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
_____ 2022 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

по специальности:

11.02.15 Инфокоммуникационные сети и системы связи

г. Архангельск
2022

Рабочая программа профессионального модуля составлена на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи, примерной основной образовательной программы по специальности 11.02.15 Инфокоммуникационные сети и системы связи и в соответствии с учебным планом по специальности 11.02.15 Инфокоммуникационные сети и системы связи.

Рабочая программа рассмотрена и одобрена цикловой комиссией Сети и системы связи

Протокол № 9 от 20.05. 2022 г.

Председатель _____ П.М. Рыжков

Составители:

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

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

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

1.1 Область применения рабочей программы

Рабочая программа профессионального модуля – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 11.02.15 Инфокоммуникационные сети и системы связи.

1.2 Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующие ему общие компетенции и профессиональные компетенции:

1.2.1 Перечень общих компетенций и личностных результатов реализации программы воспитания

Код	Наименование общих компетенций и личностных результатов
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, применять стандарты антикоррупционного поведения
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 языках
ЛР 1, ЛР 2, ЛР 3, ЛР 4, ЛР 9, ЛР 10, ЛР 11	

1.2.2 Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи
ПК 3.1	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности
ПК 3.2	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи
ПК 3.3	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования

1.2.3 В результате освоения профессионального модуля студент должен:

Иметь практический опыт в	- анализе сетевой инфраструктуры; - выявлении угроз и уязвимости в сетевой инфраструктуре; - разработке комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи; - осуществлении текущего администрирования для защиты инфокоммуникационных сетей и систем связи; - использовании специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.
уметь	- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; - определять оптимальные способы обеспечения информационной безопасности; - осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;

	- выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; - защищать базы данных при помощи специализированных программных продуктов.
знать	- принципы построения информационно-коммуникационных сетей; - международные стандарты информационной безопасности; - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия; - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия; - классификацию угроз сетевой безопасности; - методы и способы защиты информации, передаваемой по кабельным направляющим системам; - правила проведения возможных проверок согласно нормативным документам Федеральной службы по техническому и экспортному контролю; - средства защиты различных операционных систем и среды передачи информации.

1.3 Количество часов, отводимое на освоение профессионального модуля

Всего часов – 546.

Из них

на освоение МДК.03.01 – 172 часа, в том числе самостоятельная работа – 28 часов,

МДК.03.02 – 176 часов, в том числе самостоятельная работа – 32 часа,

на практики – 180 часов, в том числе учебную – 72 часа и производственную – 108 часов.

Промежуточная аттестация – 18 часов.

2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.		Объем профессионального модуля, ак. час.						
				Работа обучающихся во взаимодействии с преподавателем					Самостоятельная работа	Промежуточная аттестация (экзамен)
				Обучение по МДК			Практики			
			Всего	В том числе						
				Лабораторных и практических занятий	Курсовых работ (проектов)	Зачетные занятия	Учебная	Производственная		
ПК 3.1-3.3 ОК 01-10	**Раздел 1.** Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	**172**	**144**	78	-	2			**28**	**-**
ПК 3.1-3.3 ОК 01-10	**Раздел 2.** Применение комплексной системы защиты информации в инфокоммуникационных	**248**	**144**	72	-	2	**72**		**32**	**-**

	системах и сетях связи									
ПК 3.1-3.3 ОК 01-10	Производственная практика (по профилю специальности), часов	**108**						**108**	**-**	
ПК 3.1-3.3 ОК 01-10	Промежуточная аттестация (экзамен)	***18***						***-***	***-***	***18***
	Всего:	***546***	***288***	***150***	***-***	***4***	***72***	***108***	***60***	***18***

2.2 Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)		Объем в часах
1	**2**		**3**
Раздел ПМ.1 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи			**172**
МДК 03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи			**172**
	Содержание		**14**
Тема 1.1 Основы безопасности информационных технологий	1	Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий.	2
	2	Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.	2
	3	Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности	2
	4	Принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Принципы построения системы обеспечения безопасности	2

		информации в автоматизированной системе.	
	5	Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.	2
	6	Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации.	2
	7	Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Регистрация и оперативное оповещение о событиях безопасности.	2
	Лабораторные работы		**6**
	1	Документы, регламентирующие деятельность в области защиты информации.	4
	2	Ответственность за нарушения законодательства в сфере защиты информации.	2
	Самостоятельная работа обучающихся		**4**
	Изучение постановлений правительства, законов и других руководящих документов в области защиты информации.		2
	Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.		2
Тема 1.2 Обеспечение безопасности информационных технологий	**Содержание**		**20**
	1	Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ.	2
	2	Обязанности пользователей и ответственных за обеспечение	2

		безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников. Ответственность за нарушения. Порядок работы с носителями ключевой информации.	
	3	Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты.	2
	4	Документы, регламетирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуска сотрудников. Правила именования пользователей. Процедур авторизации сотрудников.	2
	5	Порядок изменения конфигурации программно-аппаратных средств. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация.	2
	6	Регламентация процессов разработки, внедрения и сопровождения задач. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем.	2
	7	Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов.	2
	8	Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы. Средства обеспечения непрерывной работы. Обязанности и действия персонала по обеспечению непрерывной работы.	2
	9	Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности.	2

		Организационно-правовой статус службы обеспечения безопасности информации.	
	10	Концепция безопасности информационных технологий предприятия. Назначение и статус документа. Вопросы, которые должны быть отражены в Концепции.	2
	Лабораторные работы		**10**
	3	Изучение положений о государственном лицензировании деятельности в области защиты информации.	4
	4	Изучение положений о сертификации средств защиты информации по требованиям безопасности информации.	4
	5	Анализ Доктрины ИБ РФ.	2
	Самостоятельная работа обучающихся		**8**
	Дополнительное конспектирование материала по теме «Обеспечение безопасности информационных технологий»		4
	Проведение информационное обследование защищаемых ресурсов		4
Тема 1.3 Средства защиты информации от несанкционированного доступа	**Содержание**		**12**
	1	Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абонентов.	2
	2	Рекомендации по выбору средств защиты информации от НСД. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК к средствам защиты информации.	2
	3	Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации	2
	4	Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей.	1

	5	Назначение и функциональные возможности eToken и Рутокен. Алгоритм генерации одноразовых паролей.	1
	6	Формирование электронной цифровой подписи. Вычисление ключа согласования Диффи-Хеллмана.	2
	7	Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа. Полномочное разграничение доступа. Регистрация событий, имеющих отношение к безопасности	2
	Лабораторные работы		**28**
	6	Контроль над подключением узлов к портам коммутатора.	2
	7	Списки управления доступом. Фильтрация по MAC – адресу.	2
	8	Списки управления доступом. Фильтрация по IP – адресам.	2
	9	Мониторинг трафика ARP.	4
	10	Инвентаризация сетевых ресурсов с использованием утилиты nmap.	6
	11	Анализ защищенности сетевых ресурсов	6
	12	Конфигурирование роли Active Directory на сервере	6
	Самостоятельная работа обучающихся		**8**
	Применение программно-аппаратных средств для обеспечения разграничения доступа к защищаемой информации.		2
	Составление доклада по перспективе и направлению развития программно-аппаратных средств защиты информации на основе публикаций в периодической специализированной аппаратуре.		4
	Составление таблицы сравнительных характеристик устройств аутентификации		2
Тема 1.4 Обеспечение безопасности компьютерных систем и сетей	**Содержание**		**18**
	1	Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративная сеть. Уязвимости и их классификация.	2

	2	Назначение, возможности и защитные механизмы межсетевых экранов. Угрозы, связанные с периметром сети.	2
	3	Типы межсетевых экранов. Сертификация межсетевых экранов.	2
	4	Анализ содержимого почтового и WEB-трафика. HTTP-трафик.	2
	5	Виртуальные частные сети. VPN на основе криптошлюза.	2
	6	Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями.	2
	7	Особенности сетевых агентов сканирования. Специализированный анализ защищенности. Обзор средств анализа защищенности.	2
	8	Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий.	2
	9	Введение в технологию обнаружения атак. Классификация систем обнаружения атак.	2
	Лабораторные работы		**34**
	13	Изменение MAC-адреса в ОС Windows.	2
	14	Изучение трафика атаки с помощью программы Wireshark.	2
	15	Обнаружение сетевых анализаторов с помощью программы Cain&Abel.	2
	16	Уязвимости протокола ARP. Генератор пакетов CommView.	2
	17	Уязвимости протокола ARP. Программа Cain&Abel.	2
	18	Применение антивирусной защиты в информационных системах.	2
	19	Анализ уязвимости протокола IP.	2
	20	Обнаружение неавторизованного сервера DHCP.	2
	21	Построение VPN на основе IPSec протокола.	2
	22	Удаленный доступ на базе протокола PPTP.	2
	23	Построение L2TP туннеля.	2
	24	Организация защищенного удаленного управления Windows-	2

		сервером.	
	25	Настройка межсетевого экрана DFL-210	4
	26	Настройка пакетного фильтра iptables.	6
	Самостоятельная работа обучающихся		**8**
	Применение антивирусных программ для защиты информации от несанкционированного доступа.		2
	Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа.		2
	Применение различных программ для оперативного и гарантированного восстановления информации на ПК.		2
	Составление таблицы для сравнения характеристик межсетевых экранов		2
Зачетные занятия			**2**
Раздел ПМ 2. Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи			**248**
МДК 03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи			**176**
Тема 2.1 Основы информационной безопасности	**Содержание**		**12**
	1	Основные понятия информационной безопасности. Сущность и понятия защиты информации.	2
	2	Значение информационной безопасности и ее место в системе национальной безопасности.	2
	3	Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.	2
	4	Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной	2

		безопасности Российской Федерации.	
	5	Состояние информационной безопасности РФ и основные задачи по ее обеспечению.	2
	6	Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности.	2
	Лабораторные работы		**10**
	1	Исследование возможностей профессионального нелинейного радиолокатора	2
	2	Исследование возможностей многофункционального поискового прибора	2
	3	Исследование возможностей анализатора спектра	2
	4	Исследование возможностей имитатора источника радиосигналов с различными видами модуляции	2
	5	Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга	2
	Самостоятельная работа обучающихся		**6**
	Изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере.		4
	Ознакомление с нормативными документами.		2
Тема 2.2Организационно-правовые аспекты защиты информации	**Содержание**		**10**
	1	Структура правовой защиты информации. Система документов в области защиты информации.	2
	2	Организационные основы защиты информации. Принципы организационной защиты информации.	2
	3	Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции. Обзор стандартов и методических документов в области защиты информации. Регулирующие организации в области защиты информации.	2

	4	Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности.	2
	5	Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере.	2
	Лабораторные работы		**8**
	6	Исследование возможностей скоростного приемника сигналов	2
	7	Исследование принципов работы индикаторов поля	2
	8	Исследование возможностей работы фильтров сетевых помехоподавляющих	2
	9	Исследование работы генератора шума для защиты от ПЭМИН	2
	Самостоятельная работа обучающихся		**6**
	Подготовка презентации на тему «Организационно-правовые аспекты защиты информации»		6
Тема 2.3 Комплексная система защиты информации	**Содержание**		**10**
	1	Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации. Стратегии комплексной защиты информации. Структура и основные характеристики комплексной защиты информации.	2
	2	Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна.	2
	3	Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны.	2
	4	Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение.	2

	5	Способы и средства обнаружения угроз. Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз.	2
	Лабораторные работы		**10**
	10	Исследование уязвимостей и построение модели угроз объекта защиты.	2
	11	Разработка комплексной системы инженерно-технической защиты информации на объекте.	4
	12	Исследование возможностей устройства для защиты объектов информатизации	2
	13	Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств	2
	Самостоятельная работа обучающихся		**6**
	Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности.		2
	Составление доклада по перспективе и направлению развития комплексных средств защиты информации на основе публикаций в периодической литературе.		4
Тема 2.4 Инженерно-техническая защита информации	**Содержание**		**26**
	1	Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты.	2
	2	Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации.	2
	3	Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки	2

		информации.	
	4	Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации.	2
	5	Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД.	2
	6	Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению.	2
	7	Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи.	2
	8	Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрытия речевой информации от подслушивания.	2
	9	Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок.	2
	10	Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания.	2
	11	Контроль слаботочных цепей. Принципы контроля линий заземления.	2
	12	Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации.	2
	13	Методы поиска радиоизлучений закладных устройств.	2

		Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники.	
	Лабораторные работы		**26**
	14	Исследование возможностей автоматизированной системы изменений сверхмалых величин	2
	15	Исследование технических средств и отходящих от них линий с помощью системы измерений сверхмалых величин	2
	16	Исследование возможностей системы оценки защищенности оптических линий связи	2
	17	Измерение параметров ВОСП с помощью системы оценки защищенности оптических линий связи	2
	18	Оценка защищенности оптических линий связи с помощью системы оценки защищенности оптических линий связи	2
	19	Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН	2
	20	Оценка защищённости с использованием системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН	2
	21	Измерение параметров ПЭМИН и расчет показателей защищенности технического средства	2
	22	Исследование возможностей системы оценки защищенности выделенных помещений	2
	23	Измерение уровня звукового давления вблизи и на удалении от источника с помощью комплекса оценки защищенности выделенных помещений	2
	24	Измерение уровня виброускорения в ограждающих конструкциях	2
	25	Расчет и оценка защищенности помещения по акустическому каналу	2

	26	Расчет и оценка защищенности помещения по виброакустическому каналу	2
	Самостоятельная работа обучающихся		**10**
	Разработка пакета документации по инженерно-технической защите информации на объекте.		2
	Изучение возможностей инженерно-технических средств защиты информации.		2
	Изучение технических характеристик инженерно-технических средств защиты информации.		2
	Разработка предложений по инженерно-технической защите информации на определенном объекте.		2
	Составление таблицы для сравнения характеристик средства нелинейной радиолокации.		2
Тема 2.5 Криптографическая защита информации	**Содержание**		**6**
	1	Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	1
	2	Симметричные криптосистемы. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования	1
	3	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	2
	4	Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие	2

		криптоанализа.	
	Лабораторные работы		**12**
	27	Поиск и локализация скрытых видеокамер	2
	28	Исследование методов защиты сотовых телефонов от несанкционированного прослушивания	2
	29	Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов	2
	30	Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора	2
	31	Поиск устройств негласного съема информации с помощью многофункционального поискового прибора	2
	32	Оценка защищенности помещения с помощью многофункционального поискового прибора	2
	Самостоятельная работа обучающихся		**2**
	Разработка предложений по комплексу технических мероприятий по защите линий связи объекта.		1
	Разработка предложений по защите информации от несанкционированного доступа по акустическому каналу в помещении.		1
Тема 2.6 Аттестация и лицензирование объектов защиты	**Содержание**		**6**
	1	Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ.	2
	2	Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний.	2
	3	Лицензирование деятельности в области защиты	2

		конфиденциальной информации. Документы, разрабатываемые на объектах информатизации. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании.	
	Лабораторные работы		**6**
	33	Обнаружение, идентификация и локализация цифровых радиопередающих устройств с помощью индикаторов поля	2
	34	Исследование работы генератора шума по сети электропитания и линиям заземления	2
	35	Поиск и обнаружение радиоизлучающих средств	2
	Самостоятельная работа обучающихся		**2**
	Составление списка уязвимостей предложенного объекта. Самостоятельная разработка комплекта документации на объекте информатизации.		2
Зачетные занятия			**2**
Учебная практика **Виды работ**	**Содержание учебной практики**		**72**
	1	Установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов	6
	2	Установка и настройка типовых программно-аппаратных средств защиты информации	6
	3	Использование программно-аппаратных и инженерно-технических средств	6
	4	Настройка, регулировка и ремонт оборудования средств защиты	6
	5	Выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой	6
	6	Проведение типовых операции настройки средств защиты	6

		операционных систем	
	7	Проведение аттестации объектов защиты	6
	8	Определение источников несанкционированного доступа, исходя из модели угроз	6
	9	Определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта	6
	10	Обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств	6
	11	Защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК	6
	12	Защита информации организационными методами в соответствии с инструкциями на объекте	6
Производственная практика **Виды работ** Участие в создании комплексной системы защиты на предприятии. Применение программно-аппаратных средств защиты информации на предприятии Применение инженерно-технических средств защиты информации на предприятии. Применение криптографических средств защиты информации на предприятии.			**108**
Промежуточная аттестация (экзамен)			18
		Всего	**546**

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Реализация программы модуля требует наличия кабинета компьютерного моделирования, лаборатории информационной безопасности телекоммуникационных систем, лаборатории телекоммуникационных систем.

Кабинет компьютерного моделирования, оснащенный оборудованием и техническими средствами обучения: доска на стекле – 1 шт., стол 1-тумбовый – 15 шт., стол аудиторный – 8 шт., стул ученический на металлокаркасе – 28 шт., ПК - 1 шт.: монитор 19” TFT HP LA 1908w, системный блок (Colorsit L8011/Asus P5LD2 SE/Intel Celeron 440 2.0GHz/DDR II 1Gb/GeForce 8400 GS/Seagate 80Gb SATA II/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/FE Lan), учебная доска, программное обеспечение: MS Windows XP, MS Visio 2007, MathCAD 2014, Multisim 10.1, Any Logic 7, Python 3.4, 7-Zip, Консультант+, LibreOffice 5, Foxit Reader 7, локальная сеть с доступом к ЭБС и СДО.

Лаборатория информационной безопасности телекоммуникационных систем, оснащенная оборудованием и техническими средствами обучения: Стол однотумбовый - 1 шт., стол компьютерный на металлическом каркасе - 14 шт., Доска классная ДА-32 — 1шт., телекоммуникационный шкаф 19 – 1 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), мультимедиа-проектор Mitsubishi XD211U, консольные кабели, соединительные провода, программное обеспечение: MS Windows Server 2008, MS Windows Server 2008 R2, LibreOffice 5, WinPCad., WireShark V1.8.6.

Лаборатория телекоммуникационных систем, оснащенная оборудованием и техническими средствами обучения: стол 1-тумб. - 1 шт., стол 2х тумбовый полированный - 3 шт., стол чертежный - 1 шт., табурет - 23 шт., мультиметр MAS 830b - 1 шт., дозиметр - 2 шт., акустическая система Creative SBS35 - 1 шт., прибор В3-38 - 3 шт., прибор Г3-36 - 4 шт., прибор измерительный М 890F - 1 шт., прибор измерительный М 890С - 1 шт., прибор измерительный М 890G - 1 шт., прибор УИП-2,5 - 2 шт., прибор Ц-4315 - 3 шт., анализатор AnCom TDA-5 - 1 шт., аппаратура ТТ-12 - 1 шт., аппаратура ТТ-48 - 1 шт., Анализатор потока Е1 Беркут-Е1 - 1 шт., блок ОGМ-12 - 2 шт., блок окончаний линейного тракта ОЛТ-025 - 2 шт., прибор БОЛТ 1024 - 1 шт., прибор ВУК-36/60 - 1 шт., выпрямительное устройство ВУТ - 2 шт., выпрямитель ИПС-1200 220/48 - 3 шт., выпрямительное устройство ВУК 67-70 - 1 шт., измерительный прибор П-

321М - 1 шт., комплект линейного тракта КЛТ-011-06 - 2 шт., набор инструментов для оптоволокна - 1 шт., оптический тестер 1203С - 1 шт., осциллограф С1-112 - 4 шт., паяльная станция L852D+ - 1 шт., прибор Г3-111 - 1 шт., прибор Г4-102 - 1 шт., прибор Г5-54 - 1 шт., прибор ПЭИ-ИКМ - 2 шт., прибор С1-55 - 2 шт., прибор С1-70-1 - 2 шт., прибор С1-72 - 4 шт., прибор СЛР - 8 шт., прибор СЛУК-ОП - 1 шт., прибор ТЭС-7М - 1 шт., прибор Ч3-32 - 2 шт., прибор Ч3-33 - 1 шт., прибор Ч3-34 - 2 шт., сдвоенный модуль FG-PAM-SAN - 2 шт., стойка СВКО - 1 шт., стойка СИП - 1 шт., стойка СКК-ТТ-10 - 1 шт., стойка СКП-1 - 1 шт., стойка СУГО-5М - 1 шт., универсальный конструктив FG-MRU-AC/DC - 1 шт., Ф2Д21 "Изотоп-2" - 1 шт., Ф2П21 "Изотоп-2" - 1 шт., Мультиплексор SMS-150V - 1 шт., Стойка(каркас) 2,075 для мультиплексора SDH - 1 шт., мультиплексор NEC SMS-150V - 1 шт. ПК - 7 шт.: монитор 17”SincMaster системный блок ATX P4 (корпус), GA-8IR533 S478 (материнская плата), Intel Pentium 4 1.7GHz (прцессор) 4xDDR 512Mb transcend (ОЗУ), программное обеспечение: MS Windows XP.

3.2 Информационное обеспечение реализации программы

3.2.1 Основные печатные и электронные издания

1. Бубнов, А.А. Основы информационной безопасности (3-е изд.) : учебник / А.А. Бубнов. - Академия, 2020.

2. Бубнов, А.А. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) : учебник / Бубнов, А.А. - Академия, 2019.

3. 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 зарегистр. пользователей. – Текст электронный.

4. Ворона, В. А. Технические системы охранной и пожарной сигнализации. (Серия «Обеспечение безопасности объектов», выпуск 5) / В. А. Ворона, В. А. Тихонов. - Горячая Линия - Телеком, 2018.

5. Ильин, М.Е. Криптографическая защита информации в объектах информационной инфраструктуры (1-е изд.) : учебник. / М.Е. Ильин. - Академия, 2020.

6. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для СПО / О. В. Казарин, А. С. Забабурин. - Юрайт, 2020.

7. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. / В. Г. Олифер, Н. А. Олифер. – Питер, 2020.

3.2.2 Дополнительные источники:

1. 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 зарегистр. пользователей. – Текст электронный.

2 Федорова, Г.Н. Разработка, администрирование и защита баз данных (4-е изд., стер.) : учебник / Г.Н. Федорова. - Академия, 2020.

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	- классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно; - анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный; - возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно; - мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме; - недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выявлены в полном объеме; - тестирование систем с целью определения уровня защищенности выполнено, уровень защищенности определен верно	– тестирование; – письменный опрос; – устный опрос; – оценка выступления с докладом; – оценка результатов выполнения лабораторных работ: МДК 03.01 №№1-26; МДК 03.02 №№ 1-35 – экспертное наблюдение выполнения лабораторных работ, – оценка процесса и результатов выполнения видов работ на практике –экзамен
ПК 3.2 Разрабатывать комплекс методов и средств защиты	- для обеспечения информационной безопасности выбраны	– тестирование; – письменный опрос;

информации в инфокоммуникационных сетях и системах связи	оптимальные способы; - выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях	– устный опрос; – оценка выступления с докладом; – оценка результатов выполнения лабораторных работ: МДК 03.01 №№1-26; МДК 03.02 №№ 1-35 – экспертное наблюдение выполнения лабораторных работ, – оценка процесса и результатов выполнения видов работ на практике –экзамен
ПК 3.3 Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования	- мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными; - политика безопасности сетевых элементов и логических сетей разработана в полном объеме; - расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми	– тестирование; – письменный опрос; – устный опрос; – оценка выступления с докладом; – оценка результатов выполнения лабораторных работ: МДК 03.01 №№1-26; МДК 03.02 №№ 1-35 – экспертное наблюдение выполнения лабораторных работ, – оценка процесса

	стандартами; - установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи выполнена в соответствии с отраслевыми стандартами; - конфигурирование автоматизированных систем и информационно-коммуникационных сетей осуществлено в соответствии с политикой информационной безопасности и отраслевыми стандартами; - базы данных максимально защищены при помощи специализированных программных продуктов; - ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами	и результатов выполнения видов работ на практике –экзамен
ОК 1. 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. Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и
ОК 2. 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 3. Планировать и реализовывать собственное профессиональное и личностное развитие	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы	производственной практикам. Экзамен
ОК 4. 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 5. 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 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	
ОК 7. 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 8. Использовать средства физической	- эффективность выполнения правил ТБ во	

культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	время учебных занятий, при прохождении учебной и производственной практик	
ОК 9.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 языках	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	
	МДК.03.01 – дифференцированный зачет **МДК.03.02 - дифференцированный зачет** **УП.03 - дифференцированный зачет** **ПП.03 - дифференцированный зачет** **ПМ.03 - экзамен по модулю**	