования;
- принципы построения информационно-коммуникационных сетей;
- возможные способы несанкционированного доступа;
- нормативные правовые и законодательные акты в области информационной безопасности;
- правила проведения возможных проверок;
- этапы определения конфиденциальности документов объекта защиты;
- технологии применения программных продуктов;
- возможные способы, места установки и настройки программных продуктов;
- конфигурации защищаемых сетей;
- алгоритмы работы тестовых программ;
- средства защиты различных операционных систем и сред;
- способы и методы шифрования информации.

1.3 Количество часов на освоение программы профессионального модуля

всего – 198 часов, в том числе:
максимальной учебной нагрузки обучающегося 144 часов, включая:
- обязательной аудиторной учебной нагрузки 96 часов,
- самостоятельной работы обучающегося 48 часов.

учебной практики – 36 часов, производственной практики – 18 часов.

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом деятельности **Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи**, в том числе профессиональными (ПК) и общими (ОК) компетенциями, личностными результатами (ЛР) реализации программы воспитания:

Код	Наименование результата обучения
ПК 3.1	Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи
ПК 3.2	Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению
ПК 3.3	Обеспечивать безопасное администрирование многоканальных телекоммуникационных систем и информационно-коммуникационных сетей связи
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
Личностные результаты (ЛР): ЛР 1-ЛР27.	

3 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды профессиональных компетенций	**Наименования разделов 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
			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 3.1-3.2	**Раздел 1.** Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи	**54**	**36**	**14**	**-**	**18**	**-**	**-**	**-**
ПК 3.2- 3.3	**Раздел 2.** Технология применения комплексной системы защиты информации	**126**	**60**	**34**	**-**	**30**	**-**	**36**	**-**
	Производственная практика, (по профилю специальности), часов	**18**							**18**
	Всего:	**198**	**96**	**48**		**48**		**36**	**18**

3.2 Содержание обучения по профессиональному модулю (ПМ.03)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов	Уровень освоения
1	**2**		**3**	**4**
Раздел 1. Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи			**54**	
МДК.03.01 Технология применения программно аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи			**54**	
Тема 1.1. Основы информационной безопасности	**Содержание учебного материала**		8	
	1	Понятие информационной безопасности, характеристика ее составляющих. Место информационной безопасности в системе национальной безопасности. Концептуальная модель защиты информации. Проблемы информационной безопасности в сфере телекоммуникаций: объекты защиты; виды защиты; системы защиты информации. Классификация и анализ угроз информационной безопасности в многоканальных телекоммуникационных системах. Виды уязвимости информации и формы ее проявления.		1,2
	2	Понятие о конфиденциальной информации (грифы, закон о государственной тайне, закон о личной тайне, закон о коммерческой тайне).		1,2
	3	Уровни информационной безопасности – законодательно-правовой, административно-организационный, программно-технический. Принципы построения систем защиты информации.		1,2

	Самостоятельная работа обучающихся: Подготовка к устному опросу. Работа с конспектом.		2	
Тема 1.2. Правовое обеспечение информационной безопасности	**Содержание учебного материала**		8	1,2
	1	Информация как объект права. Нормативно-правовые основы информационной безопасности в РФ. Законодательно - нормативные акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации. Конституционные гарантии прав граждан в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ. Система защиты государственной тайны, правовой режим защиты государственной тайны.		
	2	Лицензирование и сертификация в области защиты информации. Стандартизация информационной безопасности.		1,2
	Лабораторные занятия		**8**	
	1	Документы, регламентирующие деятельность в области защиты информации.	2	
	2	Ответственность за нарушения законодательства в сфере защиты информации.	2	
	3	Изучение положений о государственном лицензировании деятельности в области защиты информации.	2	
	4	Изучение положений о сертификации средств защиты информации по требованиям безопасности информации.	2	
	Самостоятельная работа обучающихся: Оформление отчетов лабораторных работ, подготовка к их защите.		8	
Тема 1.3 Организационное обеспечение информационной безопасности	**Содержание учебного материала**		6	1,2
	1	Сущность и сферы действия организационной защиты информации. Механизмы обеспечения информационной безопасности. Разработка политики безопасности.		
	2	Проведение анализа угроз и расчета рисков в области		1,2

		информационной безопасности. Выбор механизмов и средств обеспечения информационной безопасности Модели защиты информационных систем.		
	3	Правила организации работ подразделений защиты информации. Разработка инструкций по работе со средствами защиты. Организация работы персонала с конфиденциальной информацией.		1,2
	Практические занятия		**4**	
	1	Традиционные симметричные криптосистемы.	4	
	Лабораторные занятия		**2**	
	5	Анализ Доктрины ИБ РФ.	2	
	Самостоятельная работа обучающихся: Оформление отчетов лабораторных и практических работ, подготовка к их защите. Подготовка к устному опросу.		8	
Раздел 2. Технология применения комплексной системы защиты информации			**90**	
МДК.03.02 Технология применения комплексной системы защиты информации			**90**	
Тема 2.1 Программно-аппаратные средства защиты информации	**Содержание учебного материала**		18	3
	1	Информационная безопасность в многоканальных телекоммуникационных системах и сетях электросвязи. Структурные схемы систем защиты информации в типовых ИС. Показатели защищенности многоканальных телекоммуникационных систем.		

	2	Сервисы, обеспечивающие информационную безопасность в многоканальных телекоммуникационных системах и сетях электросвязи: ограничение физического доступа к автоматизированным системам; идентификация и аутентификация пользователей; ограничение доступа в систему; разграничение доступа; регистрация событий (аудит); криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам. Подсистемы безопасности		3
	3	Типовые удаленные сетевые атаки и их характеристика. Компьютерные вирусы и защита от них. Антивирусные программы и комплексы. Построение систем антивирусной защиты телекоммуникационных систем и сетей.		3
	Лабораторные занятия		**16**	
	1	Изменение MAC-адреса в ОС Windows.	2	
	2	Изучение трафика атаки с помощью программы Wireshark.	2	
	3	Обнаружение сетевых анализаторов с помощью программы Cain&Abel.	2	
	4	Уязвимости протокола ARP. Генератор пакетов CommView.	2	
	5	Уязвимости протокола ARP. Программа Cain&Abel.	2	
	6	Мониторинг трафика ARP. Программа arpwatch.	2	
	7	Мониторинг трафика ARP. Программа ARP – monitor.	2	
	8	Применение антивирусной защиты в информационных системах.	2	
	Самостоятельная работа обучающихся: Работа с конспектом. Оформление отчетов лабораторных работ и подготовка к их защите. Подготовка к устному опросу		20	
Тема 2.2 Администрирование	**Содержание учебного материала**		8	3
	1	Технологии защиты данных. Принципы криптографической защиты		

телекоммуникационных систем и сетей связи		информации (симметричные и асимметричные алгоритмы шифрования, электронная цифровая подпись, стеганография). Различные технологии аутентификации. Технологии защиты межсетевого обмена данных.		
	2	Технология обеспечения безопасности сетевых операционных систем. Основы технологии виртуальных защищенных сетей VPN. Технология обнаружения вторжений (анализ защищенности и обнаружения сетевых атак). Требования по защите от несанкционированного доступа. Технические средства обеспечения безопасности многоканальных телекоммуникационных систем.		3
	Лабораторные занятия		**18**	
	9	Контроль над подключением узлов к портам коммутатора.	2	
	10	Списки управления доступом. Фильтрация по MAC – адресу.	2	
	11	Списки управления доступом. Фильтрация по IP – адресам.	2	
	12	Анализ уязвимости протокола IP.	2	
	13	Обнаружение неавторизованного сервера DHCP.	2	
	14	Построение VPN на основе IPSec протокола.	2	
	15	Удаленный доступ на базе протокола PPTP.	2	
	16	Построение L2TP туннеля.	2	
	17	Организация защищенного удаленного управления Windows-сервером.	2	
	Самостоятельная работа обучающихся: Работа с конспектом. Оформление отчетов лабораторных работ и подготовка к их защите. Подготовка к устному опросу.		10	
Всего:			**144**	
Самостоятельная работа при изучении раздела ПМ 03. Систематическая проработка конспектов занятий, учебной и специальной технической литературы . Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к			**48**	

их защите. Поиск информации в Интернет.		
Учебная практика **Виды работ:** - Назначение, классификация межсетевых экранов. - Настройка межсетевого экрана DFL-210. - Фильтрация трафика. Пакетные фильтры. Пакетные фильтры iptables. - Настройка пакетного фильтра. - Анализ защищенности сетевых ресурсов. Управление уязвимостями. Системы управления уязвимостями. - Инвентаризация сетевых ресурсов с использованием утилиты nmap. - Архитектура систем управления уязвимостями. - Типы агентов сканирования. Особенности сетевых агентов сканирования. - Изучение сканера безопасности Nmap. - Криптографические методы защиты информации. - Шифрование различными методами. - Программы архивирования данных.	**36**	
Производственная практика **Виды работ:** - установка, настройка специализированного оборудования по защите информации; - выявление возможных атак на автоматизированные системы; - установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей; - конфигурирование автоматизированных систем и информационно-коммуникационных сетей; - проверка защищенности автоматизированных систем и информационно-коммуникационных сетей; - организации защиты в различных операционных системах и средах.	**18**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1 Требования к минимальному материально-техническому обеспечению

Реализация программы модуля требует наличия лаборатории информационной безопасности.

Оборудование лаборатории информационной безопасности и рабочих мест лаборатории:

стол однотумбовый - 1 шт., стол компьютерный на металлическом каркасе - 14 шт., коммутаторы DGS-3312SR - 2 шт., коммутаторы DES-3526 - 4 шт., коммутаторы DES-3200-24 - 3 шт., коммутаторы DES-3028 - 3 шт, межсетевые экраны DFL-210 - 2 шт., ПК 1 шт.: монитор 17” TFT Samsung 172S, системный блок (Microlab/Intel Core i3 2120 3.3GHz/ DDR III 2Gb/WD 500Gb SATA/Gigabit Lan), ПК 14 шт.: монитор 17” TFT HP 1740, системный блок (HP Compaq dx2000/Intel Pentium 4 2.8GHz/ DDR II 1Gb/Seagate 40Gb IDE/Intel Pro 100 Lan), интерактивная доска, Smart Board, мультимедиа-проектор Mitsubishi XD211U, программное обеспечение: MS Windows Server 2008, MS Windows Server 2008 R2, 7Zip, LibreOffice 5, Foxit Reader 7, Virtual Box 4.

4.2 Информационное обеспечение обучения

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] : учебное пособие / Г.А. Бузов. - Электрон. дан. - Москва: Горячая Линия–Телеком, 2018. - URL: https://ibooks.ru/reading.php?productid=354357. - Режим доступа: для зарегистрир.пользователей.—Текст : электронный.

2. Костин, В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 31 с. — ISBN 978-5-906953-53-7. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/98200 – Режим доступа: для зарегистрир.пользователей.—Текст : электронный.

3. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов : Ай Пи Эр Медиа, 2019. — 227 с. — ISBN 978-5-4486-0485-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО

PROFобразование : [сайт]. — URL: https://profspo.ru/books/80290 – Режим доступа: для зарегистрир.пользователей.—Текст : электронный.

Дополнительные источники:

1. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А. В. Васильков, И. А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-16-104336-3. - URL: https://znanium.com/catalog/product/1082470 – Режим доступа: для зарегистрир.пользователей.—Текст : электронный.

2. Мельников, Д.А. Информационная безопасность открытых систем [Электронный ресурс]: учебное пособие / Д.А. Мельников. - Электрон. дан. – Москва: Флинта, 2019. – URL: https://ibooks.ru/reading.php?productid=340843.– Режим доступа: для зарегистрир.пользователей.—Текст : электронный.

3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — URL: https://profspo.ru/books/87995– Режим доступа: для зарегистрир.пользователей.—Текст : электронный.

4.3 Общие требования к организации образовательного процесса

Обязательным условием допуска для проведения занятий по профессиональному модулю является изучение общепрофессиональных дисциплин профессионального цикла: Вычислительная техника, Теория электросвязи, Основы телекоммуникаций, Электрорадиоизмерения, Энергоснабжение телекоммуникационных систем, Теория электрических цепей.

Обязательным условием допуска к учебной практике в рамках профессионального модуля является освоение соответствующих разделов программы соответствующего междисциплинарного курса (МДК).

Обязательным условием допуска к производственной практике в рамках профессионального модуля является освоение соответствующих разделов программы профессионального модуля, учебной практики в рамках профессионального модуля.

Производственная практика проводится в организациях на основе договоров, заключаемых между образовательной организацией и организациями.

В период прохождения производственной практики обучающиеся могут зачисляться на вакантные должности, если работа соответствует требованиям программы производственной практики.

Выполнение лабораторных занятий предполагает деление группы на подгруппы по числу рабочих мест, оборудованных персональным компьютером.

4.4 Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): наличие высшего образования, соответствующего профилю модуля.

Преподаватели получают дополнительное профессиональное образование по программам повышение квалификации, в том числе в форме стажировки в профильных организациях не реже 1 раза в 3 года.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой:

инженерно-педагогический состав: дипломированные специалисты – преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин.

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

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1. Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи	− Четкое понимание проблем информационной безопасности в сфере телекоммуникаций; − Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; − Выбор механизмов и средств обеспечения информационной безопасности - программных и программно-аппаратных; − Грамотно оформлять документацию для лицензирования работ в области информационной безопасности; − Разрабатывать политики в области информационной безопасности;	**Текущий контроль:** **Устный и письменный опрос по темам:** - Основы информационной безопасности - Правовое обеспечение информационной безопасности **Практические работы:** - Традиционные симметричные криптосистемы **Лабораторные работы:** - Документы, регламентирующие деятельность в области защиты информации - Ответственность за нарушения законодательства в сфере защиты информации. - Изучение положений о государственном лицензировании деятельности в области защиты информации - Изучение положений о сертификации средств защиты информации по требованиям безопасности информации - Анализ Доктрины ИБ РФ. **Наблюдение** **Анализ** **Экспертная оценка**

ПК 3.2. Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению	− Расчет рисков в области информационной безопасности и выдача рекомендаций по их устранению; − Владеть сервисами, обеспечивающими информационную безопасность в многоканальных телекоммуникационных системах и сетях связи; − Владеть технологией аутентификации; − Обеспечивать технологию защиты межсетевого обмена данными; − Построение системы антивирусной защиты телекоммуникационных систем и сетей электросвязи.	**Текущий контроль:** **Устный и письменный опрос по темам:** - Организационное обеспечение информационной безопасности **Практические работы:** - Традиционные симметричные криптосистемы **Лабораторные работы:** - Изменение MAC-адреса в ОС Windows - Изучение трафика атаки с помощью программы Wireshark - Обнаружение сетевых анализаторов с помощью программы Cain&Abel. - Уязвимости протокола ARP. Генератор пакетов CommView. - Уязвимости протокола ARP. Программа Cain&Abel. - Мониторинг трафика ARP. Программа arpwatch. - Мониторинг трафика ARP. Программа ARP – monitor. - Применение антивирусной защиты в информационных системах. - Анализ уязвимости протокола IP. - Обнаружение неавторизованного сервера DHCP **Наблюдение** **Анализ** **Экспертная оценка**

ПК 3.3. Обеспечивать безопасное администрирование многоканальных телекоммуникационных систем и информационно-коммуникационных сетей связи	− Выбор и использование пакетов прикладных программ для безопасного администрирования сетевых операционных систем; − Обеспечение программными и программно-аппаратными методами безопасности сетей доступа, объединенных сетей и управления телекоммуникационными сетями.	**Текущий контроль:** **Устный и письменный опрос по темам:** - Программно-аппаратные средства защиты информации - Администрирование телекоммуникационных систем и сетей связи **Лабораторные работы:** - Контроль над подключением узлов к портам коммутатора. - Списки управления доступом. Фильтрация по MAC – адресу. - Списки управления доступом. Фильтрация по IP – адресам. - Построение VPN на основе IPSec протокола - Удаленный доступ на базе протокола PPTP. - Построение L2TP туннеля. - Организация защищенного удаленного управления Windows-сервером. **Наблюдение** **Анализ** **Экспертная оценка**

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 общие компетенции)	**Основные показатели оценки результата**	**Формы и методы**
ОК 1. Понимать сущность и социальную	− Понимание сущности и социальной значимости специальности в соответствии с	Текущий контроль Наблюдение Экспертная оценка

значимость своей будущей профессии, проявлять к ней устойчивый интерес	нормативными документами (квалификационная характеристика, ФГОС). – Демонстрация устойчивого интереса в процессе освоения специальности	
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество	– Организация собственной деятельности в соответствии с выбором методов и способов выполнения профессиональный задач – Оценка эффективности и качества решения профессиональных задач в соответствии с менеджментом качества	Текущий контроль Наблюдение Экспертная оценка
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность	– Принятие решений в собственной деятельности в соответствии с рабочей ситуацией в учебных и производственных условиях. – Демонстрация способности нести ответственность за результаты своей работы в учебных и производственных условиях.	Текущий контроль Наблюдение Экспертная оценка
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития	– Поиск информации в соответствии с эффективным выполнением профессиональных задач	Текущий контроль Наблюдение Экспертная оценка
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности	– Демонстрация использования информационно - коммуникационных технологий в учебной и профессиональной деятельности	Текущий контроль Наблюдение Экспертная оценка

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями	– Работа в коллективе и команде в соответствии с правилами менеджмента. – Общение с коллегами, руководством, потребителями в соответствии с правилами психологии общения.	Текущий контроль Наблюдение Экспертная оценка
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий	Демонстрация способности нести ответственность за результаты работы членов команды (подчиненных) и результата выполнения задания в учебных и производственных условиях.	Текущий контроль Наблюдение Экспертная оценка
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	Планирование самообразования и повышения квалификации в соответствии с изменениями требований работодателей.	Текущий контроль Наблюдение Экспертная оценка
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности	Демонстрация способности ориентироваться в условиях частой смены технологий в профессиональной деятельности	Текущий контроль Наблюдение Экспертная оценка
Промежуточная аттестация: **МДК.03.01, МДК.03.02 - дифференцированный зачет комплексный** **УП.03, ПП.03 - дифференцированный зачет комплексный** **ПМ.03 - экзамен (квалификационный)**		