ДЕПАРТАМЕНТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ТОМСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«ТОМСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

для специальности:

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Томск

2020 год

ОДОБРЕНО

Предметной (цикловой) комиссией

информационных технологий

Председатель

_____ А.М. Вернигора

Протокол № 8

от «15 » июня 2020 г.

УТВЕРЖДАЮ

Зам. директора по УМР

_____ Л.В. Сидакова

от «29 » июня 2020 г.

Заведующий библиотекой

_____ О.А Пинаева

от «22 » июня 2020 г.

Рабочая программа учебной дисциплины разработана на основе приказа Министерства образования и науки Российской Федерации от 09.12.2016 № 1551 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования» по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Организация-разработчик: ОГБПОУ «Томский индустриальный техникум»

Разработчик:

Терехова Валентина Андреевна, преподаватель первой квалификационной категории

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 примерной программы

Рабочая программа профессионального модуля является частью примерной основной образовательной программы в соответствии с ФГОС СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности: эксплуатация информационно-телекоммуникационных систем и сетей и соответствующие ему профессиональные и общие компетенции:

1.2.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных

	ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.

1.2.2. Перечень профессиональных компетенций

Выпускник, освоивший программу СПО по профессии (специальности) должен обладать профессиональными компетенциями

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД 3	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты
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 будут освоены следующие действия умения и знания:

Спецификация ПК/ разделов профессионального модуля

Коды формируемых компетенций	Действия (дескрипторы)	Умения	Знания
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты			
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно-телекоммуникационных системах и сетях	установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам	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	способов защиты информации от утечки по техническим каналам с использованием технических средств защиты; основных типов технических средств защиты информации от утечки по техническим каналам; законодательства в области информационной безопасности, структуру государственной системы защиты информации, нормативных актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности
ПК 3.2. Проводить техническое обслуживание,	установка, монтажа, настройки и испытаний	проводить установку, монтаж, настройку и	основных типов технических средств защиты информации от

диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях	технических средств защиты информации от утечки по техническим каналам	испытание технических средств защиты информации от утечки по техническим каналам;	утечки по техническим каналам
	проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей	применять нормативные правовые акты и нормативные методические документы по обеспечению защиты информации проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам	организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам порядка и правил ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам
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	защиты информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями	проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; проводить измерение параметров электромагнитных	способов 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

предъявляемыми требованиями		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	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; порядка и правил ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам
ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.	проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	использовать средства физической защиты линий связи ИТКС	содержание и организацию работ по физической защите линий связи ИТКС; принципы действия и основные характеристики технических средств физической защиты
	выявление технических каналов утечки информации	применять инженерно-технические средства физической защиты объектов информатизации	принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях

1.3. Количество часов, отводимое на освоение профессионального модуля

Всего часов: **454 часа.**

Из них на освоение МДК **274 часов:**

МДК.03.01. Защита информации в ИТКС с использованием технических средств защиты- **176 час;**

МДК.03.02. Физическая защита линий связи ИТКС – **98 часов.**

На практики учебную и производственную -**180 часов.**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образова-тельной программы, час.	Объем образовательной программы, час.					
			Занятия во взаимодействии с преподавателем, час.					Самостоятельная работа
			Обучение по МДК, в час.			Практики		
			всего, часов	Лабораторных и практических занятий	Курсовых работ (проектов)	учебная, часов	производственная часов (если предусмотрена рассредоточенная практика)	
1	2	3	4	5	6	7	8	9
ПК 3.1- ПК.3.4 ОК 1 – ОК 7, ОК 9	Раздел 1. Защита информации в ИТКС и сетях с использованием технических средств защиты	176	165	94	15			11
ПК 3.5 ОК 1 – ОК 7, ОК 9	Раздел 2.Физическая защита линий связи ИТКС и сетей	98	89	30	15			9

Учебная практика	36				36		
Производственная практика	144					144	
Всего:	454	434	124	30	36	144	20

2.2. Тематический план и содержание профессионального модуля (ПМ.03)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект))		Объем часов
1	*2*		*3*
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты			**176**
МДК.03.01.Защита информации в ИТКС с использованием технических средств защиты			176
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	***Уровень освоения***	2
	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.	3	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**		
	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.	3	2
Тема 2.1. Информация как предмет защиты	**Содержание**		
	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. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2	2
	Практические и лабораторные работы		**4**
	Практическое занятие №1-2. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.		4
Тема 2.2. Технические каналы утечки информации	**Содержание**		
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки	3	4

	информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.		
	Практические и лабораторные работы		**6**
	Практическое занятие №3. Сравнительная характеристика каналов утечки информации.		2
	Практическое занятие №4-5. Содержательный анализ оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации		4
Тема 2.3. Методы и средства технической разведки	**Содержание**		
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки.	2	4
	Практические и лабораторные работы		**4**
	Практическое занятие №6-7. Анализ известных методов противодействия техническим разведкам.		4
	Консультация №1. Средства дистанционного съема информации.		2
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**		
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. 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	4
	Практические и лабораторные работы		**4**
	Практическое занятие №8-9. Измерение параметров физических полей		4
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**		
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований.	2	2
	Практические и лабораторные работы		**6**
	Практическое занятие №10-12. Постановка радиопомех в помещении для переговоров		6
	Консультация №2. Экранирование. Зашумление.		2
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**		
	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.	3	4

	Практические и лабораторные работы		**4**
	Практическое занятие №13-14.Защита от утечки по акустическому каналу		4
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**		
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	2	2
	Практические и лабораторные работы		**4**
	Практическое занятие №15-16.Проектирование контролируемой зоны		4
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**		
	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.	2	2
	Практические и лабораторные работы		**6**
	Практическое занятие №17-19. Защита от утечки по виброакустическому каналу		6
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**		
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	3	2
	Практические и лабораторные работы		**12**
	Практическое занятие №20-22.Определение каналов утечки ПЭМИН		6
	Практическое занятие №23-25.Защита от утечки по цепям электропитания и заземления		6
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**		
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	2	2
	Практические и лабораторные работы		**6**
	Практическое занятие №26-28. Монтаж системы защиты по вибро-акустическому каналу передачи информации.		6

Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**		
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	2	4
	Практические и лабораторные работы		**6**
	Практическое занятие №29-31. Анализ низкочастотное устройство съема информации		6
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**		
	Телевизионные системы наблюдения. Приборы ночного видения.	2	2
	Практические и лабораторные работы		**4**
	Практическое занятие №32-33.Сравнительный анализ приборов ночного видения		4
	Консультация №3. Системы защиты информации по оптическому каналу.		2
Тема 5.1. Применение технических средств защиты информации	**Содержание**		
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.	2	4
	Практические и лабораторные работы		**6**
	Практическое занятие №34-36.Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		6
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**		
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.	2	6
	Практические и лабораторные работы		**18**
	Практическое занятие №37-39. Размещение видео-регистрирующей аппаратуры. Видео-мониторинг контролируемой зоны.		6
	Практическое занятие №40-43. Построение модели угроз и модели нарушителя.		8
	Практическое занятие №44-47. Классификация информации по степени конфиденциальности.		8
	Консультация №4. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.		2

Самостоятельная учебная работа при изучении раздела 1 Защита информации в ИТКС с использованием технических средств защиты 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.			**11**
Курсовой проект (работа) **Тематика курсовых проектов (работ):** 1. Модель угроз НСД на предприятии 2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии 3. Проведение классификации ПО по требованиям ФСТЭК на предприятии 4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии 5. Построение модели нарушителя по требованиям ФСТЭК на предприятии 6. Построение модели нарушителя по требованиям ФСБ на предприятии			
Обязательная аудиторная учебная нагрузка по курсовой работе (проекту) Разработка схемы организации связи. Выбор топологии сети. Выбор типа оборудования. Выбор типа и конструкции оптического кабеля. Расчет основных параметров оптического линейного тракта. Расчет показателей надежности.			**15**
Раздел 2. Физическая защита линий связи ИТКС			**98**
МДК.03.02. Физическая защита линий связи ИТКС			**98**
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**Уровень освоения**	
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	**2**	4
Тема 1.2. Общие	**Содержание**		6

сведения о комплексах инженерно-технических средств физической защиты	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	***2***	
	Практические и лабораторные работы		**8**
	Практическое занятие №1-2.Классификация и состав интегрированных систем охраны		4
	Практическое занятие №3-4. Требования к инженерным средствам физической защиты		4
Тема 2.1. Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**		
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия.	2	4
	Практические и лабораторные работы		4
	Практическое занятие №5-6. Монтаж датчиков пожарной и охранной сигнализации		4
	Консультация №1. Объектовые средства обнаружения: назначение, устройство, принцип действия.		2
Тема 2.2. Система контроля и управления доступом	**Содержание**		
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	2	4
	Практические и лабораторные работы		**6**
	Практическое занятие №7-8. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя		4
	Практическое занятие №9. Рассмотрение принципов устройства, работы и применения средств контроля доступа		2
Тема 2.3. Система телевизионного наблюдения	**Содержание**		
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	2	4

	Практические и лабораторные работы		**4**
	Практическое занятие №10-11. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.		4
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**		
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	2	4
	Практические и лабораторные работы		**2**
	Практическое занятие №12. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.		2
Тема 2.5. Система воздействия	**Содержание**		
	Назначение и классификация технических средств воздействия.	2	4
	Практические и лабораторные работы		**6**
	Практическое занятие №13-15. Анализ основных показателей технических средств воздействия		6
	Консультация №2. Основные показатели технических средств воздействия.		2
Тема 3.1. Применение инженерно-технических средств физической защиты	**Содержание**		
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	2	4
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**		
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	2	4
	Консультация №3. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.		2

Самостоятельная учебная работа при изучении раздела 2 Физическая защита линий связи ИТКС Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.	**9**
Курсовой проект (работа) **Тематика курсовых проектов (работ):** 1. Модель угроз безопасности ИС персональных данных на предприятии 2. Комплексная модель защиты информации на предприятии. 3. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 4. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 5. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание).	
Обязательная аудиторная учебная нагрузка по курсовой работе (проекту) Разработка схемы организации связи. Выбор топологии сети. Выбор типа оборудования. Выбор типа и конструкции оптического кабеля. Расчет основных параметров оптического линейного тракта. Расчет показателей надежности.	**15**
Учебная практика по профессиональному модулю **1.** Монтаж различных типов датчиков. **2.** Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. **3.** Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. **4.** Рассмотрение системы контроля и управления доступом. **5.** Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. **6.** Рассмотрение датчиков периметра, их принципов работы. **7.** Выполнение звукоизоляции помещений системы зашумления. **8.** Реализация защиты от утечки по цепям электропитания и заземления. **9.** Разработка организационных и технических мероприятий по заданию преподавателя; **10.** Разработка основной документации по инженерно-технической защите информации.	**36**
Производственная практика профессионального модуля **Виды работ** **1.** Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; **2.** Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; **3.** Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам; **4.** Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации	**144**

техническими средствами.	
Внеаудиторная (самостоятельная) учебная работа обучающегося над курсовым проектом (работой) 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. 8.Управление системой воздействия.	
Всего:	**454**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля предполагает наличия

Для МДК.03.01, МДК.03.02, УП.03

Учебной аудитории № 405 «Лаборатория информационно-телекоммуникационных систем и сетей»

- Оборудование: Презентационное оборудование, интерактивная панель, 12 ПК, учебная мебель.

- Учебно-наглядное пособие: комплект УМК по дисциплине (дидактические материалы, контрольно-оценочные средства, наглядные материалы и т.д.)

- Программное обеспечение: ОС Linux Debian 10

3.2. Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания:

МДК.03.01

Основная литература

Знаниум (Братко)

Дополнительная литература

Ворона В.А., Тихонов В.А. Системы контроля и управления доступом/ В.А. Ворона, В.А. Тихонов. – М.: Горячая линия – Телеком, 2018. – 272с.: ил. – ISBN 978-5-9912-0059-2. - Текст: непосредственный.

Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам/ Г.А. Бузов.- М.: Горячая линия- Телеком, 2017. – 586с.: ил. - Текст: непосредственный

МДК.03.01

Основная литература

Николаев, Н.С. Теория электросвязи : учебное пособие / Н.С. Николаев . — Москва : КноРус, 2020. — 183 с. — ISBN 978-5-406-01728-9. — URL: https://book.ru/book/938682 (дата обращения: 26.06.2020). — Текст : электронный. Рек. экспертным советом УМО

Дополнительная литература

Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам/ Г.А. Бузов.- М.: Горячая линия- Телеком, 2017. – 586с.: ил. - Текст: непосредственный

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ПО РАЗДЕЛАМ)

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 защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты	Экспертное наблюдение
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