

Приложение ППСЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 2022-2023 уч.г.: Рабочая программа профессионального модуля ПМ.03  
Защита информации техническими средствами

МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ  
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

**Рабочая программа профессионального модуля**

# **ПМ.03 Защита информации техническими средствами**

**для специальности**

**10.02.05 Обеспечение информационной безопасности  
автоматизированных систем**

г. Алексеевка  
2022

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

Разработчик:

И.Д. Гадяцкая, преподаватель ОГАПОУ «Алексеевский колледж»

## **СОДЕРЖАНИЕ**

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ  
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО  
МОДУЛЯ

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО  
МОДУЛЯ

4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ  
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

# **1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

## **ПМ. 03 Защита информации техническими средствами**

### **1.1. Область применения рабочей программы**

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы среднего профессионального образования - программы подготовки специалистов среднего звена в соответствии с ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения вида деятельности (ВД): Защита информации техническими средствами и соответствующих профессиональных компетенций (ПК):

- 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.

### **1.2. Цели и задачи ПМ – требования к результатам освоения профессионального модуля**

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

**иметь практический опыт:**

- установки, монтажа и настройки технических средств защиты информации;
- технического обслуживания технических средств защиты информации;
- применения основных типов технических средств защиты информации;
- выявления технических каналов утечки информации;
- участия в мониторинге эффективности технических средств защиты информации;

- диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;
  - проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
  - проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;
- установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

**уметь:**

- применять технические средства для криптографической защиты информации конфиденциального характера;
  - применять технические средства для уничтожения информации и носителей информации;
  - применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;
  - применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
  - применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
- применять инженерно-технические средства физической защиты объектов информатизации.

**знать:**

- порядок технического обслуживания технических средств защиты информации;
- номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
- физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

- методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
- номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;
- основные принципы действия и характеристики технических средств физической защиты;
- основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации.

**Перечень знаний, умений, навыков в соответствии со спецификацией стандарта компетенции Ворлдскиллс Корпоративная защита от внутренних угроз информационной безопасности, которые актуализируются при изучении учебной дисциплины:**

- 1) знать и понимать: типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- 2) знать и понимать: каналы передачи данных: определение и виды;
- 3) знать и понимать: технологии работы с политиками информационной безопасности;
- 4) уметь: создать объекты защиты и политику ИБ, используя технологии анализа в системе корпоративной защиты;
- 5) уметь: администрирование автоматизированных технические средства управления и контроля информации и информационных потоков;
- 6) уметь: создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты.

### **1.3. Планируемые личностные результаты освоения рабочей программы**

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде лично и профессионального конструктивного «цифрового следа»

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

#### **1.4. Количество часов на освоение рабочей программы профессионального модуля:**

Всего – 536 часов, в том числе:

максимальная учебная нагрузка обучающегося – 536 часов, из них в форме практической подготовки – 426 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 278 часов, в том числе практические занятия – 136 часов;

самостоятельной работы обучающегося – 6 часов; консультаций – 18 часов;

учебной практики – 108 часов; производственной практики – 108 часов.

## **2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

Результатом освоения профессионального модуля является овладение обучающимися видом деятельности – Защита информации техническими средствами, в том числе общие компетенции (ОК) и профессиональными компетенциями (ПК):

<b>Код</b>	<b>Наименование результата обучения</b>
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами

ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
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.

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1. Тематический план профессионального модуля

Коды профессиональных компетенций, коды личностных результатов	Наименование разделов профессионального модуля	Объем профессионального модуля, ак. час									
		Работа обучающихся во взаимодействии с преподавателем									Самостоятельная работа обучающегося
		Всего часов (макс. учебная нагрузка и практики)	В т.ч. в форме практи. подготовки	Обучение по МДК				Практика		Консультации	
				Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч. лабораторные работы и практические занятия в форме практической подготовки, часов	в т.ч., курсовая работа (проект), часов	Учебная, часов	Производственная часов		
1	2	3	4	5	6	7	8	9	10	11	12
ПК 3.1-.35 ЛР 4,7,9-11	<b>МДК.03.01</b> Техническая защита информации	150	<b>110</b>	<b>128</b>	66	66	*	*	*	12	4
ПК 3.1-.35 ЛР 4,7,9-11	<b>МДК.03.02</b> Инженерно-технические средства физической защиты объектов информатизации	164	<b>100</b>	<b>150</b>	70	70	30	*	*	6	2
ПК 3.1-.35 ЛР 4,7,9-11	УП. 03 Учебная практика	108	<b>108</b>					<b>108</b>			
ПК 3.1-.35	ПП. 03 Производственная	108	<b>108</b>						<b>108</b>		

ЛР 4,7,9-11	практика (по профилю специальности)										
	<b>Всего:</b>	<b>536</b>	<b>426</b>	<b>278</b>	<b>136</b>	<b>136</b>	<b>30</b>	<b>108</b>	<b>108</b>	<b>18</b>	<b>6</b>

### 3.2. Содержание обучения по профессиональному модулю ПМ.03 Защита информации техническими средствами

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и Практические занятия, в том числе в форме практической подготовки, самостоятельная работа обучающихся, курсовая работа (проект)	Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем
1	2	3
<b>МДК.03.01 Техническая защита информации</b>		
<b>Раздел 1. Концепция инженерно-технической защиты информации</b>		
<b>Тема 1.1.</b> Предмет и задачи технической защиты информации	Содержание	<b>4/0</b>
	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.	<b>4/0</b>
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	*
	Контрольные работы	*
<b>Тема 1.2.</b> Общие положения защиты информации техническими средствами	Содержание	<b>4/0</b>
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	<b>4/0</b>
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	*
	Контрольные работы	*

<b>Раздел 2. Теоретические основы инженерно-технической защиты информации</b>		
<b>Тема 2.1.</b>	Содержание	<b>6/2</b>
Информация как предмет защиты	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	<b>4/0</b>
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	<b>2/2</b>
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	
	Контрольные работы	*
<b>Тема 2.2.</b>	Содержание	<b>8/4</b>
Технические каналы утечки информации	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	<b>4/0</b>
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	<b>4/4</b>
	Классификация демаскирующих признаков Основные виды угроз информации Обоснование выбора кабинета как объекта защиты Составление плана кабинета как объекта защиты	
	Контрольные работы	*
<b>Тема 2.3. Методы и средства</b>	Содержание	<b>8/6</b>
	Классификация технических средств разведки. Методы и средства технической разведки.	<b>4/2</b>

технической разведки	Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	4/4
	Типовая структура технических каналов утечки Моделирование каналов утечки информации Методы добывания информации о вещественных носителях	
	Контрольные работы	*
<b>Раздел 3. Физические основы технической защиты информации</b>		
<b>Тема 3.1.</b>	<b>Содержание</b>	<b>8/8</b>
Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	4/4
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	4/4
	Измерение параметров физических полей	
	Контрольные работы	*
<b>Тема 3.2.</b>	<b>Содержание</b>	<b>8/8</b>
Физические процессы при подавлении опасных сигналов	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	4/4
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	4/4
	Защита аппаратуры от электромагнитных полей	
	Контрольные работы	*
<b>Раздел 4. Системы защиты от утечки информации</b>		

<b>Тема 4.1.</b> Системы защиты от утечки информации по акустическому каналу	Содержание	<b>8/8</b>
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	<b>4/4</b>
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	<b>4/4</b>
	Защита от утечки по акустическому каналу	
	Контрольные работы	*
<b>Тема 4.2.</b> Системы защиты от утечки информации по проводному каналу	Содержание	<b>8/8</b>
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	<b>4/4</b>
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	<b>4/4</b>
	Системы защиты от утечки информации по проводному каналу	
	Контрольные работы	*
<b>Тема 4.3.</b> Системы защиты от утечки информации по вибрационному каналу	Содержание	<b>8/8</b>
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	<b>4/4</b>
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	<b>4/4</b>
	Защита от утечки по виброакустическому каналу	
	Контрольные работы	*
<b>Тема 4.4.</b> Системы	Содержание	<b>12/12</b>

защиты от утечки информации по электромагнитному каналу	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	4/4
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	8/8
	Определение каналов утечки ПЭМИН	
	Защита от утечки по цепям электропитания и заземления	
	Контрольные работы	*
<b>Тема 4.5.</b> Системы защиты от утечки информации по телефонному каналу	Содержание	8/8
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	4/4
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	4/4
	Технические средства защиты информации в телефонных линиях	
	Контрольные работы	*
<b>Тема 4.6.</b> Системы защиты от утечки информации по электросетевому каналу	Содержание	4
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	4/4
	Системы защиты от утечки информации по электросетевому каналу	

	Контрольные работы	*
<b>Тема 4.7.</b> Системы защиты от утечки информации по оптическому каналу	Содержание	2/2
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	2/2
	Системы защиты от утечки информации по оптическому каналу	
	Контрольные работы	*
<b>Раздел 5. Применение и эксплуатация технических средств защиты информации</b>		
<b>Тема 5.1.</b> Применение технических средств защиты информации	Содержание	14/14
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	4/4
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	10/10
	Применение технических средств защиты Представление моделей объектов информационной безопасности Определение путей проникновения злоумышленника к источнику информации Типовые индикаторы каналов утечки Комплексная система защиты	
	Контрольные работы	*
<b>Тема 5.2.</b> Эксплуатация технических средств	Содержание	12/12
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка	4/4

защиты информации	и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	<b>8/8</b>
	Эксплуатация технических средств защиты Комплексы обнаружения и пеленгации Анализаторы телефонных линий Гарантированное уничтожение информации на магнитных носителях	
	Контрольные работы	*
	Консультации	<b>12</b>
<b>Экзамен</b>		<b>6</b>
<b>МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации</b>		
<b>Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты</b>		
<b>Тема 1.1.</b> Цели и задачи физической защиты объектов информатизации	<b>Содержание</b>	<b>10/10</b>
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	<b>6/6</b>
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	<b>4/4</b>
	Характеристика объекта защиты	
	Контрольные работы	*
	<b>Самостоятельная работа обучающихся</b> Подготовка презентации на тему: «Меры по защите информации внутри зоны»	<b>2</b>
<b>Тема 1.2.</b> Общие	Содержание	<b>16/16</b>

сведения о комплексах инженерно-технических средств физической защиты	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	6/6
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	10/10
	Анализ нормативно-правовой базы физической защиты. Формирование требований физической защите объекта. Измерение параметров электрической цепи комбинированным прибором. Измерение напряжений цифровым вольтметром.	
	Контрольные работы	*
<b>Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты</b>		
<b>Тема 2.1</b> Система обнаружения комплекса инженерно-технических средств физической защиты	Содержание	6
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	10/10
	Монтаж датчиков пожарной и охранной сигнализации	
	Контрольные работы	*
<b>Тема 2.2.</b> Система контроля и управления доступом	Содержание	14/14
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация	8/8

	средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	<b>6/6</b>
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя Рассмотрение принципов устройства, работы и применения средств контроля доступа	
	Контрольные работы	*
<b>Тема 2.3.</b> Система телевизионного наблюдения	Содержание	<b>12/10</b>
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	<b>6/4</b>
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	<b>6/6</b>
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
	Контрольные работы	*
<b>Тема 2.4.</b> Система сбора, обработки, отображения и документирования информации	Содержание	<b>12/6</b>
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	<b>6/0</b>
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	<b>6/6</b>
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
	Контрольные работы	*
<b>Тема 2.5</b> Система	Содержание	<b>8/6</b>

воздействия	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	2/0
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	6/6
	Выбор и обоснование средств подсистемы задержки	
	Контрольные работы	*
<b>Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты</b>		
<b>Тема 3.1</b>	Содержание	<b>18/12</b>
Применение инженерно-технических средств физической защиты	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	6/0
	Лабораторные работы	*
	Практические занятия, в том числе в форме практической подготовки:	12/12
	Разработка структурной схемы и спецификации оборудования Обоснование выбора кабинета как объекта защиты Составление плана кабинета как объекта защиты Представление моделей объектов информационной безопасности	
	Контрольные работы	*
	<b>Тема 3.2.</b>	Содержание
Эксплуатация инженерно-технических средств физической защиты	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	4/0
	Лабораторные работы	*

	Практические занятия, в том числе в форме практической подготовки:	<b>10/10</b>
	Эксплуатация инженерно-технических средств физической защиты Типовые инженерные конструкции Исследование систем охраны Определение путей проникновения злоумышленника к источнику информации	
	Контрольные работы	*
	Консультации	<b>6</b>
<b>Курсовой проект (работа)</b>		<b>30</b>
<b>Примерная тематика курсового проекта (работы)</b>		
<ol style="list-style-type: none"> <li>1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации.</li> <li>2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации.</li> <li>3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.</li> <li>4. Моделирование объекта защиты и угроз безопасности информации для коммерческого предприятия</li> <li>5. Разработка комплексной системы безопасности и мер по защите информации производственного объекта</li> <li>6. Моделирование объекта защиты и угроз безопасности информации для общественного учреждения</li> <li>7. Разработка комплексной системы безопасности и мер по защите информации некоммерческой организации.</li> <li>8. Комплексная система безопасности информации предприятия</li> <li>9. Разработка комплексной системы безопасности и мер по защите информации общественной организации</li> <li>10. Комплексная система безопасности информации общественного здания</li> <li>11. Расчет системы безопасности и контроля доступа коммерческой организации</li> <li>12. Моделирование объекта защиты и угроз безопасности информации для некоммерческой организации</li> <li>13. Расчет системы безопасности и контроля доступа производственного здания</li> <li>14. Комплексная система безопасности информации коммерческой организации</li> </ol>		
<b>Экзамен</b>		<b>6</b>
<b>Самостоятельная работа при изучении профессионального модуля</b>		<b>6</b>

<ol style="list-style-type: none"> <li>1. Подготовка информационного сообщения на тему: «Основные проблемы реализации систем защиты информации»</li> <li>2. Поиск информации по теме: «Биометрическая идентификация»</li> <li>3. Подготовка презентации на тему: «Меры по защите информации внутри зоны»</li> </ol>	
<p><b>Учебная практика</b> <b>Виды работ</b></p> <ol style="list-style-type: none"> <li>1. Измерение параметров физических полей.</li> <li>2. Определение каналов утечки ПЭМИН.</li> <li>3. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.</li> <li>4. Установка и настройка технических средств защиты информации.</li> <li>5. Проведение измерений параметров побочных электромагнитных излучений и наводок.</li> <li>6. Проведение аттестации объектов информатизации.</li> <li>7. Монтаж различных типов датчиков.</li> <li>8. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.</li> <li>9. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.</li> <li>10. Рассмотрение системы контроля и управления доступом.</li> <li>11. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.</li> <li>12. Рассмотрение датчиков периметра, их принципов работы.</li> <li>13. Выполнение звукоизоляции помещений системы шумления.</li> <li>14. Реализация защиты от утечки по цепям электропитания и заземления.</li> <li>15. Разработка организационных и технических мероприятий по заданию преподавателя;</li> <li>16. Разработка основной документации по инженерно-технической защите информации.</li> </ol>	<p><b>108</b></p>

## Производственная практика

### Виды работ

1. Исследование угроз и методологии оценки уязвимости информации.
2. Оценка информационных рисков.
3. Исследование методов и моделей оценки уязвимости информации.
4. Исследование аналитических моделей для определения базовых показателей уязвимости информации.
5. Участие в проектировании политики безопасности информационного объекта.
6. Проектирование политики безопасности информационного объекта на конкретном примере.
7. Мероприятия по выявлению каналов утечки информации (специальные обследования).
8. Участие в монтаже технических средств защиты информации в телефонных линиях
9. Участие в обслуживании и эксплуатации технических средств защиты информации в телефонных линиях
10. Оценка эффективности защиты речевой информации
11. Инструментально-расчётная оценка защищённости защищаемого помещения от утечки речевой информации
12. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности: датчики движения для охраны помещений
13. Участие в монтаже, обслуживании и эксплуатации средств инженерной защиты и технической охраны объектов: системы защиты от утечки информации по оптическому каналу
14. Проектирование системы видеонаблюдения за протяженным периметром. Проектирование системы идентификации людей на входе в здание. Проектирование системы видеонаблюдения в транспорте.
15. Проектирование системы видеонаблюдения в школе
16. Участие в монтаже систем видеонаблюдения. Участие в обслуживании систем видеонаблюдения. Участие в эксплуатации систем видеонаблюдения. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам: защита информации от утечки по акустическому каналу пассивными методами
17. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от

108

<p>несанкционированного съёма, и утечки по техническим каналам: системы защиты от утечки информации по электросетевому каналу</p> <p>18. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам: защита информации от утечки по электромагнитному каналу пассивными методами. Система физической защиты объекта</p> <p>19. Применение нормативно-правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами</p> <p>20. Организация аттестации выделенного помещения по требованиям безопасности информации.</p>	
<b>Экзамен по модулю</b>	<b>6</b>
<b>Всего</b>	<b>536</b>

## **4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

### **4.1. Требования к минимальному материально-техническому обеспечению:**

Реализация рабочей программы профессионального модуля предполагает наличие **лаборатории технических средств защиты информации** - 65,4 кв.м.

Оборудование учебного кабинета: доска, 15 автоматизированных рабочих мест для студентов: столы-15 шт., стулья -15 шт., ПК-15 шт., автоматизированное рабочее место для преподавателя – 1 шт., сканер-1 шт., принтер-1 шт., проектор – 1шт., экран – 1 шт.; программное обеспечение общего и профессионального назначения, лабораторные учебные макеты.

Основное оборудование: учебно-методическая документация; аппаратные средства аутентификации пользователя.

**лекционной аудитории с мультимедийным оборудованием** - 11,8 кв.м.

Оборудование учебного кабинета: доска – 1 шт., шкаф – 4 шт., 32 посадочных места для студентов (32 стула, 16 столов), рабочее место преподавателя – 1 шт., телевизор «Sony» - 1 шт; интерактивная доска – 1шт.; мультимедийный проектор «Acer» - 1 шт, компьютер – 1шт., принтер – 1 шт.

Основное оборудование: стенды «Техника безопасности», «Уголок группы», «Сегодня на учебном занятии», «Лучшие работы студентов», комплект учебно-методической документации.

Демонстрационные средства обучения:раздаточный материал для проведения учебных занятий по дисциплине, набор презентаций и видеоматериалов.

Рабочая программа может быть реализована с применением различных образовательных технологий, в том числе с применением дистанционных образовательных технологий и электронного обучения.

Предусматриваются следующие виды практик, реализуемых в форме практической подготовки: учебная практика, производственная практика (по профилю специальности). Практики проводятся в рамках дуального обучения концентрировано. В последний день практики сдается дифференцированный зачет

Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся на основе договоров, заключаемых между ОГАПОУ «Алексеевский колледж» и

организациями.

Материально-техническая база должна соответствовать действующим санитарным и противопожарным нормам.

#### **4.2. Информационное обеспечение обучения**

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

##### **Основные источники:**

1. Гребенюк Е. И., Гребенюк Н. А. Технические средства информатизации. Учебник для СПО М.: ИЦ Академия, 2019 – 352 с.
2. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) учебник Бубнов А.А., М.: ИЦ Академия, 2019 – 272 с.

##### **Дополнительные 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», 2017 – 336 с
5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 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 Академия, - 336 с. – 2012
7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд во: ДМК Пресс, - 2012
8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012 – 416 с.

9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
13. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
14. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
15. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
16. 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».
17. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
18. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
19. 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.
20. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
21. 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.
22. 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.

23. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России

24. от 30 августа 2002 г. № 282.

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

26. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России

27. от 31 августа 2010 г. № 416/489.

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

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

30. 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 недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

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

32. 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

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

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

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

36. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
37. 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
38. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
39. 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
40. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
41. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
42. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
43. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
44. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
45. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
47. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
48. Номенклатура показателей качества. Ростехрегулирование, 2005.
49. 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.

50. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
51. 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.
52. 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.
53. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
54. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
55. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
56. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
57. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
58. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
59. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
60. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
61. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

### Электронные издания (электронные ресурсы):

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с.
2. <https://urait.ru/bcode/456793>
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.
4. <https://urait.ru/bcode/449548>
5. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с.
6. <https://urait.ru/bcode/451933>
7. Интерфейсы периферийных устройств –  
<https://intuit.ru/studies/courses/92/92/lecture/28396>
8. О компонентах системного блока — подробно –  
<https://intuit.ru/studies/courses/3685/927/lecture/19564?page=2>
9. Портативные компьютеры –  
<https://intuit.ru/studies/courses/13910/1276/lecture/24146>
10. Сравнительные характеристики процессоров –  
<https://intuit.ru/studies/courses/15812/478/lecture/21074>
11. Технические средства информационных технологий –  
<https://intuit.ru/studies/courses/3481/723/lecture/14240>
12. Устройства ввода информации –  
<https://intuit.ru/studies/courses/3460/702/lecture/14158>
13. Устройства вывода информации –  
<https://intuit.ru/studies/courses/3460/702/lecture/14157>
14. Цифровая образовательная среда СПО PROФобразование:
  - Старостин, А. А. Технические средства автоматизации и управления : учебное пособие для СПО / А. А. Старостин, А. В. Лаптева ; под редакцией Ю. Н. Чеснокова. — 2-е изд. — Саратов, Екатеринбург : Профобразование, Уральский федеральный университет, 2019. — 168 с. — ISBN 978-5-4488-0503-5, 978-5-7996-2842-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование : [сайт]. — URL: <https://profspo.ru/books/87882>

(дата обращения: 31.08.2020). — Режим доступа: для авторизир. пользователей

**Электронно-библиотечная система:**

IPRBOOKS - <http://www.iprbookshop.ru/78574.html>

**Веб-система для организации дистанционного обучения и управления им:**

Система дистанционного обучения ОГАПОУ «Алексеевский колледж»  
<http://moodle.alcollege.ru/>

#### **4.3. Общие требования к организации образовательного процесса**

Освоение программы модуля базируется на изучении общепрофессиональных Основы алгоритмизации и программирования, Технические средства информатизации, Защита информационных процессов в компьютерных системах, Информационные технологии.

Обязательным условием допуска к производственной практике (по профилю специальности) в рамках модуля является освоение учебной практики для получения первичных профессиональных навыков в рамках профессионального модуля.

При освоении программ профессиональных модулей в последнем семестре изучения формой промежуточной аттестации по модулю является экзамен по модулю, который представляет собой форму независимой оценки результатов обучения с участием работодателей. Условием допуска к экзамену по модулю является успешное освоение обучающимися всех элементов программы профессионального модуля теоретической части модуля (МДК) и практик.

Экзамен по модулю проверяет готовность обучающегося к выполнению указанного вида профессиональной деятельности и сформированность у него профессиональных компетенций. Итогом проверки является однозначное решение: «вид деятельности освоен / не освоен». В зачетной книжке запись будет иметь вид: «ВД освоен» или «ВД не освоен». Данное решение подтверждается оценкой по пятибалльной системе.

#### **4.4. Кадровое обеспечение образовательного процесса**

Реализация рабочей программы профессионального модуля должна обеспечиваться педагогическими кадрами, имеющими высшее образование,

соответствующее профилю модуля. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимся профессионального цикла, эти преподаватели должны проходить стажировку в профильных организациях не реже 1 раза в 3 года.

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

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

		результатов выполнения видов работ на практике экзамен по модулю
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 экзамен по модулю
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 экзамен по модулю