Федеральное агентство связи
Колледж телекоммуникаций
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Согласовано:
Генеральный директор
Андрианова Светлана Сергеевна
ООО «Аудиторы корпоративной безопасности»
_____ /Андрианова С.С. /
«__» _____ 2020 г.

УТВЕРЖДЕНО
приказом директора КТ МТУСИ
№ 01-03-113/1 от «19» июня 2020
_____ С.Н. Ильиных

# РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

**для специальности**
**10.02.04 Организация информационной безопасности телекоммуникационных систем**
**(очная форма обучения)**

Москва, 2020 г.

ОДОБРЕНА
**предметной (цикловой) комиссией**
Компьютерных систем и безопасности
наименование комиссии

**Протокол № 5**
от «09» июня 2020 г.

**Председатель предметной (цикловой) комиссии**

_____ / Сергеева М.Б/

Разработано на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (приказ Минобрнауки России № 1551 от 09 декабря 2016 года) и примерной основной образовательной программы 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем. Зарегистрировано в государственном реестре примерных основных образовательных программ. Реквизиты решения ФУМО о включении ПООП в реестр: Протокол № 1 от 28.03.2017

Рассмотрено и одобрено на заседании методического совета
«10» июня 2020 г. Протокол № 5

СОГЛАСОВАНА:
**Начальник методического отдела**

_____ / Л.М.Кузнецова/
Подпись Ф.И.О.

Организация-разработчик:
КТ МТУСИ, Г. Москва

Разработчик:
Преподаватель КТМТУСИ: Сергеева М.Б.

# СОДЕРЖАНИЕ

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## 1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) – является частью образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в части освоения основного вида деятельности (ВД): **Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты** и соответствующих **профессиональных компетенций (ПК):**

ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях;

ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях;

ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и в профессиональной подготовке, в программах повышения квалификации и переподготовки по должностям служащих. Рабочая программа профессионального модуля может быть использована на очной и очно-заочной формах обучения.

**общих компетенций:**

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.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

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

| | |
|---|---|
| Иметь практический опыт | -выявление технических каналов утечки информации;<br>-защита информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;<br>-проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;<br>-проведение технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;<br>-установка, монтаж, настройка и испытание технических средств защиты информации от утечки по техническим каналам; |
| Уметь | -применять нормативные правовые акты и нормативные методические документы в области защиты информации;<br>-применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;<br>-проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС;<br>-проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;<br>-проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;<br>-проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам.<br>- использовать средства физической защиты линий связи ИТКС |
| Знать | – способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;<br>– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.<br>– основные типы технических средств защиты информации от утечки по техническим каналам;<br>– методики измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;<br>– организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;<br>– порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;<br>– содержание и организацию работ по физической защите линий связи ИТКС;<br>– принципы действия и основные характеристики технических средств физической защиты;<br>– законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности; |

| | |
|---|---|
| | – принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях. |

**1.3. Использование часов вариативной части ОП***

Вариативная часть в объеме 85 часов использована на расширение основных видов деятельности, к которым должен быть готов выпускник, освоивший образовательную программу, согласно получаемой квалификации, указанной в пункте 1.12 настоящего ФГОС СПО и введение дополнительных образовательных результатов МДК, выявленных как квалификационные дефициты в результате соотнесения требований WSR по компетенции Информационные кабельные сети.. Содержание рабочей программы профессионального модуля ориентировано на следующие минимальные требования к навыкам (умениям), указанным в техническом описании компетенции:

| Дополнительные знания, умения, действия | № наименование темы | Количество часов | Обоснование включения в рабочую программу |
|---|---|---|---|
| Постановка защиты от утечки по цепям электропитания и заземления<br>Система защиты от утечки по акустическому каналу | Тема 5.2. Эксплуатация технических средств защиты информации | 30 | Углубленная подготовка, современные требования опережающего образования |
| Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. | Тема 3.2. Эксплуатация инженерно-технических средств физической защиты | 55 | |
| | Всего | 85 | |

**1.4. Количество часов, отводимое на освоение профессионального модуля**

Объем учебной нагрузки: 544 часа

Из них на освоение МДК – 352.часа.

МДК.03.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей

Во взаимодействии с преподавателем – 320 часов, в том числе консультации – 2 часов
Самостоятельная работа обучающегося – 26 часов;
На практики учебную и производственную – 180 часов.
Промежуточная аттестация в форме – экзамена по МДК (комплексный) и по ПМ – 18 часов.

## 2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**Цель и планируемые результаты освоения профессионального модуля**

В результате изучения профессионального модуля студент должен освоить основной вид деятельности: **Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты** и соответствующие ему профессиональные и общие компетенции:

| Код | Наименование видов деятельности и профессиональных компетенций |
|---|---|
| ВД 3 | Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты |
| ПК 3.1 | Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях |
| ПК 3.2 | Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях |
| ПК 3.3 | Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями |
| ПК 3.4 | Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей. |
| 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. |
| ОК 07 | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 09 | Использовать информационные технологии в профессиональной деятельности. |

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 3.1. Структура профессионального модуля

| Коды профессиональных общих компетенций | Наименования разделов профессионального модуля | Суммарный объем нагрузки, час. | Промежуточная аттестация | Самостоят. работа | Консультации | Объем профессионального модуля, час. | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Обучение по МДК | | | Практики | |
| | | | | | | Всего | Лабораторных и практических занятий | Курсовых работ (проектов) | Учебная | Производственная |
| ПК 3.1- ПК.3.4 ОК 01. – ОК 07., ОК 9 | **Раздел 1.** Защита информации в ИТКС с использованием технических средств защиты | 174 | | 14 | | 160 | 70 | | | |
| ПК 3.5 ОК 01. – ОК 07., ОК 9 | **Раздел 2.**Физическая защита линий связи ИТКС | 178 | 6 | 12 | 2 | 160 | 83 | | | |
| ПК 1.1-ПК 1.4 ОК 01. – ОК 07., ОК 9 | Учебная практика | 36 | | | | | | | 36 | |
| ПК 1.1-ПК 1.4 ОК 01. – ОК 07., ОК 9 | Производственная практика, часов | 144 | | | | | | | | 144 |
| | Промежуточная аттестация | 12 | | | | | | | | |
| | **Всего:** | **544** | **6** | **26** | **2** | **320** | **153** | **-** | **36** | **144** |

**3.2. Тематический план и содержание профессионального модуля**

| Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК) | Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены) | Объем часов |
|---|---|---|
| 1 | 2 | 3 |
| **Раздел 1. Защита информации в ИТКС с использованием технических средств защиты** | | **174** |
| **МДК.03.01.Защита информации в ИТКС с использованием технических средств защиты** | | 174 |
| **Тема 1.1.** Предмет и задачи технической защиты информации | **Содержание** | |
| | 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. | 6 |
| **Тема 1.2.** Общие положения защиты информации техническими средствами | **Содержание** | |
| | Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации. | 6 |
| **Тема 2.1.** Информация как предмет защиты | **Содержание** | |
| | Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке. | 6 |
| **Тема 2.2.** Технические каналы утечки | **Содержание** | |
| | Понятие и особенности утечки информации. Структура канала утечки информации. Классификация | 8 |

| | | |
|---|---|---|
| информации | существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. | |
| **Тема 2.3.** Методы и средства технической разведки | **Содержание** | |
| | Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации. | 6 |
| **Тема 3.1.** Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок | **Содержание** | |
| | Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей | 12 |
| **Тема 3.2.** Физические процессы при подавлении опасных сигналов | **Содержание** | |
| | Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление. | 4 |
| **Тема 4.1.** Системы защиты от утечки информации по акустическому каналу | **Содержание** | |
| | Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу. | 8 |
| **Тема 4.2.** Системы защиты от утечки информации по проводному каналу | **Содержание** | |
| | Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу. | 4 |
| **Тема 4.3.** Системы | **Содержание** | |

| | | |
|---|---|---|
| защиты от утечки информации по вибрационному каналу | Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу. | 2 |
| **Тема 4.4.** Системы защиты от утечки информации по электромагнитному каналу | **Содержание** | |
| | Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу. | 4 |
| **Тема 4.5.** Системы защиты от утечки информации по телефонному каналу | **Содержание** | |
| | Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу. | 6 |
| **Тема 4.6.** Системы защиты от утечки информации по электросетевому каналу | **Содержание** | |
| | Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу. | 4 |
| **Тема 4.7.** Системы защиты от утечки информации по оптическому каналу | **Содержание** | |
| | Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу. | 2 |
| **Тема 5.1.** Применение технических средств защиты информации | **Содержание** | |
| | Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических | 6 |

| | | |
|---|---|---|
| | полей, создаваемых техническими средствами защиты информации. | |
| **Тема 5.2.** Эксплуатация технических средств защиты информации | **Содержание** | |
| | Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации. | 6 |
| | **Практические занятия** | |
| | Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.<br>Измерение параметров физических полей<br>Защита от утечки по акустическому каналу<br>Защита от утечки по виброакустическому каналу<br>Определение каналов утечки ПЭМИН<br>Защита от утечки по цепям электропитания и заземления<br>Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.<br>Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.<br>Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.<br>Технические средства для уничтожения информации и носителей информации, порядок применения. | 70 |
| **Самостоятельная работа:**<br>1. Классификация способов и средств защиты информации.<br>2. Основные и вспомогательные технические средства и системы.<br>3. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации.<br>4. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы | | 14 |

| | | |
|---|---|---|
| утечки информации, их характеристика. | | |
| **Раздел 2. Физическая защита линий связи ИТКС** | | **178** |
| **МДК.03.02. Физическая защита линий связи ИТКС** | | **178** |
| **Тема 1.1.** Цели и задачи физической защиты объектов информатизации | **Содержание** | |
| | 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. | 10 |
| **Тема 1.2.** Общие сведения о комплексах инженерно-технических средств физической защиты | **Содержание** | |
| | 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 |
| **Тема 2.1.** Система обнаружения комплекса инженерно-технических средств физической защиты | **Содержание** | |
| | Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия. | 6 |
| **Тема 2.2.** Система контроля и управления доступом | **Содержание** | |
| | Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ. | 14 |
| **Тема 2.3.** Система телевизионного | **Содержание** | |
| | Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. | 10 |

| | | |
|---|---|---|
| наблюдения | Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения. | |
| **Тема 2.4.** Система сбора, обработки, отображения и документирования информации | **Содержание** | |
| | Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации. | 6 |
| **Тема 2.5.** Система воздействия | **Содержание** | |
| | Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия. | 2 |
| **Тема 3.1.** Применение инженерно-технических средств физической защиты | **Содержание** | |
| | Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия. | 16 |
| **Тема 3.2.** Эксплуатация инженерно-технических средств физической защиты | **Содержание** | |
| | Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты. | 7 |
| | **Практические и лабораторные занятия** | |
| | Монтаж датчиков пожарной и охранной сигнализации<br>Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя<br>Рассмотрение принципов устройства, работы и применения средств контроля доступа<br>Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.<br>Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. | **83** |

| | |
|---|---|
| **Самостоятельная работа**<br>Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)<br>Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите. | **12** |
| **Экзамен** | **6** |
| **Учебная практика по профессиональному модулю**<br>1. Монтаж различных типов датчиков.<br>2. Проектирование установки системы охранно-пожарной сигнализации по заданию и ее реализация.<br>3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.<br>4. Рассмотрение системы контроля и управления доступом.<br>5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.<br>6. Рассмотрение датчиков периметра, их принципов работы.<br>7. Выполнение звукоизоляции помещений системы зашумления.<br>8. Реализация защиты от утечки по цепям электропитания и заземления.<br>9. Разработка организационных и технических мероприятий по заданию преподавателя.<br>10. Разработка основной документации по инженерно-технической защите информации | **36** |
| **Производственная практика профессионального модуля**<br>**Виды работ**<br>1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации.<br>2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.<br>3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам.<br>4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. | **144** |
| **Промежуточная аттестация** | **18** |

| | |
|---|---|
| **Консультации** | **2** |
| **Во взаимодействии с преподавателем** | **320** |
| **Самостоятельная работа** | **26** |
| **Объем учебной нагрузки** | **544** |

## 4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**4.1. Для реализации программы профессионального модуля предусмотрены следующие специальные помещения**

**Лаборатория «Защиты информации от утечки по техническим каналам»** оборудована для проведения занятий лекционного типа, практических занятий, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации.

Перечень основного оборудования, находящегося в кабинете:

- рабочее место преподавателя (стол, стул, персональный компьютер);
- учебная мебель (столы, стулья);
- персональные компьютеры не ниже Core i3;
- коммутатор;
- интерактивная доска;
- проектор;
- аппаратно-программные средства обеспечения разграничения и контроля доступа пользователей АПМДЗ "КРИПТОН-ЗАМОК/К" (М-526А) в комплекте со считывателем смарт карт и устройством для подключения iButton;
- аппаратный шифратор для PC-совместимых компьютеров «КРИПТОН-8/PCI» в комплекте со считывателем смарт карт и устройством для подключения iButton;
- многофункциональный поисковый прибор ST 031 "Пиранья";
- абонентское устройство защиты телефонных линий «Гранит-8»;
- устройство защиты аналогового ТА «МП-1А»;
- устройство защиты цифрового ТА «МП-1А в евророзетке»;
- СИСТЕМНЫЙ КОМПЛЕКТ ARBYTE SILEX M115Q G3/G4400/8GB/4*1TB/RAID;
- SATA/k+m/2GLAN/500W/minitower;
- ПАК ViPNet IDS100 2.x;
- ПАК ViPNet Coordinator HW50 A 4.x;
- Рутокен PINPad;
- РУТОКЕН ЭЦП 2.0 память 64 Кбайт;
- Рутокен ЭЦП Bluetooth;
- Рутокен S 128КБ;
- USB-токен JaCarta PKI;
- S-Terra.

Используемое программное обеспечение:

- контракт № 29ЭА44-2018 от 06.09.2018 ( Лицензия на использование JaCarta Management System от 14.09.2018 серийный номер 96d93439-984b-49be-93e0-db5e33051556 бессрочная, Лицензия на использование Secret Disk Server NG для файлового сервера на 10 пользователей (одновременных подключений)(лицензия сервера - E8E3-5990-3795-131C, лицензия администратора 0AEA-7027-899B-36D1) бессрочная, Передача права на использование ПО ViPNet Client for Windows 4.x (КС2)и ПО ViPNet Administrator 4.x (КС2)рег. Номер № 025-00173 от 21.11.2018 – бессрочная, Лицензия на право использования СКЗИ "КриптоПро CSP" версии 4.0 от 30.08.2018 срок неограничен;
- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Microsoft Windows 10 Professional (предустановленное ПО, Контракт № 64ЭА44-2018 от 09.01.2019 с ООО «Азон», бессрочная);
- 7-Zip (свободно распространяемое ПО);

- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);
- Yandex Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- Adobe Reader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

Учебно-методическая документация.

**Библиотека, читальный зал**, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Перечень основного оборудования, находящегося в кабинете:
- рабочее место педагога-библиотекаря (стол, стул, персональный компьютер);
- учебная мебель (столы, стулья);
- персональные компьютеры.

Используемое программное обеспечение:
- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Astra Linux Common Edition релиз «Орел» (свободно распространяемое ПО);
- 7-Zip (свободно распространяемое ПО);
- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);
- Yandex Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- Adobe Reader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление до-ступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

**Кабинет для самостоятельной работы** (компьютерный класс), оснащенный компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Перечень основного оборудования, находящегося в кабинете:
- учебная мебель (столы, стулья);
- персональные компьютеры;
- принтеры.

Используемое программное обеспечение:
- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Astra Linux Common Edition релиз «Орел» (свободно распространяемое ПО);
- 7-Zip (свободно распространяемое ПО);

- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);
- Yandex Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- Adobe Reader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление до-ступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

**Учебная аудитория «Кабинет подготовки к итоговой аттестации и защиты выпускной квалификационной работы,** включая подготовку к процедуре защиты и процедуру защиты»

Перечень основного оборудования, находящегося в аудитории:
- мультимедийный проектор;
- экран;
- учебная мебель (столы, стулья, доска);
- учебно-наглядные пособия;
- ноутбук.

Используемое программное обеспечение:
- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Astra Linux Common Edition релиз «Орел» (свободно распространяемое ПО);
- Python (свободно распространяемое ПО);
- Visual Basic (свободно распространяемое ПО);
- 7-Zip (свободно распространяемое ПО);
- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);
- Yandex Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- Adobe Reader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

**Методический кабинет,** оснащенный компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду.

Перечень основного оборудования, находящегося в кабинете:
- столы, стулья, шкафы;
- персональные компьютеры;
- принтеры.

Используемое программное обеспечение:

- Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. Educational Renewal, срок действия 2 года (Контракт № 20ЭА44-2019 от 29.07.2019);
- ОС Astra Linux Common Edition релиз «Орел» (свободно распространяемое ПО);
- 7-Zip (свободно распространяемое ПО);
- Mozilla Firefox (свободно распространяемое ПО);
- Foxit Reader (свободно распространяемое ПО);
- Yandex Browser (свободно распространяемое ПО);
- VSCodium (свободно распространяемое ПО);
- Pinta (свободно распространяемое ПО);
- Adobe Reader (свободно распространяемое ПО);
- LibreOffice (свободно распространяемое ПО).

Электронная библиотечная система IPRbooks (лицензионный договор № 5890/19 от 13 декабря 2019г. с ООО «Ай Пи Ар Медиа» на предоставление доступа к ЭБС IPRbooks, срок действия с 01.01.2020г. по 31.12.2020г.; лицензионный договор № № 7269/20 от 04 декабря 2020 г. с ООО «Ай Пи Ар Медиа» на предоставление до-ступа к ЭБС IPRbooks, срок действия с 01.01.2021г. по 31.12.2021г.).

### 4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

#### 4.2.1. Основная литература


1. Белов Е.Б. 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.
2. Богомазова Г.Н. Обеспечение информационной безопасности компьютерных сетей: учеб. для студ. учреждений сред. проф. образования / Г.Н.Богомазова. - М.: Издательский центр «Академия», 2017. – 224 с.
3. Костров Б.В. Сети и системы передачи информации: учебник для студ. учреждений сред. проф. образования / Б.В.Костров, В.Н.Ручкин.– М.: Издательский центр «Академия», 2017. – 256 с.
4. Бурькова, Е. В. Физическая защита объектов информатизации : учебное пособие / Е. В. Бурькова. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2017. — 158 с. — ISBN 978-5-7410-1697-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/71349.html


#### 4.2.2. Дополнительная литература


1. Рудаков, А.В. Технология разработки программных продуктов[Текст]: учебник для студ. учреждений сред. проф. образования/ А.В. Рудаков. – 11-е изд., стер. – М.: Издательский центр «Академия»,2017. – 208с. (кол-во 15 экз.)
2. Майстренко, А. В. Мультимедийные средства обработки информации : учебное пособие для СПО / А. В. Майстренко, Н. В. Майстренко. — Саратов : Профобразование, 2020. — 81 с. — ISBN 978-5-4488-0734-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/90169.html
3. Соловьев, Н. А. Цифровая обработка информации в задачах и примерах : учебное пособие для СПО / Н. А. Соловьев, Н. А. Тишина, Л. А. Юркевская. — Саратов : Профобразование, 2020. — 122 с. — ISBN 978-5-4488-0596-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/92201.html

4. Вайспапир, В. Я. Проектирование радиочастотных линий связи : учебно-методическое пособие / В. Я. Вайспапир, А. А. Пряхина. — Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2016. — 36 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/69553.html

**43. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья**

Обучение по образовательным программам среднего профессионального образования обучающихся с ограниченными возможностями здоровья осуществляется на основе образовательных программ среднего профессионального образования, адаптированных при необходимости для обучения данной категории обучающихся.

Образование обучающихся с ограниченными возможностями здоровья организовано совместно с другими обучающимися.

Обучение по образовательным программам среднего профессионального образования обучающихся с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

В колледже созданы специальные условия для получения среднего профессионального образования, без которых невозможно или затруднено освоение образовательных программ обучающимися с ограниченными возможностями здоровья:

- создание специальных социально-бытовых условий, обеспечивающих возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения колледжа, а также их пребывания в указанных помещениях (пандусы с входными группами, телескопические пандусы, перекатные пандусы, гусеничные мобильные подъемники, поручни) для лиц с нарушениями опорно-двигательного аппарата;

- использование в образовательном процессе специальных методов обучения и воспитания (организация отдельного учебного места вблизи размещения демонстрационного оборудования, дублирование основного содержания учебно-методического обеспечения в адаптированных раздаточных материалах, обеспечение облегченной практической деятельности на учебных занятиях, предупреждение признаков переутомления с помощью динамических пауз, соблюдение рационального акустического режима и обеспечение надлежащими звуковыми средствами воспроизведения информации, замедленный темп индивидуального обучения, многократное повторение, опора на сохранные анализаторы, функции и системы организма, опора на положительные личностные качества);

- обеспечение преподавателем-предметником организации технической помощи обучающимся с ограниченными возможностями здоровья;

- дублирование справочной информации, расписания учебных занятий в адаптированной форме в зданиях колледжа на информационных мониторах и наличие адаптированного официального сайта колледжа по адресу http://ctmtuci.ru/.

## 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

| **Результаты (освоенные профессиональные компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях. | - проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;<br>- применять нормативные правовые акты и нормативные методические документы в области защиты информации;<br>- постановка защиты от утечки по цепям электропитания и заземления;<br>- постановка защиты от утечки по цепям электропитания и заземления;<br>Система защиты от утечки по акустическому | *Текущий контроль в форме:*<br>*- защиты практических занятий;*<br>*- контрольных работ по темам МДК;*<br>*- тестирование по темам МДК Диф. зачеты по производственной практике и по каждому из разделов профессионального модуля.*<br>*Комплексный экзамен по МДК.* |
| ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях. | - проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;<br>- проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;<br>- применять нормативные правовые акты и нормативные методические документы в области защиты информации. | |
| ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями. | - проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС;<br>- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;<br>- применять нормативные правовые акты и нормативные методические документы в области защиты информации;<br>- применять систему защиты от утечки по акустическому каналу<br>- рассмотрение принципов устройства, работы и применения средств видеонаблюдения.<br>- рассмотрение принципов устройства | |

| | | |
|---|---|---|
| ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей. | выявлять и оценивать угрозы безопасности информации в ИТКС;<br>настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;<br>проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; | |

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

| **Результаты (освоенные общие компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. | – обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;<br>- адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач; | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практик.<br><br>Промежуточная аттестация в форме экзамена по ПМ |
| ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. | - использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач; | |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. | - демонстрация ответственности за принятые решения;<br>- обоснованность самоанализа и коррекция результатов собственной работы; | |
| ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. | - взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;<br>- обоснованность анализа работы членов команды (подчиненных); | |

| | | |
|---|---|---|
| ОК 09. Использовать информационные технологии в профессиональной деятельности. | - эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту; | |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке. | - эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке. | |