Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Липецкий филиал Финуниверситета

СОГЛАСОВАНО

ПАО «Ростелеком»

Директор Липецкого филиала
ПАО «Ростелеком»

_____ К.В. Власов

«24» апреля 2024 г.

УТВЕРЖДАЮ

Заместитель директора
по учебно-методической работе
Липецкого филиала Финуниверситета

_____ О.Н. Левчегов

«24» апреля 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

Липецк - 2024

Рабочая программа профессионального модуля «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Разработчики:

Черпаков Игорь Владимирович, к.ф.-м.н., доцент кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Рабочая программа профессионального модуля рассмотрена и рекомендована к утверждению на заседании кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Протокол от 23.04.2024 г. №10

Заведующий кафедрой

Учет и информационные технологии в бизнесе  Н.С. Морозова

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Рабочая программа профессионального модуля «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» является частью основной профессиональной программы (далее ОПОП) в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рабочая программа профессионального модуля «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке обучающихся данной специальности.

Рабочая программа составлена для обучающихся очной формы обучения, в том числе с применением элементов дистанционных образовательных технологий и электронного обучения.

При обучении инвалидов и лиц с ограниченными возможностями здоровья дистанционные образовательные технологии и электронное обучение предусматривает возможность приема-передачи информации в доступных для них формах.

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен овладеть соответствующими профессиональными и общими компетенциями:

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.

1.1.1. Перечень 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 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранных языках.

1.1.2. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	– выявление технических каналов утечки информации; – использование основных методов и средств инженерно-технической защиты информации; – диагностики, устранения отказов и восстановления работоспособности инженерно-технических средств обеспечения информационной безопасности; – участие в мониторинге эффективности инженерно-технических средств обеспечения информационной безопасности; – решение частных технических задач, возникающих при аттестации объектов, помещений, технических средств.
Уметь	– применять технические средства защиты информации; – использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; – использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам; – применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами.
Знать	– физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации; – основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съема и утечки по техническим каналам; – номенклатуру применяемых средств охраны объектов, систем видеонаблюдения.

1.2. Количество часов на освоение рабочей программы профессионального модуля

Всего часов: **468 час.**
Из них на освоение МДК – **304 час.:**
МДК.03.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты – **174 час.;**
МДК.03.02 Физическая защита линий связи информационно-телекоммуникационных систем и сетей – **130 час.;**
В том числе самостоятельная работа – **112 час.**
Практики, в том числе учебная – **36 час.**
производственная (по профилю специальности) – **108 час.**
Экзамен по модулю – **20 час.**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименование разделов профессионального модуля (МДК)	Суммарный объем нагрузки, часов	В т.ч. в форме практической подготовки	Объем профессионального модуля, часов						
				Работа обучающихся во взаимодействии с преподавателем						Самостоятельная работа
				Обучение по МДК				Практики		
				Всего	Промежуточная аттестация	В том числе		Учебная	Производственная	
						лабораторные и практические занятия	Курсовые проекты (работы)			
ОК 1-7, ОК 9 ПК 3.1-3.4	МДК.03.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	174	-	100	10	32	-	-	-	64
ОК 1-7, ОК 9 ПК 3.1-3.4	МДК.03.02 Физическая защита линий связи информационно-телекоммуникационных систем и сетей	130	-	72	10	30	-	-	-	48
Учебная практика		36	36					36		
Производственная практика (по профилю специальности)		108	108						108	
Экзамен по модулю		20	X							
Всего:		**468**		**172**	**20**	**62**	**-**	**36**	**108**	**112**

2.2 Тематический план и содержание профессионального модуля

Наименование разделов профессионального модуля, междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) работа обучающихся	Объем часов
1	*2*	*3*
МДК.03.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты		**174**
Подраздел 1. Применение инженерно-технических средств обеспечения информационно безопасности		
Тема 1.1. Объекты информационной защиты	**Содержание учебного материала**	
	1. Введение 2. Средства информации ка предмета защиты техническими средствами. 3. Демаскирующие признаки объектов защиты. Демаскирующие признаки сигналов, веществ. 4. Носители и источники информации. Запись и съем информации с ее носителя. 5. Источники угроз безопасности информации. 6. Опасные сигналы и их источники.	**16**
	Практические занятия	
	Классификация демаскирующих признаков.	**1**
	Основные виды угроз информации	**1**
Тема 1.2. Угрозы информационной безопасности	**Содержание учебного материала**	
	1. Виды угроз безопасности информации, защищаемой техническими средствами. Органы добывания информации. Технология добывания информации. 2. Добывание информации без физического проникновения в контролируемую зону. Способы несанкционированного доступа к источнику информации. Способы и средства добывания информации техническими средствами. Способы и средства перехвата сигналов. Классификация и структура технических каналов утечки информации. Акустические каналы утечки. 3. Оптические каналы утечки. Радиоэлектронные каналы утечки информации. Вещественные 4 3 каналы утечки информации.	**8**
	Практические занятия	
	Работа остронаправленных микрофонов.	**1**
	Работа диктофонов со скрытой записью.	**1**
	Утечка информации по цепям.	**1**

	Типовая структура технических каналов утечки.	**1**
	Моделирование каналов утечки информации.	**1**
	Опасность электрических сигналов и радиосигналов в радиоэлектронном канале.	**1**
	Методы добывания информации о вещественных носителях.	**1**
Тема 1.3. Методы инженерно-технической защиты информации	**Содержание учебного материала**	
	1. Концепция инженерно-технической защиты информации. 2. Факторы обеспечения защиты информации от угроз воздействия утечки. Методы физической защиты информации. Способы и средства защиты информации от наблюдения. Методы противодействия радиолокальному и гидроакустическому наблюдению. 3. Методы противодействия подслушиванию. 4. Способы и средства предотвращения утечки информации через ПЭМИН. Способы предотвращения утечки информации по материально-вещественному каналу. Защита объектов от химической, радиационной и магнитометрической разведок, системы защиты от утечки информации по электросетевому каналу, моделирование объектов защиты и каналов утечки информации	**16**
	Практические занятия	
	Типовые инженерные конструкции	**1**
	Способы и средства обнаружения злоумышленников и пожаров.	**1**
	Способы и средства видеоконтроля.	**1**
	Средства пожаротушения и тревожной сигнализации.	**1**
	Средства управления системой охраны.	**1**
	Маскировка в видимом и ИК диапазонах света.	**1**
	Активное подавление сигналов радиолокатора.	**1**
	Работа скремблеров и вокодеров.	**1**
	Энергетическое скрытие акустических сигналов: звукоизоляция и звукопоглощение.	**1**
	Применение генераторов акустического и вибрационного зашумления.	**1**
	Работа обнаружителей электромагнитного поля.	**1**
	Представление моделей объектов информационной безопасности.	**1**
	Определение путей проникновения злоумышленника к источнику информации.	**1**
	Типовые индикаторы каналов утечки.	**1**
	Комплексная система защиты.	**1**
	Содержание учебного материала	

Тема 1.4 Технические основы добывания и инженерно-технической защиты информации	1. Инженерно-техническая защита информации. Характеристика средств технической разведки. Возможности средств технической разведки. 2. Акустические приемники. Диктофоны. Закладные устройства. Лазерные средства подслушивания.	**8**
	Практические занятия	
	Обнаружители и подавители диктофонов.	**2**
Тема 1.5 Средства скрытого наблюдения	**Содержание учебного материала**	
	Оптические системы. Визуально-оптические приборы. Фото и видео аппараты. Средства видеонаблюдения, видеоконтроля, видео охраны.	**4**
	Практические занятия	
	Структурная схема видеонаблюдения.	**1**
	Выбор оптимального устройства видеозаписи.	**1**
Тема 1.6 Средства перехвата сигналов	**Содержание учебного материала**	
	1. Средства перехвата радиосигналов. Технические средства анализа сигналов. 2. Средства определения координат источников радио сигналов и перехвата оптических и электрических сигналов. Определение координат источников радиоизлучений и анализа сигналов. 3. Способы и средства уничтожения информации. Способы и средства стирания информации на магнитных носителях. 4. Средства инженерной защиты. Инженерные конструкции. 5. Ограждение территорий, зданий, помещений. Двери, окна, Ворота. Металлические сейфы, хранилища. Запирающие устройства. 6. Подходы к проектированию систем защиты информации. Принципы построения системы защиты информации. 7. Методологические основы системы защиты информации. Методика определения состава защищаемой информации. Выявление каналов доступа к информации. 8. Определение источников дестабилизирующего воздействия на информацию. 9. Понятие модели объекта. Технологическое построение системы защиты информации. Кадровое обеспечение защиты информации. Кодекс корпоративного поведения. Нормативно-методическое обеспечение защиты информации. Управление системой защиты информации. Разработка системы ИТЗИ. Построение системы безопасности предприятия.	**16**
	Практические занятия	
	Комплексы обнаружения и пеленгации.	**2**

	Анализаторы телефонных линий.	**2**
Самостоятельная работа при изучении МДК 03.01		**64**
Рекомендуемая примерная тематика внеаудиторной самостоятельной работы: 1. Систематическая проработка конспектов занятий, учебной литературы. Составление конспектов (таблиц, схем) по вопросам преподавателя. Подготовка к практическим работам. Написание рефератов. Примерная тематика домашних заданий 2. Написание рефератов по темам разделов: 3. «Направление комплексного проектирования систем защиты информации» «Основные проблемы реализации систем защиты информации» «Требования к КСЗИ» 4. «Задачи стратегии защиты информации» 5. «Верификация» 6. «Дискреционный контроль доступа» 7. «Биометрическая идентификация» 8. «Биометрия по клавиатурному почерку» 9. «Классификация признаков голоса и речи» 10. «Средства высоконадежной биометрической аутентификации» 11. «Шпионаж, сбор служебной информации, сканирование эфира, обработка неучтенных источников» 12. «Меры по защите информации внутри зоны» 13. «Автоматическое обнаружение движущегося нарушителя» 14. «Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведки» 15. «Контроль эффективности инженерно-технической защиты информации» 16. «Пути оптимизации мер инженерно-технической защиты информации» Принципы оценки эффективности инженерно-технической защиты информации» «Источники опасных сигналов» 17. «Типы побочных излучений и наводок, возможные «антенны»» «Помехи» 18. «Физические основы побочных излучений и наводок» «Возможные наводки в аппаратуре» 19. «Особенности распространения сигналов в помещениях» 20. Ознакомление и литературой, описывающей сканирующие приемники. Изучение инструкции сканера. Ознакомление с литературой, описывающей нелинейные локаторы. Изучение инструкции нелинейного локаторы. Ознакомление с литературой и Интернет-ресурсами по теме космической и авиаразведки.		
Промежуточная аттестация в форме экзамена		**10**
Всего по МДК 03.01		**174**
МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей		**130**
Тема 2.1 Основные теории измерения	**Содержание учебного материала**	
	1. Виды, методы и погрешности. 2. Классификация измерительных приборов.	**6**

	Практические занятия	
	Инструктаж по технике безопасности при электрорадиоизмерениях.	**4**
	Определение погрешности измерений.	**4**
Тема 2.2 Измерение тока, напряжения и мощности	**Содержание учебного материала**	
	1. Амперметры и вольтметры. Включение их в цепь.	**4**
	Практические занятия	
	Измерение параметров электрической цепи комбинированным прибором.	**6**
	Измерение напряжений цифровым вольтметром.	**4**
Тема 2.3. Приборы формирования стандартных измерительных сигналов	**Содержание учебного материала**	
	1. Генераторы измерительные. 2. Генераторы шума.	**4**
Тема 2.4 Исследование формы сигналов	**Содержание учебного материала**	
	1. Универсальные осциллографы. 2. Способы отсчета напряжения и временных интервалов электрических сигналов.	**8**
	Практические занятия	
	Исследование органов управления, включение и калибровки электронного осциллографа.	**4**
	Изучение электронно-лучевых осциллографов со ждущей разверсткой.	**4**
	Измерение параметров различных сигналов двухканальным осциллографом.	**4**
Тема 2.5 Измерение параметров сигналов	**Содержание учебного материала**	
	Исследование технических характеристик, режимов работы и органов управления электронно-счётного частотомера. Изучение Электронно-счётного осциллографа и применение их для измерения частоты сигналов. Изучение затухающих электромагнитных колебаний.	**12**
Тема 2.6 Измерение параметров и характеристик электрорадиотехнических цепей и компонентов.	**Содержание учебного материала**	
	Измерение параметров с сосредоточенными параметрами. Измерение АЧХ. Измерение параметров полупроводниковых приборов.	**8**
Самостоятельная работа **Рекомендуемая тематика самостоятельной работы**		**48**
1. Выполнение электрических расчетов 2. Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя Проработка конспектов занятий, учебной и специальной технической литературы		

3. Написание отчетов 4. Написание рефератов и подготовка сообщений по темам разделов	
Промежуточная аттестация в форме экзамена	**10**
Всего по МДК 03.02	**130**
Учебная практика (по профилю специальности) итоговая по ПМ **Виды работ** Введение Изучение средств перехвата информации Микрофоны Акустические антенны Выбор типа микрофона и места его установки Изучение устройств подавления микрофонов Изучение устройств для перехвата речевой информации в проводных каналах Изучение оптико-акустической аппаратуры перехвата речевой информации Оптико-механические приборы Приборы ночного видения Средства скрытой фотосъемки Зоны подключения в линиях связи Перехват телефонных переговоров в зонах «А», «Б», «В», «Г», «Д», «Е» Изучение перехвата сообщений в каналах сотовой связи Методы поиска закладных устройств как физических объектов и электронных средств Панорамные приемники Аппаратура контроля и защиты линии связи Средства создания акустических и электромагнитных маскирующих помех Измерение токов, напряжений и сопротивлений, исследование двухполюсников с помощью мультиметра Прямые и косвенные однократные измерения Обработка и представление однократных измерений при наличии систематической погрешности Стандартная обработка результатов прямых измерений с многократным наблюдением Обработка результатов прямых измерений с многократным наблюдением при наличии грубых погрешностей Определение погрешности цифрового вольтметра сличения и прямых измерений Измерение мощности и силы постоянного электромагнитного тока Измерение постоянного напряжения методом компенсации Измерение переменного электрического напряжения Измерение частоты и периода электрических сигналов Терморезисторные измерительные преобразователи. Измерители температуры	**36**

Емкостные измерительные преобразователи. Измерение размера Индуктивные измерительные преобразователи. Измерение перемещения Термоэлектрические измерительные преобразователи. Измерение температуры Пьезоэлектрические измерительные преобразователи. Измерение переменных ускорений	
Производственная практика (по профилю специальности) итоговая по ПМ **Виды работ** Выполнение подбора, настройки и применения технических средств защиты информации Использование средств охраны и безопасности объекта Организация и реализация технической охраны объектов Выполнение мероприятий по предотвращению несанкционированного доступа к информации Настройка системы защиты информации от съема и утечки по техническим каналам Изучение порядка применения нормативных правовых актов Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами Выявление технических каналов утечки информации Применение существующих способов выявления опасности целостности информации Анализ объектов информатизации предприятий, учреждений, организаций Анализ ресурсов обеспечения инженерно-технической защиты информации Изучение основных этапов проектирования системы защиты информации техническими средствами Проектирование рабочих проектов по системе пожарно-охранной сигнализации, видеонаблюдения, СКУД Оформление технической и технологической документации.	**108**
КВАЛИФИКАЦИОННЫЙ ЭКЗАМЕН ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ 03	**20**
Всего по ПМ 03:	
Теоретических занятий	**110**
Практических занятий	**62**
Самостоятельной работы	**112**
Учебная практика	**36**
Производственная практика	**108**
Экзамен по ПМ 03	**20**
ИТОГО	**468**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения (в соответствии с ФГОС и ПООП):

1. Лаборатория информационно-телекоммуникационных систем и сетей

Специализированная мебель:
Компьютерные столы – 16 шт.
Стол письменный – 6 шт.
Кресло компьютерное – 16 шт.
Стулья – 12 шт.
Шкаф для документов – 1 шт.
Экран настенный – 1 шт

Технические средства обучения:
Компьютер преподавателя – 1 шт
Персональные компьютеры – 15 шт.
Мультимедиа проектор– 1 шт.
Аудиоколонки – 1шт

стенды телекоммуникационных сетей; комплекты структурированных кабельных систем; комплекты устройств приема, передачи и обработки сигналов; антенные системы; эмуляторы активного сетевого оборудования

Перечень лицензионного программного обеспечения:
1) Антивирусная защита Kaspersky Endpoint Security
2) Astra Linux, Libre Office
3) Специализированное программное обеспечение сетевого оборудования;

Помещение обеспечено доступом к сети «Интернет» и электронной информационно-образовательной среде Финансового университета.

2. Лаборатория программных и программно-аппаратных средств защиты информации

Специализированная мебель:
Лекционные парты – 26 шт.
Стулья – 53 шт.
Стол компьютерный – 1 шт.
Учебная доска – 1 шт.
Экран настенный– 1 шт.

Технические средства обучения:
Компьютер преподавателя – 1 шт
Мультимедиа проектор – 1 шт.
Аудиоколонки – 1шт
Сервер – 2 шт.
Источники бесперебойного питания – 2 шт.
Многофункциональное устройство -1 шт.

Антивирусные программные комплексы; аппаратные средства аутентификации пользователя; программно-аппаратные средства управления доступом к данным и защиты (шифрования) информации; средства защиты информации от несанкционированного доступа, блокирования доступа и нарушения целостности; программные средства криптографической защиты информации; программные средства

выявления уязвимостей и оценки защищенности информационно-телекоммуникационной системы, анализа сетевого трафика.

Перечень лицензионного программного обеспечения:
1) Антивирусная защита Kaspersky Endpoint Security
2) Astra Linux, Libre Office
3) Программные средства криптографической защиты информации
4) Программно-аппаратные средства управления доступом к данным и защиты (шифрования) информации, средствами защиты информации от НСД, блокирования доступа и нарушения целостности;

Помещение обеспечено доступом к сети «Интернет» и электронной информационно-образовательной среде Финансового университета.

3. Лаборатория защиты информации от утечки по техническим каналам

Специализированная мебель:
Стол письменный – 19 шт.
Стулья – 48 шт.
Стол переговорочный – 2 шт.
Стол компьютерный – 1 шт.

Технические средства обучения:
Стенды физической защиты объектов информатизации – 2 шт.
Компьютер преподавателя – 1 шт
Мультимедиа проектор – 1 шт.
Экран настенный – 1 шт
Аудиоколонки – 1шт

Средства защиты информации от утечки по акустическому (виброакустическому) каналу; средства защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок; средства контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок.

Перечень лицензионного программного обеспечения:
1) Антивирусная защита Kaspersky Endpoint Security
2) Astra Linux, Libre Office
3) СПС «Гарант»

Помещение обеспечено доступом к сети «Интернет» и электронной информационно-образовательной среде Финансового университета.

4. Учебная аудитория для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации
(Методический кабинет)

Специализированная мебель:
Компьютерные столы – 20 шт.
Стол письменный – 13 шт.
Кресло компьютерное – 20 шт.
Стулья – 26 шт.
Шкаф для учебно-методических материалов – 6 шт.

Технические средства обучения:
Персональные компьютеры – 18 шт.
Мультимедиа проектор – 1 шт.
Экран настенный – 1 шт.
Аудиоколонки – 1шт.

5. Помещения для самостоятельной работы: Библиотека и читальный зал с выходом в сеть Интернет

Специализированная мебель:
Стол кафедра – 3 шт.
Каталожный ящик – 1 шт.
Шкаф для читательских формуляров – 3 шт.
Витрина для книг – 3 шт.
Стол ученический – 24 шт.
Кресло компьютерное – 2 шт.
Стул - 48 шт.
Стол эргономичный с тумбой – 1 шт.
Шкаф для документов – 3 шт.

Технические средства обучения:
Персональные компьютеры– 18 шт.

Реализация профессионального модуля предполагает обязательную учебную и производственную практику (по профилю специальности). Учебная практика проводится концентрированно в учебном заведении, производственная практика (по профилю специальности) проводится концентрированно в организациях работодателей, с которыми заключены договоры о практической подготовке обучающихся.

3.2. Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации имеет электронные издания и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

1.Технические средства и методы защиты информации / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. 7-е изд., испр. - Москва :Гор. линия-Телеком , 2023. -616 с.

2. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учебное издание / Белов Е.Б., Пржегорлинский В. Н. - Москва : Академия, 2021. - 336 с. (Специальности среднего профессионального образования). - URL: https://academia-moscow.ru - Режим доступа: Электронная библиотека «Academia-moscow». - Текст : электронный

3.Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. - 2-е изд. - Москва : ДМК Пресс, 2023. - 594 с. - ISBN 978-5-89818-506-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/2107178 (дата обращения: 28.03.2024)

4. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1912987 (дата обращения: 01.04.2024)

5. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с.— DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642 (дата обращения: 01.04.2024).

6. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст :

электронный // Образовательная платформа Юрайт [сайт]. — URL: https://ezpro.fa.ru:2058/bcode/543873 (дата обращения: 01.04.2024)

7. Мельников, В. П., Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. — Москва : КноРус, 2023. — 371 с. — ISBN 978-5-406-11960-0. — URL: https://book.ru/book/950148 (дата обращения: 01.04.2024)

8. Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1359091 (дата обращения: 01.04.2024).

9. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2022. — 256 с. - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1861659 (дата обращения: 01.04.2024).

10. Фомичев, В. М. Криптографические методы защиты информации (курс лекций) : учебное пособие / В. М. Фомичев. - Москва : Прометей, 2023. - 340 с. - ISBN 978-5-00172-538-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2124893 (дата обращения: 01.04.2024)

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

http://www.morion.ru/

http://www.nateks.ru/

http://www.iskratel.com/

http://www.ps-ufa.ru/

http://3m.com/

http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор»

3.2.3. Дополнительные источники

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
- Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
- Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
- Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- 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».

- Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
- Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
- Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
- 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.
- Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
- Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
- 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.
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
- Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
- Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
- Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
- Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
- Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

- 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
- ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
- ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
- ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
- ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
- ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
- ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
- ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
- ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
- ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
- ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
- ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
- ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
- ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
- ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
- 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. Росстандарт, 2012.
- ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства

обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
- Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
- Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
- Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Отечественные журналы:

- "InformationSecurity/ Информационная безопасность"
- Системный администратор
- Компьютер ПРЕСС
- Системы безопасности. Журнал для руководителей и специалистов в области безопасности
- Сети и системы связи

Интернет Ресурсы:

- http://cryptogrof.ru/

В соответствии со ст. 43 Конституции Российской Федерации, 273-ФЗ «Об образовании в Российской Федерации» от 29.12.2012, приказом Минобрнауки России от 09.11.2015 N 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи», ГОСТ Р 57723-2017 «Информационно-коммуникационные технологии в образовании. Системы электронно-библиотечные. Общие положения», ГОСТ Р 52872-2019 «Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. Требования доступности для людей с инвалидностью и других лиц с ограничениями жизнедеятельности», все предлагаемые электронные ресурсы максимально комфортны для чтения слабовидящими людьми. Масштабирование текста достигает 300 процентов. При изменении масштаба сохраняется возможность видеть всю страницу текста, не обрезая его.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

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 ИТКС.	- 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 ИТКС.	- 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 ИТКС 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 ИТКС.	выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства	Экспертное наблюдение

	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 Экзамен
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	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 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
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение Экзамен