МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

СПбГУТ))) Документ подписан простой электронной подписью

Сертификат: 008a56eb36a1808f06
Владелец: Машков Георгий Михайлович
Действителен с 07.05.2022 по 06.05.2027

УТВЕРЖДАЮ
И.о. первого проректора – проректора по учебной работе
_____ С.И. Ивасишин
«14» марта 2022 г.

Регистрационный № 11.09.22/162

РАБОЧАЯ ПРОГРАММА

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

(наименование профессионального модуля)

программа подготовки специалистов среднего звена

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код и наименование специальности)

квалификация
техник по защите информации

Санкт-Петербург
2022

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена (индекс – ПМ.03) среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 31 марта 2022 г., протокол № 3.

Составитель:

Преподаватель _____ Н.В.Кривоносова
(подпись)

СОГЛАСОВАНО
Главный специалист НТБ УИОР _____ Р.Х. Ахтреева
(подпись)

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 9 (Информационной безопасности телекоммуникационных систем)
09 февраля 2022 г., протокол № 6

Председатель предметной (цикловой) комиссии: _____ Н.В.Кривоносова
(подпись)

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля
16 февраля 2022 г., протокол № 4

Заместитель директора по учебной работе колледжа СПб ГУТ
_____ Н.В. Калинина
(подпись)

СОГЛАСОВАНО

Директор колледжа СПб ГУТ
_____ Т.Н. Сиротская
(подпись)

СОГЛАСОВАНО

Директор департамента ОКОД
_____ С.И. Ивасишин
(подпись)

СОГЛАСОВАНО:
Заместитель генерального директора
по безопасности АО «НПП «Сигнал» _____ В.В. Петров

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена (индекс – ПМ.03) среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 31 марта 2022 г., протокол №3.

СОГЛАСОВАНО

Заместитель руководителя
Управления Роскомнадзора
по Северо-Западному федеральному округу И.Ю. Потехин

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 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 основной 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 и личностных результатов реализации программы воспитания

Код	Наименование общих компетенций и личностных результатов
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.
ЛР1–ЛР4, ЛР9, ЛР10, ЛР13-ЛР15, ЛР20, ЛР23–ЛР28	

1.2.2 Перечень профессиональных компетенций

Код	Наименование профессиональных компетенций
ПК 3.1	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала 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 в	– установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам; – защите информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями; – проведении 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 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 каналам;

	– 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.

1.2 Количество часов, отводимое на освоение профессионального модуля

Всего часов: **736 часа.**

Из них а освоение МДК**:**

МДК.03.01. Защита информации в ИТКС с использованием технических средств защиты **- 261 час;**

МДК.03.02. Физическая защита линий связи ИТКС –**169 часов.**

На практики учебную и производственную **-288 часов.**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, час.						
				Работа обучающихся во взаимодействии с преподавателем					Самостоятельная работа	Промежуточная аттестация
				Обучение по МДК, в час.			Практики			
				Всего, часов	Лабораторные работы и практические занятия	в т.ч., курсовая работа (проект)	Учебная	Производственная (по профилю специальности)		
ПК 3.1- ПК.3.4 ОК 01 – ОК 07, ОК 09	Раздел 1. Защита информации в ИТКС с использованием технических средств защиты	**261**	100	**188**	70	30			**69**	**4**
ПК 3.5 ОК 01 – ОК 07, ОК 09	Раздел 2. Физическая защита линий связи ИТКС	**169**	70	**142**	70	-			**25**	**2**
Учебная практика		**108**	108							
Производственная практика (по профилю специальности)		**180**	180							
Промежуточная аттестация		**18**								18
Всего:		**736**	458	**330**	140	30	**108**	**180**	**94**	**26**

2.2 Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект)		Объем часов
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты			
МДК.03.01.Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты			**261**
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание учебного материала**		4
	1	**Занятие 1. Предмет и задачи технической защиты информации.** Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации	
	2	**Занятие 2. Концепция технической защиты информации** Обобщённая структура государственной системы защиты информации. Основные документы по противодействию иностранным техническим разведкам. Концепция технической защиты информации. Основные положения системного подхода к технической защите информации. Модель системы защиты информации (СЗИ).	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание учебного материала**		10
	1	**Занятие 3. Общие положения защиты информации техническими средствами** Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	
	2	**Занятие 4. Основные направления технической защиты информации в организации** Цели и задачи технической защиты информации в инфокоммуникационных системах и сетях. Направления технической защиты информации. Основные факторы обеспечения защиты информации от угроз утечки информации. Этапы процесса утечки информации. Основные направления защиты: физическая защита; скрытие информации; нейтрализация источников опасных сигналов. Основные методы технической защиты информации: инженерная защита; техническая охрана объектов; пространственное (структурное, временное и энергетическое)	

		скрытие.	
	3	**Занятие 5. Информация как предмет защиты** Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы.	
	4	**Занятие 6. Правовое и нормативное обеспечение технической защиты информации** Основные правовые, руководящие, нормативные и методические документы в области технической защиты информации. Права и обязанности работников службы технической защиты информации. Ответственность за нарушение требований технической защиты информации.	
	5	**Занятие 7. Техническая разведка** Понятие технической разведки. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
	Практические занятия		
	1	**Занятие 8.** Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	4
	2	**Занятие 9.** Обоснование необходимости создания подсистемы технической защиты инфокоммуникационной системы на основе нормативных и методических документов.	
Тема 1.3. Технические каналы утечки информации	**Содержание учебного материала**		
	1	**Занятие 10. Типовая структура и виды технических каналов утечки информации** Типовая структура и виды технических каналов утечки информации (ТКУИ). Классификация ТКУИ. Основные показатели ТКУИ.	
	2	**Занятие 11. Акустические, виброакустические каналы утечки информации.** Понятие и основные характеристики акустического, виброакустического и оптического каналов утечки информации. Пассивные и активные способы защиты информации в выделенных помещениях от несанкционированного прослушивания. Рекомендации по выбору систем акустической и виброакустической защиты.	12
	3	**Занятие 12. Оптические каналы утечки информации** Характеристика и противодействие оптическим каналам утечки информации. Средства противодействия наблюдению в оптическом диапазоне	
	4	**Занятие 13. Электромагнитные каналы утечки информации, образуемые средствами вычислительной техники.**	

		Характеристика режимов обработки информации в ПЭВМ с точки зрения утечки информации. Режим вывода информации на экран монитора. Потенциально информативные и неинформативные излучения. Условия возникновения электромагнитного канала утечки информации. Электрические каналы утечки информации. Сосредоточенные и распределённые случайные антенны. Специально создаваемые технические каналы утечки информации. Аппаратные закладки для перехвата изображений, выводимых на экран монитора. Аппаратные закладки для перехвата информации, записываемой на жёсткий диск. Программные закладки.	
	5	**Занятие 14. Электромагнитный технический канал утечки информации.** **П**обочные электромагнитные излучения и наводки (ПЭМИН). Паразитные антенны. Утечка электромагнитных сигналов по цепям питания и заземления.	
	6	**Занятие 15. Средства технической разведки.** Технические средства добывания защищаемой информации. Способы организации технических каналов доступа к защищаемой информации.	
	Практические занятия		16
	3	**Занятие 16.** Особенности утечки информации в проводных линиях связи.	
	4	**Занятие 17.** Особенности утечки информации в беспроводных линиях связи.	
	5	**Занятие 18.** Исследование уязвимостей и построение модели угроз объекта защиты	
	6	**Занятие 19.** Исследование возможностей системы оценки защищенности оптических линий связи	
	7	**Занятие 20.** Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН	
	8	**Занятие 21.** Исследование возможностей системы оценки защищенности выделенных помещений	
	9	**Занятие 22.** Оценка защищенности информации по акустическому каналу.	
	10	**Занятие 23.** Оценка защищенности информации по электромагнитному каналу.	
Тема 1.4. Методы и средства технической разведки	**Содержание учебного материала**		12
	1	**Занятие 24. Классификация технических средств разведки.** Понятие технической разведки. Цели, задачи, принципы организации технической разведки. Классификация технических разведок по видам носителей аппаратуры. Методы и средства технической разведки.	
	2	**Занятие 25. Средства несанкционированного доступа к акустической информации.** Средства и возможности акустической разведки. Средства дистанционного съема информации.	

	3	**Занятие 26. Средства несанкционированного доступа к видовой информации.** Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	4	**Занятие 27. Средства несанкционированного доступа к информации ПЭМИН.** Средства и возможности электромагнитной разведки. Средства дистанционного съема информации.	
	5	**Занятие 28. Радиоэлектронная разведка.** Общая характеристика радиоэлектронной разведки. Особенности, основные показатели технических средств радио-, радиотехнической, радиолокационной и радиотепловой разведки	
	6	**Занятие 29. Характеристики видов разведки** Космическая разведка. Воздушная разведка. Морская разведка. Наземная разведка. Обработка разведывательной информации	
Тема 1.5. Физические основы утечки информации	**Содержание учебного материала**		8
	1	**Занятие 30. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок** Физические основы побочных электромагнитных излучений и наводок. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	2	**Занятие 31. Физические основы утечки акустической информации** Акустика, структура звука и его характеристики. Акустоэлектрические преобразования.	
	3	**Занятие 30. Физические основы утечки видовой информации** Видовая информация. Оптические свойства света.	
	4	**Занятие 31. Физические процессы при подавлении опасных сигналов** Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
Тема 1.6. Системы защиты от утечки информации	**Содержание учебного материала**		42
	1	**Занятие 32. Основные положения современной концепции защиты информации техническими средствами.** Основные направления инженерно-технической защиты информации. Задачи и принципы инженерно-технической защиты информации. Характеристика зонового принципа защиты информации.	

2	**Занятие 33. Методы и средства защиты информации обрабатываемой ТСПИ от утечки по техническим каналам.** Пассивные методы защиты информации, обрабатываемой ТСПИ: экранирование технических средств, заземление технических средств, фильтрация информационных сигналов. Экологически чистые технологии пассивной защиты информации**.** Активные методы и средства защиты информации, обрабатываемой ТСПИ. Методы и средства пространственного и линейного зашумления.
3	**Занятие 35. Системы защиты от утечки информации по акустическому каналу** Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.
4	**Занятие 37. Методы и средства защиты акустической информации от утечки по техническим каналам** Задачи, решаемые пассивными методами защиты акустической информации. Звукоизоляция помещений. Акустические экраны. Звукопоглощающие материалы. Звукоизолирующая способность различных конструкций. Задачи, решаемые активными методами защиты акустической информации. Виброакустическая маскировка. Современные средства виброакустической защиты. Методы и средства защиты акустической информации, передаваемой по телефонным линиям.
5	**Занятие 39. Системы защиты от утечки информации по проводному каналу** Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны.
6	**Занятие 40. Системы защиты от утечки информации по проводному каналу** Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.
7	**Занятие 41. Системы защиты от утечки информации по вибрационному каналу** Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.
8	**Занятие 42. Системы защиты от утечки информации по электромагнитному каналу**

	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации с пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.
9	**Занятие 43. Методы и средства защиты информации обрабатываемой ТСПИ от утечки по техническим каналам.** Пассивные методы защиты информации, обрабатываемой ТСПИ: экранирование технических средств, заземление технических средств, фильтрация информационных сигналов. Экологически чистые технологии пассивной защиты информации. Активные методы и средства защиты информации, обрабатываемой ТСПИ. Методы и средства пространственного и линейного зашумления.
10	**Занятие 44. Системы защиты от утечки информации по телефонному каналу** Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке.
11	**Занятие 45. Системы защиты от утечки информации по телефонному каналу** Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.
12	**Занятие 46. Системы защиты от утечки информации по электросетевому каналу** Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.
13	**Занятие 47. Системы защиты от утечки информации по оптическому каналу** Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.
14	**Занятие 48. Особенности обработки информации при инструментальном контроле эффективности ее защиты.** Основные виды погрешностей измерений и погрешностей средств измерений, оказывающих влияние на качество обработки информации при оценивании эффективности ее защиты. Обработка результатов прямых однократных измерений при инструментальном контроле эффективности ее защиты.

15	**Занятие 49. Особенности обработки информации при инструментальном контроле эффективности ее защиты.** Обработка результатов прямых многократных измерений параметров, оценивающих эффективность защиты информации. Обработка результатов косвенного инструментального контроля эффективности защиты информации.	
16	**Занятие 50. Методы и средства контроля эффективности защиты информации** Методы и средства контроля эффективности защиты информации от ее утечки по электромагнитным каналам. Измерительные антенны. Калибровка измерительных антенн. Методы и средства измерения параметров опасных сигналов в электромагнитном поле.	
17	**Занятие 51. Методы и средства контроля эффективности защиты информации** Современные средства автоматизации измерений при специсследованиях технических средств. Методы и средства оценивания эффективности защиты акустической информации от утечки по виброакустическим каналам с использованием инструментальных средств.	
18	**Занятие 52. Мероприятия по выявлению средств технической разведки.** Мероприятия по выявлению средств технической разведки. Специальные технические средства (СТС). Методика поиска СТС. Радиомониторинг. Локализация радиоизлучающих СТС. Проверка наличия инфракрасных (ИК) излучений.	
19	**Занятие 53. Методика поиска специальных технических средств** Выявление низкочастотных (НЧ) магнитных полей. Проверка электросети и телефонных коммуникаций. Проверка помещения на наличие акустических каналов утечки. Физический поиск СТС	
20	**Занятие 54. Методы и средства поиска и нейтрализации несанкционированного съема информации.** Методы и средства поиска с использованием индикаторов, радиочастотомеров. Сканирующие приемники и анализаторы спектра для поиска устройств перехвата информации. Программно-аппаратные комплексы радиоконтроля.	
21	**Занятие 55. Методы и средства поиска и нейтрализации несанкционированного съема информации.** Методы поиска устройств съема информации с использованием нелинейных локаторов, металлоискателей, рентгеновских аппаратов. Средства и методы контроля проводных линий. Специальные проверки служебных помещений. Программа организации работ	
Практические занятия		18
11	**Занятие 55.** Определение каналов утечки ПЭМИН	

	12	**Занятие 56.** Работа с оборудованием по защите от утечки по ПЭМИН	
	13	**Занятие 57.** Работа с оборудованием по защите от утечки по ПЭМИН	
	14	**Занятие 58.** Определение утечки по цепям электропитания и заземления	
	15	**Занятие 59.** Защита от утечки по цепям электропитания и заземления	
	16	**Занятие 60.** Определение утечки информации по акустическому каналу	
	17	**Занятие 61.** Работа с оборудованием по защите от утечки по акустическому каналу	
	18	**Занятие 62.** Определение утечки информации по виброакустическому каналу	
	19	**Занятие 63.** Работа с оборудованием по защите от утечки по виброакустическому каналу	
	Лабораторные работы		
	1	**Занятие 64.** Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.	
	2	**Занятие 65.** Поиск и локализация скрытых видеокамер	
	3	**Занятие 66.** Исследование методов защиты сотовых телефонов от несанкционированного прослушивания	
	4	**Занятие 67.** Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов	
	5	**Занятие 68.** Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора	
	6	**Занятие 69.** Инженерно-техническая защита информации.	
	7	**Занятие 70.** Выявление и фиксация следов противоправной деятельности, связанной с использованием компьютерной деятельности	32
	8	**Занятие 71.** Исследование уровня побочного электромагнитного излучения ПК	
	9	**Занятие 72.** Снятие диаграммы направленного микрофона	
	10	**Занятие 73.** Исследование спектра речевого сигнала	
	11	**Занятие 74.** Определение уровня побочного излучения в канале электросвязи	
	12	**Занятие 75.**Определение уровня побочного излучения в канале виброакустики	
	13	**Занятие 76.** Измерение уровня маскирующего виброакустического шума	
	14	**Занятие 77.** Измерение уровня маскирующего цифрового шума	
	15	**Занятие 78.** Испытание учебной аудитории на утечку информации по каналу ПЭМИН	
	16	**Занятие 79.**Испытание учебной аудитории на утечку информации по виброакустическому каналу	
	Самостоятельная работа обучающихся		69

<table>
<tr><td></td><td colspan="2">Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем).
Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторных работ, отчетов и подготовка к их защите.
Тематика домашних заданий, сообщений, рефератов:
1. Классификация способов и средств защиты информации.
2. Основные и вспомогательные технические средства и системы.
3. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации.
4. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.
5. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.
6. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.
7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.
8. Технические средства для уничтожения информации и носителей информации, порядок применения.</td><td></td></tr>
<tr><td rowspan="14">Курсовое проектирование</td><td colspan="2">Обязательные аудиторные учебные занятия по курсовому проекту</td><td rowspan="14">30</td></tr>
<tr><td>1</td><td>Занятие 80. Введение. Выдача заданий</td></tr>
<tr><td>2</td><td>Занятие 81. Анализ поставленной задачи</td></tr>
<tr><td>3</td><td>Занятие 82. Определение защищаемых информационных активов. Категорирование информации</td></tr>
<tr><td>4</td><td>Занятие 83. Определение уязвимостей и угроз</td></tr>
<tr><td>5</td><td>Занятие 84. Анализ и выбор возможных решений по защите</td></tr>
<tr><td>6</td><td>Занятие 85. Анализ механизмов защиты</td></tr>
<tr><td>7</td><td>Занятие 86. Анализ требуемых компонентов</td></tr>
<tr><td>8</td><td>Занятие 87. Проектирование модели угроз</td></tr>
<tr><td>9</td><td>Занятие 88. Настройка компонентов защиты</td></tr>
<tr><td>10</td><td>Занятие 89. Конфигурирование пользовательских задач</td></tr>
<tr><td>11</td><td>Занятие 90. Проектирование эксперимента по внедрению системы защиты</td></tr>
<tr><td>12</td><td>Занятие 91. Нормативно-правовое обеспечение проекта</td></tr>
<tr><td>13</td><td>Занятие 92. Расчет индекса ROSI</td></tr>
</table>

	14	**Занятие 93.** Подготовка пояснительной записки к курсовому проекту	
	15	**Занятие 94.** Защита курсового проекта	
Тематика курсовых проектов	1. Комплексный подход к построению технической защиты информации на объекте информатизации. 2. Основные положения и принципы построения технической защиты информации. 3. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте защиты. 4. Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам. 5. Модель поведения инсайдера на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам. 6. Условия и факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации. 7. Условия и субъективные факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации. 8. Методы защиты видовых демаскирующих признаков от технических средств разведок. 9. Методы защиты сигнальных демаскирующих признаков от технических средств разведок. 10. Методы защиты радиосигналов от перехвата техническими средствами разведок. 11. Методы защиты электрических сигналов от перехвата техническими средствами разведок. 12. Методы защиты материальных и вещественных демаскирующих признаков от технических средств разведок. 13. Технические средства наблюдения в видимом и ИК диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения. 14. Технические средства наблюдения в радио диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения. 15. Технические средства перехвата конфиденциальной информации передаваемой по линии связи, методы и средства противодействия перехвата конфиденциальной информации. 16. Методы и технические средства съема конфиденциальной речевой информации с использованием вторичных переизлучателей. 17. Методы и технические средства съема конфиденциальной речевой информации с использованием оптоволоконных линий связи. 18. Методы и технические средства съема конфиденциальной речевой информации с использованием средств высокочастотного навязывания.	

	19. Технические средства подслушивания, методы и средства противодействия средствам подслушивания. 20. Технические средства анализа демаскирующих признаков веществ, методы и средства нейтрализации (утилизации) отходов производства. 21. Технические средства контроля, обнаружения, уничтожение закладных устройств, порядок проведения ЗПМ. 22. Технические средства контроля, обнаружения, уничтожение закладных устройств, в слаботочных линиях связи, порядок проведения ЗПМ. 23. Технические средства контроля, обнаружения, уничтожение закладных устройств в телефонных линиях связи, порядок проведения ЗПМ. 24. Технические средства контроля, обнаружения, уничтожение закладных устройств, в электросетях, цепях заземления, порядок проведения ЗПМ. 25. Способы и средства контроля и порядок проведения ЗПМ в защищаемых помещений на отсутствие закладных устройств. 26. Моделирование вербального объекта защиты, возможных угроз безопасности информации для оптических каналов утечки информации в видимом и ИК диапазонах, разработка способов, методов и технических средств защиты информации. 27. Математические методы моделирования для вербального объекта защиты от возможных угроз безопасности информации для акустических каналов утечки информации. 28. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустических каналов утечки информации, разработка методов и технические средств защиты информации. 29. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустикорадиоэлектронных каналов утечки информации, разработка методов и технических средств защиты информации. 30. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустико-оптических каналов утечки информации, разработка методов и технических средств защиты информации. 31. Моделирование вербального объекта защиты, где производится обработка информации с использованием СВТ (АС), возможных угроз безопасности информации и технических каналов утечки информации, разработка методов и технических средств защиты информации. 32. Моделирование вербального объекта защиты, где производится обработка информации с использованием технических средств обработки информации, возможных угроз безопасности	

	информации и технических каналов утечки информации, разработка методов и технических средств защиты информации. 33. Моделирование вербального объекта защиты, возможных угроз безопасности информации для материально-вещественных каналов утечки информации, разработка методов и технических средств защиты информации. 34. Порядок проведения аттестационных испытаний по требованиям безопасности информации на примере вербального объекта информатизации. 35. Порядок проведения работ по созданию системы защиты информации для вербального объекта информатизации. 36. Организационные методы контроля эффективности защиты информации на примере вербального объекта информатизации. 37. Технические средства контроля эффективности защиты информации на примере вербального объекта информатизации.		
Промежуточная аттестация в форме дифференцированного зачета			**4**
Раздел 2. Физическая защита линий связи ИТКС			
МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей			**169**
Тема 2.1. Цели и задачи физической защиты объектов информатизации	**Содержание учебного материала**		4
	1	**Занятие 1. Физическая защита информации** Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты.	
	2	**Занятие 2. Категорирование объектов информатизации.** Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов	
	Практические занятия		4
	1	**Занятие 3.** Исследование возможностей СЗИ «Страж NT»	
	2	**Занятие 4.** Исследование программной среды «Страж NT»	
Тема 2.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание учебного материала**		4
	1	**Занятие 5. Общие принципы обеспечения безопасности объектов.** Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны.	
	2	**Занятие 6. Требования к инженерным средствам физической защиты.**	

		Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
	Практические занятия		10
	3	**Занятие 7.** Управление пользователями «Страж NT», учет пользователей «Страж NT»	
	4	**Занятие 8.** Избирательное управление «Страж NT»	
	5	**Занятие 9.** Сортировка и поиск с «Страж NT»	
	6	**Занятие 10.** Редактирование пользователей «Страж NT»	
	7	**Занятие 11.** Изменение настроек «Страж NT»	
Тема 2.3. Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание учебного материала**		4
	1	**Занятие 12. Информационные основы построения системы охранной сигнализации.** Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта.	
	2	**Занятие 13. Средства обнаружения** Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Практические занятия		8
	8	**Занятие 14.** Исследование возможностей «Сигурд М19»	
	9	**Занятие 15.** Подготовка к работе «Сигурд М19»	
	10	**Занятие 16.** Поиск сигналов ПЭМИН «Сигурд М19»	
	11	**Занятие 17.** Анализ сигналов «Сигурд М19»	
Тема 2.4. Система контроля и управления доступом	**Содержание учебного материала**		14
	1	**Занятие 18. СКУД** Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД.	
	2	**Занятие 19. Периферийное оборудование и носители информации в СКУД.** Основы построения и принципы функционирования СКУД. Классификация средств управления доступом.	
	3	**Занятие 20. Идентификация в СКУД** Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	
	4	**Занятие 21. Правовое и нормативное обеспечение.**	

		Основные правовые, руководящие, нормативные и методические документы в области применения СКУД. Права и обязанности работников службы обеспечения информационной безопасности и режима. Ответственность за нарушение требований защиты информации и режима.	
	5	**Занятие 22. Методы и средства построения систем контроля и управления доступом** Основные методы и средства защиты от утечки по материально-вещественному каналу. Организационные методы защиты. Системы охраны периметра предприятия. Многозональная и многорубежная защита. Структурные схемы СКУД. Одно дверные и много дверные СКУД. Одно контроллерные и много контроллерные СКУД. Организация передачи, хранения и документирования информации в СКУД. Дополнительные функции СКУД.	
	6	**Занятие 23. Организационные основы создания и эксплуатации систем контроля и управления доступом** Организация работы СКУД. Номенклатура и порядок разработки организационно-распорядительных документов по эксплуатации СКУД. Структура службы режима. Планирование работ по эксплуатации СКУД. Лицензирование и сертификация. Порядок сертификации технических средств СКУД и лицензирования деятельности. Основные документы в сфере лицензирования и сертификации. Подготовка и переподготовка кадров в области внедрения и эксплуатации СКУД.	
	7	**Занятие 24. Методы и средства контроля эффективности систем контроля и управления доступом.** Показатели эффективности СКУД на объекте информатизации. Методы и средства контроля эффективности СКУД. Вероятностный подход к оценке эффективности СКУД	
	Практические занятия		12
	12	**Занятие 25.** Обоснование необходимости создания СКУД объекта информатизации на основе нормативных и методических документов.	
	13	**Занятие 26.** Модели нарушителей физической безопасности объекта информатизации.	
	14	**Занятие 27.** Разработка топологии многозональной и многорубежной системы физической защиты объекта	
	15	**Занятие 28.** Разработка структурной и функциональной схем СКУД.	
	16	**Занятие 29.** Разработка основных организационных документов службы режима предприят**ия.**	
	17	**Занятие 30.** Разработка методик контроля эффективности СКУД.	
	Содержание учебного материала		4
	1	**Занятие 31. Система телевизионного наблюдения**	

Тема 2.5. Система телевизионного наблюдения		Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения.	
	2	**Занятие 32. Оборудование систем видеонаблюдения** Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	
	Практические занятия		
	18	**Занятие 33.** Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	4
	19	**Занятие 34.** Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.6. Система сбора, обработки, отображения и документирования информации	**Содержание учебного материала**		
	1	**Занятие 35. 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	4
	2	**Занятие 36. Обзор отечественных решений ССОИ**	
	Практические занятия		
	20	**Занятие 37.** Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации	4
	21	**Занятие 38.** Сравнение отечественных ССОИ	
Тема 2.7. Система воздействия	**Содержание учебного материала**		
	1	**Занятие 39. Системы воздействия** Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	2
	Практические занятия		
	22	**Занятие 40.** Исследование возможностей радиолокатора NR-900EMS	6
	23	**Занятие 41.** Исследование возможностей прибора ST 033P Пиранья	
	24	**Занятие 42.** Исследование возможностей анализатора спектра OSCOR Green	
Тема 2.8. Применение инженерно-технических средств физической защиты	**Содержание учебного материала**		
	1	**Занятие 43. Организационные основы инженерно-технической защиты информации** Задачи и структура государственной системы инженерно-технической защиты информации. Организация инженерно-технической защиты информации на предприятиях, в учреждениях. Нормативно-правовая база инженерно-технической защиты информации. Основные	16

		организационные и технические меры по обеспечению инженерно-технической защиты информации. Контроль эффективности инженерно-технической защиты информации	
	2	**Занятие 44. Методическое обеспечение инженерно-технической защиты информации** Алгоритм проектирования системы защиты информации. Моделирование объектов защиты. Моделирование угроз информации. Моделирование каналов несанкционированного доступа к информации. Моделирование каналов утечки информации	
	3	**Занятие 45. Методическое обеспечение инженерно-технической защиты информации** Организация защиты источников информации при помощи активного оборудования. Выбор технических средств охраны. Типовые меры по защите информации от наблюдения. Типовые меры по защите информации от подслушивания. Типовые меры по защите информации от перехвата	
	4	**Занятие 46. Система инженерно-технической защиты информации** Ограждения территории. Ограждения зданий и сооружений. Металлические шкафы, сейфы и хранилища. Средства систем контроля и управления доступом. Средства обнаружения злоумышленников и пожара. Извещатели. Средства контроля и управления средствами охраны. Средства телевизионной охраны. Средства оповещения. Средства нейтрализации угроз	
	5	**Занятие 47. Система инженерно-технической защиты информации** Средства противодействия наблюдению в различных диапазонах. Средства звукоизоляции и звукопоглощения акустического сигнала. Средства предотвращения утечки информации с помощью закладных подслушивающих устройств. Классификация средств обнаружения и локализации. Аппаратура радиоконтроля. Средства контроля телефонных линий и цепей электропитания. Технические средства подавления сигнала закладных устройств. Средства контроля помещений на отсутствие закладных устройств	
	6	**Занятие 48. Демаскирующие признаки объектов защиты.** Опознавательные признаки и признаки деятельности объектов. Видовые, сигнальные и вещественные демаскирующие признаки. Информативность признаков. Понятие о признаковых структурах.	
	7	**Занятие 49. Классификация демаскирующих признаков** Основные видовые демаскирующие признаки объектов наблюдения. Основные признаки, характеризующие физические и хи-мические свойства материальных тел. Понятие о демаскирующих объектах, сигналах и веществах	
	8	**Занятие 50. Основы противодействия техническим средствам разведки** Способы комплексного использования злоумышленниками технических каналов утечки информации. Методы энергетического скрытия акустических сигналов: звукоизоляция и	

		звукопоглощение. Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей. Способы повышения звукоизоляции окон и дверей. Основные звукопоглощающие материалы и способы их применения.	
	Практические занятия		6
	25	**Занятие 51.** Проведение анализа защищаемой в кабинете руководителя информации	
	26	**Занятие 52.** Моделирование угроз воздействия на источники информации	
	27	**Занятие 53.** Разработка и осуществление мер по предотвращению проникновения злоумышленника к источникам информации	
Тема 2.9. Эксплуатация инженерно-технических средств физической защиты	**Содержание учебного материала**		20
	1	**Занятие 54. Кибербезопасность: основные понятия и определения** Кибербезопасность (информационная безопасность) киберфизических систем, кибербезопасность в «Интернет-вещей»: основные стандарты, понятия, определения.	
	2	**Занятие 55. Стандарты кибербезопасности** Киберфизические системы и «Интернет-вещей»: обзор основных проблем, связанных с кибербезопасностью; основные угрозы и уязвимости в сфере кибербезопасности. Регулирование вопросов кибербезопасности в «Интернет-вещей»: международное, в РФ.	
	3	**Занятие 56. Функциональная безопасность: основные понятия и определения** Функциональная безопасность: основные стандарты, понятия и определения. Обзор основных стандартов в сфере функциональной безопасности.	
	4	**Занятие 57. Кибербезопасность в «Интернет-вещей»** Кибербезопасность в «Интернет-вещей» для граждан: классификация продуктов «Интернет-вещей» для граждан, угрозы, уязвимости, риски на примере популярных продуктов. «Интернет-вещей» в сфере здравоохранения – риски и проблемы. «Умный дом» - риски и проблемы. Юридические инциденты – примеры Цели обеспечения кибербезопасности в «Интернет-вещей» для граждан	
	5	**Занятие 58. Кибербезопасность для систем «Умного города»** «Умный город»: состав систем (категории систем, классификация), зрелость Smart City: понятие, критерии оценки, угрозы, риски и проблемы, модель угроз (структура, особенности), обзор стандартов по направлению «Умный город» (Smart City). «Интернет-вещей» и его применение в Smart Grid, проблемы кибербезопасности	
	6	**Занятие 59. Кибербезопасность в «Интернет-вещей» в промышленности**	

		Киберфизические системы и «Интернет-вещей» в промышленности: понятие «Индустриальный Интернет-вещей», соотношение с понятием «киберфизическая система», классификация продуктов «Интернет-вещей», соотношение с понятиями АСУТП, ICS; угрозы, уязвимости, риски	
	7	**Занятие 60. Критическая информационная инфраструктура: основные понятия, определения, проектирование систем безопасности.** Критическая информационная инфраструктура, основные понятия, стандарты. Критическая информационная инфраструктура РФ, основные понятия, НПА, требования.	
	8	**Занятие 61. Объекты КИИ** Категорирование объектов КИИ РФ, порядок и критерии Основные подсистемы обеспечения ИБ объектов КИИ. Средства обеспечения кибербезопасности (обзор) Проектирование систем безопасности значимых объектов КИИ	
	9	**Занятие 62. СМИБ для объектов КИИ** Силы обеспечения кибербезопасности объектов КИИ Требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры. Построение СМИБ для объектов КИИ на промышленных объектах: Обзор стандартов семейства ISO / ГОСТ 27К. Состав СМИБ. Особенности создания СМИБ для объектов КИИ на промышленных объектах	
	10	**Занятие 63. Стандарты безопасности объектов КИИ** Ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК	
	Лабораторные работы		16
	1	**Занятие 64.** Исследование возможностей имитатора АВРОРА-3	
	2	**Занятие 65.** Исследование возможностей комплекса КРОНА-ПРО	
	3	**Занятие 66.** Исследование возможностей приемника СКОРПИОН-XL	
	4	**Занятие 67.** Исследование принципов работы индикатора поля РИЧ-8	
	5	**Занятие 68.** Исследование принципов работы индикатора поля MFP-8000	
	6	**Занятие 69.** Исследование принципов работы индикатора поля ST-107	
	7	**Занятие 70.** Исследование принципов работы индикатора поля PST-165	
	8	**Занятие 71.** Исследование возможностей системы ШЕПОТ	
	Самостоятельная работа обучающихся		
	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем).		25

	Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторных работ, отчетов и подготовка к их защите. **Тематика домашних заданий, сообщений, рефератов:** 1. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов. 2. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. 3. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. 4. Объектовые средства обнаружения: назначение, устройство, принцип действия. 5. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. 6. Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. 7. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации		
Учебная практика	**Виды работ**		
	1	**Занятие 1.** Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике.	**108**
	2	**Занятие 2.** Монтаж различных типов датчиков.	
	3	**Занятие 3.** Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.	
	4	**Занятие 4.** Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации	
	5	**Занятие 5.** Рассмотрение системы контроля и управления доступом	
	6	**Занятие 6.** Рассмотрение принципов работы системы видеонаблюдения и ее проектирование	
	7	**Занятие 7.** Рассмотрение датчиков периметра, их принципов работы	
	8	**Занятие 8.** Выполнение звукоизоляции помещений системы зашумления	
	9	**Занятие 9.** Реализация защиты от утечки по цепям электропитания и заземления	
	10	**Занятие 10.** Рассмотрение принципов работы ЛВП-10 Электромагнитный вибропреобразователь к ЛГШ-404 (для окон, стен, труб)	

	11	**Занятие 11.** Рассмотрение многозонной системы обнаружения и блокирования мобильных средств связи для образовательных учреждений	
	12	**Занятие 12.** Монтаж различных типов датчиков	
	13	**Занятие 13.** Рассмотрение устройств обнаружения скрытых видеокамер «Алмаз»	
	14	**Занятие 14.** Применение промышленных осциллографов, частотомеров и генераторов акустического шума, двухканального генератора, системы постановки виброакустических помех и другого оборудования для защиты информации.	
	15	**Занятие 15.** Рассмотрение системы контроля и управления доступом	
	16	**Занятие 16.** Рассмотрение принципов работы программно-аппаратного комплекса защиты объектов информационных технологий от разведки ПЭМИ, 0,009 - 1000 МГц	
	17	**Занятие 17.** Рассмотрение датчиков периметра, их принципов работы	
	18	**Занятие 18.** Изучение средств перехвата информации	
	19	**Занятие 19.** Микрофоны	
	20	**Занятие 20.** Акустические антенны	
	21	**Занятие 21.** Выбор типа микрофона и места его установки	
	22	**Занятие 22.** Изучение устройств подавления микрофонов	
	23	**Занятие 23.** Изучение устройств для перехвата речевой информации в проводных каналах	
	24	**Занятие 24.** Изучение оптико-акустической аппаратуры перехвата речевой информации	
	25	**Занятие 25.** Оптико-механические приборы	
	26	**Занятие 26.** Приборы ночного видения	
	27	**Занятие 27.** Средства скрытой фотосъемки	
	28	**Занятие 28.** Зоны подключения в линиях связи	
	29	**Занятие 29.** Перехват телефонных переговоров в зонах «А», «Б», «В», «Г», «Д», «Е»	
	30	**Занятие 30.** Изучение перехвата сообщений в каналах сотовой связи	
	31	**Занятие 31.** Методы поиска закладных устройств как физических объектов и электронных средств	
	32	**Занятие 32.** Панорамные приемники	
	33	**Занятие 33.** Аппаратура контроля и защиты линии связи	
	34	**Занятие 34.** Средства создания акустических и электромагнитных маскирующих помех	
	35	**Занятие 35.** Измерение токов, напряжений и сопротивлений	
	36	**Занятие 36.** Исследование двухполюсников с помощью мультиметра	
	37	**Занятие 37.** Прямые и косвенные однократные измерения	

	38	**Занятие 38.** Обработка и представление однократных измерений при наличии систематической погрешности	
	39	**Занятие 39.** Стандартная обработка результатов прямых измерений с многократным наблюдением	
	40	**Занятие 40.** Обработка результатов прямых измерений с многократным наблюдением при наличии грубых погрешностей	
	41	**Занятие 41.** Определение погрешности цифрового вольтметра сличения и прямых измерений	
	42	**Занятие 42.** Измерение мощности и силы постоянного электромагнитного тока	
	43	**Занятие 43.** Измерение постоянного напряжения методом компенсации	
	44	**Занятие 44.** Измерение переменного электрического напряжения	
	45	**Занятие 45.** Измерение частоты и периода электрических сигналов	
	46	**Занятие 46.** Терморезисторные измерительные преобразователи. Измерители температуры	
	47	**Занятие 47.** Емкостные измерительные преобразователи. Измерение размера	
	48	**Занятие 48.** Индуктивные измерительные преобразователи. Измерение перемещения	
	49	**Занятие 49.** Термоэлектрические измерительные преобразователи. Измерение температуры	
	50	**Занятие 50.** Пьезоэлектрические измерительные преобразователи. Измерение переменных ускорений	
	51	**Занятие 51.** Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами	
	52	**Занятие 52.** Применение существующих способов выявления опасности целостности информации	
	53	**Занятие 53.** Выявление технических каналов утечки информации	
	54	**Занятие 54.** Оформление отчета по учебной практике	
Производственная практика (по профилю специальности)	**Виды работ**		
	1	Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Получение заданий по тематике	**180**
	2	Определение исходных данных по защищаемому объекту и плана работ по созданию системы защиты речевой информации (СЗРИ)	
	3	Выявление технических каналов утечки (ТКУ) речевой информации с использованием современных средств контроля и контрольно-измерительной аппаратуры	
	4	Подготовка предложений в проект технического задания на создание СЗРИ, в том числе специального защищенного (экранированного) помещения (СЗП)	

5	Разработка рекомендаций по совершенствованию мер защиты речевой информации и предложения по корректировке СЗРИ и СЗП
6	Монтаж средств защиты информации и их настройка, инструментальная оценка эффективности защиты речевой информации и электромагнитного экранирования СЗП
7	Опытная эксплуатация СЗРИ и СЗП в целях проверки их работоспособности
8	Участие в монтаже средств охраны и безопасности, инженерной защиты
9	Анализ уязвимости системы
10	Выявление ПЭМИН в информационной системе и защита от них
11	Восстановление информации при перехвате ПЭМИН
12	Предотвращение утечки информации через ПЭМИН ПК
13	Организационные мероприятия по технической защите информации от утечки по каналам ПЭМИН
14	Организационные мероприятия по технической защите информации в средствах вычислительной техники, автоматизированных системах и сетях от утечки по каналам ПЭМИН
15	Применение активных методов защиты информации от утечки по каналам ПЭМИН
16	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами
17	Оценка защищенности основных технических средств в составе автоматизированной системы от утечки информации по каналу побочных электромагнитных излучений
18	Оценка защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от её утечки за счет наводок информативного сигнала
19	Участие в обслуживании технических средств защиты информации
20	Выполнение подбора, настройки и применения технических средств защиты информации
21	Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения
22	Использование средств охраны и безопасности объекта
23	Организация и реализация технической охраны объектов
24	Парольная аутентификация в системах ИБ и PIN-код в СКУД
25	Участие в организации работ по технической защите конфиденциальной информации
26	Контроль доступа к неструктурированным данным
27	Внутренний контроль обработки ПДн
28	Контроль за соответствием обработки ПДн

29	Участие в перехвате побочных электромагнитных излучений
30	Поиск и измерение ПЭМИ монитора на ЭЛТ (монитора на ЖК) в автоматическом и режиме управляющей программы
31	Составление протокол исследования с помощью расчетной программы
32	Съем наводок ПЭМИ ТСОИ с соединительных линий ВТСС и посторонних проводников
33	Защита информации в АСУ
34	Защита информации при передаче данных
35	Защита информации ограниченного доступа
36	Защита информации на жестком диске
37	Защита информации при использовании электронной почты
38	Комплексная защита информации в корпоративных системах
39	Защита информации в компьютерных сетях
40	Защита информации в локальных вычислительных сетях
41	Защита информации в VPN-сетях
42	Защита информации от несанкционированного доступа в сетях
43	Контроль доступа к информации
44	Управление доступом к информации
45	Техническая защита информации на предприятии
46	Инженерно-техническая защита информации на предприятии
47	Защита информации, составляющей коммерческую тайну
48	Разработка модели КСЗИ
49	Технологическое и организационное построение КСЗИ
50	Кадровое обеспечение функционирования КСЗИ
51	Участие в эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения
52	Участие в эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам
53	Установка и настройка средств защиты информации
54	Участие в монтаже технических средств защиты информации
55	Участие в монтаже средств охраны и безопасности, технической охраны объектов
56	Участие в монтаже средств защиты информации от несанкционированного съёма и утечки по техническим каналам

57	Настройка системы защиты информации от съема и утечки по техническим каналам
58	Выявление технических каналов
59	Поиск ЗУ и других технических каналов
60	Выявление путей утечки информации в ИС
61	Оценка уязвимости системы
62	Участие в монтаже средств охраны и безопасности и систем видеонаблюдения
63	Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам
64	Определение требований к системе защиты информации
65	Проектирование системы защиты информации
66	Разработка эксплуатационной документации на систему защиты информации
67	Установка и настройка средств защиты информации
68	Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта
69	Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению
70	Испытания и опытная эксплуатации системы защиты информации
71	Подтверждение соответствия системы защиты информации
72	Выполнение мероприятий по предотвращению несанкционированного доступа к информации
73	Оценка эффективности использованных мер и средств защиты информации
74	Контроль эффективности защиты информации
75	Защита информации обрабатываемой ТСПИ от утечки по техническим каналам
76	Защита от утечки информации по телефонному каналу
77	Защита от утечки информации по электросетевому каналу
78	Защита от утечки информации по вибрационному каналу
79	Защита от утечки информации по проводному каналу
80	Формирование требований к системе защиты информации
81	Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности обрабатываемой информации
82	Изучение порядка применения нормативных правовых актов

	83	Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами	
	84	Выявление технических каналов утечки информации	
	85	Применение существующих способов выявления опасности целостности информации	
	86	Анализ объектов информатизации предприятий, учреждений, организаций	
	87	Анализ ресурсов обеспечения инженерно-технической защиты информации	
	88	Изучение основных этапов проектирования системы защиты информации техническими средствами	
	89	Проектирование рабочих проектов по системе пожарно-охранной сигнализации, видеонаблюдения, СКУД	
	90	Оформление отчета	
Самостоятельная работа при подготовке к экзамену по профессиональному модулю			**8**
Консультации			**2**
Промежуточная аттестация в форме экзамена по профессиональному модулю			**8**
Всего по ПМ			**736**

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Для реализации программы предусмотрены следующие специальные помещения

Лаборатория «Защиты информации от утечки по техническим каналам». Лаборатория должна быть оснащена средствами защиты информации от утечки по акустическому (виброакустическому) каналу; средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок; средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок;

шумогенераторы;
комплексный поисковый прибор;
прожигатели телефонных линий;
устройство обнаружения скрытых видеокамер;
виброакустические генераторы;
подавители диктофонов;
подавители устройств сотовой связи;
устройство защиты аналоговых сигналов;
устройство защиты цифровых сигналов;

стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения, охранно-пожарной сигнализации и охраны объектов;

комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

3.2 Информационное обеспечение реализации программы

3.2.1. Основные печатные и электронные издания:

1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А.Бузов. - Москва: Горячая линия-Телеком, 2018. - URL: https://ibooks.ru/products/354357
2. Васильков, А.В. Безопасность и управление доступом в информационных системах: учебное пособие для СПО /А.В.Васильков, И.А.Васильков. - Москва: ФОРУМ, 2020. - URL: https://znanium.com/catalog/product/1082470
3. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019. - URL: https://znanium.com/catalog/product/1018901
4. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А.П.Зайцев, Р.В.Мещеряков, А.А.Шелупанов. – 7-е изд., испр. – Москва: Горячая Линия–Телеком, 2018. - URL: https://ibooks.ru/products/333981
5. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО /В.Я.Ищейнов, М.В.Мецатунян. - Москва: Форум: ИНФРА-М, 2018. - URL: https://znanium.com/catalog/product/927190
6. Партыка, Т.Л. Информационная безопасность: учебное пособие для студ. учрежд. СПО /Т.Л.Партыка, И.И.Попов. - Москва: Форум, 2020. - URL: https://znanium.com/catalog/product/1081318
7. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учрежд. СПО. - Москва: ФОРУМ: ИНФРА-М, 2020. - URL: https://znanium.com/catalog/document?id=358701

8. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА-М, 2020. - URL: https://znanium.com/catalog/product/1093695.

Электронные ресурсы:

1. Стандарты и регламенты//РОССТАНДАРТ. Федеральное агентство по техническому регулированию и метрологии: официальный сайт. - URL: https://www.rst.gov.ru/portal/gost//home/standarts
2. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. - URL: www.fstec.ru
3. Электронный фонд правовой и нормативно-технической документации/АО «Кодекс»: Профессиональные справочные системы: официальный сайт. – URL: http://docs.cntd.ru
4. Elibrary.ru. Научная электронная библиотека: официальный сайт. – URL: www.elibrary.ru
5. Глобус –Телеком: официальный сайт. – URL: http:/www.globus-telecom.com
6. Морион. Российский разработчик и производитель оборудования связи. –URL: http://www.morion.ru/
7. НАТЕКС: официальный сайт. – URL: http://www.nateks.ru/
8. ISKRATEL: официальный сайт. – URL: http://www.iskratel.com/
9. Промсвязь: официальный сайт. – URL: http://www.ps-ufa.ru/
10. 3М. Наука, воплощенная в жизнь: [сайт]. – URL: http://3m.com/
11. ОАО «Ферроприбор»: официальный сайт. – URL: http://www.rusgates.ru/index/php
12. SecurityLab. Защита информации и информационная безопасность: информационный портал/ООО "Positive Technologies". – URL: http://www.securitylab.ru
13. Безопасность информационных технологий: рецензируемый научный журнал НИЯУ МИФИ: официальный сайт. - URL: http://bit.mephi.ru/
14. Вопросы кибербезопасности: научный, периодический, информационно-методический журнал: официальный сайт. - URL: http://cyberrus.com/
15. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: учебное пособие / Л.В. Астахова. – Челябинск: Издательский центр ЮУрГУ, 2014. – URL: https://lib.susu.ru/ftd?base=SUSU_METHOD&key=000540003&dtype=F&etype=.pdf
16. Волхонский, В.В. Устройства охранной сигнализации/В.В.Волхонский; НИУ ИТМО. – Санкт-Петербург: Университет ИТМО, 2015. – URL: https://books.ifmo.ru/book/1633/ustroystva_ohrannoy_signalizacii.htm
17. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. - Екатеринбург: Изд-во Урал. ун-та, 2019. – URL: http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
18. Горбунов, А.В. Волоконно-оптический ответвитель-прищепка для съёма информации в волоконно-оптических линиях связи: учебное пособие /А.В.Горбунов. - Таганрог: Изд-во ТТИ ЮФУ, 2009. – URL: http://ntb.tgn.sfedu.ru/UML/UML_4399.pdf
19. Гуляев, В.П. Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации: учебно-методический комплект / В. П. Гуляев. – Екатеринбург: Изд-во Урал. ун-та, 2014. – URL: http://elar.urfu.ru/bitstream/10995/28779/1/978-5-7996-1120-0_2014.pdf
20. Защита информации в оптоволоконных локальных сетях: методические указания по выполнению лабораторных работ/ФГАУ ВО Северо-Кавказский федеральный университет. - Пятигорск, 2020. – URL:

https://www.ncfu.ru/NCFU_PYATIGORSK/.doc/obrazovanie/OP/2020/bakalavriat/10.03.01/MD-10.03.01/Metod_ZIvOLS_SR_10.03.01_2020.pdf
21. Каторин, Ю.Ф. Защита информации техническими средствами: учебное пособие / Ю.Ф.Каторин, А.В.Разумовский, А.И.Спивак; под редакцией Ю.Ф. Каторина. – С.-Петербург: НИУ ИТМО, 2012. – URL: https://books.ifmo.ru/file/pdf/975.pdf
22. Меньшаков, Ю.К. Теоретические основы технических разведок: учебное пособие / Ю.К.Меньшаков; под ред. Ю.Н. Лаврухина. – Москва: Изд-во МГТУ им. Н.Э. Баумана, 2008. – URL: https://rusneb.ru/catalog/000199_000009_02000010254/
23. Руководство по применению адресно-аналоговых систем пожарной сигнализации/ С.М. Щипицын, А. Н. Членов, И. В. Павлов, А. Е. Атаманов. - Москва: Систем Сенсор Фаир Детекторс, 2012// СИГМА: группа компаний: официальный сайт. – URL: http://www.sigma-is.ru/files/education/Rukovodstvo_AASPS_2012.pdf
24. Рыжова, В.А. Проектирование и исследование комплексных систем безопасности/В.А.Рыжова; НИУ ИТМО. – С.-Петербург: НИУ ИТМО, 2013. – URL: https://books.ifmo.ru/file/pdf/1018.pdf
25. Теория информационной безопасности и методология защиты информации /Ю.А.Гатчин, В.В.Сухостат, А.С.Куракин, Ю.В.Донецкая. – 2-е изд., испр. и доп. – С.-Петербург: Университет ИТМО, 2018. – URL: https://books.ifmo.ru/file/pdf/2372.pdf.

3.2.2. Дополнительные источники:

1. Бубнов, А. А. Техническая защита информации в объектах информационной инфраструктуры: учебник для среднего проф. образования/А.А. Бубнов, В.Н.Пржегорлинский, К.Ю.Фомина. – Москва: Академия, 2019.
2. Ворона, В. А. Инженерно-техническая и пожарная защита объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая Линия–Телеком, 2012. - URL: https://ibooks.ru/products/333380
3. Ворона, В.А. Системы контроля и управления доступом/В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2013. - URL: https://ibooks.ru/products/333378
4. Ворона, В.А. Технические системы охранной и пожарной сигнализации /В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2012. - URL: https://ibooks.ru/products/333381
5. Ворона, В.А. Технические средства наблюдения в охране объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая линия-Телеком, 2011. - URL: https://ibooks.ru/products/333379
6. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - Москва: Форум: ИНФРА-М, 2019. .- URL: https://znanium.com/catalog/product/1001363
7. Груба, И.И. Системы охранной сигнализации. Технические средства обнаружения: справочное пособие / И.И.Груба. - Москва: СОЛОН-Пресс, 2020. - URL: https://znanium.com/catalog/product/1858802
8. Коваленко, Ю.Ю. Правовой режим лицензирования и сертификации в сфере информационной безопасности: учебное пособие / Ю.Ю.Коваленко. – Москва: Горячая линия – Телеком, 2012. - URL: https://ibooks.ru/products/333992
9. Малюк, А. А. Защита информации в информационном обществе: учебное пособие для вузов /А.А. Малюк. - Москва: Горячая линия-Телеком, 2015. - URL: https://ibooks.ru/products/354360
10. Новикова, Е.Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи: учебник для среднего проф. образования /Е.Л.Новикова. – Москва: Академия, 2018.

11. Пескин, А.Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации / А.Е. Пескин. - Москва: Горячая линия-Телеком, 2013. - URL: https://ibooks.ru/products/334018
12. Скрипник, Д.А. Общие вопросы технической защиты информации/ Д.А.Скрипник. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — URL: https://e.lanbook.com/book/100275
13. Шейдаков, Н. Е. Физические основы защиты информации: учеб. пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. - Москва: РИОР: ИНФРА-М, 2019. - URL: https://znanium.com/catalog/product/916070
14. Ярочкина, Г.В. Монтаж и эксплуатация систем видеонаблюдения и систем безопасности: учебник для среднего проф. образования/Г.В.Ярочкина. – Москва: Академия, 2020.

Нормативные документы:

1. Кодекс Российской Федерации об административных правонарушениях//Гарант: справочно-правовая система. – URL: https://base.garant.ru/12125267/
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12148555/
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12148567/
4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12129354/
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12185475/
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12136635/
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/10200083/
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/192944/
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608//Гарант: справочно-правовая система. – URL: https://base.garant.ru/102670/
10. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г. //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/en/component/attachments/download/288
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21 //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21
12. Меры защиты информации в государственных информационных системах.

Утверждены ФСТЭК России 11 февраля 2014 г. //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 17 июля 2017 г. N 134// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/administrativnye-reglamenty/1362-prikaz-fstek-rossii-ot-17-iyulya-2017-g-n-134-2
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/administrativnye-reglamenty/478-prikaz-fstek-rossii-ot-12-iyulya-2012-g-n-84
15. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702
16. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/370
17. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». – URL: https://base.garant.ru/187947/
18. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: https://docs.cntd.ru/document/1200095034
19. ГОСТ Р 34-11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200095035
20. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. –URL: http://docs.cntd.ru/document/1200058320
21. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/gost-r-51275-2006
22. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. –

URL: http://docs.cntd.ru/document/1200108858
23. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. – URL: http://docs.cntd.ru/document/1200102287
24. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200044725
25. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200113006
26. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200113336
27. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: https://docs.cntd.ru/document/1200048398
28. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс». – URL: https://docs.cntd.ru/document/1200101777
29. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200105710
30. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: https://docs.cntd.ru/document/1200105711
31. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. - URL: http://docs.cntd.ru/document/1200103619
32. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010
33. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети//Электронный фонд правовых и нормативно-технических

документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200048416
34. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380

Периодические издания:

1. Information Security/Информационная безопасность: официальный сайт. - URL: https://lib.itsec.ru/imag/
2. Защита информации Inside.
3. Электросвязь.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенции, 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;	Экспертное наблюдение
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;	Экспертное наблюдение
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.	- 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; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
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	Экспертное наблюдение

	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 Экзамен
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен
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);	Экспертное наблюдение Экзамен
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	Экспертное наблюдение
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	Экзамен
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективное выполнение правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности	Экспертное наблюдение
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен
ЛР1–ЛР4, ЛР9, ЛР10, ЛР13-ЛР15, ЛР20, ЛР23–ЛР28		

Приложение 1

Информационные ресурсы, используемые при выполнении самостоятельной работы

*рекомендуется пользоваться Интернет-ресурсами при самостоятельной работе по всем разделам дисциплины

МДК.03.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

№ занятия	**Рекомендуемые издания**
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты	
Занятие 1	[1] с.201-209
Занятие 2	[1] с. 27-30, 31-44
Занятие 3	[1] с. 186-218
Занятие 4	[2] с. 10-14
Занятие 5	[2] с. 4-5, 12-14
Занятие 6	[3] с. 14-22
Занятие 7	[1] с. 62-68
Занятие 8	[1] с. 62-68
Занятие 9	[3] с. 14-18
Занятие 10	[4] с. 377-379
Занятие 11	[5] с. 545-554
Занятие 12	[5] с. 547-549
Занятие 13	[5] с. 548-550
Занятие 14	[5] с. 560-562
Занятие 15	[1] с. 62-68
Занятие 16	[4] с. 376-377
Занятие 17	[4] с. 376-377
Занятие 18	[6] с. 42-46
Занятие 19	[5] с. 11-13
Занятие 20	[5] с. 560-562
Занятие 21	[1] с. 155-161
Занятие 22	[5] с. 545-554
Занятие 23	[5] с. 548-550
Занятие 24	[1] с. 62-68
Занятие 25	[1] с. 59
Занятие 26	[1] с. 59
Занятие 27	[7] с. 88-102
Занятие 28	[8] с. 22-24
Занятие 29	[8] с. 21-25
Занятие 30	[9] с. 109-110
Занятие 31	[1] с. 119-121
Занятие 32	[10] с. 57-59
Занятие 33	[5] с. 562-564
Занятие 34	[4] с. 163-164
Занятие 35	[5] с. 547-550
Занятие 36	[1] с. 149-151
Занятие 37	[5] с. 562-565
Занятие 38	[4] с. 377-379
Занятие 39	[4] с.563-564

Занятие 40	[11] с. 57-59
Занятие 41	[5] с. 476-479
Занятие 42	[5] с. 562-564
Занятие 43	[1] с. 194-200
Занятие 44	[1] с. 194-200
Занятие 45	[5] с. 548-550
Занятие 46	[9] с. 101-105
Занятие 47	[12] с. 161-162
Занятие 48	[12] с. 161-162
Занятие 49	[12] с. 20-22
Занятие 50	[12] с. 20-22
Занятие 51	[8] с. 18-20
Занятие 52	[11] с. 40
Занятие 53	[11] с. 20
Занятие 54	[1] с. 209
Занятие 55	[5] с. 560-562
Занятие 56	[1] с. 287-290
Занятие 57	[1] с. 287-290
Занятие 58	[7] с. 69-70
Занятие 59	[7] с. 69-70
Занятие 60	[13] с. 7-16
Занятие 61	[13] с. 31-50
Занятие 62	[13] с. 7-16
Занятие 63	[13] с. 31-50
Занятие 64	[1] с. 257-258
Занятие 65	[1] с. 278-279
Занятие 66	[9] с. 90-91
Занятие 67	[14] с. 29-31
Занятие 68	[1] с. 108-114
Занятие 69	[1] с. 186-218
Занятие 70	[10] с. 57-59
Занятие 71	[1] с. 287-290
Занятие 72	[7] с. 86-88
Занятие 73	[16] с. 13-18
Занятие 74	[7] с. 65-67
Занятие 75	[7] с. 65-67
Занятие 76	[1] с. 136-139
Занятие 77	[1] с. 136-139
Занятие 78	[1] с. 229-233
Занятие 79	[5] с. 547-549

МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей

№ занятия	**Рекомендуемые издания**
Раздел 2. Физическая защита линий связи ИТКС	
Занятие 1	[17] с. 21-23
Занятие 2	[1] с. 68-70
Занятие 3	[15] с. 37
Занятие 4	[15] с. 37

Занятие 5	[4] с. 5-6
Занятие 6	[1] с. 68-70
Занятие 7	[15] с. 37-38
Занятие 8	[15] с. 37-38
Занятие 9	[15] с. 37
Занятие 10	[15] с. 37-38
Занятие 11	[15] с. 37-38
Занятие 12	[18] с. 12-19
Занятие 13	[1] с. 257-258
Занятие 14	[19] с. 29-32
Занятие 15	[19] с. 29-32
Занятие 16	[19] с. 29-32
Занятие 17	[19] с. 29-32
Занятие 18	[20] с. 95-103
Занятие 19	[20] с. 106-115
Занятие 20	[20] с. 95-96
Занятие 21	[20] с. 87-95
Занятие 22	[20] с. 77-90
Занятие 23	[20] с. 62-68
Занятие 24	[20] с. 20
Занятие 25	[20] с.64
Занятие 26	[18] с. 7-10
Занятие 27	[4] с. 57-61
Занятие 28	[20] с. 106-115
Занятие 29	[20] с. 8-9
Занятие 30	[20] с. 106-115
Занятие 31	[21] с. 26-33
Занятие 32	[21] с. 33-43
Занятие 33	[21] с. 14-21
Занятие 34	[20] с. 87-90
Занятие 35	[18] с. 43-44
Занятие 36	[5] с. 63-66
Занятие 37	[18] с. 43-44
Занятие 38	[5] с. 63-66
Занятие 39	[3] с.38-41
Занятие 40	[22] с.45-51
Занятие 41	[23] с. 43-51
Занятие 42	[11] с. 20-23
Занятие 43	[15] с. 37-38
Занятие 44	[4] с. 361-364
Занятие 45	[5] с. 553-557
Занятие 46	[4] с. 13-15
Занятие 47	[11] с.41-44
Занятие 48	[1] с. 229-233
Занятие 49	[1] с. 229-233
Занятие 50	[8] с. 33-42
Занятие 51	[3] с. 25-42
Занятие 52	[5] с. 560-562
Занятие 53	[1] с. 68-70

Занятие 54	[24] с.7-16, 141-152
Занятие 55	[14] с. 54-56
Занятие 56	[25] с. 38-40
Занятие 57	[25] с. 41, 44
Занятие 58	[25] с. 41
Занятие 59	[25] с.44
Занятие 60	[4] с. 367-368
Занятие 61	[9] с. 194
Занятие 62	[9] с. 194
Занятие 63	[9] с.195
Занятие 64	[26] с. 216 - 220
Занятие 65	[26] с. 314-321
Занятие 66	[26] с. 121-123
Занятие 67	[26] с. 139-146
Занятие 68	[26] с. 145-153
Занятие 69	[26] с.474-482
Занятие 70	[26] с. 482-491
Занятие 71	[26] с. 501-505