Министерство образования, науки и молодежной политики
Краснодарского края
Государственное бюджетное профессиональное образовательное учреждение
Краснодарского края «Пашковский сельскохозяйственный колледж»

Рассмотрена на заседании методического объединения
информационных технологий

Протокол № 1
от « 28 » сент. 2022г.
Н.Я. Пушкарева

Рассмотрена на заседании педагогического совета
Протокол № 2
от « 26 » 10 2022г.

СОГЛАСОВАНО
Зам. директора по учебной работе
А.Н. Сиденко
«____» ______ 2022г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

По специальности:

10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Краснодар, 2022

Входит в структуру основной образовательной программы, предназначена для ее реализации в соответствии с требованиями ФГОС среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, (Приказ Министерства образования и науки РФ от 09 декабря 2016 г. №1553 (ред. 17.12.2020)), зарегистрирован в Минюсте России от 26.12.2016 №44938.

Организация разработчик: ГБПОУ КК ПСХК

Разработчик:

Пушкарева Н.Я., преподаватель компьютерных дисциплин ГБПОУ КК ПСХК, высшей квалификационной категории, математик, преподаватель информатики и ИКТ.

Белова О.Л., преподаватель компьютерных дисциплин ГБПОУ КК ПСХК, инженер по специальности физика и техника оптической связи, магистр техники и технологии по направлению телекоммуникаций.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации техническими средствами* и соответствующие ему профессиональные компетенции:

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.
ПК 3.6.	*Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах*
ПК 3.7.	*Выявлять и анализировать возможные угрозы информационной безопасности объектов*
ПК 3.8.	*Ориентироваться в условиях частой смены технологий в профессиональной деятельности*
ПК.3.9.	*Проводить регламентные работы и фиксировать отказы средств защиты*

1.1.2. Общие компетенции:

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.

1.1.3. В результате освоения профессионального модуля студент 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. – *корректировки конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, контроля и испытаний;* – *отработки конструкции средств защиты информации на технологичность с учетом стандартов ЕСТД;* – *заключения договоров с поставщиками комплектующих изделий и материалов, и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности;*

	– *сертификационных испытаний технических средств защиты информации от несанкционированного доступа на соответствие требованиям безопасности информации;* – *испытания опытного образца защищенного технического средства обработки информации на соответствие техническим условиям;* – *использования основных методов и средств обеспечения информационной безопасности компьютерных средств;* – *применения методов криптографической защиты и аутентификации.*
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; – *оценивать защищенность ограждающих конструкций помещения от утечки информации по акустическому каналу;* – *оценивать защищенность ограждающих конструкций помещения от утечки информации по виброакустическому каналу;* – *проводить статистический анализ загрузки заданного диапазона и обнаружения радиозакладных устройств в защищаемом помещении;* – *проводить техническое обслуживание и устранять выявленные неисправности технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок;* – *оценивать защищенность телефонных каналов;* – *оценивать защищенность помещения от утечки информации по каналам акустоэлектрических преобразований технических средств;* – *обнаруживать ПЭМИ по электрической составляющей электромагнитного поля;* – *проводить испытания защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами;* – *организовывать технический контроль эффективности мер защиты информации;*

	– *проводить оценку защищенности объекта информатизации;* – *разрабатывать проект системы видеонаблюдения для организации;* – *проводить оценку разведдоступности;* – *проводить комплекс работ по проверке возможности утечки информации по техническим каналам;* – *проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации;* – *выполнять правила эксплуатации средств защиты информации* – *ставить цели, формулировать задачи, связанные с обеспечением корпоративной защиты от внутренних угроз информационной безопасности;* – *анализировать тенденции развития систем обеспечения корпоративной защиты от внутренних угроз информационной безопасности;* – *осуществлять установку, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз;* – *применять знания о корпоративной защите от внутренних угроз информационной безопасности в решении поставленных задач;* – *осуществлять разработку политик безопасности в системе* – *корпоративной защиты информации от внутренних угроз;* – *классифицировать информацию с ограниченным доступом применительно к видам тайны;* – *грамотно применять методы криптографической защиты;* – *применять системы управления средствами безопасности;* – *проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;* – *администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;* – *осуществлять установку и конфигурирование систем VPN;* – *создавать (обновлять) узлы, пользователей, ключи, сертификаты для обеспечения работоспособности защищенной связи с использованием VPN-системы*.
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; – *технические каналы утечки информации при передаче ее по каналам связи;* – *демаскирующие признаки объектов;* – *средства выявления каналов утечки информации;* – *возможности технической разведки, формы разведывательной деятельности;* – *основные этапы и процедуры добывания информации технической разведкой;* – *нормативные документы по противодействию технической разведке;* – *возможности средств акустической речевой разведки;* – *особенности реализации пассивных мер защиты в виброакустических каналах утечки речевой информации;* – *средства контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок;* – *порядок устранения неисправностей средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок;* – *организацию ремонта средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок;* – *возможности приборов видеонаблюдения;* – *защиту информации в оптическом диапазоне частот;* – *средства оценки и анализа оптического канала утечки информации;* – *способы уничтожения информации;*

	– *специальные средства для экспресс-копирования (или ее уничтожения) с магнитных носителей;* – *специальные технические средства для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи;* – *нормативные документы, регламентирующие применения технических средств защиты информации;* – *скрытие и защита информации по техническим каналам;* – *методы и средства инженерной защиты и технической охраны объектов;* – *порядок эксплуатации программных и технических средств и систем защиты секретной информации от НСД;* – *порядок приемки СЗСИ перед сдачей в эксплуатацию в составе АС;* – *типовой вариант КПП;* – *быстроразвертываемые комплексы ТСО, их состав, особенности, преимущества от внедрения;* – *номенклатуру применяемых средств обнаружения (вибрационные, комбинированные, магнитеметрические, объектовые);* – *сравнительный анализ применения шлюзового турникета и маятниковой двери-шлюза;* – *организацию охраны объектов с применением технических средств воздействия;* – *нормативную документацию использования технических средств физической защиты;* – *единую систему конструкторской документации;* – *единую систему технологической документации;* – *особенности выбора инженерно-технических средств физической защиты периметров протяженных объектов, особенности их монтажа;* – *объекты компьютерных технологий, используемые в обеспечении корпоративной защиты от внутренних угроз информационной безопасности;* – *понятийный аппарат информационных технологий и особенности терминологии в области корпоративной защиты от внутренних угроз информационной безопасности;* – *базовые составляющие в области развития систем информационной безопасности;* – *методы выявления утечек информации с использованием технологии Data Leakage Prevention (DLP);* – *методы проведения анализа в области обеспечения корпоративной защиты от внутренних угроз информационной безопасности;*

	– *современные технологии, применяемых в области корпоративной защиты от внутренних угроз информационной безопасности;* – *функционирование системы управления средствами безопасности;* – *основные типы моделей управления доступом;* – *обследование (аудит) организации с целью защиты от угроз информационной безопасности;* – *методы защиты сетевого трафика с использованием VPN-технологий.*

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 992 часов, в том числе практической подготовки – 722 часа.
Из них на освоение МДК.03.01 – 140 часов, в том числе практической подготовки – 70 часов, самостоятельной работы обучающегося – 8 часов. Промежуточная аттестация в форме экзамена.
На освоение МДК.03.02 – 172 часа, в том числе практической подготовки – 70 часа, самостоятельной работы обучающегося – 10 часов, курсовой работы (проекта) – 30 часов. Промежуточная аттестация в форме дифференцированного зачета.
На освоение МДК.03.03 – 248 часов, в том числе практической подготовки – 148 часов, из них самостоятельной работы –16 часов; всего самостоятельной работы обучающегося – 24 часа. Промежуточная аттестация в форме экзамена.
Учебной практики – 216 часов. Промежуточная аттестация в форме дифференцированного зачета.
Производственной практики – 216 часов. Промежуточная аттестация в форме дифференцированного зачета.
Промежуточная аттестация форме экзамена по профессиональному модулю.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.03 Защита информации техническими средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.				Практики	
			всего, часов	в том числе			учебная практика, часов	производственная практика, часов
				лабораторных и практических занятий	курсовая работа (проект), часов	Самостоятельная работа		
ПК 3.1- ПК.3.4 ОК 01– ОК10	МДК.03.01 Техническая защита информации	**140**	140	70	–	8	–	–
ПК 3.5 ОК 01–ОК10	МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации	**172**	172	70	30	10	–	–
ПК 3.6-ПК 3.9 ОК 01–ОК10	МДК 03.03 Корпоративная защита от внутренних угроз информационной безопасности	**248**	248	148	–	24	–	–
	УП.03 Учебная практика	**216**					216	–
	ПП.03 Производственная практика	**216**						216

	Промежуточная аттестация в форме экзамена по модулю		–	–	–	–	–	–
	Всего:	**992**	**560**	**288**	**30**	**42**	**216**	**216**

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)		Объем часов	Уровень освоения
1	2		3	4
МДК.03.01 Техническая защита информации			**140**	
Раздел 1. Концепция инженерно-технической защиты информации			**6**	
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание учебного материала**		2	
	1	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.		2
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание учебного материала**		4	2
	1	Задачи и требования к способам и средствам защиты информации техническими средствами.		
	2	Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.		
Раздел 2. Теоретические основы инженерно-технической защиты информации			**20**	
Тема 2.1. Информация как предмет защиты	**Самостоятельная работа**		2	
	1	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации.		
	Содержание учебного материала		2	2
	1	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.		
	Практические занятия		2	
	1	*Практическая работа № 1. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.*		
Тема 2.2. Технические каналы утечки информации	**Содержание учебного материала**		4	2
	1	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации.		
	2	Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.		
	Практические занятия		2	
	1	*Практическая работа № 2. Определение канала утечки информации. Проведение сравнительного анализа каналов.*		
Тема 2.3. Методы и средства технической разведки	**Содержание учебного материала**		4	2,3
	1	*Техническая разведка: определение, классификация, возможности. Формы разведывательной деятельности. Основные этапы и процедуры добывания информации технической разведки.*		
	2	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации.		
	Самостоятельная работа		2	
	1	Средства и возможности оптической разведки. Средства дистанционного съема информации.		
	Практические занятия		2	
	1	*Практическая работа № 3. Планирование мероприятий по определению возможных средств организации технической разведки.*		
Раздел 3. Физические основы технической защиты информации			**18**	

Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание учебного материала**		6	2,3
	1	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования.		
	2	Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.		
	3	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		
	Практические занятия		8	
	1	*Практическая работа № 4. Расчет наводок в каналах связи.*		
	2	*Практическая работа № 5. Побочные электромагнитные излучения ПК. Заземление технических средств и подавление информационных сигналов в цепях заземления.*		
	3	*Практическая работа № 6. Восстановление информации при перехвате побочных э*		
	4	*Практическая работа № 7. Съем информации по электрическим каналам утечки*		
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание учебного материала**		2	3
	1	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.		
	Практические занятия		2	
	1	Практическая работа № 8. Организация мероприятий по скрытию речевой информации.		
Раздел 4. Системы защиты от утечки информации			**56**	
Тема 4.1. Системы защиты от утечки	**Содержание учебного материала**		4	2,3
	1	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами.		

информации по акустическому каналу	2	Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.		
	Практические занятия		2	
	1	Практическая работа № 9. Защита от утечки по акустическому каналу.		
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание учебного материала**		4	2,3
	1	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны.		
	2	Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.		
	Практические занятия		6	
	1	*Практическая работа № 10. Осуществление акустического контроля источников звуков с помощью направленных микрофонов. Сравнение и оценка направленных микрофонов.*		
	2	*Практическая работа № 11. Организация применения направленных микрофонов на открытой местности, в помещениях.*		
	3	*Практическая работа № 12. Выбор типа микрофона и места его установки. Организация сеанса деловой звукозаписи.*		
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание учебного материала**		4	2,3
	1	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи.		
	2	Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.		
	Практические занятия		4	
	1	Практическая работа № 13. Защита от утечки по виброакустическому каналу.		
	2	*Практическая работа № 14. Оценка защищенности ограждающих конструкций от утечки информации по виброакустичекому каналу.*		
	Содержание учебного материала		4	2,3

Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	1	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладках.		
	2	Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.		
	Практические занятия		6	
	1	Практическая работа № 15. Определение каналов утечки ПЭМИН.		
	2	Практическая работа №16. Защита от утечки по цепям электропитания и заземления.		
	3	*Практическая работа №17. Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении.*		
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание учебного материала**		4	2,3
	1	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.		
	2	Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.		
	Практические занятия		4	
	1	Практическая работа № 18. Защита от утечки информации по телефонному каналу.		
	2	*Практическая работа № 19. Оценка защищенности телефонных каналов*.		
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание учебного материала**		4	2,3
	1	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.		
	2	Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.		
	Практические занятия		6	
	1	Практическая работа № 20. Организация защиты информации от несанкционированной утечки по электросетевому каналу.		

	2	*Практическая работа № 21. Оценка защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств.*		
	3	*Практическая работа № 22. Организация защиты информации от несанкционированной утечки по электросетевому каналу.*		
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание учебного материала**		2	2,3
	1	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.		
	Практические занятия		2	
	1	*Практическая работа № 23. Организация защиты информации по оптическому каналу*		
Раздел 5. Применение и эксплуатация технических средств защиты информации			**40**	
Тема 5.1. Применение технических средств защиты информации	**Самостоятельная работа**		2	
	1	Технические средства для уничтожения информации и носителей информации, порядок применения.		
	Содержание учебного материала		6	2,3
	1	Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.		
	2	Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.		
	3	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		
	Практические занятия		10	
	1	Практическая работа № 24. Организация защиты информации в условиях применения мобильных устройств обработки и передачи данных.		
	2	Практическая работа № 25. Измерение параметров побочных электромагнитных излучений и наводок при проведении аттестации объектов.		

	3	*Практическая работа № 26. Проведение испытаний защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами.*		
	4	Практическая работа № 27. Проведение измерений параметров фоновых шумов при использовании технических средств защиты информации.		
	5	*Практическая работа № 28. Организация технического контроля эффективности мер защиты информации.*		
Тема 5.2. Эксплуатация технических средств защиты информации	**Самостоятельная работа**		2	
	1	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.		
	Содержание учебного материала		6	2,3
	1	Установка и настройка технических средств защиты информации.		
	2	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.		
	3	*Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.*		
	Практические занятия		14	
	1	Практическая работа № 29. Проведение технического обслуживания телефонных аппаратов.		
	2	Практическая работа № 30. Проведение технического обслуживания шредеров.		
	3	*Практическая работа № 31. Проведение первичного осмотра помещений при аттестации объекта информатизации.*		
	4	*Практическая работа № 32. Проведение оценки разведдоступности.*		
	5	*Практическая работа № 33. Комплекс работ по проверке возможности утечки информации по техническим каналам.*		
	6	*Практическая работа № 34. Оценка защищенности объекта информатизации.*		
	7	*Практическая работа № 35. Подготовка пакета документов для проведения аттестации объекта информатизации.*		
Промежуточная аттестация по МДК.03.01 - экзамен				

Виды самостоятельной работы при изучении МДК.03.01 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (в том числе учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.				
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации			**172**	
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты			**30**	
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание учебного материала**		4	1,2
	1	*Предмет и задачи технической защиты информации. Системный подход при решении задач инженерно-технической защиты объектов. Задачи и требования к способам и средствам защиты информации техническими средствами.*		
	2	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации.		
	Самостоятельная работа		2	
	1	Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации.		
	Содержание учебного материала		2	2
	1	Модель нарушителя и возможные пути, и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.		
	Практические занятия		4	
	1	Практическая работа № 1. Построение модели нарушителя, определение способов его проникновения на объект, на примере образовательной организации.		
	2	Практическая работа № 2. Построение модели нарушителя, определение способов его проникновения на объект, на примере производственной организации.		
Тема 1.2. Общие сведения о комплексах	**Содержание учебного материала**		10	2,3
	1	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны.		

инженерно-технических средств физической защиты	2	Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты.		
	3	Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.		
	4	*Типовой вариант КПП.*		
	5	*Быстро развертываемые комплексы ТСО: состав, отличительные особенности, преимущества от внедрения.*		
	Практические занятия		8	
	1	Практическая работа № 3. Формирование требований к физической защите объекта. Анализ нормативно-правовых документов.		
	2	Практическая работа № 4. Формирование перечня требований к защите объекта.		
	3	*Практическая работа № 5. Определение состава инженерных конструкций, необходимых для предотвращения проникновения злоумышленника.*		
	4	*Практическая работа № 6. Разработка проекта монтажа инженерных конструкций на территории организации.*		
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты			**72**	
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание учебного материала**		8	2,3
	1	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта.		
	2	Периметровые средства обнаружения: назначение, устройство, принцип действия.		
	3	Объектовые средства обнаружения: назначение, устройство, принцип действия.		
	4	*Номенклатура применяемых средств обнаружения (вибрационные, магнитометрические, объектовые).*		
	Практические занятия		4	
	1	Практическая работа № 7. Монтаж датчиков пожарной сигнализации.		
	2	Практическая работа № 8. Монтаж датчиков охранной сигнализации		
	Содержание учебного материала		8	2,3

Тема 2.2. Система контроля и управления доступом	1	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД.		
	2	Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД.		
	3	Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.		
	4	Обнаружение металлических предметов и радиоактивных веществ.		
	Практические занятия		10	
	1	Практическая работа № 9. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя.		
	2	Практическая работа № 10. Рассмотрение принципов устройства, работы и применения средств контроля доступа.		
	3	*Практическая работа № 11. Особенности построения и размещения СКУД.*		
	4	*Практическая работа № 12. Периферийное оборудование и носители информации в СКУД. Методы удостоверения личности, применяемые в СКУД.*		
	5	*Практическая работа № 13. Сравнительный анализ применения шлюзового турникета и маятниковой двери-шлюза.*		
Тема 2.3. Система телевизионного наблюдения	**Самостоятельная работа**		2	
	1	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения.		
	Содержание учебного материала		6	2,3
	1	Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы.		
	2	Состав системы телевизионного наблюдения. Инфракрасные осветители. Детекторы движения.		
		Дополнительное оборудование систем телевизионного наблюдения		
	Практические занятия		10	

	1	Практическая работа № 14. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.		
	2	*Практическая работа № 15. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.*		
	3	*Практическая работа № 16. Управление системой телевизионного наблюдения с автоматизированного рабочего места.*		
	4	*Практическая работа № 17. Разработка проекта системы видеонаблюдения для организации.*		
	5	*Практическая работа № 18. Настройка систем телевизионного наблюдения с учетом специфики деятельности организации*		
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание учебного материала**		4	2
	1	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации.		
	2	Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.		
	Практические занятия		8	
	1	Практическая работа № 19. Рассмотрение принципов устройства системы сбора и обработки информации.		
	2	Практическая работа № 20. Рассмотрение принципов работы и применения системы сбора и обработки информации.		
	3	*Практическая работа № 21. Практическое исследование особенностей применения систем сбора, обработки, отображения и документирования информации.*		
	4	*Практическая работа № 22. Определение состава ССОИ для образовательной организации.*		
Тема 2.5 Система воздействия	**Содержание учебного материала**		4	2,3
	1	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.		
	2	*Организация охраны объектов с применением технических средств воздействия.*		
	Практические занятия		8	

	1	*Практическая работа № 23. Мониторинг эффективности технических средств воздействия для гражданских организаций.*		
	2	*Практическая работа № 24. Определение эффективности технических средств воздействия для гражданских организаций.*		
	3	*Практическая работа № 25. Испытание на устойчивость технических средств охраны.*		
	4	*Практическая работа № 26. Разработка проекта применения технических средств воздействия для образовательной организации.*		
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты			**38**	
Тема 3.1 Применение инженерно-технических средств физической защиты	**Самостоятельная работа**		2	
	1	*Нормативная документация использования технических средств физической защиты. Единая система конструкторской документации. Единая система технологической документации.*		
	Содержание учебного материала		8	2,3
	1	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом.		
	2	*Особенности выбора инженерно-технических средств физической защиты периметров протяженных объектов. Особенности монтажа.*		
	3	Особенности организации пропускного режима на КПП.		
	4	Управление системой телевизионного наблюдения с автоматизированного рабочего места.		
	Самостоятельная работа		2	
	1	*Порядок применения устройств отображения и документирования информации. Управление системой воздействия.*		
	Практические занятия		8	
	1	*Практическая работа № 27. Разработка структурной схемы оборудования инженерно-технических средств физической защиты.*		
	2	*Практическая работа № 28. Представление моделей объектов информационной безопасности.*		

	3	*Практическая работа № 29. Разработка спецификации оборудования физической защиты объекта.*		
	4	*Практическая работа № 30. Определение эффективности применения сигнально-охранных пиротехнических устройств для гражданских организаций.*		
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Самостоятельная работа**		2	
	1	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.		
	Содержание учебного материала		6	2,3
	1	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.		
	2	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.		
	3	*Организация ремонта технических средств физической защиты.*		
	Практические занятия		10	
	1	*Практическая работа № 31. Проведение диагностики систем видеонаблюдения.*		
	2	*Практическая работа № 32. Устранение отказов и восстановление работоспособности систем видеонаблюдения.*		
	3	*Практическая работа № 33. Отработка конструкции технического средства защиты информации на технологичность с учетом стандартов ЕСТД.*		
	4	*Практическая работа № 34. Проверка работоспособности средств защиты информации от несанкционированного доступа и специальных воздействий.*		
	5	*Практическая работа № 35. Выполнение правил эксплуатации средств защиты информации.*		
Курсовой проект (работа)			**30**	3
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.				

4. Разработка проекта системы контроля и управления доступом служебного офиса. 5. Разработка проекта системы обеспечения безопасности для торговой организации. 6. Разработка проекта системы обеспечения безопасности для образовательной организации. 7. Разработка проекта системы обеспечения безопасности для промышленного предприятия. 8. Разработка проекта системы обеспечения безопасности для банковской организации. 9. Разработка проекта КПП для гражданской организации. 10. Разработка проекта систем телевизионного наблюдения для образовательной организации. 11. Разработка мероприятий применения пассивных методов защиты акустической информации. 12. Разработка мероприятий применения активных методов защиты акустической информации. 13. Подготовка пакета документов для проведения аттестации объекта информатизации на примере организации. 14. Разработка требований к инженерно-техническим средствам для физической защиты автоматизированных рабочих мест на объекте. 15. Разработка требований по защите информации от несанкционированного доступа к объекту информатизации. 16. Использование комплексного обеспечения информационной безопасности при реализации угрозы попытки доступа в удаленную систему. 17. Реализация комплексного подхода к обеспечению защиты конфиденциальной информации в компании. 18. Разработка концепции политики безопасности и систем контроля доступа для локальной вычислительной сети. 19. Организация порядка установления внутри объектного спец режима на объекте информатизации. 20. Организация противодействия угрозам безопасности персонала организации. 21. Разработка основных направлений, принципов и методов обеспечения информационной безопасности предприятия. 22. Построение типовой модели угроз безопасности информации кредитной организации. 23. Разработка комплексной системы защиты коммерческой информации на предприятии. 24. Разработка мер по технической защите конфиденциальной информации в организации. 25. Разработка мер информационной безопасности предприятия. 26. Реализация комплексного подхода к обеспечению защиты конфиденциальной информации в компании. 27. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 28. Разработка структуры службы безопасности предприятия. 29. Разработка рабочего проекта охранной безопасности на предприятии.		

30. Инженерно-технические средства обеспечения безопасности предприятия.				
Промежуточная аттестация по МДК.03.02 дифференцированный зачет			**2**	
Виды самостоятельной работы при изучении МДК.03.02 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (в том числе учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.				
МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности			**248**	
Раздел 1. ***Защита информации от внутренних угроз информационной безопасности с использованием DLP-технологий***				
Тема 1.1. *Основы защиты информации от внутренних угроз информационной безопасности.*	**Содержание учебного материала**		2	2
	1	*Основы защиты корпоративной информации. Цели, задачи, методы и средства защиты информации.*		
		Самостоятельная работа	2	
	1	*Правовые основы защиты корпоративной информации. Ключевые алгоритмы и системы. Основные понятия. Безопасность информационных систем. Угрозы информационной безопасности. Уязвимости. Риски. Атаки.*		
	Содержание учебного материала		6	2
	1	*Защита информации от внутренних угроз информационной безопасности. Выявление утечек с использованием технологии Data Leakage Prevention (DLP). Теория и практика применения DLP систем.*		
	2	*Назначение системы Info Watch Traffic Monitor (IW TM). Контролируемые каналы передачи данных. Архитектура продукта IW TM.*		

	3	*Технологии анализа детектируемых объектов. Задачи и принципы работы дополнительных модулей системы IW Device Monitor (IW DM) и IW Crawler. Визуальная аналитика данных.*		
Тема 1.2. *Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз*		**Содержание учебного материала**	4	2
	1	*Сетевое окружение. Сетевые протоколы. Методы выявления и построения путей движения информации в организации. Подходы к построению сети. Настройка сетевых устройств для эффективного взаимодействия. Типы сетевых устройств.*		
	2	*Разнообразие операционных систем, их возможности с точки зрения использования и развертывания компонент систем защиты от внутренних угроз. Процесс выбора драйверов и программного обеспечения для различных аппаратных средств и операционных систем.*		
		Самостоятельная работа	2	
	1	*Этапы установки систем корпоративной защиты от внутренних угроз. Назначение компонент системы корпоративной защиты от внутренних угроз.*		
		Содержание учебного материала	4	2,3
	1	*Технологии программной и аппаратной виртуализации. Конфигурация сетевой инфраструктуры: настройка хост машины, сетевого окружения, виртуальных машин, и т.п.*		
	2	*Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развертывании и настройке.* *Установка и настройка агентского мониторинга. Синхронизация с LDAPсервером.*		
		Практические занятия	12	
	1	*Практическая работа № 1. Конфигурация сетевой инфраструктуры: настройка хост машины, сетевого окружения, виртуальных машин.*		
	2	*Практическая работа № 2. Установка сервера Traffic Monitor.*		

	3	*Практическая работа № 3. Установка лицензии Traffic Monitor. Установка Базы данных.*		
	4	*Практическая работа № 4 Установка подсистемы Краулер. Установка рабочего места Офицера Безопасности. Создание пользователя виртуальной машины IWDM (Офицер Безопасности). Настройка рабочего места Офицера Безопасности. Конфигурация сетевой инфраструктуры: настройка хост машины, сетевого окружения, виртуальных машин.*		
	5	*Практическая работа № 5. Установка серверной части Info Watch Device Monitor. Установка рабочего места потенциального нарушителя. Настройка сетевого взаимодействия. Создание пользователя виртуальной машины Agent1 (Потенциальный нарушитель). Настройка рабочего места на машине Agent1. Установка DM Client.*		
	6	*Практическая работа № 6. Работа в Консоли управления Device Monitor. Авторизация и соединение с сервером InfoWatch Device Monitor. Главное окно Консоли управления (DM). Разделы Консоли управления (DM).*		
Тема 1.3. *Исследование (аудит) организации с целью защиты от внутренних угроз*		**Содержание учебного материала**	4	2
	1	*Угрозы информационной безопасности. Исследование (аудит) организации на основании полученных материалов («модели организации»), обследование корпоративных информационных систем.*		
	2	*Определение объектов защиты. Перечень субъектов, персон, роли пользователей, права доступа.*		
		Практические занятия	6	
	1	*Практическая работа № 7. Изучение структуры организации. Обследование корпоративных информационных систем.*		
	2	*Практическая работа № 8. Добавление роли Администратора системы. Добавление роли пользователя для проведения аудита.*		
	3	*Практическая работа № 9. Создание подразделений организации с использованием AD сервера. Синхронизация каталога пользователей и компьютеров.*		

Тема 1.4. *Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз*		**Содержание учебного материала**	6	2,3
	1	*Работа с интерфейсом управления системы корпоративной защиты информации. Раздел Технологии.*		
	2	*Работа с объектами защиты в интерфейсе управление системой.*		
	3	*Политика безопасности. Модификация политики безопасности в системе IWTM.*		
		Практические занятия	8	
	1	*Практическая работа № 10. Работа с категориями и терминами.*		
	2	*Практическая работа № 11. Работа с текстовыми объектами.*		
	3	*Практическая работа № 12. Работа с эталонными документами.*		
	4	*Практическая работа № 13. Работа с бланками.*		
		Самостоятельная работа	4	
	1	*Практическая работа № 14. Работа с печатями.*		
	2	*Практическая работа № 15. Работа с выгрузками.*		
		Практические занятия	12	
	1	*Практическая работа № 16. Работа с графическими объектами.*		
	2	*Практическая работа № 17. Экспорт и импорт базы технологий.*		
	3	*Практическая работа № 18. Работа с объектами защиты. Создание каталога объектов защиты. Создание объекта защиты.*		
	4	*Практическая работа № 19. Добавление элементов технологий. Добавление условий обнаружения. Создание политики для объектов защиты и их каталогов.*		
	5	*Практическая работа № 20. Добавление новой политики: создание политики защиты данных, создание политики защиты данных на агентах, создание политики контроля персон.*		

	6	*Практическая работа № 21. Добавление правил в политику. Фильтрация списка политик.*		
Тема 1.5. *Технологии агентского мониторинга*		**Содержание учебного материала**	4	2
	1	*Состав серверной части InfoWatch Device Monitor: база данных, сервер InfoWatch Device Monitor, консоль управления InfoWatch Device Monitor.*		
	2	*Общие принципы работы с Консолью управления InfoWatch Device Monitor (DM): авторизация и соединение с сервером InfoWatch Device Monitor, главное окно Консоли управления, разделы Консоли управления.*		
		Самостоятельная работа	2	
	1	*Способы установки Агента Device Monitor на рабочие станции: Локальная установка, удаленная, через задачи распространения в Консоли управления, установка с помощью средств распространения программного обеспечения.*		
		Практические занятия	12	
	1	*Практическая работа № 22. Учетные записи пользователей Консоли управления (DM). Добавление учетной записи Консоли управления. Редактирование учетной записи Консоли управления (DM). Блокирование и разблокирование учетной записи Консоли управления (DM). Удаление учетной записи Консоли управления (DM).*		
	2	*Практическая работа № 23. Роли пользователей Консоли управления (DM). Добавление роли пользователя Консоли управления. Редактирование роли пользователя. Удаление роли пользователя.*		
	3	*Практическая работа № 24. Общие настройки Агентов. Контроль сетевых соединений. Контроль сетевого трафика.*		
	4	*Практическая работа № 25. Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor. Соединение и синхронизация со службами каталогов.*		
	5	*Практическая работа № 26. Настройка уведомлений сотрудников о нарушении правил (DM). Исключение приложений из перехвата.*		
	6	*Практическая работа № 27. Контроль приложений и снимки экрана. Хранение событий. Синхронизация политик Traffic Monitor. Контроль ввода с клавиатуры.*		

		Содержание учебного материала	10	2,3
	1	*Управление схемой безопасности. Организация схемы безопасности. Политики безопасности и правила (DM).*		
	2	*Сотрудники и группы сотрудников. Компьютеры и группы компьютеров. Загрузка схемы безопасности на контролируемые компьютеры.*		
	3	*Общие действия при управлении схемой безопасности. Просмотр действующей версии схемы безопасности. Редактирование и обновление схемы безопасности. Экспорт/импорт конфигурации.*		
	4	*Настройка схемы безопасности. Политики безопасности (DM). Просмотр политик безопасности (DM). Создание и настройка политики безопасности (DM). Редактирование политики безопасности (DM). Удаление политики безопасности (DM).*		
	5	*Правила (DM). Применение правил (DM). Типы правил. Создание, редактирование, копирование и удаление правил (DM).*		
		Практические занятия	10	
	1	*Практическая работа № 28. Настройка Правила для Application Monitor. Правило для Clipboard Monitor. Правило для Cloud Storage Monitor. Правило для Device Monitor.*		
	2	*Практическая работа № 29. Правило (DM) для File Monitor. Правило для File Operations Monitor. Правило для FTP Monitor. Правило для HTTP(S) Monitor. Правило для IM Client Monitor.*		
	3	*Практическая работа № 30. Правило (DM) для Mail Monitor. Правило для Network Monitor. Правило для Print Monitor. Правило для ScreenShot Control Monitor. Правило для ScreenShot Monitor.*		
	4	*Практическая работа № 31. Белые списки устройств. Просмотр сведений о белых списках. Добавление белого списка. Установка периода действия записи. Редактирование белого списка. Удаление белого списка.*		

	5	*Практическая работа № 32. Приложения. Создание и изменение списка приложений. Добавление приложения в список автоматически. Добавление приложения в список вручную. Экспорт протокола приложения.*		
		Самостоятельная работа	2	
	1	*Практическая работа № 33. Временный доступ сотрудника к сети. Временный доступ сотрудника к устройствам.*		
		Содержание учебного материала	4	2,3
	1	*Удаленная установка, обновление и удаление Агентов. Управление задачами в Консоли управления DM.*		
	2	*Просмотр событий DM. Фильтры событий.*		
		Практические занятия	2	
	1	*Практическая работа № 34. Создание задачи первичного распространения. Создание задачи обновления, задачи смены пароля деинсталляции.*		
		Самостоятельная работа	4	
	1	*Практическая работа № 35. Создание задачи удаления. Запуск, остановка, редактирование и удаление задачи.*		
	2	*Практическая работа № 36. Просмотр событий DM. Фильтры событий. Удаление событий.*		
Тема 1.6. *Анализ выявленных инцидентов*		**Содержание учебного материала**	4	2
	1	*Создание тестовой политики в IWTM. Создание тестовой политики в DM.*		
	2	*Работа в тематических разделах Сводка, События интерфейса Консоли управления Traffic Monitor. Отчеты интерфейса Консоли управления Traffic Monitor.*		
		Практические занятия	10	
	1	*Практическая работа № 37. Создание тестовой политики в IWTM.*		
	2	*Практическая работа № 38. Создание тестовой политики в DM.*		

	3	*Практическая работа № 39. Генерация событий для тестирования политики.*		
	5	*Практическая работа №40. Работа с отчетами. Создание и просмотр отчетов. Создание папки с отчетами.*		
	6	*Практическая работа № 41. Создание и настройка виджета. Просмотр готовых отчетов.*		
Раздел 2. ***Технология анализа и защиты сетевого трафика***				
Тема 2.1. *Программные решения построения и управления виртуальными и защищенными сетями*		**Содержание учебного материала**	4	2
	1	*Технология защиты информации VipNet. Структура сети VipNet. Типы связей в сети VipNet. Управляющий драйвер. Виртуальные адреса сети VipNet.*		
	2	*Основные компоненты сети VipNet. Базовые модули VipNet. VipNet Администратор. VipNet Координатор. VipNet Клиент. VipNet Policy Manager.*		
Тема 2.2. *Базовый программный комплекс VipNet Administrator*		**Содержание учебного материала**	10	2,3
	1	*VipNet Центр управления сетью (ЦУС). Основные функциональные возможности. Архитектура программы VipNet ЦУС. Взаимодействие с программой VipNet Удостоверяющий и ключевой центр и с программой VipNet Registration Point. Связи между объектами сети VipNet. Роли сетевых узлов. Справочники и ключи VipNet.*		
	2	*Топология сети: основные понятия сетевого уровня. Функции координатора в защищенной сети VipNet. Туннелирование. Принципы осуществления соединений в сети VipNet. Организация межсетевого взаимодействия.*		
	3	*VipNet Удостоверяющий и ключевой центр (УКЦ). Основные функции VipNet УКЦ. Программный комплекс VipNet Удостоверяющий центр (УЦ). Инфраструктура открытых ключей KPI. Электронная подпись данных. Шифрование данных. Работа Удостоверяющего центра. Использование центра регистрации.*		
	4	*Архитектура KPI. Модели установления доверительных отношений. Программный комплекс VipNet УЦ.*		
	5	*Ключевая система в ПО VipNet. Формирование ключевой информации в VipNet. Мастер-ключи. Формирование ключей при первоначальном развертывании сети.*		

		Дистрибутивы ключей. Ключи пользователя. Ключи узла. Компрометация ключей. Резервный набор персональных ключей. Межсетевые мастер-ключи. Электронная подпись. Сертификат ключа проверки ЭП.		
		Практические занятия	14	
	1	*Практическая работа № 42. Планирование защищенной сети* VipNet*. Проработка схемы сети.*		
	2	*Практическая работа № 43. Подготовка виртуального стенда. Создание и настройка виртуальных машин.*		
	3	*Практическая работа № 44. Установка и первичная настройка компонентов программного обеспечения ViPNet Administrator.*		
	4	*Практическая работа № 45. Создание структуры защищенной сети.*		
	5	*Практическая работа № 46. Создание межсерверных каналов и связей.*		
	6	*Практическая работа № 47. Первый запуск программы ViPNet Удостоверяющий и ключевой центр. Выдача дистрибутивов ключей.*		
	7	*Практическая работа № 48. Настройка резервного копирования и восстановление данных в ПО ViPNet Administrator.*		
Тема 2.3. *Программное обеспечение ViPNet Client*		**Содержание учебного материала**	6	2,3
	1	*Назначение ПО ViPNet Client. Функции ПО ViPNet Client. Состав ПО ViPNet Client. Драйвер сетевой защиты.*		
	2	*Программа VipNet Монитор. Основные принципы фильтрации трафика. Обмен защищенными сообщениями. Конференция. Файловый обмен. вызов внешних приложений. Просмотр веб-ресурсов сетевого узла.*		
	3	*Транспортный модуль VipNet MFTP. Контроль приложений VipNet. Деловая почта VipNet. Криптопровайдер VipNet CSP. Система обновления VipNet.*		
		Практические занятия	4	
	1	*Практическая работа № 49. Развертывание рабочего места помощника главного администратора.*		

	2	*Практическая работа № 50. Миграция ПО ViPNet Administrator.*		
		Самостоятельная работа	2	
	1	*Практическая работа № 51. Модификация защищенной сети.*		
		Практические занятия	4	
	1	*Практическая работа № 52. Смена пароля администратора УКЦ. Смена мастер-ключей. Формирование нового сертификата ключа проверки электронной подписи.*		
	2	*Практическая работа № 53. Компрометация ключей пользователя.*		
Тема 2.4. *Центр управления политиками безопасности ViPNet Policy Manager*		**Содержание учебного материала**	2	2
	1	*Принципы централизованного управления политиками безопасности сетевых узлов. Основные возможности ViPNet Policy Manager. Формирование результирующей политики безопасности.*		
		Практические занятия	2	
	1	*Практическая работа № 54. Настройка политик безопасности в ViPNet Policy Manager.*		
Тема 2.5. *Координатор*		**Содержание учебного материала**	12	2,3
	1	*Функциональные возможности Координатора. Общие принципы взаимодействия сетевых узлов (СУ). Сервер IP-адресов. Сервер-Маршрутизатор. Сервер-Межсетевой экран.*		
	2	*Режимы работы узлов VipNet.*		
	3	*Маршрутизация трафика. Общие сведения. Принципы формирования. Протокол OSPF. Статическая маршрутизация. Балансировка IP-трафика.*		
	4	*Обработка прикладных протоколов. Агрегация сетевых интерфейсов.*		
	5	*Туннелирование незащищенных узлов. Фильтрация трафика. Антиспуфинг.*		
	6	*Понятие технологии трансляции сетевых адресов NAT. Реализация NAT в Координаторе. Сервер открытого Интернета.*		

Тема 2.6. *Программно-аппаратный комплекс (ПАК) Координатор VipNet HW4*		**Содержание учебного материала**	8	2,3
	1	*ПАК VipNet Coordinator HW4. Назначение. Функциональные возможности. Общий обзор базовой линейки программно-аппаратных комплексов VipNet.*		
	2	*Администрирование. Сценарии применения ПАК.*		
	3	*Программное обеспечение ПАК VipNet Coordinator HW. Инсталляция ПО. Верификация образа ПО. Запись образа ПО на носитель. Развертывание ключевых баз.*		
	4	*Работа с командной строкой. Общие принципы работы с конфигурационными файлами.*		
		Самостоятельная работа	2	
	1	*Система защиты от сбоев. Режимы работы: одиночный режим, режим кластера.*		
		Содержание учебного материала	2	2
	1	*Удаленное управление ПАК. Работа с веб-интерфейсом.*		
		Практические занятия	20	
	1	*Практическая работа № 55. Межсетевое взаимодействие. Установка VipNet Coordinator в качестве межсетевого шлюза. Первоначальная настройка межсетевого взаимодействия.*		
	2	*Практическая работа № 56. Модификация межсетевого взаимодействия.*		
	3	*Практическая работа № 57. Firewall. Фильтры по умолчанию.*		
	4	*Практическая работа № 58. Фильтрация незащищенного локального трафика.*		
	5	*Практическая работа № 59. Фильтрация незащищенного транзитного трафика.*		
	6	*Практическая работа № 60. Включение антиспуфинга.*		
	7	*Практическая работа № 61. Настройка трансляции сетевых адресов.*		
	8	*Практическая работа № 62. Фильтрация защищенного трафика.*		

	9	*Практическая работа № 63. Настройка Автономного режима*.		
	10	*Практическая работа № 64. Настройка полутуннеля.*		
		Самостоятельная работа	4	
	1	*Практическая работа № 65. Сохранение настроек ПАК.*		
	2	*Практическая работа № 66. Настройка расписания в правилах фильтрации.*		
		Практические занятия	16	
	1	*Практическая работа № 67. Агрегация каналов.*		
	2	*Практическая работа № 68. Включение и настройка протокола динамической маршрутизации OSPF.*		
	3	*Практическая работа № 69. Настройка кластера горячего резервирования.*		
	4	*Практическая работа № 70. Криптопровайдер* VipNet CSP. Работа с сертификатами. Работа с ЭП.		
	5	*Практическая работа № 71. Работа с приложениями VipNet. Установка прямого взаимодействия по каналу MFTP.*		
	6	*Практическая работа № 72. Настройка автопроцессинга в программе ViPNet Деловая почта.*		
	7	*Практическая работа № 73. Настройка взаимодействия сетей ViPNet.*		
	8	*Практическая работа № 74. Настройка межсетевого взаимодействия после компрометации ключевой информации.*		
Промежуточная аттестация экзамен				
Виды самостоятельной работы при изучении МДК.03.03 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (в том числе учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.				
УП.03 Учебная практика			**216**	

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;* – *конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п.;* – *установка и настройка системы корпоративной защиты от внутренних угроз;* – *самостоятельный поиск и устранение неисправностей при развёртывании и настройке системы корпоративной защиты от внутренних угроз;* – *установка и настройка агентского мониторинга;* – *проведение синхронизация с LDAP-сервером;* – *запуск системы корпоративной защиты от внутренних угроз, проверка ее работоспособности.* – *проведение имитации процесса утечки конфиденциальной информации в системе;*		

– *настройка защищенного домена, групповых политик AD;* – *создание и установка цифровых сертификатов;* – *настройка защищенного соединения между элементами сетевой инфраструктуры: SSH, HTTPS и т.п.* – *исследование (аудит) организации с целью защиты от внутренних угроз;* – *разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз;* – *разработка новых и/или модификация существующих политик безопасности, перекрывающие каналы передачи данных и возможные инциденты;* – *разработать или/и модификация объектов защиты, категорий, технологий защиты в DLP-системе и т.п.;* – *использование различных технологий защиты: печатей, бланков, графических объектов, баз данных и т.п.;* – *занесение политик информационной безопасности в DLP систему;* – *модификация политик безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата;* – *применение политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизирование числа выявленных инцидентов безопасности;* – *работа с интерфейсом управления системы корпоративной защиты информации;* – *применение технологии анализа и защиты сетевого трафика;* – *применение технологии агентского мониторинга;* – *разработка и применение политики агентского мониторинга для работы с носителями и устройствами;* – *разработка и применение политики агентского мониторинга для работы с файлами;* – *работа с исключениями из перехвата;* – *защита узлов. Групповые политики AD, файерволы и т.п.;* – *проведение анализа выявленных инцидентов;* – *подготовка отчётов о нарушениях;* – *применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов;* – *проведение классификации уровня угроз инцидентов;*		

– *разработка плана по дальнейшему расследованию выявленных инцидентов и противодействию нарушителям с опорой на нормативную базу;* – *развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре;* – *развёртывание, настройка и проверка работоспособности IDS-системы на существующей и вычислительной инфраструктуре;* – *работа с узлами и пользователями VPN;* – *компрометация узлов, ключей, пользователей VPN. Восстановление связи. Обновление ключевой информации VPN;* – *межсетевое взаимодействие и туннелированные VPN;* – *применение централизованных политик безопасности VPN. Защита рабочих мест.* ***Дифференцированный зачет***		
ПП.03 Производственная практика профессионального модуля **Виды работ** – участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; – участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; – участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам; – *техническое обслуживание средств защиты информации;* – *участие в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности;* – *проведение контрольных проверок работоспособности и эффективности действующих систем и технических средств защиты информации, составление и оформление акты контрольных проверок;* – применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами; – участия в мониторинге эффективности технических средств защиты информации; – диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации;	**216**	

– проведение 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; – проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты; – применение технических средств для криптографической защиты информации конфиденциального характера; – применение технических средств для уничтожения информации и носителей информации; – *оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу;* – *проведение статистического анализа загрузки заданного диапазона и обнаружения радиозакладных устройств в защищаемом помещении;* – *проведение технического обслуживания и устранение выявленных неисправностей технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок;* – *оценка защищенности телефонных каналов;* – *оценка защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств;* – *проведение испытания защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами;* – *организация технического контроля эффективности мер защиты информации;* – *разработка проекта системы видеонаблюдения для организации;* – *изучение структуры организации на основании полученных материалов («модели организации»), проведение обследования корпоративных информационных систем;* – *определение объектов защиты предприятия;* – *разработка перечня субъектов/персон, роли пользователей, прав доступа в корпоративные информационные системы организации;*		

– *определение каналов передачи данных и потенциальных утечек информации в корпоративной информационной системе;* – *определение типов циркулирующих данных в корпоративной информационной системе;* – *выявление потоков передачи данных и возможные каналы утечки информации в корпоративной информационной системе;* – *разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз;* – *разработка новых и/или модификация существующих политик безопасности, перекрывающие каналы передачи данных и возможные инциденты;* – *использование различных технологий защиты: печатей, бланков, графических объектов, баз данных и т.п.;* – *применение политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизирование числа выявленных инцидентов безопасности;* – *заполнение шаблона модели угроз;* – *подготовка отчёта о результатах аудита, включая потоки данных, потенциальные каналы утечек, уровни рисков роли пользователей, объекты защиты (с привязкой к нормативной базе и методикам оценки последствий), ролями пользователей и т.п.* – *определить перечень нормативных актов РФ, задействованных в рамках модели угроз;* – *разработка перечня, описание и шаблонов нормативно правовых документов организации по легальному применению корпоративной защиты от внутренних угроз информационной безопасности;* ***Дифференцированный зачет***		
Экзамен по профессиональному модулю		
Всего	***992***	

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

- лекционные аудитории с мультимедийным оборудованием;
- лаборатория «Технических средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест по числу обучающихся, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

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

- рабочие места студентов, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- аппаратные средства аутентификации пользователя;
- средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок;
- средства измерения параметров физических полей;
- стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;
- рабочее место преподавателя;
- учебно-методическое обеспечение модуля;
- мультимедийный проектор, персональный компьютер, комплект презентаций.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.

2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.

4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2021. – 336с

5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2018.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2018

7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2019

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.

3.2.2. 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 .

3.2.3 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

3.3. Общие требования к организации образовательного процесса

3.3.1. Для реализации программы профессионального модуля предусмотрены следующие специальные организационные условия образовательного процесса:

Освоение профессионального модуля ПМ.03 Защита информации техническими средствами производится в соответствии с учебным планом по специальности 10.02.05 Организация и технология защиты информации и календарным графиком.

Образовательный процесс организуется строго по расписанию занятий. График освоения профессионального модуля предполагает последовательное освоение профессионального модуля, включающего в себя изучение междисциплинарных курсов МДК.03.01 Техническая защита информации, МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации, МДК 03.03 Корпоративная защита от внутренних угроз информационной безопасности, учебную и производственную практики.

В процессе освоения профессионального модуля предполагается проведение рубежного контроля знаний, умений у студентов. Сдача рубежного контроля является обязательной для всех обучающихся. Результатом освоения профессионального модуля выступают профессиональные компетенции, оценка которых представляет собой создание и сбор свидетельств деятельности на основе заранее определенных критериев.

С целью оказания помощи студентам при освоении теоретического и практического материала, выполнения самостоятельной работы разрабатываются учебно-методические комплексы.

При освоении профессионального модуля каждым преподавателем устанавливаются часы дополнительных занятий, в рамках которых для студентов

проводятся консультации. График проведения консультаций доводится до сведений студентам.

При проведении практических занятий, учебной практики предусмотрено деление учебной группы студентов на две подгруппы.

УП.03. Учебная практика проводится концентрированно после освоения разделов: МДК.03.01 Техническая защита информации и сдачи экзамена, МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации и сдачи дифференцированного зачета, МДК 03.03 Корпоративная защита от внутренних угроз информационной безопасности и сдачи экзамена.

ПП.03. Производственная практика проводится концентрированно, после полного завершения изучения теоретического и практического курса разделов МДК.03.01 Техническая защита информации, МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации, МДК 03.03 Корпоративная защита от внутренних угроз информационной безопасности и УП.03. Учебная практика. Формой промежуточного контроля ПП.03. Производственная практика является дифференцированный зачет.

Освоению ПМ.03 Защита информации техническими средствами предшествует изучение дисциплин: ОУД.07. Информатика, ЕН.02. Информатика, ОП.01 Основы информационной безопасности, ОП.02 Организационно-правовое обеспечение информационной безопасности, ОП.03 Основы алгоритмизации и программирования, ОП.04 Электроника и схемотехника, ОП.07 Технические средства информатизации, ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении, ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами, ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

3.3.2. Кадровое обеспечение образовательного процесса

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: связь, информационные и коммуникационные технологии, обеспечение безопасности (имеющих стаж работы в данной профессиональной области не менее 3 лет).

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.

3.3.2.1. Требования к квалификации педагогических кадров, осуществляющих руководство практикой

Инженерно-педагогический состав: дипломированные специалисты — преподаватели междисциплинарных курсов, а также общепрофессиональных дисциплин.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы 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 и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, 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, 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, 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, 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, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.6. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах	*Проводить работы с защищенными автоматизированными системами. Передавать информацию по защищенным каналам связи*	тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.7. Выявлять и анализировать возможные угрозы информационной безопасности объектов	*Проявлять умения и практический опыт выявления возможных угроз информационной*	тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач,

		оценка процесса и результатов выполнения видов работ на практике
ПК 3.8. Ориентироваться в условиях частой смены технологий в профессиональной деятельности	*Иметь практический опыт выявления возможных угроз информационной безопасности объектов защиты*	тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК.3.9. Проводить регламентные работы и фиксировать отказы средств защиты	*Фиксировать отказы в работе средств вычислительной техники*	тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
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	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
ОП 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, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной 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	- эффективность использования информационно-коммуникационных	

профессиональной деятельности.	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.	