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)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 7EDEC31CD7768B9DAE1B249DD415B9F5
Владелец: Топанов Александр Павлович
Действителен: с 02.05.2023 до 25.07.2024

УТВЕРЖДАЮ
Зам. директора по учебной работе
_____ М.А. Цыганкова
28 03 2024 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

по специальности:

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

г. Архангельск
2024

Рабочая программа профессионального модуля составлена на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, примерной основной образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем и в соответствии с учебным планом по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рабочая программа рассмотрена и одобрена цикловой комиссией Информационной безопасности инфокоммуникационных систем

Протокол № 4 от 23 05 2024 г.

Председатель _____ А.А. Садков

Составитель:

А.А. Садков, преподаватель первой квалификационной категории АКТ (ф) СПбГУТ.

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

1.1 Область применения рабочей программы

Рабочая программа профессионального модуля – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.2 Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» и соответствующие ему общие компетенции и профессиональные компетенции:

1.2.1 Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 09	Использовать информационные технологии в профессиональной

	деятельности.

1.2.2 Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	**Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты**
ПК 3.1	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях
ПК 3.2	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях
ПК 3.3	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями
ПК 3.4	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

1.2.3 В результате освоения профессионального модуля студент должен:

Иметь практический опыт	- установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам; - защиты информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями; - проведения отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.
уметь	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС;

	- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - использовать средства физической защиты линий связи ИТКС; - применять нормативные правовые акты и нормативные методические документы в области защиты информации.
знать	- способы защиты информации от утечки по техническим каналам с использованием технических средств защиты; - основные типы технических средств защиты информации от утечки по техническим каналам; - методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам; - порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим причинам; - содержание и организацию работ по физической защите линий связи ИТКС; - принципы действия и основные характеристики технических средств физической защиты; - законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности; - принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

1.3 Количество часов, отводимое на освоение профессионального модуля

Всего часов – 732
в том числе в форме практической подготовки – 432.
Из них
на освоение МДК.03.01 – 257 часов, в том числе самостоятельная работа – 49 часов.
МДК.03.02 –169 часов, в том числе самостоятельная работа – 25 часов.
на практики –288 часов, в том числе учебную – 108 часов и производственную – 180 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			Учебная	Производственная		
				Лабораторных и практических занятий	Курсовых работ (проектов)	Итоговые занятия				
ПК 3.1- ПК.3.4 ОК 1 – ОК 7, ОК 9	**Раздел 1.** Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	**257**	**208**	74	-	**2**	-	-	**49**	-
ПК 3.5 ОК 1 – ОК 7, ОК 9	**Раздел 2.** Физическая защита линий связи информационно-телекоммуникационных систем и сетей	**169**	**144**	70		**2**	-	-	**25**	-
ПК 3.1- ПК.3.4 ОК 1 – ОК 7, ОК 9	Учебная практика	**108**					**108**	-	-	-
ПК 3.1- ПК.3.4 ОК 1 – ОК 7, ОК 9	Производственная практика	**180**						**180**	-	-
ПК 3.1- ПК.3.4	Промежуточная	**18**						-	-	***18***

ОК 1 – ОК 7, ОК 9	аттестация (экзамен)									
	Всего:	***732***	***352***	*144*	-	***4***	***108***	***180***	***74***	***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
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты			**257**
МДК.03.01. Защита информации в ИТКС с использованием технических средств защиты			**257**
Тема 1.1 Предмет и задачи технической защиты информации	**Содержание**		**8**
	1	Защищаемая информация и информационные ресурсы. Объекты информатизации, их классификация и характеристика.	2
	2	Основные понятия термины и определения в области технической защиты информации. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в РФ.	2
	3	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.	2
	4	Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	2
Тема 1.2 Общие положения защиты информации техническими средствами	**Содержание**		**4**
	1	Задачи и требования к способам и средствам защиты информации техническими средствами. Классификация способов и средств защиты информации.	2
	2	Принципы системного анализа проблем инженерно-технической защиты информации.	2
Тема 1.3 Информация как	**Содержание**		**8**

предмет защиты	1	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.	2
	2	Понятие об опасном сигнале. Источники опасных сигналов.	2
	3	Основные и вспомогательные технические средства и системы.	2
	4	Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2
	Практические занятия		**2**
	1	Разработка концепции инженерной защиты информации	2
	Лабораторные занятия		**4**
	1	Запись информации с носителя информации	2
	2	Съем информации с носителя информации	2
	Самостоятельная работа обучающихся.		**10**
	1	Выявление опытным путем характеристик опасного сигнала.	2
	2	Изучение демаскирующих признаков сигналов.	2
	3	Изучение демаскирующих признаков объектов.	2
	4	Изучение видов технические средств и систем.	2
	5	Противдействие технической разведке.	2
Тема 1.4 Технические каналы утечки информации	**Содержание**		**6**
	1	Понятие и особенности утечки информации. Структура канала утечки информации. Характеристика каналов утечки информации.	2
	2	Классификация существующих физических полей и технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	4
	Практические занятия		**2**
	2	Построение матрицы угроз объекта	2

	Самостоятельная работа обучающихся		**4**
	6	Изучение видов каналов утечки информации и их характеристик	4
Тема 1.5 Методы и средства технической разведки	**Содержание**		**8**
	1	Классификация технических средств разведки. Методы и средства технической разведки.	2
	2	Средства несанкционированного доступа к информации.	2
	3	Средства и возможности оптической разведки.	2
	4	Средства дистанционного съема информации.	2
	Практические занятия		**4**
	3	Анализ угроз безопасности информации	2
	4	Разработка политики инженерной защиты информации	2
	Самостоятельная работа обучающихся		**10**
	7	Изучение средств технической разведки, их особенностей.	2
	8	Исследование методов технической разведки.	2
	9	Выявление несанкционированного доступа к информации.	2
	10	Изучение средств оптической разведки, их особенностей.	2
	11	Выявление дистанционного съема информации.	2
Тема 1.6 Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**		**12**
	1	Физические основы побочных электромагнитных излучений и наводок.	2
	2	Акустоэлектрические преобразования.	2
	3	Паразитная генерация радиоэлектронных средств.	2
	4	Виды паразитных связей и наводок.	2
	5	Физические явления, вызывающие утечку информации по цепям электропитания и заземления.	2
	6	Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей.	2

	Лабораторные занятия		**4**
	3	Изучение методов съема сигнала наводки и ее экранирования	2
	4	Изучение методов защиты технических каналов утечки информации	2
	Практические занятия		**8**
	5	Изучение методов предотвращения утечки информации по цепям электропитания	2
	6	Изучение способов предотвращения утечки информации по цепям электропитания	2
	7	Изучение методов предотвращения утечки информации по цепям заземления	2
	8	Изучение способов предотвращения утечки информации по цепям заземления	2
	Самостоятельная работа обучающихся		**10**
	12	Изучение видов утечек информации.	2
	13	Исследование возможных последствий утечки информации.	2
	14	Изучение видов паразитных связей и наводок.	2
	15	Исследование методов съема информации.	2
	16	Изучение способов предотвращения утечек информации.	2
Тема 1.7 Физические процессы при подавлении опасных сигналов	**Содержание**		**8**
	1	Скрытие речевой информации в каналах связи.	2
	2	Подавление опасных сигналов акустоэлектрических преобразований.	2
	3	Экранирование электрических, магнитных и электромагнитных полей.	2
	4	Зашумление опасных сигналов помехами.	2
	Практические занятия		**4**
	9	Изучение возможностей средств инженерно-технической защиты	2

		информации	
	10	Изучение способов выявления технических каналов утечки информации	2
	Лабораторные занятия		**2**
	5	Разработка плана ввода инженерно-технической защиты информации объекта	2
	Самостоятельная работа обучающихся		**4**
	17	Выявление каналов утечки информации.	4
Тема 1.8 Системы защиты от утечки информации по акустическому каналу	**Содержание**		**8**
	1	Технические средства акустической разведки.	2
	2	Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами.	2
	3	Система защиты от утечки по акустическому каналу.	2
	4	Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	2
	Практические занятия		**2**
	11	Работа с акустическими каналами утечки информации	2
	Самостоятельная работа обучающихся		**6**
	18	Изучение принципов и особенностей акустической разведки.	2
	19	Способы подслушивания информации.	2
	20	Подслушивание информации посредством микрофонов.	2
Тема 1.9 Системы защиты от утечки информации по проводному каналу	**Содержание**		**6**
	1	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов.	2
	2	Негласная запись информации на диктофоны. Системы защиты от диктофонов.	2

	3	Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	2
	Практические занятия		
	12	Работа со сравнительными характеристиками методов противодействия подслушиванию	2
	13	Работа со сравнительными характеристиками средств противодействия вторжениям	2
	Лабораторные занятия		**2**
	6	Контроль средств инженерно - технической защиты информации	2
Тема 1.10 Системы защиты от утечки информации по вибрационному каналу	**Содержание**		**6**
	1	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи.	2
	2	Принцип работы виброакустического канала. Системы защиты информации от утечки по вибрационному каналу.	2
	3	Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	2
	Практические занятия		**2**
	14	Защита от утечки по виброакустическому каналу	2
Тема 1.11 Системы защиты от утечки информации по электромагнитному каналу	**Содержание**		**10**
	1	Прослушивание информации от радиотелефонов.	2
	2	Прослушивание информации от работающей аппаратуры.	2
	3	Прослушивание информации от радиозакладок. Приемники информации с радиозакладок.	2
	4	Прослушивание информации от пассивных закладок. Системы защиты от утечки по электромагнитному каналу.	2
	5	Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	2

	Лабораторные занятия		**4**
	7	Определение каналов утечки ПЭМИН	2
	8	Защита от утечки по цепям электропитания и заземления	2
Тема 1.12 Системы защиты от утечки информации по телефонному каналу	**Содержание**		**6**
	1	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.	2
	2	Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи.	2
	3	Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	2
	Лабораторные занятия		**2**
	9	Работа с основными характеристиками систем противодействия наблюдению	2
	Практические занятия		**4**
	15	Изучение методов применения на практике противодействия наблюдению	2
	16	Изучение методов противодействия наблюдению в оптическом диапазоне и радиолокационному наблюдению	2
Тема 1.13 Системы защиты от утечки информации по электросетевому каналу	**Содержание**		**6**
	1	Низкочастотное устройство съема информации.	2
	2	Высокочастотное устройство съема информации.	2
	3	Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	2
	Практические занятия		**6**
	17	Работа со сравнительными характеристиками средств противодействия подслушиванию	2
	18	Работа со сравнительными характеристиками средств противодействия несанкционированному доступу	2
	19	Работа со сравнительными характеристиками средств	2

		противодействия съема информации	
Тема 1.14 Системы защиты от утечки информации по оптическому каналу	**Содержание**		**6**
	1	Характеристики оптического канала утечки информации.	2
	2	Телевизионные системы наблюдения. Приборы ночного видения.	2
	3	Системы защиты информации по оптическому каналу.	2
	Лабораторные занятия		**4**
	10	Сравнение параметров средств перехвата и охранных систем	2
	11	Сравнение характеристик средств перехвата и охранных систем	2
Тема 1.15 Применение технических средств защиты информации	**Содержание**		**14**
	1	Технические средства для уничтожения информации и носителей информации, порядок применения.	2
	2	Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.	4
	3	Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.	4
	4	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	4
	Лабораторные занятия		**4**
	12	Обеспечение защиты информации от угроз воздействия	2
	13	Обеспечение защиты информации от угроз утечки информации	2
	Практические занятия		**4**
	20	Управление силами и средствами системы инженерно-технической защиты информации	2
	21	Управление средствами системы инженерно-технической защиты информации	2

	Самостоятельная работа обучающихся		**5**
	21	Изучение видов уничтожения носителей информации.	2
	22	Исследование принципов аттестация объектов информатизации.	3
Тема 1.16 Эксплуатация технических средств защиты информации	**Содержание**		**16**
	1	Этапы эксплуатации технических средств защиты информации.	2
	2	Виды, содержание и порядок проведения технического обслуживания средств защиты информации.	2
	3	Установка и настройка технических средств защиты информации.	4
	4	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.	2
	5	Организация ремонта технических средств защиты информации.	2
	6	Проведение аттестации объектов информатизации.	4
	Лабораторные занятия		**6**
	14	Изучение методов физической защиты информации	2
	15	Работа со сравнительными характеристиками средств обеспечения физической безопасности объектов	2
	16	Сравнительный анализ типовых решений инженерно-технической защиты информации	2
Итоговое занятие			**2**
Раздел 2. Физическая защита линий связи ИТКС			**169**
МДК.03.02. Физическая защита линий связи ИТКС			**169**
Тема 2.1 Цели и задачи физической защиты объектов информатизации	**Содержание**		**10**
	1	Характеристики потенциально опасных объектов.	2
	2	Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты.	2
	3	Категорирование объектов информатизации.	2

	4	Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.	2
	5	Особенности задач охраны различных типов объектов.	2
	Практические занятия		**4**
	1	Выполнение категорирования объекта информатизации.	2
	2	Составление модели нарушителя для организации.	2
	Лабораторные занятия		**6**
	1	Исследование наведенного параметра ослабления экранированием.	2
	2	Исследование наведенного сигнала ослабления экранированием.	2
	3	Исследование этапов подготовки к проведению специальных исследований основных технических средств и систем (ОТСС).	2
	Самостоятельная работа обучающихся		**5**
	1	Выполнение категорирования объектов информатизации по предложенной методологии.	3
	2	Составление модели нарушителя для конкретной организации.	2
Тема 2.2 Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**		**8**
	1	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты.	2
	2	Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны.	2
	3	Требования к инженерным средствам физической защиты.	2
	4	Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	2
	Практические занятия		**6**
	3	Исследование спектральных характеристик тестовых сигналов ПЭМИН	2
	4	Исследование динамических характеристик сигнала в канале утечки информации	2

	5	Исследование протоколов стендовых специальных исследований и предписания на эксплуатацию СВТ	2
	Самостоятельная работа обучающихся		**4**
	3	Изучение каналов утечки информации.	2
	4	Исследование побочных электромагнитных излучений и наводок.	2
Тема 2.3 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**		**10**
	1	Информационные основы построения системы охранной сигнализации.	2
	2	Назначение, классификация технических средств обнаружения.	2
	3	Построение систем обеспечения безопасности объекта.	2
	4	Периметровые средства обнаружения: назначение, устройство, принцип действия.	2
	5	Объектовые средства обнаружения: назначение, устройство, принцип действия.	2
	Лабораторные занятия		**6**
	4	Монтаж датчиков пожарной и охранной сигнализации	2
	5	Исследование инструментального контроля защищенности ОТСС, обрабатывающих цифровую информацию, представленную в виде электрических сигналов в эфире	2
	6	Исследование инструментального контроля защищенности ОТСС, обрабатывающих цифровую информацию, представленную в виде электрических сигналов в линиях	2
	Самостоятельная работа обучающихся		**6**
	1	Изучение последовательности монтажа датчиков пожарной сигнализации.	2
	2	Изучение последовательности монтажа датчиков охранной сигнализации.	2
	3	Виды средств обнаружения и их характеристики.	2
Тема 2.4 Система контроля и	**Содержание**		**18**

управления доступом	1	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности.	2
	2	Особенности построения и размещения СКУД.	2
	3	Структура и состав СКУД.	2
	4	Периферийное оборудование и носители информации в СКУД.	2
	5	Основы построения и принципы функционирования СКУД.	2
	6	Классификация средств управления доступом.	2
	7	Средства идентификации и аутентификации.	2
	8	Методы удостоверения личности, применяемые в СКУД.	2
	9	Обнаружение металлических предметов и радиоактивных веществ.	2
	Лабораторные занятия		**2**
	7	Измерение параметров сигнала при внешнем электромагнитном зашумлении	2
	Практические занятия		**4**
	6	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	2
	7	Рассмотрение принципов устройства, работы и применения средств контроля доступа	2
	Самостоятельная работа обучающихся		**6**
	1	Исследование систем контроля и управления доступом, настройка и эксплуатация.	2
	2	Изучение видов систем идентификации.	2
	3	Изучение видов систем аутентификации.	2
Тема 2.5 Система телевизионного наблюдения	**Содержание**		**6**
	1	Аналоговые и цифровые системы видеонаблюдения.	2

	2	Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения.	2
	3	Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	2
	Практические занятия		**8**
	8	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	2
	9	Выбор размещения (уточнение) точек контроля показателя защищенности в эфире. Организация тестовых режимов работы при оценке эффективности активных средств	2
	10	Выбор размещения (уточнение) точек контроля показателя защищенности в линиях. Организация тестовых режимов работы при оценке эффективности активных средств защиты	2
	11	Построение контролируемой зоны выделенного помещения.	2
	Самостоятельная работа обучающихся		**4**
	1	Изучение особенностей аналогового сигнала, выделение достоинств и недостатков.	2
	2	Изучение особенностей цифрового сигнала, выделение достоинств и недостатков.	2
Тема 2.6 Система сбора, обработки, отображения и документирования информации	**Содержание**		**2**
	1	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	2
	Практические занятия		**2**
	12	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	2
	Лабораторные занятия		**6**

	8	Исследование параметров акустического сигнала в условиях эффекта акустического маскирования	2
	9	Исследование параметров акустического сигнала в условиях зашумления	2
	10	Исследование спектральных характеристик сигналов СВТ	2
Тема 2.7 Система воздействия	**Содержание**		**2**
	1	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	2
	Лабораторные занятия		**6**
	11	Исследование характеристик шумовых сигналов активных средств защиты информации	2
	12	Исследование реального затухания тестовых и шумовых сигналов средств защиты информации на объекте информатизации до выбранных точек возможного ведения разведки	2
	13	Исследование параметров сигнала перехвата узконаправленного антенного приемника	2
Тема 2.8 Применение инженерно-технических средств физической защиты	**Содержание**		**6**
	1	Периметровые и объектовые средства обнаружения, порядок применения. Особенности организации пропускного режима на КПП.	2
	2	Работа с периферийным оборудованием системы контроля и управления доступом.	2
	3	Управление системой телевизионного наблюдения с автоматизированного рабочего места.	2
	Практические занятия		**4**
	13	Организация пропускного режима для организации.	2
	14	Составление матрицы доступа.	2
	Лабораторные занятия		**8**
	14	Исследование монтажа эксплуатационных параметров охранной	2

		системы	
	15	Исследование эксплуатационных характеристик охранной системы	2
	16	Исследование этапов эксплуатационных характеристик охранной системы	2
	17	Исследование эксплуатационных параметров охранной системы	2
Тема 2.9 Эксплуатация инженерно-технических средств физической защиты	**Содержание**		**10**
	1	Этапы эксплуатации инженерно-технических средств физической защиты.	2
	2	Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.	2
	3	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	2
	4	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.	2
	5	Организация ремонта технических средств физической защиты.	2
	Практические занятия		**2**
	15	Расчет требуемых показателей защищенности (показателя δ). Оформление протоколов оценки эффективности средств защиты информации и предписания на эксплуатацию объекта информатизации	2
	Лабораторные занятия		**6**
	18	Установка технических средств физической защиты.	2
	19	Настройка технических средств физической защиты.	2
	20	Диагностика технических средств физической защиты.	2
Итоговое занятие			**2**
Учебная практика	**Содержание учебной практики**		**108**

Виды работ	1	Изучение видов датчиков охранной и пожарной систем сигнализации. Изучение последовательности монтажа датчиков охранной и пожарной систем сигнализации.	6
	2	Монтаж датчиков охранной системы сигнализации.	6
	3	Монтаж датчиков пожарной системы сигнализации.	6
	4	Проектирование установки системы пожарно-охранной сигнализации по заданию.	6
	5	Реализация спроектированной системы пожарно-охранной сигнализации.	6
	6	Применение промышленных осциллографов для защиты информации	6
	7	Применение промышленных частотомеров для защиты информации	6
	8	Применение промышленных генераторов для защиты информации	6
	9	Рассмотрение системы контроля и управления доступом	6
	10	Проектирование и реализация системы контроля и управления доступом по заданию.	6
	11	Рассмотрение принципов работы системы видеонаблюдения и ее проектирование	6
	12	Рассмотрение датчиков периметра, их принципов работы	6
	13	Выполнение звукоизоляции помещений системы зашумления	6
	14	Проектирование системы защиты от утечки по цепям электропитания и заземления	6
	15	Реализация спроектированной системы защиты от утечки по цепям электропитания и заземления	6
	16	Разработка организационных мероприятий по заданию преподавателя	6
	17	Разработка технических мероприятий по заданию преподавателя	6
	18	Разработка основной документации по инженерно-технической	6

		защите информации	
Производственная практика **Виды работ**	**Содержание производственной практики**		**180**
	1	Монтаж, установка, настройка и проведение испытания технических средств защиты информации от утечки по техническим каналам в ИТКС	
	2	Проведение технического обслуживания, диагностики, устранение неисправностей и ремонт технических средств защиты информации в ИТКС	
	3	Осуществление защиты информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями	
	4	Проведение отдельных работ по физической защите линий связи ИТКС	
Промежуточная аттестация (экзамен)			**18**
Всего			**732**

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Реализация программы модуля требует наличия лаборатории программных и программно-аппаратных средств защиты информации, лаборатории защиты информации от утечки по техническим каналам, кабинет информационной безопасности, мастерской лаборатории информационных технологий.

Лаборатория программных и программно-аппаратных средств защиты информации, мастерская лаборатория информационных технологий, оснащенная оборудованием и техническими средствами обучения: доска классная – 1 шт., стол компьютерный– 13 шт., стул – 13 шт., компьютерные кресла – 13 шт., системный блок (CPU AMD Ryzen 7 3700x (8 Cores/32MB/8T/3.6GHz); 16 Гбайт (16 Гбайт) памяти DDR4, 2 666 МГц, без ECC; твердотельный накопитель M.2 PCIe NVMe, 512 Гбайт, класс 35) – 13 шт., монитор (Asus 23”8) – 13 шт., клавиатура (Oklick 530S) – 14 шт., мышь для компьютера (Defender OPTICAL MB-160) – 14 шт., источник бесперебойного питания – 13 шт., проектор – 1 шт., активная колонка - 1шт., офисный пакет Microsoft Office Professional 2016 - 13 шт, виртуальный межсетевой экран следующего поколения Cisco Firepower в составе с FMC- 10 шт., ОС Microsoft Windows Server - 1 шт., ОС Microsoft Windows 10 - 13 шт., сервер SuperMicro CSE-113AC2-R706WB2 2x750W black Intel Xeon Silver 4216 256 ГБ ОЗУ, 960 GB SSD - 1 шт., монитор 23,6 – 1 шт., источник бесперебойного питания для сервера - 1 шт., стойка двухрамная (стк-24.2-9005 цмо) – 1 шт., телевизор на стойке (huawei 55”) – 1 шт., экран для проектора (SAKURA CINEMA WALLSCREEN) – 1 шт., МФУ (Xerox B205) – 1 шт., ПАК Arduino - 3 шт.,Анализатор спектра IFR 2398 - 1 шт.,Электронный осциллограф IBIS-1 — 1шт.,Соболь 3.0 kb-sobol 3.0 k1 v1-SP1Y - 2 шт .,Видео регистратор jassun jsr-H0415mini - 1 шт.,Видео регистратор vesta VDRV-5004M - 1 шт.,Коммутатор Alcatel OmniStack LS 6224 - 5 шт .,Программные межсетевые экраны для маршрутизаторов Cisco 1700 (Cisco 1721) - 2 шт.,Стенд : пульт защиты помещений — 1 шт.,стенд: исследование утечки информации по звуковым каналам — 1 шт., стойки для монтажа сетевого оборудования - 2 шт..

Программное обеспечение: MS Windows Server 2008 R2, OS Debian Linux 9, Audacity 2.3, Zoneminder 1.32, Open VAS 8, LibreOffice 6, OS Ubuntu Linux 14.04, Virtual Box 5, Open SSL 1.0, Open VPN 2.4, Сервер обновлений WSUS, Zabbix 4.0, Apache 2.4, MySQL 14.12, GNS3 2, Ossec 3.2, IredMail 0.9.9, OS FreeBSD 11,12. Asterisk 13, PHP MyAdmin 5, Wireshark 2.2.6, Zenmap 7.7, Platinum Pack 4.0., Eset Nod32 Fire Wall 5.,Крипто Про.,RedCheck 2.0.,DevieeLock 8.

Лаборатория защиты информации от утечки по техническим каналам, оснащенная оборудованием и техническими средствами обучения: стол преподавателя на металлокаркасе -1шт., кресло Юпитер -2шт., стол компьютерный на металлокаркасе левый- 4шт., стол компьютерный на металлокаркасе правый -10шт., стол на металлокаркасе- 1шт., стул СМ-9ГП-14шт., табурет СМ-31- 14шт., тележка под системный блок- 1шт., рабочее место преподавателя – ПК -1 шт: Монитор 19" TFT LG Flatron L1942SE-BF -1 шт., Foxconn TSAA-700 (Корпус)-1 шт., ASRock H67DE3 (Материнская плата)-1 шт., Intel HD Graphics (Видеокарта)-1 шт., Realtek PCIe GBE (Сетевая плата)-1 шт., Realtek HDA (Звуковая плата)-1 шт., Intel Core i3 2120 3.3GHz (Процессор)-1 шт., 4xDDR III 2Gb Samsung (ОЗУ)-1 шт., D-Link DGE-528T (Сетевая плата)-1 шт, WD (500Gb) SATA III (Жесткий диск)-1 шт.,рабочие места обучающихся – ПК 14 шт: Монитор 19" TFT LG Flatron L1942SE-BF - 14 шт, Foxconn TSAA-700 (Корпус)- 14 шт,ASRock H67DE3 (Материнская плата)- 14 шт, Intel HD Graphics (Видеокарта)- 14 шт, Realtek PCIe GBE (Сетевая плата)- 14 шт, Realtek HDA (Звуковая плата)- 14 шт, Intel Core i3 2120 3.3GHz (Процессор)- 14 шт, 4xDDR III 2Gb Samsung (ОЗУ)- 14 шт,D-Link DGE-528T (Сетевая плата) - 14 шт, WD (500Gb) SATA III (Жесткий диск)- 14 шт, мультимедиа-проектор (Epson EB-X12),- 1шт, экран (Screen Media GoldView MW),- 1 шт, учебная доска -1шт., маршрутизатор D-Link Dir-320-1шт., маршрутизатор D-Link DSR-500N-1шт., маршрутизатор D-link DFL-800- 1шт., коммутатор D-Link DGS-3312SR – 2шт., коммутатор D-Link DES-3528 – 8шт., стойка для монтажа сетевого оборудования – 2 шт., патч-панель – 2шт., клещи обжимные – 8шт., розетки распределительные под RJ-45 – 4шт., конекторы RJ-45 –50шт.

Программное обеспечение: MS Windows Server 2008 R2, MS Windows Server 2012 R2, MS Windows Server 2016, OpenVAS 8, LibreOffice 6, ОС Ubuntu Linux 14.04, VirtualBox 5, OpenSSL 1, OpenVPN 2.4, Сервер обновлений WSUS, Zabbix 4.0, Apache 2.4, MySQL 14.12, GNS3 2.0.2, Ossec 3.2, IredMail 0.9.9, PhpMyAdmin 5, Wireshark 2.2.6, Zenmap 7.70, Denver 3, MySQL Workbench 6.3, Joomla 2, Notepade++ 4.0.2, GNU PG 2.ail, Packet tracer.

Кабинет информационной безопасности, оснащенный оборудованием и техническими средствами обучения: доска классная – 1 шт., стол компьютерный– 13 шт., стул – 13 шт., компьютерные кресла – 13 шт., системный блок (CPU AMD Ryzen 7 3700x (8 Cores/32MB/8T/3.6GHz); 16 Гбайт (16 Гбайт) памяти DDR4, 2 666 МГц, без ECC; твердотельный накопитель M.2 PCIe NVMe, 512 Гбайт, класс 35) – 13 шт., монитор (Asus 23"8) – 13 шт., клавиатура (Oklick 530S) – 14 шт., мышь для компьютера (Defender OPTICAL MB-160) – 14 шт., источник бесперебойного питания – 13 шт., проектор – 1 шт., активная колонка - 1шт., офисный пакет Microsoft Office Professional 2016 - 13 шт, виртуальный межсетевой экран следующего поколения Cisco Firepower в составе с FMC- 10 шт., ОС Microsoft Windows Server - 1 шт., ОС Microsoft Windows 10 - 13 шт., сервер SuperMicro CSE-113AC2-R706WB2 2x750W black Intel Xeon Silver 4216 256 ГБ ОЗУ, 960 GB SSD - 1 шт., монитор 23,6 – 1 шт., источник бесперебойного питания для сервера - 1 шт., стойка двухрамная (стк-24.2-9005 цмо) – 1 шт., телевизор на стойке (huawei 55") – 1 шт., экран для

проектора (SAKURA CINEMA WALLSCREEN) – 1 шт., МФУ (Xerox B205) – 1 шт., ПАК Arduino - 3 шт., Анализатор спектра IFR 2398 - 1 шт., Электронный осциллограф IBIS-1 — 1шт.,Соболь 3.0 kb-sobol 3.0 k1 v1-SP1Y - 2 шт ., Видео регистратор jassun jsr-H0415mini - 1 шт.,Видео регистратор vesta VDRV-5004M - 1 шт.,К оммутатор Alcatel OmniStack LS 6224 - 5 шт .,Программные межсетевые экраны для маршрутизаторов Cisco 1700 (Cisco 1721) - 2 шт.,Стенд : пульт защиты помещений — 1 шт.,стенд: исследование утечки информации по звуковым каналам — 1 шт., стойки для монтажа сетевого оборудования - 2 шт..

Программное обеспечение: MS Windows Server 2008 R2, OS Debian Linux 9, Audacity 2.3, Zoneminder 1.32, Open VAS 8, LibreOffice 6, OS Ubuntu Linux 14.04, Virtual Box 5, Open SSL 1.0, Open VPN 2.4, Сервер обновлений WSUS, Zabbix 4.0, Apache 2.4, MySQL 14.12, GNS3 2, Ossec 3.2, IredMail 0.9.9, OS FreeBSD 11,12. Asterisk 13, PHP MyAdmin 5, Wireshark 2.2.6, Zenmap 7.7, Platinum Pack 4.0., Eset Nod32 Fire Wall 5.,Крипто Про.,RedCheck 2.0.,DevieeLock 8.

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. - Москва: Академия, 2020.

2. 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. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1082470. - Режим доступа: для зарегистр. пользователей. – Текст электронный.

3. Зверева, В. П. Участие в планировании и организации работ по обеспечению защиты объекта: учебник / В.П. Зверева, А.В. Назаров. — Москва: КУРС: ИНФРА-М, 2020. — 320 с. - ISBN 978-5-16-105204-4. - URL: https://new.znanium.com/catalog/product/1055808. - Режим доступа: для зарегистр. пользователей. – Текст электронный.

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

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

6. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - URL: https://znanium.com/catalog/product/1081318. – Режим доступа: для зарегистрир.пользователей.—Текст : электронный.

3.2.2. Дополнительные источники:

1. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2024. — 216 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016534-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/2131865– Режим доступа: по подписке.

2. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - URL: https://znanium.com/catalog/product/1191479. – Режим доступа: для зарегистрир.пользователей.—Текст : электронный.

3. Шейдаков, Н. Е. Физические основы защиты информации : учебное пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. — Москва : РИОР : ИНФРА-М, 2022. — 204 с. — (Высшее образование). — DOI: https://doi.org/10.12737/21158. - ISBN 978-5-369-01603-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1851140 – Режим доступа: по подписке.

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 Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	– оценка результатов выполнения лабораторных работ по МДК 03.01 №№1-16; по МДК 03.02 №№1-20; - оценка результатов выполнения практических работ по МДК 03.01 №№31-21; по МДК 03.02 № №1-15; - оценка результатов выполнения самостоятельной работы; – оценка процесса и результатов выполнения видов работ на практике; –экзамен.
ПК 3.2 Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	
ПК 3.3 Осуществлять защиту информации от утечки по техническим каналам в информационно –	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение	

телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями	параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	
ПК 3.4 Проводить отдельные работы по физической защите линий связи информационно – телекоммуникационных систем и сетей	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	
ОК. 01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	- Экспертное наблюдение выполнения лабораторных и практических работ; – оценка процесса и результатов выполнения видов работ на практике; –экзамен.
ОК.02 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач	- использование различных источников, включая электронные ресурсы, медиа ресурсы, Интернет-ресурсы, периодические издания по специальности для решения	

профессиональной деятельности	профессиональных задач
ОК. 03 Планировать и реализовывать собственное профессиональное и личностное развитие	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;
ОК.04 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)
ОК.05 Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	- демонстрировать грамотность устной и письменной речи; - ясность формулирования и изложения мыслей.
ОК.06 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.07 Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - демонстрация знаний и использование ресурсосберегающих технологий в

	профессиональной деятельности
ОК.09 Использовать информационные технологии в профессиональной деятельности	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту.
	Промежуточная аттестация: **МДК.03.01 – -, дифференцированный зачет** **МДК.03.02 – дифференцированный зачет** **УП.03 – дифференцированный зачет** **ПП.03 - дифференцированный зачет** **ПМ.03 - экзамен по модулю**