

**Санкт-Петербургское государственное бюджетное профессиональное  
образовательное учреждение  
«Академия управления городской средой, градостроительства и печати»**

**ПРИНЯТО**

На заседании педагогического совета  
Протокол № 3

«05» июля 2022г



**РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ  
ПМ.03 «ПРОГРАММНО-АППАРАТНЫЕ И ТЕХНИЧЕСКИЕ  
СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»**

для специальности 10.02.01 «Организация и технология защиты информации»

среднего профессионального образования

(базовой подготовки)

Санкт-Петербург

2022 г.

ОДОБРЕНА  
Цикловой комиссией  
Общетехнических дисциплин  
и компьютерных технологий  
Протокол № 9  
от «24» мая 2022 г.

  
\_\_\_\_\_ Андреев В.В.

РАССМОТРЕНА  
Методическим советом  
«АУГСГиП»  
Протокол № 6  
от «28» июня 2022 г.

Рабочая программа профессионального модуля ПМ.03 «Программно-аппаратные и технические средства защиты информации» разработана на основе Федерального государственного образовательного стандарта по специальности 10.02.01 «Организация и технология защиты информации»

**Разработчик:**

Андреев В.В., преподаватель СПб ГБПОУ «Академия управления городской средой, градостроительства и печати»

## **СОДЕРЖАНИЕ**

- 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ

## ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### ПМ.03 «Программно-аппаратные и технические средства защиты информации»

#### 1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности - «Программно-аппаратные и технические средства защиты информации» и профессиональные компетенции:

##### 1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности
ОК 10	Применять математический аппарат для решения профессиональных задач.
ОК 11	Оценивать значимость документов, применяемых в профессиональной деятельности.
ОК 12	Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

##### 1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ПК 3.1	Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах
ПК 3.2	Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3	Проводить регламентные работы и фиксировать отказы средств защиты.
ПК 3.4	Выявлять и анализировать возможные угрозы информационной безопасности объектов

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none"> <li>– участия в эксплуатации систем и средств защиты информации защищаемых объектов;</li> <li>– применения технических средств защиты информации;</li> <li>– выявления возможных угроз информационной безопасности объектов защиты;</li> </ul>
уметь	<ul style="list-style-type: none"> <li>– работать с техническими средствами защиты информации;</li> <li>– работать с защищенными автоматизированными системами;</li> <li>– передавать информацию по защищенным каналам связи;</li> <li>– фиксировать отказы в работе средств вычислительной техники;</li> </ul>
знать	<ul style="list-style-type: none"> <li>– виды, источники и носители защищаемой информации;</li> <li>– источники опасных сигналов;</li> <li>– структуру, классификацию и основные характеристики технических каналов утечки информации;</li> <li>– классификацию технических разведок и методы противодействия им;</li> <li>– методы и средства технической защиты информации;</li> <li>– методы скрытия информации;</li> <li>– программно-аппаратные средства защиты информации;</li> <li>– структуру подсистемы безопасности операционных систем и выполняемые ею функции;</li> <li>– средства защиты в вычислительных сетях;</li> <li>– средства обеспечения защиты информации в системах управления базами данных;</li> <li>– критерии защищенности компьютерных систем;</li> <li>– методики проверки защищенности объектов информатизации на соответствие требованиям нормативных правовых актов.</li> </ul>

## 1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 705 часов,

из них на освоение МДК 326 часов,

на практики, в том числе учебную 144 часов и производственную 72 часа,

самостоятельная работа – 163 часа.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ПМ.03) «Программно-аппаратные и технические средства защиты информации»

### 2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, ак. час.						Самостоятельная работа	
			Работа обучающихся во взаимодействии с преподавателем					Учебная		Производственная
			Обучение по МДК			Практики				
			Всего	В том числе		Курсовых работ (проектов)	Производственная			
Лабораторных и практических занятий		Учебная								
1	2	3	4	5	6	7	8	9		
ПК 3.1 – ПК 3.4 ОК1-ОК12	Раздел 1. Технические методы и средства, технологии защиты информации	264	176	52	20			88		
ПК 3.1 – ПК 3.4 ОК1-ОК12	Раздел 2. Программно-аппаратные средства защиты информации	225	150	38				75		
ПК 3.1 – ПК 3.4 ОК1-ОК12	Учебная практика	144	144			144				
ПК 3.1 – ПК 3.4 ОК1-ОК12	Производственная практика (по профилю специальности), часов	72					72			
	<b>Всего:</b>	<b>705</b>	<b>470</b>	<b>90</b>	<b>20</b>	<b>144</b>	<b>72</b>	<b>163</b>		

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

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
<b>ПМ.03 Программно-аппаратные и технические средства защиты информации</b>		<b>705</b>	
<b>Раздел 1 Технические методы и средства, технологии защиты информации</b>		<b>264</b>	
<b>Тема 1.1. Предмет и задачи технической защиты информации</b>	<b>Содержание учебного материала</b>	<b>6</b>	1
	1.1.1. Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.	2	
	1.1.2. Задачи и требования к способам и средствам защиты информации техническими средствами.	2	
	1.1.3. Нормативно-правовые документы по технической защите информации	2	
<b>Тема 1.2. Информация как объект защиты техническими средствами.</b>	<b>Содержание учебного материала</b>	<b>8</b>	1
	1.2.1. Информация как объект защиты техническими средствами. Виды, источники и носители защищаемой информации.	2	
	1.2.2. Свойства информации, влияющие на возможности ее защиты техническими средствами.	2	
	1.2.3. Демаскирующие признаки объектов защиты.	2	
	1.2.4. Виды угроз безопасности информации, защищаемой техническими средствами. Источники опасных сигналов.	2	
<b>Тема 1.3. Технические каналы утечки информации</b>	<b>Содержание учебного материала</b>	<b>10</b>	1
	1.3.1. Технические каналы утечки, классификация	2	
	1.3.2. Каналы утечки речевой информации	2	
	1.3.3. Каналы утечки информации, обрабатываемой ТСПИ	2	
	1.3.4. Каналы утечки информации при ее передаче по каналам связи	2	
	1.3.5. Технические каналы утечки видовой информации	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	<b>Практические занятия</b>	<b>2</b>	2
	<b>Практическое занятие № 1.</b> Анализ возможных технических каналов утечки информации, подбор средств и методов их защиты	2	
<b>Тема 1.4. Средства технической разведки</b>	<b>Содержание учебного материала</b>	<b>4</b>	1
	1.4.1. Классификация технических разведок. Методы и средства защиты от технической разведки	2	
	1.4.2. Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.	2	
	<b>Практические занятия</b>	<b>6</b>	
	<b>Практическое занятие №2.</b> Разработка плана применения технических мер по предотвращению проникновения злоумышленника к источникам информации.	2	
	<b>Практическое занятие № 3.</b> Сравнительный анализ технических средств обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации.	2	
<b>Тема 1.5. Защита от утечки информации по акустическому каналу</b>	<b>Содержание учебного материала</b>	<b>16</b>	1
	1.5.1. Общие сведения о закладных устройствах. Радиозакладки.	2	
	1.5.2. Приемники излучения радиозакладных устройств. Закладные устройства с передачей информации по проводным каналам.	2	
	1.5.3. Микрофон. Акустические антенны. Комбинированные микрофоны. Групповые микрофоны.	2	
	1.5.4 Средства обеспечения скрытности оперативной звукозаписи. Аппаратура звукозаписи.	2	
	1.5.5 Цифровые диктофоны. Обнаружители диктофонов.	2	
	1.5.6. Факторы, влияющие на качество звукозаписи. Выбор типа микрофона и места его установки.	2	



Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	1.5.7. Защита от акустического канала утечки информации	2	2
	1.5.8. Перехват речевой информации с использованием радиоканала. Оптико-акустическая аппаратура перехвата речевой информации	2	
	<b>Практические занятия</b>	<b>4</b>	
	<b>Практическое занятие № 5.</b> Сравнительный анализ микрофонов.	2	
	<b>Практическое занятие № 6.</b> Сравнительный анализ диктофонов.	2	
<b>Тема 1.6. Защита информации от утечек по материально-вещественному каналу</b>	<b>Содержание учебного материала</b>	<b>4</b>	1
	1.6.1. Структура вещественных каналов. Методы получения информации с использованием вещественных каналов	2	
	1.6.2. Защита информации от утечки по материально-вещественным каналам	2	
<b>Тема 1.7. Защита от утечки информации по оптическому каналу</b>	<b>Содержание учебного материала</b>	<b>4</b>	1
	1.7.1. Характеристики оптического канала утечки информации	2	
	1.7.2. Устройства съема данных. Предотвращение утечки информации по оптическим каналам	2	
<b>Тема 1.8. Защита информации от электрических и электромагнитных каналов утечки информации</b>	<b>Содержание учебного материала</b>	<b>4</b>	1
	1.8.1. Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок	2	
	1.8.2. Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.	2	
	<b>Практические занятия</b>	<b>6</b>	2
	<b>Практическое занятие № 7.</b> Определение порядка работы с техническими средствами защиты речевой информации в телефонных линиях	2	
	<b>Практическое занятие № 8.</b> Составление инструкции для работы с техническими средствами защиты от утечек информации по проводным линиям	2	
	<b>Практическое занятие № 9 .</b> Составление инструкции для работы с устройствами защиты от прослушивания проводных телефонных линий.	2	
<b>Тема 1.9. Технические средства добывания</b>	<b>Содержание учебного материала</b>	<b>10</b>	1
	1.9.1. Технические средства добывания информации. Классификация средств	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
<b>информации</b>	добывания информации		
	1.9.2. Оптическая разведка. Радиоэлектронная разведка	2	
	1.9.3. Акустическая разведка	2	
	1.9.4. Добывание информации без физического проникновения в контролируемую зону	2	
	1.9.5. Специальные технические средства, предназначенные для негласного получения информации. Ответственность, предусмотренная законодательством за их незаконный оборот	2	
<b>Тема 1.10. Средства выявления каналов утечки информации</b>	<b>Содержание учебного материала</b>	<b>12</b>	1
	1.10.1. Индикаторы электромагнитного поля	2	
	1.10.2. Сканирующие радиоприемники	2	
	1.10.3. Анализаторы спектра, радиочастотомеры	2	
	1.10.4. Многофункциональные комплекты для выявления каналов утечки информации	2	
	1.10.5. Нелинейные локаторы. Комплексы измерения ПЭМИН	2	
	1.10.6. Металлодетекторы. Металлоискатели. Досмотровые эндоскопы	2	
<b>Практические занятия</b>	<b>2</b>	2	
<b>Практическое занятие № 10.</b> Обнаружение закладных устройств нелинейным локатором	2		
<b>Тема 1.11. Технические методы и средства защиты информации</b>	<b>Содержание учебного материала</b>	<b>22</b>	1
	1.11.1. Средства технической защиты информации. Классификация устройств технической защиты информации.	2	
	1.11.2. Концепция и методы инженерно-технической защиты информации	2	
	1.11.3. Экранирование электромагнитных волн. Устройства контроля и защиты слаботочных линий и сети	2	
	1.11.4. Электромагнитное экранирование и развязывающие цепи. Экранированные помещения	2	
	1.11.5. Фильтрация информационных сигналов. Помехоподавляющие фильтры	2	
	1.11.6. Пространственное и линейное зашумление	2	
	1.11.7. Подавление емкостных паразитных связей. Устройства контроля и защиты проводных линий от утечки информации	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	1.11.8. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам	2	2
	1.11.9. Заземление технических средств и подавление информационных сигналов в цепях заземления	2	
	1.11.10. Устройства контроля и защиты слаботочных линий и сети.	2	
	1.11.11. Комплексы радиомониторинга.	2	
	<b>Практические занятия</b>	<b>24</b>	
	<b>Практическое занятие № 11.</b> Решение ситуационных задач. Оценка вероятности утечки речевой информации.	2	
	<b>Практическое занятие № 12.</b> Работа с системой защиты «ГРОМ-ЗИ»	2	
	<b>Практическое занятие № 13.</b> Работа с КАЗ РИ «Орбита-3»	2	
	<b>Практическое занятие № 14.</b> Решение ситуационных задач. Оценка вероятности утечки видовой информации.	2	
	<b>Практическое занятие № 15.</b> Разработка системы инженерно-технической защиты информации	2	
	<b>Практическое занятие № 16.</b> Сравнительный анализ генераторов шума	2	
	<b>Практическое занятие № 17.</b> Сравнительный анализ средств для поиска электромагнитных излучений	2	
	<b>Практическое занятие № 18.</b> Работа с тепловизором	2	
	<b>Практическое занятие № 19.</b> Работа с виброакустическим средством Соната	2	
	<b>Практическое занятие № 20.</b> Работа с сетевыми помехоподавляющими фильтрами и генераторами	2	
	<b>Практическое занятие № 21.</b> Методы и средства съема информации с телефонных линий.	2	
<b>Практическое занятие № 22.</b> Прослушивание помещений высокочастотным навязыванием.	2		
<b>Тема 1.12. Разработка комплекса мер технической защиты информации в</b>	<b>Содержание учебного материала</b>	<b>4</b>	1
	1.11.1. Структура разработки комплекса мер технической защиты информации в организации	2	
	1.11.2. Подготовка документации по технической защите в организации	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
организации	<b>Практические занятия</b>	<b>8</b>	2
	<b>Практическое занятие № 23.</b> Анализ деятельности организации, защищаемой информации, средств технической защиты организации	2	
	<b>Практическое занятие № 24.</b> Разработка схемы технической защиты информации организации	2	
	<b>Практическое занятие № 25.</b> Определение вариантов дополнительных мер защиты с оценкой затрат на их обеспечение, выбор рациональных вариантов.	2	
	<b>Практическое занятие № 26.</b> Подготовка технической документации для выбранных средств и методов технической защиты	2	
	<b>Дифференцированный зачет</b>	2	
<b>Самостоятельная работа</b>			
Заполнение рабочей тетради для самостоятельных работ по МДК.03.01 в СДО на платформе Moodle		88	
<b>Раздел 2. Программно-аппаратные средства защиты информации</b>		<b>150</b>	
<b>Тема 2.1 Общие понятия программно-аппаратных средств защиты информации</b>	<b>Содержание учебного материала</b>	<b>4</b>	1
	2.1.1. Виды программно-аппаратных средств защиты информации. Понятие комплексных решений.	2	
	2.1.2. Методы скрытия информации	2	
<b>Тема 2.2. Защита программ и данных</b>	<b>Содержание учебного материала</b>	<b>10</b>	1
	2.2.1. Структура и функции подсистемы безопасности операционных систем	2	
	2.2.2. Подсистема безопасности Windows.	2	
	2.2.3. Подсистема безопасности Linux	2	
	2.2.4. Средства обеспечения защиты информации в системах управления базами данных	2	
	2.2.5. Критерии защищённости компьютерных систем.	2	
<b>Тема 2.3. Защита в компьютерных сетях</b>	<b>Содержание учебного материала</b>	<b>12</b>	1
	2.3.1. Методы защиты компьютерных сетей	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	2.3.2. Средства защиты в вычислительных сетях	2	
	2.3.3. Защита информации в VPN-сетях	2	
	2.3.4. Защита электронной почты	2	
	2.3.5. Защита web-приложений от мошенничества	2	
	2.3.6. Защита электронной подписи	2	
<b>Тема 2.4. Антивирусная защита данных</b>	<b>Содержание учебного материала</b>	<b>4</b>	1
	2.4.1. Защита от вредоносного ПО	2	
	2.4.2. Современные программные средства для защиты от вредоносных программ	2	
<b>Тема 2.5. Криптографические методы и средства обеспечения информационной безопасности</b>	<b>Содержание учебного материала</b>	<b>8</b>	1
	2.5.1. Основные понятия криптографической защиты информации	2	
	2.5.2. Симметричные криптосистемы шифрования	2	
	2.5.3 Асимметричные криптосистемы шифрования	2	
	2.5.4. Криптографические алгоритмы	2	
<b>Тема 2.6. Средства защиты на компьютерах с операционной системой Windows</b>	<b>Содержание учебного материала</b>	<b>14</b>	1
	2.6.1. Использование Active Directory и политик безопасности. Понятие домена. Роли контроллера домена	2	
	2.6.2. Создание и внесение пользователей и компьютеров в домен	2	
	2.6.3 Локальные политики домена	2	
	2.6.4 Глобальные политики домена	2	
	2.6.5. Разграничение прав доступа	2	
	2.6.6. Средства защиты информации Dallas Lock. Возможности Dallas Lock. Принцип работы. Параметры установки	2	
	2.6.7. Средство доверенной загрузки Secret Net Studio . Возможности Secret Net Studio. Принцип работы. Параметры установки	2	
	<b>Практические занятия</b>	<b>6</b>	2

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	<b>Практическое занятие № 1</b> Установка серверной версии Windows. Установка и настройка домена Active Directory	2	
	<b>Практическое занятие № 2</b> Создание и применение глобальных политик домена	2	
	<b>Практическое занятие № 3</b> Создание и применение локальных политик домена	2	
<b>Тема 2.7 Методики проверки защищённости объектов информатизации</b>	<b>Содержание учебного материала</b>	<b>4</b>	1
	2.7.1. Методики проверки защищённости объектов информатизации на соответствие требованиям нормативных правовых актов	2	
	2.7.2. Нормативно-методические документы, регламентирующие порядок проведения аттестации объектов информатизации и содержащие требования к объектам информатизации	2	
	<b>Практические занятия</b>	<b>2</b>	
	<b>Практическое занятие № 4</b> Работа с требованиями и рекомендациями по технической защите конфиденциальной информации	2	
<b>Тема 2.8. Использование DLP-системы Infowatch для защиты от внутренних утечек информации</b>	<b>Содержание учебного материала</b>	<b>26</b>	1
	2.8.1. Общая характеристика и принципы функционирования dlp-системы Infowatch	2	
	2.8.2. Виды политик, способы их создания в Traffic monitor	2	
	2.8.3. Принципы построения регулярных выражений для создания политик	2	
	2.8.4. Виды правил и способы создания правил в Device monitor	2	
	2.8.5. Работа с Задачами и Журналом в Device monitor	2	
	2.8.6. Добавление ролей, редактирование ролей, удаление ролей в Traffic monitor	2	
	2.8.7. Работа с терминами и списками в Traffic monitor	2	
	2.8.8. Работа с тегами и объектами в Traffic monitor	2	
	2.8.9. Создание политик контроля персон в Traffic monitor	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	2.8.10. Правила передачи в Traffic monitor	2	
	2.8.11. Правила хранения в Traffic monitor	2	
	2.8.12. Правила копирования в Traffic monitor	2	
	2.8.13. Отчёты в Traffic Monitor	2	
	<b>Практические занятия</b>	<b>16</b>	2
	<b>Практическое занятие № 5</b> Установка и настройка Traffic monitor	2	
	<b>Практическое занятие № 6</b> Установка и настройка Device monitor	2	
	<b>Практическое занятие № 7</b> Установка клиента Device monitor	2	
	<b>Практическое занятие № 8</b> Создание правил и проверка их работоспособности в Device monitor	2	
	<b>Практическое занятие № 9</b> Создание правил с использованием «белых» и «чёрных» списков в Device monitor	2	
	<b>Практическое занятие № 10</b> Создание политик защиты данных в Traffic monitor	2	
	<b>Практическое занятие № 11</b> Создание политик с использованием регулярных выражений в Traffic monitor	2	
<b>Практическое занятие № 12</b> Создание и изменение отчётов в Traffic Monitor	2		
<b>Тема 2.9. Использование программно-аппаратных средств для создания защищённой сети</b>	<b>Содержание учебного материала</b>	<b>10</b>	1
	2.9.1. Общая характеристика продуктов ViPNet для создания защищённой сети	2	
	2.9.2. Понятие построения виртуальной защищённой сети	2	
	2.9.3. Компрометация ключей в защищённой сети ViPNet	2	
	2.9.4. Настройка политик безопасности в VipNet Policy Manager	2	
	2.9.5. Организация межсетевое взаимодействия. Модификация межсетевого взаимодействия в защищённой сети ViPNet	2	
	<b>Практические занятия</b>	<b>8</b>	2

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	<b>Практическое занятие № 13</b> Развёртывание защищённой сети VipNet. Учет отказов в работе средств вычислительной техники.	2	
	<b>Практическое занятие № 14</b> Создание структуры защищённой сети VipNet	2	
	<b>Практическое занятие № 15</b> Создание защищённой сети VipNet	2	
	<b>Практическое занятие № 16</b> Модификация защищённой сети VipNet	2	
<b>Тема 2.10. Защита передачи данных через Интернет</b>	<b>Содержание учебного материала</b>	<b>10</b>	
	2.10.1. Понятие https. Технология Secure Socket Layer (SSL)	2	
	2.10.2. Сертификаты, подписанные центром сертификации (CA). Сертификаты домена Самозаверяющие сертификаты	2	
	2.10.3. Установка openssl	2	
	2.10.4. Установка Nginx для последующей настройки прокси-сервера	2	
	2.10.5. Настройка правильной работы ssl	2	
	<b>Практические занятия</b>	<b>2</b>	
	<b>Практическое занятие № 17</b> Настройка прокси-сервера с помощью Nginx	2	
<b>Тема 2.11 Средства защиты на компьютерах с операционной системой Linux</b>	<b>Содержание учебного материала</b>	<b>8</b>	
	2.11.1. Средства защиты компьютерных сетей с использованием Samba и политик безопасности на Linux-сервере. Особенности серверов на Linux.	2	
	2.11.2. Программные средства для поднятия контроллера домена на Linux	2	
	2.11.3. Принципы использования систем обнаружения вторжения	2	
	2.10.4. Синтаксис написания правил для IDS систем	2	
	<b>Практические занятия</b>	<b>4</b>	
	<b>Практическое занятие № 18</b> Установка и настройка VipNet IDS	2	
	<b>Практическое занятие № 19</b> Написание правил для VipNet IDS	2	
<b>Дифференцированный зачет</b>	<b>2</b>		
<b>Внеаудиторная (самостоятельная) учебная работа при изучении раздела</b> Заполнение рабочей тетради для самостоятельных работ по МДК.03.02 в СДО на платформе Moodle		<b>75</b>	



Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
<b>Курсовая работа</b>			
<b>Тематика курсовых работ</b> <b>«» по индивидуальным вариантам</b>		20	
<p>Обязательные аудиторные учебные занятия по курсовой работе:</p> <ol style="list-style-type: none"> <li>1. Распределение тем. Выдача задания на курсовую работу. Правила оформления курсовой работы</li> <li>2. Составление плана теоретической части курсовой работы. Составление Введения</li> <li>3. Выполнение теоретической части</li> <li>4. Выполнение практической части</li> <li>5. Составление Заключения</li> <li>6. Подготовка доклада для защиты курсовой работы</li> <li>7. Подготовка презентации для защиты курсовой работы</li> <li>8. Защита курсовой работы</li> </ol>			
<b>Учебная практика</b>		<b>144</b>	
<ol style="list-style-type: none"> <li>1. Составление номенклатуры необходимых программно-аппаратных средств защиты информации на защищаемом объекте</li> <li>2. Составление номенклатуры необходимых технических средств защиты информации на защищаемом объекте</li> <li>3. Разработка системы инженерно-технической защиты информации на защищаемом объекте</li> <li>4. Разработка схемы технической защиты информации на защищаемом объекте</li> <li>5. Подготовка технической документации для выбранных средств и методов технической защиты</li> <li>6. Расчёт стоимости необходимых программно-аппаратных средств защиты информации на защищаемом объекте</li> <li>7. Расчёт стоимости необходимых технических средств защиты информации на защищаемом объекте</li> <li>8. Установка домена для последующего использования локальных и глобальных политик безопасности на защищаемом объекте</li> <li>9. Настройка домена для последующего использования локальных и глобальных политик безопасности на защищаемом объекте</li> <li>10. Создание и применение локальных и глобальных политик безопасности в сети на защищаемом объекте</li> <li>11. Создание пользователей домена с различными уровнями прав на защищаемом объекте</li> <li>12. Установка средств доверенной загрузки ОС на рабочей станции, работающей под ОС Windows с помощью</li> </ol>			

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	<p>программно-аппаратных комплексов средств защиты информации</p> <p>13. Настройка средств доверенной загрузки ОС на рабочей станции, работающей под ОС Linux с помощью программно-аппаратных комплексов средств защиты информации</p> <p>14. Создание индивидуальной для пользователя изолированной рабочей программной среды в ОС Windows с помощью программно-аппаратных комплексов средств защиты информации</p> <p>15. Проверка корректной работы изолированной рабочей программной среды в ОС Windows</p> <p>16. Подбор программных средств для защиты от вредоносных программ на защищаемом объекте</p> <p>17. Установка в сети программных средств для защиты от вредоносных программ на защищаемом объекте</p> <p>18. Проверка на корректную работу программных средств для защиты от вредоносных программ на защищаемом объекте</p> <p>19. Установка серверной версии ОС Linux для последующей установки сетевого экрана для защиты информации от внешних атак</p> <p>20. Установка межсетевое экрана для защиты инфраструктуры защищаемого объекта</p> <p>21. Настройка межсетевое экрана для защиты инфраструктуры защищаемого объекта</p> <p>22. Проверка работоспособности межсетевое экрана для защиты инфраструктуры</p> <p>23. Модификация настроек межсетевое экрана для защиты инфраструктуры защищаемого объекта</p> <p>24. Установка системы обнаружения вторжений</p> <p>25. Настройка системы обнаружения вторжений</p> <p>26. Создание первичных правил для системы обнаружения вторжений</p> <p>27. Проверка работоспособности правил, написанных для системы обнаружения вторжений</p> <p>28. Корректировка правил и создание дополнительных правил для системы обнаружения вторжения</p> <p>29. Установка виртуальной машины для последующей эмуляции вторжений</p> <p>30. Эмуляция вторжений для анализа информационной безопасности объекта</p> <p>31. Выявление попыток вторжения с помощью системы обнаружения вторжений</p> <p>32. Исправление настройки системы обнаружения вторжений после выявления вторжений</p> <p>33. Применение средств доверенной загрузки ОС на рабочей станции, работающей под ОС Linux с помощью программно-аппаратных комплексов средств защиты информации</p> <p>34. Создание индивидуальной для пользователя изолированной рабочей программной среды в ОС Linux с помощью программно-аппаратных комплексов средств защиты информации</p> <p>35. Проверка корректной работы изолированной рабочей программной среды в ОС Linux</p> <p>36. Настройка запрета запуска неразрешённых программ и разграничение доступа пользователей к массивам</p>		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	<p>данных и программ с помощью дискреционного контроля доступа</p> <p>37. Развёртывание DLP-системы (установка Traffic Monitor) для защиты от внутренних угроз</p> <p>38. Развёртывание DLP-системы (установка Device Monitor) для защиты от внутренних угроз</p> <p>39. Развёртывание DLP-системы (установка агента на рабочие станции) для защиты от внутренних угроз</p> <p>40. Первичная проверка работоспособности DLP-системы</p> <p>41. Установка дополнительного клиента IWDM на отдельную машину и создание нового пользователя – офицера безопасности</p> <p>42. Устранение неисправностей при развёртывании DLP-системы на защищаемом объекте</p> <p>43. Планирование защищённой сети VPN</p> <p>44. Развёртывание защищённой сети на основе технологий VPN</p> <p>45. Проверка работоспособности защищённой сети на основе технологии VPN</p> <p>46. Модификация защищённой сети на основе технологий VPN</p> <p>47. Применение защищённой сети для отправки деловой почты по защищённому каналу</p> <p>48. Применение защищённой сети для отправки документов по защищённому каналу</p> <p>49. Эмуляция компрометации ключей в защищённой сети</p> <p>50. Отработка действий в случае компрометации ключей в защищённой сети на основе технологий VPN</p> <p>51. Поднятие защищённой сети после компрометации ключей</p> <p>52. Настройка политик безопасности в защищённой сети на основе технологий VPN</p> <p>53. Первичная настройка межсетевого взаимодействия в защищённой сети на основе технологий VPN</p> <p>54. Модификация межсетевого взаимодействия в защищённой сети на основе технологий VPN</p> <p>55. Исправление ошибок после модификации межсетевого взаимодействия в защищённой сети</p> <p>56. Настройка межсетевого взаимодействия с применением асимметричного межсетевого мастер ключа</p> <p>57. Настройка туннелирования незащищённых узлов в защищённой сети на основе технологии VPN</p> <p>58. Добавление дополнительных незащищённых узлов при туннелировании в защищённой сети на основе технологии VPN</p> <p>59. Настройка фильтрации трафика в защищённой сети на основе технологии VPN</p> <p>60. Применение фильтрации трафика в защищённой сети на основе технологии VPN</p> <p>61. Применение DLP-системы для написания правил безопасности для применения на рабочих станциях</p> <p>62. Проверка работоспособности правил, выявление некорректной работы правил</p> <p>63. Корректировка агентских правил безопасности в DLP-системе</p> <p>64. Применение DLP-системы для написания простых политик безопасности для применения на рабочих</p>		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
	<p>станциях</p> <p>65. Проверка работоспособности простых политик безопасности, выявление некорректной работы политик безопасности</p> <p>66. Корректировка простых политик безопасности в DLP-системе</p> <p>67. Применение DLP-системы для защиты документов и печати защищаемого объекта</p> <p>68. Проверка работоспособности DLP-системы для защиты документов и печати защищаемого объекта</p> <p>69. Применение DLP-системы для написания сложных политик безопасности с лингвистическим разбором на защищаемом объекте</p> <p>70. Проверка работоспособности DLP-системы для написания сложных политик безопасности с лингвистическим разбором на защищаемом объекте</p> <p>71. Составление отчёта по событиям домена</p> <p>72. Фиксирование отказов средств защиты на основе отчёта по событиям домена на защищаемом объекте</p> <p>73. Составление отчёта по событиям системы на рабочей станции</p> <p>74. Ведение протокола регистрируемых событий в энергонезависимой памяти аппаратной части комплекса с помощью программно-аппаратных средств защиты информации</p> <p>75. Составление сводок по работе DLP-системы и выявление отказов средств защиты</p> <p>76. Составление виджетов по работе DLP-системы и выявление отказов средств защиты</p> <p>77. Составление отчётов по работе DLP-системы и выявление отказов средств защиты</p> <p>78. Составление на основе сводок, виджетом и отчётов по работе DLP-системы плана проведения работ по устранению отказов средств защиты</p> <p>79. Анализ возможных технических каналов утечки информации после проведённых работ по защите объекта</p> <p>80. Подбор дополнительных средств и методов защиты на защищаемом объекте</p> <p>81. Составление инструкции для работы с техническими средствами защиты от утечек информации по проводным линиям</p> <p>82. Разработка плана применения технических мер по предотвращению проникновения злоумышленника к источникам информации</p> <p>83. Составление списка возможных угроз информационной безопасности объекта</p> <p>84. Анализ внешних угроз информационной безопасности объекта</p> <p>85. Анализ внутренних угроз информационной безопасности объекта</p> <p>86. Расчёт эффективности применения средств защиты информации</p> <p>87. Сравнительный анализ продуктов SIEM</p>		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование	Объем часов	Уровень освоения
88. Подбор и расчёт стоимости продукта SIEM			
<b>Производственная практика</b>		<b>72</b>	
1.1. Ознакомление с основной деятельностью организации 1.2. Определение информационных активов организации 1.3. Ознакомление с используемыми техническими и инженерно-техническими средствами защиты информации в организации 1.4. Ознакомление с используемыми программно-аппаратными средствами защиты информации в организации 2.1. Выявление утечек информации по техническим каналам 2.2. Выявление утечек информации при эксплуатации программно-аппаратных средств 3.1. Фиксирование отказов средств защиты по техническим каналам 3.2. Фиксирование отказов средств защиты при эксплуатации программно-аппаратных средств		<b>72</b>	
<b>Всего по ПМ.03</b>		<b>705</b>	

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

#### **3.1. Требования к минимальному материально-техническому обеспечению**

Реализация учебной дисциплины требует наличия учебного кабинета «Ведение домашнего хозяйства», мастерской «Технологии уборочных работ».

Оборудование учебного кабинета:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно - наглядных пособий;
- стенд «Умный дом»;
- сантехнический комплекс;
- предметы сервировки стола;
- стенд энергоснабжения.

Технические средства обучения: компьютер, проектор, интерактивная доска, программное обеспечение.

Оборудование мастерской:

- поломоечные машины;
- однодисковые машины;
- подметальные машины;
- пылесосы;
- пылеводососы;
- экстракционная машина и пенный экстрактор для чистки ковров.

Реализация программы профессионального модуля (ПМ.01) «Обеспечение работ по ведению домашнего хозяйства» предполагает обязательную учебную и производственную практику.

Учебная практика реализуется в мастерской «Технологии уборочных работ». Производственная практика реализуется в организациях профиля ЖКХ и домашнего хозяйства, обеспечивающих деятельность обучающихся по овладению видом профессиональной деятельности (ВД 1) «Обеспечение работ по ведению домашнего хозяйства» и соответствующими ему профессиональными компетенциями.

### **3.2. Информационное обеспечение реализации программы**

#### **МДК 03.01 ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА, ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ**

##### **Основная литература**

Жук А. П. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — URL: <http://znanium.com>. — Режим доступа: по подписке.

Казарин О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для СПО/ О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — URL: <https://urait.ru>. — Режим доступа: по подписке.

##### **Дополнительная литература**

Емельянова Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Среднее профессиональное образование). — URL: <http://znanium.com>. — Режим доступа: по подписке.

Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. — Москва : ИД ФОРУМ : НИЦ ИНФРА-М, 2023. — 416 с.: ил. — (Среднее профессиональное образование). — URL: <http://znanium.com>. — Режим доступа: по подписке.

Ищейнов В. Я. Основные положения информационной безопасности : учебное пособие / В. Я. Ищейнов, М. В. Мещатунян — Москва : Форум, НИЦ ИНФРА-М, 2021. — 208 с. — (Среднее профессиональное образование). — URL: <http://znanium.com>. — Режим доступа: по подписке.

Партыка Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). — URL: <http://znanium.com>. — Режим доступа: по подписке.

Внуков А. А. Основы информационной безопасности: защита информации : учебное пособие для СПО / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — URL: <https://urait.ru>. — Режим доступа: по подписке.

## **МДК 03.02 ПРОГРАММНО – АППАРАТНЫЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ**

### **Основная литература**

Мельников В.П. Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов. — Москва : КноРус, 2022. — 267 с. — (Среднее профессиональное образование). — URL: <https://www.book.ru>. — Режим доступа: по подписке.

Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для СПО / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — URL: <https://urait.ru>. — Режим доступа: по подписке.

Хорев П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. — 2-е изд., испр. и доп. — Москва : Форум : НИЦ ИНФРА-М, 2021. — 352 с.: ил. — (Среднее профессиональное образование). — URL: <http://znanium.com>. — Режим доступа: по подписке.

Казарин О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для СПО / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — URL: <https://urait.ru>. — Режим доступа: по подписке.

### **Дополнительная литература**

Ищейнов В. Я. Основные положения информационной безопасности : учебное пособие / В. Я.Ищейнов, М. В. Мещатунян – Москва : Форум, НИЦ ИНФРА-М, 2021. - 208 с. — (Среднее профессиональное образование). — URL: <http://znanium.com>. — Режим доступа: по подписке.

Партыка Т. Л. Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — URL: <http://znanium.com>. — Режим доступа: по подписке.

Жук А. П. Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2023. — 400 с. — URL: <http://znanium.com>. — Режим доступа: по подписке.



**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ  
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ 03**

<b>Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля</b>	<b>Критерии оценки</b>	<b>Методы оценки</b>
<p>Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах</p>	<p>Использование программно-аппаратных и технических средств защиты информации на защищаемых объектах</p>	<p>Текущий контроль в форме:</p> <p>устных зачетов по темам;</p> <p>оценки выполнения практических работ;</p> <p>оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов.</p> <p>Экзамен по ПМ.</p>
<p>Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.</p>	<p>Формирование и применение политик и правил безопасности</p>	<p>Текущий контроль в форме:</p> <p>устных зачетов по темам;</p> <p>оценки выполнения практических работ;</p> <p>оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов.</p> <p>Экзамен по ПМ.</p>

<b>Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля</b>	<b>Критерии оценки</b>	<b>Методы оценки</b>
Проводить регламентные работы и фиксировать отказы средств защиты.	Проведение регламентных работ, подготовка соответствующей отчетной документации	<p>Текущий контроль в форме:</p> <p>устных зачетов по темам;</p> <p>оценки выполнения практических работ;</p> <p>оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов</p> <p>Наблюдения при выполнении практических работ и наблюдение в процессе практики</p> <p>Экзамен по ПМ.</p>
Выявлять и анализировать возможные угрозы информационной безопасности объектов	Выявление возможных угроз информационной безопасности объектов	<p>Текущий контроль в форме:</p> <p>устных зачетов по темам;</p> <p>оценки выполнения практических работ;</p> <p>оценки выполнения самостоятельной работы.</p> <p>Экспертная оценка разработанных материалов</p> <p>Наблюдения при выполнении</p>

<b>Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля</b>	<b>Критерии оценки</b>	<b>Методы оценки</b>
		<p>практических работ и наблюдение в процессе практики</p> <p>Экзамен по ПМ.</p>
<p>Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности</p>	<p>проявление интереса к будущей профессии в процессе теоретического обучения, производственной практики</p>	<p>Проверка качества выполнения практических работ, проверка отчетной документации по практике</p>
<p>Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.</p>	<p>выбор и применение эффективных методов и способов решения профессиональных задач в профессиональной области;</p> <p>собственная оценка эффективности и качества выполнения заданий.</p>	<p>Анализ результатов практических работ</p>
<p>Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность</p>	<p>решение стандартных и нестандартных профессиональных задач</p>	<p>Анализ результатов практических работ</p>
<p>Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития</p>	<p>эффективный поиск необходимой информации;</p> <p>использование различных источников, включая электронные</p>	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p>
<p>Использовать информационно-коммуникационные технологии в</p>	<p>работа с различными прикладными программами</p>	<p>Анализ результатов практических работ</p>

<b>Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля</b>	<b>Критерии оценки</b>	<b>Методы оценки</b>
профессиональной деятельности		
Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями	взаимодействие с обучающимися, преподавателями в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий	работа в группах, выполнение групповых заданий	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации	взаимодействие с обучающимися, преподавателями в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
Ориентироваться в условиях частой смены технологий в профессиональной деятельности	Анализ инноваций в сфере защиты информации; работа с различными прикладными программами	Анализ результатов практических работ
Применять математический аппарат для решения профессиональных задач.	Применение математических расчетов в ходе решения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы  Анализ результатов практических работ

<b>Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля</b>	<b>Критерии оценки</b>	<b>Методы оценки</b>
Оценивать значимость документов, применяемых в профессиональной деятельности.	работа с различными источниками информации нормативно-правой информации	Анализ результатов практических работ
Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.	работа с различными источниками информации нормативно-правой информации	Анализ результатов практических работ