МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ХАБАРОВСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ХАБАРОВСКИЙ ТЕХНИКУМ ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ И ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ»

СОГЛАСОВАНО
Работодатель
Директор ООО «ПРОФИТ ДВ»,
г. Хабаровск
_____ Сёмин С. А.
«_04_» _____мая_____2022 г

РАБОЧАЯ ПРОГРАММА

ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ 03 «Защита информации техническими средствами»

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

базовой подготовки

г. Хабаровск

2021

Рабочая программа профессионального модуля составлена на основе Федерального образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Организация-разработчик: КГБ ПОУ ХТТБПТ

Разработчики: Соцков Михаил Юрьевич, преподаватель краевого государственного бюджетного профессионального образовательного учреждения «Хабаровский техникум техносферной безопасности и промышленных технологий».

Рассмотрено и одобрено на заседании

ПЦК Информатики и вычислительной техники

Протокол № _____ от «____»_____20_____г.

Председатель ПЦК _____ (Иващенко Л. В.).

Согласовано на заседании методического совета

Протокол № _____ от «____»_____20_____г.

Председатель МС _____ (Линевич О.Г.).

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ 03 «ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ»

1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО

10.02.05 Обеспечение информационной безопасности автоматизированных систем

в части освоения основного вида профессиональной деятельности (ВПД):

Защита информации техническими средствами и соответствующие ему профессиональные компетенции:

Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных 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 поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	**Защита информации техническими средствами**
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

.

- личностные результаты

Личностные результаты реализации программы воспитания *(дескрипторы)*	**Код личностных результатов реализации Программы воспитания**
Портрет выпускника ПОО	
Осознающий себя гражданином и защитником великой страны	**ЛР 1**
Готовый использовать свой личный и профессиональный потенциал для защиты национальных интересов России	**ЛР 2**
Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России	**ЛР 3**
Принимающий семейные ценности своего народа, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания	**ЛР 4**
Занимающий активную гражданскую позицию избирателя, волонтера, общественного деятеля	**ЛР 5**
Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение	**ЛР 6**
Готовый соответствовать ожиданиям работодателей: проектно мыслящий, эффективно взаимодействующий с членами команды и сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, ответственный, пунктуальный, дисциплинированный, трудолюбивый, критически мыслящий, нацеленный на достижение поставленных целей; демонстрирующий профессиональную жизнестойкость	**ЛР 7**
Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы; управляющий собственным профессиональным развитием; рефлексивно оценивающий собственный жизненный опыт, критерии личной успешности	**ЛР 8**
Уважающий этнокультурные, религиозные права человека, в том числе с особенностями развития; ценящий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности»	**ЛР 9**
Принимающий активное участие в социально значимых мероприятиях, соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России; готовый оказать поддержку нуждающимся	**ЛР 10**

Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением	**ЛР 11**
Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих	**ЛР 12**
Способный в цифровой среде использовать различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»	**ЛР 13**
Способный ставить перед собой цели под возникающие жизненные задачи, подбирать способы решения и средства развития, в том числе с использованием цифровых средств; содействующий поддержанию престижа своей профессии и образовательной организации	**ЛР 14**
Способный генерировать новые идеи для решения задач цифровой экономики, перестраивать сложившиеся способы решения задач, выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов; позиционирующий себя в сети как результативный и привлекательный участник трудовых отношений.	**ЛР 15**
Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве.	**ЛР 16**
Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению	**ЛР 17**
Осознающий значимость системного познания мира, критического осмысления накопленного опыта	**ЛР 18**
Развивающий творческие способности, способный креативно мыслить	**ЛР 19**
Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации	**ЛР 20**
Готовый к профессиональной конкуренции и конструктивной реакции на критику	**ЛР 21**
Демонстрирующий приверженность принципам честности, порядочности, открытости	**ЛР 22**
Самостоятельный и ответственный в принятии решений во всех сферах своей деятельности, готовый к исполнению разнообразных социальных ролей, востребованных бизнесом, обществом и государством	**ЛР 23**
Проявляющий эмпатию, выражающий активную гражданскую позицию, участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций, а также некоммерческих организаций, заинтересованных в развитии гражданского общества и оказывающих поддержку нуждающимся	**ЛР 24**
Препятствующий действиям, направленным на ущемление прав или унижение достоинства (в отношении себя или других людей)	**ЛР 25**
Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп	**ЛР 26**
Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства	**ЛР 27**

Вступающий в конструктивное профессионально значимое взаимодействие с представителями разных субкультур	**ЛР 28**
Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д.	**ЛР 29**
Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой	**ЛР 30**
Гармонично, разносторонне развитый, активно выражающий отношение к преобразованию общественных пространств, промышленной и технологической эстетике предприятия, корпоративному дизайну, товарным знакам	**ЛР 31**
Оценивающий возможные ограничители свободы своего профессионального выбора, предопределенные психофизиологическими особенностями или состоянием здоровья, мотивированный к сохранению здоровья в процессе профессиональной деятельности	**ЛР 32**
Открытый к текущим и перспективным изменениям в мире труда и профессий	**ЛР 33**
Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики	**ЛР 34**
Экономически активный, предприимчивый, готовый к самозанятости	**ЛР 35**
Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях	**ЛР 36**

Рабочая программа профессионального модуля может быть использована В программах ДПО повышения квалификации и профессиональной переподготовки по направлению 10.00.00.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- установки, монтажа и настройки технических средств защиты информации;
- технического обслуживания технических средств защиты информации;
- применения основных типов технических средств защиты информации;
- выявления технических каналов утечки информации;
- участия в мониторинге эффективности технических средств защиты информации;
- диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;
- проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации,

для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

− проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

уметь:

− применять технические средства для криптографической защиты информации конфиденциального характера;

− применять технические средства для уничтожения информации и носителей информации;

− применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

− применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

− применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

применять инженерно-технические средства физической защиты объектов информатизации

знать:

− порядок технического обслуживания технических средств защиты информации;

− номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

− физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

− порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

− методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

− номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

− основные принципы действия и характеристики технических средств физической защиты;

− основные способы физической защиты объектов информатизации;

номенклатуру применяемых средств физической защиты объектов информатизации.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – _584__ часа, в том числе:
максимальной учебной нагрузки обучающегося – 470 часа, включая:
обязательной аудиторной учебной нагрузки обучающегося – _454 часа;
в том числе за счет вариативной части - _____ часов;
самостоятельной работы обучающегося – 10 часов;
учебной и производственной практики – 108 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности Защита информации техническими средствами, в том числе профессиональными (ПК), общими (ОК) компетенциями и личностными результатами (ЛР), указанными в п. 1.1.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды профессиональных компетенций	**Наименования разделов профессионального модуля**	**Всего часов** *(макс. учебная нагрузка и практики)*	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**		**Экзамен по модулю,** часов	**Консультации,** часов
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** часов *(если предусмотрена рассредоточенная практика)*		
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч., курсовая работа (проект),** часов	**Всего,** часов	**в т.ч., курсовая работа (проект),** часов				
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**		
ПК 3.1 ОК 1– ОК10 ЛР 1-36	МДК.03.01 Техническая защита информации	**144**	**140**	58	–	**3**	–	–	**-**	**1**	**2**
ПК 3.2 ОК 01–ОК10 ЛР 1-36	МДК.03.02 Инженерно-технические средства физической защиты объектов информации	**144**	**140**	54	30	**2**	–	**-**	**-**	**2**	**2**
ПК.3.3 ОК 1– ОК10 ЛР 1-36	МДК.03.03 Основы построения защищенных компьютерных сетей	**80**	**76**	30		**3**	**-**	**-**	**-**	**1**	**2**
П.К. 3.1-3.4 ОК 1– ОК10 ЛР 1-36	МДК.03.04 Организация электронной системы управления документооборотом	**102**	**98**	42		**2**	**-**	**-**	**-**	**2**	**2**

П.К. 3.1-3.4 ОК 1– ОК10	Учебная практика	**36**	**-**	-	-	-	-	*36*	-	-	-
П.К. 3.1-3.4 ОК 1– ОК10 ЛР 1-36	**Производственная практика**	**72**							**72**	-	-
	Экзамен по модулю	**6**									
	Консультации	**8**									
	Всего:	**584**	**454**	184	**30**	**10**	**-**	**36**	**108**	**6**	**8**

Ячейки в столбцах 3, 4, 7, 9, 10 заполняются жирным шрифтом, в 5, 6, 8 - обычным. Если какой-либо вид учебной работы не предусмотрен, необходимо в соответствующей ячейке поставить прочерк. Количество часов, указанное в ячейках столбца 3, должно быть равно сумме чисел в соответствующих ячейках столбцов 4, 7, 9, 10 (жирный шрифт) по горизонтали. Количество часов, указанное в ячейках строки «Всего», должно быть равно сумме чисел соответствующих столбцов 3, 4, 5, 6, 7, 8, 9, 10 по вертикали. Количество часов, указанное в ячейке столбца 3 строки «Всего», должно соответствовать количеству часов на освоение программы профессионального модуля в пункте 1.3 паспорта программы. Количество часов на самостоятельную работу обучающегося должно соответствовать указанному в пункте 1.3 паспорта программы. Сумма количества часов на учебную и производственную практику (в строке «Всего» в столбцах 9 и 10) должна соответствовать указанному в пункте 1.3 паспорта программы. Для соответствия сумм значений следует повторить объем часов на производственную практику по профилю специальности (концентрированную) в колонке «Всего часов» и в предпоследней строке столбца «Производственная, часов». И учебная, и производственная (по профилю специальности) практики могут проводиться параллельно с теоретическими занятиями междисциплинарного курса (рассредоточено) или в специально выделенный период (концентрированно)

3.2. Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	**Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)** *(если предусмотрены)*	**Объем часов**	**Уровень освоения**	**ОК, ПК, ЛР**
1	2	3		
МДК.03.01 Техническая защита информации		**144**		
Раздел 1. Концепция инженерно-технической защиты информации				
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**4**		**ОК 1-10 ПК 3.1 ЛР 1-36**
	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**	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**4**		**ОК 1-10 ПК 3.1 ЛР 1-36**
	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**	
Раздел 2. Теоретические основы инженерно-технической защиты информации				
Тема 2.1. Информация как предмет защиты	**Содержание**	**4**		**ОК 1-10 ПК 3.1 ЛР 1-36**
	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**	

	Тематика практических занятий и лабораторных работ	**6**		
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.		**3**	
Тема 2.2. Технические каналы утечки информации	**Содержание**	**4**		
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.		**2**	**ОК 1-10 ПК 3.1 ЛР 1-36**
	Тематика практических занятий и лабораторных работ	**4**		
	Угрозы ИБ. Организация аттестации выделенного помещения по требованиям безопасности информации.		**3**	
Тема 2.3. Методы и средства технической разведки	**Содержание**	**4**		**ОК 1-10 ПК 3.1 ЛР 1-36**
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Классификация технических средств разведки. Анализ рынка современных средств разведки.		**3**	
Раздел 3. Физические основы технической защиты информации				
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**6**		**ОК 1-10 ПК 3.1 ЛР 1-36**
	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**	

	Тематика практических занятий и лабораторных работ	**4**		
	Измерение параметров физических полей		**3**	
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**4**		**ОК 1-10** **ПК 3.1** **ЛР 1-36**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Защита аппаратуры от электромагнитных полей		**3**	
Раздел 4. Системы защиты от утечки информации				
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**6**		**ОК 1-10** **ПК 3.1** **ЛР 1-36**
	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.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Защита от утечки по акустическому каналу		**3**	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**6**		**ОК 1-10** **ПК 3.1** **ЛР 1-36**
	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**	
	Тематика практических занятий и лабораторных работ	**4**		
	Системы защиты от утечки информации по проводному каналу		**3**	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**6**		**ОК 1-10** **ПК 3.1** **ЛР 1-36**
	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**	
	Тематика практических занятий и лабораторных работ	**4**		

	Защита от утечки по виброакустическому каналу		**3**	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**6**		**ОК 1-10** **ПК 3.1** **ЛР 1-36**
	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.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Определение каналов утечки ПЭМИН		**3**	
	Защита от утечки по цепям электропитания и заземления			
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**6**		**ОК 1-10** **ПК 3.1** **ЛР 1-36**
	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**	
	Тематика практических занятий и лабораторных работ	**4**		
	Технические средства защиты информации в телефонных линиях		**3**	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**4**		**ОК 1-10** **ПК 3.1** **ЛР 1-36**
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Система защиты от утечки информации по электросетевому каналу		**3**	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**4**		**ОК 1-10** **ПК 3.1** **ЛР 1-36**
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Системы защиты от утечки информации по оптическому каналу		***3***	

Раздел 5. Применение и эксплуатация технических средств защиты информации				
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**6**		**ОК 1-10** **ПК 3.1** **ЛР 1-36**
	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. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		***2***	
	Тематика практических занятий и лабораторных работ	**4**		
	Применение технических средств защиты информации		**3**	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**6**		**ОК 1-10** **ПК 3.1** **ЛР 1-36**
	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. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Эксплуатация технических средств защиты информации		**3**	
Всего		**140**		
Самостоятельная работа **Примерные виды самостоятельной работы при изучении раздела 1 модуля** Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		**3ч**		
Консультации		2		

Экзамен		**8сем (1ч)**		
ИТОГО		**144**		
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**140**		
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты				
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**6**		ПК 3.2 ОК 01–ОК10 ЛР 1-36
	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**	
	Тематика практических занятий и лабораторных работ	**6**		
	Характеристика объекта защиты		***3***	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**6**		ПК 3.2 ОК 01–ОК10 ЛР 1-36
	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**	
	Тематика практических занятий и лабораторных работ	**6**		
	Анализ нормативно-правовой базы физической защиты. Формирование требований к физической защите объекта		3	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты				
Тема 2.1 Система обнаружения комплекса инженерно-	**Содержание**	**6**		ПК 3.2 ОК 01–ОК10 ЛР 1-36
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства		2	

технических средств физической защиты	обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.			
	Тематика практических занятий и лабораторных работ	**6**		
	Монтаж датчиков пожарной и охранной сигнализации		3	
Тема 2.2. Система контроля и управления доступом	**Содержание**	**8**		ПК 3.2 ОК 01–ОК10 ЛР 1-36
	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	
	Тематика практических занятий и лабораторных работ	**6**		
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя		3	
	Рассмотрение принципов устройства, работы и применения средств контроля доступа			
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**6**		ПК 3.2 ОК 01–ОК10 ЛР 1-36
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.		**2**	
	Тематика практических занятий и лабораторных работ	**6**		
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.		3	
Тема 2.4. Система сбора, обработки, отображения и	**Содержание**	**6**		ПК 3.2 ОК 01–ОК10
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты		**2**	

документирования информации	структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.			ЛР 1-36
	Тематика практических занятий и лабораторных работ	**6**		
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.		3	
Тема 2.5 Система воздействия	**Содержание**	**4**		ПК 3.2 ОК 01– ОК10 ЛР 1-36
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.		**2**	
	Тематика практических занятий и лабораторных работ	**6**		
	Выбор и обоснование средств подсистемы задержки		3	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты				
Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание**	**6**		ПК 3.2 ОК 01– ОК10 ЛР 1-36
	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	
	Тематика практических занятий и лабораторных работ	**6**		
	Разработка структурной схемы и спецификации оборудования		3	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**6**		ПК 3.2 ОК 01– ОК10 ЛР 1-36
	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. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.		2	
	Тематика практических занятий и лабораторных работ	**6**		
	Эксплуатация инженерно-технических средств физической защиты		**3**	

Самостоятельная работа **Примерная тематика самостоятельной работы при изучении МДК.03.02** – Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. – Размещение периметровых средств обнаружения на местности. – Самостоятельнее изучения порядка допуска субъектов на охраняемые объекты.		**2**		
Консультации		2		
Курсовая работа		**30**		
Примерная тематика курсового проекта (работы) 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.				
Экзамен		**2ч (8сем)**		
Итого		***144***		
МДК 03.03 Основы построения защищенных компьютерных сетей		***80***		
Тема 1 Сетевые атаки	**Содержание учебного материала**	**6**		ПК.3.3 ОК 1–ОК10 ЛР 1-36
	Стадии проведения сетевой атаки. Классификации сетевых угроз, уязвимостей и атак. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.		**2**	
	Тематика практических занятий и лабораторных работ	**2**		
	Классификация типов и видов сетевых атак		**3**	
Тема 2. Механизмы реализации атак в сетях TCP/IP	**Содержание учебного материала**	**8**		ПК.3.3 ОК 1–ОК10 ЛР 1-36
	Удаленное определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP. Методы сканирования портов. Методы обнаружения пакетных сниферов. Методы обхода МЭ		**2**	
	Тематика практических занятий и лабораторных работ	**4**		

	Установка и настройка Nmap		**3**	
Тема 3. Методы перехвата сетевых соединений в сетях TCP/IP	**Содержание учебного материала**	**6**		ПК.3.3 ОК 1–ОК10 ЛР 1-36
	Имперсонация вслепую. Десинхронизация TCP-соединений. Атаки, направленные на сетевую инфраструктуру.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Установка и работа с Wireshark		**3**	
Тема 4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак.	**Содержание учебного материала**	**6**		ПК.3.3 ОК 1–ОК10 ЛР 1-36
	Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак		**2**	
	Тематика практических занятий и лабораторных работ	**2**		
	Установка и работа с программой Nmap		**3**	
Тема 5. Криптографические протоколы обеспечения безопасности	**Содержание учебного материала**	**4**		ПК.3.3 ОК 1–ОК10 ЛР 1-36
	Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.		**2**	
	Тематика практических занятий и лабораторных работ	**2**		
	Работа с протоколами Kerberos и SSL/TLS Работа в OpenSSL		**3**	
Тема 6. Защита виртуальных частных сетей (VPN)	**Содержание учебного материала**	**4**		ПК.3.3 ОК 1–ОК10 ЛР 1-36
	Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IPSEC в туннельном и транспортном режимах. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.		**2**	
	Тематика практических занятий и лабораторных работ	**2**		

	Развертывание VPN с использованием IPSec Настройка параметров регистрации и аудита Регистрация и контроль действий пользователей. Изменение параметров учетной записи		**3**	
Тема 7. Разработка защищенных сетевых приложений	**Содержание учебного материала**	**4**		ПК.3.3 ОК 1–ОК10 ЛР 1-36
	Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс OpenSSL.		**2**	
	Тематика практических занятий и лабораторных работ	**2**		
	Инструментальны средства проведения сетевых атак		**3**	
Тема 8. Средства защиты локальных сетей при подключении к Интернет.	**Содержание учебного материала**	**4**		ПК.3.3 ОК 1–ОК10 ЛР 1-36
	Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.		**2**	
	Тематика практических занятий и лабораторных работ	**6**		
	Настройка и использование межсетевого экранирования в современных ОС. Дополнительное ПО Agnitum Outpost 9 и Kerio		**3**	
Тема 9. Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений	**Содержание учебного материала**	**4**		ПК.3.3 ОК 1–ОК10 ЛР 1-36
	Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Способы противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell).		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Установка и работа с программным комплексом VipNet IDS и TEAS		**3**	
Самостоятельная работа		**3**		

консультации		**2**		
Экзамен		**1**		
Итого		**80**		
МДК.03.04 «Организация электронной системы управления документооборотом»		**102**		
Тема 1. Ведение в курс «Электронный документооборот»	**Содержание учебного материала**	**4**		ОК 1; ОК 3; ЛР 1-12
	Понятие технологии управления, технологического процесса управления. Обоснование необходимости перехода к безбумажной технологии управления. Основные концепции безбумажной технологии управления. Место системы электронного документооборота (СЭДО) в экономической информационной системе.		**1**	
	Тематика практических занятий и лабораторных работ	**6**		
	Общие требования к созданию документов Оформление бланков документов. Требования к оформлению документов»		**3**	
Тема 2. Терминология делопроизводства. Понятие и структура документооборота	**Содержание учебного материала**	**4**		ОК 2; ЛР1-12 ЛР 13
	Основные понятия делопроизводства. Формы организации документооборота		**2**	
	Тематика практических занятий и лабораторных работ	**2**		
	Определение объема документооборота организации		**3**	
Тема 3. Служба делопроизводства	**Содержание учебного материала**	**6**		ОК 1; ОК 3; ЛР 1-12; ЛР 13
	Организация службы делопроизводства. Задачи и функции служб делопроизводства. Ответственность работников службы делопроизводства за сохранность документов и информации.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Разделение функций между подразделениями делопроизводства и исполнителями		**3**	
Тема 4. Значимость автоматизации документооборота и законодательство в данной сфере	**Содержание учебного материала**	**2**		ОК 2; ОК 3; ЛР 1-12; ЛР 16
	Преимущества автоматизации документооборота. Основные нормативные правовые акты, регулирующие общественные отношения, возникающие в процессе реализации документооборота в бумажной форме и перехода к автоматизированным технологиям.		**2**	

Тема 5. Понятие и принципы функционирования систем электронного документооборота и баз данных	**Содержание учебного материала**	**2**		ОК 2; ОК 3; ЛР 1-12; ЛР 16; ЛР 20
	Понятие и принципы функционирования систем электронного документооборота и баз данных		**2**	
	Тематика практических занятий и лабораторных работ	**2**		
	Принципы функционирования СЭД		**3**	
Тема 6. Основные характеристики систем электронного документооборота	**Содержание учебного материала**	**2**		ОК 2
	Классификация систем электронного документооборота.		**2**	
Тема 7. Классификация систем электронного документооборота	**Содержание учебного материала**	**2**		ОК 2; ОК 3; ЛР1-12; ЛР 16; ЛР 20
	Классификация систем электронного документооборота		**2**	
	Тематика практических занятий и лабораторных работ	**2**		
	Классификация систем электронного документооборота		**3**	
Тема 8. Системы электронного документооборота в российском информационном	**Содержание учебного материала**	**2**		ОК 2; ОК 3; ЛР1-12; ЛР 16; ЛР 20
	Системы электронного документооборота в российском информационном пространстве		**2**	
Тема 9. Специфика внедрения систем электронного документооборота	**Содержание учебного материала**	**4**		ОК 2; ОК 3; ЛР1-12; ЛР 16; ЛР 20
	Основные задачи организации системы электронного документооборота (СЭД). Этапы развития СЭД. Обзор основных систем документооборота, представленных в России		**2**	
	Тематика практических занятий и лабораторных работ	**2**		
	Система электронного документооборота		**3**	
Тема 10.	**Содержание учебного материала**	**4**		ОК 2;

Основные требования к системе электронного документооборота	Критерии выбора систем электронного документооборота. Общие требования к делопроизводственным функциям, к функциям контроля исполнения, поддержке процессов разработки и согласования документов, к механизмам интеграции СЭД с другими приложениями, к возможностям настройки СЭД, к стандартизации, унификации		**2**	ОК 3; ЛР1-12; ЛР 16; ЛР 20
	Тематика практических занятий и лабораторных работ	**4**		
	Процессы разработки документов и согласование в СЭД		**3**	
Тема 11. Настройка системы СЭД - DocsVision.	**Содержание учебного материала**	**4**		ОК 2; ОК 3; ЛР 1-12; ЛР 16; ЛР 20
	Структурированное хранение, навигация. Настраиваемые виды и атрибуты. Смысловые ссылочные связи. Атрибутивный и полнотекстовый поиск. Разграничение доступа.		**2**	
	Тематика практических занятий и лабораторных работ	**2**		
	Настройки системы СЭД		**3**	
Тема 12. Работа со справочниками СЭД - DocsVision	**Содержание учебного материала**	**4**		ОК 2; ОК 3; ЛР 1-12; ЛР 16; ЛР 20
	Заполнение основных справочников в системе электронного документооборота DocsVision		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Заполнение справочников		**3**	
Тема 13. Работа с документами в системе СЭД – Docs	**Содержание учебного материала**	**4**		ОК 2; ОК 3; ЛР 1-12; ЛР 16; ЛР 20
	Создание, согласование, хранение, поиск. Входящая и исходящая корреспонденция. Внутренние документы: организационные, распорядительные, справочно-информационные. Маршрутизация документов. Контроль исполнительской дисциплины.		**2**	
	Тематика практических занятий и лабораторных работ	**6**		
	Работа с документами в СЭД DocsVision		**3**	
Тема 14. Работа с карточкой СЭД - DocsVision	**Содержание учебного материала**	**6**		ОК 2; ОК 3; ЛР1-12; ЛР 16; ЛР 20
	Создание новых видов для существующего пользовательского типа карточки.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Заполнение карточек		**3**	

Тема 15. Работа с уведомлениями СЭД – DocsVision	**Содержание учебного материала**	**4**		ОК 2; ОК 3; ЛР 1-12;
	Создание и настройка уведомлений, рассылаемых в процессе обработки карточек.		**2**	
	Тематика практических занятий и лабораторных работ	**4**		
	Обработка карточек и настройки рассылок уведомлений		**3**	
Самостоятельная работа		**2**		
консультации		**2**		
Экзамен		**2**		
Итого		**102**		
Учебная практика **Виды работ:** – Измерение параметров физических полей. – Определение каналов утечки ПЭМИН. – Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. – Установка и настройка технических средств защиты информации. – Проведение измерений параметров побочных электромагнитных излучений и наводок. – Проведение аттестации объектов информатизации – Монтаж различных типов датчиков. – Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. – Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. – Рассмотрение системы контроля и управления доступом. – Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. – Рассмотрение датчиков периметра, их принципов работы. – Выполнение звукоизоляции помещений системы зашумления. – Реализация защиты от утечки по цепям электропитания и заземления. – Разработка организационных и технических мероприятий по заданию преподавателя; – Разработка основной документации по инженерно-технической защите информации.		**36**		
Производственная практика профессионального модуля		**72**		

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 техническими средствами.			
Экзамен по профессиональному модулю	**6**		
Всего	**584**		

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (узнавание ранее изученных объектов, свойств);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие учебных кабинетов:

лекционные аудитории с мультимедийным оборудованием;

лаборатория «Технических средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест – не менее 25, рабочее место преподавателя, проектор, персональный компьютер, интерактивная доска, комплект презентаций.

Оборудование лаборатории «Технических средств защиты информации» и рабочих мест лаборатории:

1) рабочие места студентов, оборудованные персональными компьютерами;
2) лабораторные учебные макеты;
3) аппаратные средства аутентификации пользователя;
4) средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок;
5) средства измерения параметров физических полей;
6) стенд физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;
7) рабочее место преподавателя;
8) учебно-методическое обеспечение модуля;
9) интерактивная доска, комплект презентаций.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Бубнов А.А. и др. Техническая защита информации в объектах информационной структуры. СПО. М.; Академия, 2019.-10

2. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2016

3. Галицкий А.В. Защита информации в сети - анализ технологий и синтез решений. М: ДМК,2014 -5

4. Грибунин В.Г. Комплексная система защиты информации на предприятии. М.: Академия,2014

5. Зайцев, А. П., Мещеряков, Р. В., Шелупанов, А. А. Технические средства и методы защиты информации / Под ред. А. П. Зайцева, А. А. Шелупанова. - 7-е изд., испр. - М.: Горячая линия, 2018. - 442 с. ISBN 978-5-9912-0233-6 Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2016.

6. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2016.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

7. Исмаилова, Р. Н. Управление внутренней документированной информацией / Р. Н. Исмаилова, С. М. Горюнова, И. М. Захарова // Вестник Технологического университета. – 2018. – Т. 21. – № 8. – С. 136-139.

8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2017. – 416 с.

9. Никифоров, С.Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс] : учеб. пособие / С.Н. Никифоров. — Электрон. дан. — Санкт-Петербург : Лань, 2018. — 96 с. — Режим доступа: https://e.lanbook.com/book/107306. — Загл. с экрана.

10. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2017. – 172 с.

11. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

12. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2017.

13. Петренко, В.И. Защита персональных данных в информационных системах. Практикум [Электронный ресурс] : учебное пособие / В.И. Петренко, И.В. Мандрица.

— Электрон. дан. — Санкт-Петербург : Лань, 2019. — 108 с. — Режим доступа: https://e.lanbook.com/book/111916. — Загл. с экрана

14. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2016

Дополнительные печатные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

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».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. 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.

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.

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13. 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.

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.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
от 30 августа 2002 г. № 282.

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

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.

18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. 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.

21. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

22. 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

23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

27. 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

28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

29. 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

30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38. 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.

39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых

электромагнитных воздействий. Общие требования. Росстандарт, 2014.

40. 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.

41. 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.

42.ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

45. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

48. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

49. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

50. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru

4.3. Общие требования к организации образовательного процесса

Обучение проводится с соблюдением образовательных стандартов, требований санитарной гигиены и охраны труда. Образовательный процесс осуществляется с учетом индивидуальных особенностей обучающихся.

Для достижения поставленных целей профессионального модуля необходимо предварительное изучение общепрофессиональных дисциплин, предусмотренных учебным планом.

4.4. Кадровое обеспечение образовательного процесса

4.4.1. Реализация образовательной программы обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности, имеющих стаж работы в данной профессиональной области не менее 3 лет.

4.4.2. Квалификация педагогических работников образовательной организации должна отвечать квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональных стандартах (при наличии).

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях, направление деятельности которых соответствует области профессиональной деятельности, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее 3 лет в организациях, направление деятельности которых соответствует области профессиональной деятельности, в общем числе педагогических работников, реализующих образовательную программу, должна быть не менее 25 процентов.

Педагогический состав: _____.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке ипроведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач,

		оценка процесса и результатов выполнения видов работ на практике
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты **(освоенные общие компетенции)**	– **Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 01. Выбирать способы решения задач профессиональной	– обоснованность постановки цели, выбора и применения методов и	

деятельности, применительно к различным контекстам.	способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
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	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
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,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению,	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной	

эффективно действовать в чрезвычайных ситуациях.	и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

Результаты указываются в соответствии с паспортом программы и разделом 2. Перечень форм контроля должен быть конкретизирован с учетом специфики обучения по программе профессионального модуля.

***Правила определения основных показателей результатов подготовки:*

1. Основные показатели результатов подготовки должны вытекать из профессиональных компетенций как результат выполнения действий.

2. Основные показатели результатов подготовки могут отражать как комплексный результат деятельности (характеризующий целостный опыт деятельности), так и элементарный результат выполнения отдельный действий и/или операций. Показателем может быть продукт или процесс

выполнения (выполнение работы в соответствии .....).

3. Дескриптор основного показателя результата подготовки формулируются с помощью отглагольных существительных, стоящих вначале предложения.

4. Формулировка показателя не должна повторять формулировку компетенции.

5. Каждой компетенции должно соответствовать не менее двух показателей.

6. Формулировка дескриптора основного показателя результата подготовки должна быть: – ясной и понятной: использование доступных понятий; простые предложения и стиль изложения, в то же время не обедняющие языковой опыт обучающихся; логичность (последовательность, непротиворечивость); – четкой и конкретной, способствующей однозначному пониманию качественных и количественных характеристик результата деятельности

Допускается оформление согласно примерной программы модуля:

Профессиональные компетенции	Оцениваемые знания и умения, действия	Методы оценки	Критерии оценки
ПК 3.1 – 3.5	Знания:		
		Тестирование	75% правильных ответов
		Контрольная работа	75% выполненных заданий
	Умения:		
		Практическое задание	Экспертное наблюдение
		Практическое задание	Экспертное наблюдение
	Действия:		
		Экзамен	Выполнение теоретических и практических заданий
	Умения: Знания:	Ролевая игра	Экспертное наблюдение
	Умения: Знания:	Ситуационные задачи	Экспертное наблюдение
	Знания:		
		Контрольная работа	75% выполненных заданий
		Тестирование	75% правильных ответов
ОК 1.		Тестирование	75% правильных ответов
ОК 2.		Контрольная работа	75% выполненных заданий

Лист изменений и дополнений

в рабочую программу профессионального модуля

_____

по специальности _____

(код и наименование специальности)

№ изменения, дата изменения; номер страницы с изменением *Например:* Изменение №1, 16.06.15 г., стр. № 14	
БЫЛО …… ……	**СТАЛО** …… ……
Основание:…….	

_____/_____

подпись *Инициалы, фамилия , внесшего изменения*

Рассмотрено и одобрено на заседании ЦМК№ ____

Протокол № ____ «____»_____20____г.

Председатель ЦМК: _____/_____

подпись *Инициалы, фамилия*