***Приложение II.2***

***к программе СПО 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»***

**РАБОЧАЯ ПРОГРАММА**

 **ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты**

**2022**

**Составитель:**

 **Арефьев Александр Валерьевич, преподаватель ГБПОУ УКРТБ**

**Бокуменко Алекс Витальевич, преподаватель ГБПОУ УКРТБ**

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| 1. Общая характеристика рабочей программы профессионального модуля
2. Структура и содержание профессионального модуля
3. Условия реализация программы профессионального модуля
4. Контроль и оценка результатов освоения профессионального модуля

Приложение 1 |  |

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

|  |
| --- |
| ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты |

*наименование профессионального модуля*

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

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

Перечень общих компетенций

|  |  |
| --- | --- |
| **Код** | **Наименование общих компетенций** |
| ОК 1. | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам |
| ОК 2. | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности |
| ОК 3. | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 4. | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. |
| ОК 5. | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 6. | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. |
| ОК 7. | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 8. | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. |
| ОК 9. | Использовать информационные технологии в профессиональной деятельности |
| ОК 10. | Пользоваться профессиональной документацией на государственном и иностранном языках. |
| ОК 11. | Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере. |

Перечень профессиональных компетенций

|  |  |
| --- | --- |
| **Код** | **Наименование видов деятельности и профессиональных компетенций** |
| 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. |

В ходе освоения профессионального модуля учитывается движение к достижению личностных результатов обучающимися ЛР 17,18

В результате освоения профессионального модуля студент должен:

|  |  |
| --- | --- |
| Иметь практический опыт в | установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;защите информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей. |
| уметь | проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС;проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;использовать средства физической защиты линий связи ИТКС;применять нормативные правовые акты и нормативные методические документы в области защиты информации. |
| знать | способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;основные типы технических средств защиты информации от утечки по техническим каналам;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;организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;содержание и организацию работ по физической защите линий связи ИТКС;принципы действия и основные характеристики технических средств физической защиты;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.*Вариативные знания* |

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

Всего часов –**560** часа, в том числе:

- **205** часов вариативной части, направленных на усиление обязательной части программы профессионального модуля.

**2. СТРУКТУРА и содержание профессионального модуля**

**2.1. Структура профессионального модуля**

|  |  |  |  |
| --- | --- | --- | --- |
| **Коды профессиональных компетенций** | **Наименования разделов профессионального модуля[[1]](#footnote-1)\*** | **Суммарный объем нагрузки, час** | **Объем профессионального модуля, час** |
| **Обучение по МДК** | **Практика** | **Промежуточная аттестация** |
| **Всего,**часов | **в т.ч. лабораторные работы и практические занятия,**часов | **в т.ч., курсовая работа (проект),**часов | **Самостоятельная работа** | **Учебная,**часов | **Производственная (по профилю специальности),**часов |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **ПК 3.1-****ПК 3.4** | **Раздел 1.** Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты | **172** | **154** | **84** | - | **12** | **-** | **-** | **6** |
| **ПК 3.1-****ПК 3.4** | **Раздел 2.** Организация физической защиты линий связи информационно-телекоммуникационных систем и сетей | **124** | **108** | **54** | **-** | **10** | **-** | **-** | **6** |
| **ПК 3.1-****ПК 3.4** | **Учебная практика** | **108** |  | **108** |  |  |
|  | **Производственная практика (по профилю специальности)**, часов | **144** |  |  | **144** |  |
|  | **Промежуточная аттестация (экзамен (квалификационный))** | **5** |  |  |  |  |  |  | **5** |
|  | **Всего:** | **553** | **262** | **138** | **-** | **22** | **108** | **144** | **17** |

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

|  |  |  |
| --- | --- | --- |
| **Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)** | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся , курсовая работ (проект)** | **Объем часов** |
| **1** | **2** | **3** |
| **Раздел 1. Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты** |  |
| **МДК.3.1 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты** |  |
| **Тема.1 Построение комплексной системы защиты информации** | **Содержание** | **58** |
| **1** | **Предмет и задачи технической защиты информации.** Системный подход при решении задач инженерно-технической защиты информации. Нормативно-правовая основа в области обеспечения безопасности информации с позиции создания КСЗИ. Международные стандарты Российские стандарты | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 143-145 |  |
| **2** | **Цели и задачи комплексной системы защиты информации** | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.145-146 |  |
| **3** | **Уровень защищенности объекта защиты. Уровни достаточности и эффективности КСЗИ** | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.146-149 |  |
| **4** | **Методическое обеспечение работ по созданию КСЗИ Организационное обеспечение работ по созданию КСЗИ Инженерно-техническое обеспечение работ по созданию КСЗИ** | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.149-152 |  |
| **5** | **Обследование объекта защиты информации.** Руководящие документы. Организационные мероприятия | **2** |
| **Домашнее задание:** чтение и анализ литературы [8-10]  |  |
| **6** | **Анализ информационных активов объекта защиты.** Информация как предмет защиты Свойства информации. Виды, источники и носители защищаемой информации. Анализ режимов обработки информации | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.4-7 |
| **Практические занятия** | **42** |
| **1** | Изучение международных стандартов безопасности |
| **2** | Изучение российских стандартов безопасности |
| **3** | Разработка Политики ИБ предприятия |
| **4** | Анализ защищенности объекта защиты. Приказ о создании комиссии. Описание объекта защиты. |
| **5** | Анализ защищенности объекта защиты. Территория. Ограждение, ворота, калитки. |
| **6** | Анализ защищенности объекта защиты. Территория. Видеонаблюдение. Зоны покрытия. |
| **7** | Анализ защищенности объекта защиты. Здание. Окна, двери. |
| **8** | Анализ защищенности объекта защиты. Здание. Запирающие устройства. |
| **9** | Анализ защищенности объекта защиты. Здание. СКУД. |
| **10** | Анализ защищенности объекта защиты. Здание. Видеонаблюдение. Зоны покрытия. |
| **11** | Анализ защищенности объекта защиты. Помещение. Охранная сигнализация. Пожарная сигнализация. Двери. Окна. Видеонаблюдение. |
| **12** | Анализ защищенности объекта защиты. Помещение. Коммуникации |
| **13** | Акт обследования объекта защиты. |
| **14** | Составление перечня информационных активов предприятия |
| **15** | Составление списка режимов обработки информации |
| **16** | Определение угроз ИА объекта защиты |
| **17** | Расчет рисков потенциальных угроз ИБ |
| **18-19** | Методы снижения риска. Выбор технических средств по методике попарного сравнения. |
| **20-21** | Количественная и качественная оценка комплексной защиты информации |
| **Самостоятельная работа** | **4** |
| Подготовить выступление на тему «Информация как предмет защиты» |
| Подготовить выступление на тему «Перечень информационных активов предприятия» |
| **Тема 2** **Технические каналы утечки информации** | **Содержание** | **34** |
| **1** | **Опасные сигналы** Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке. | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 7-10 |
| **2** | **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. | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.10-15 |
| **3** | **Акустический канал утечки информации.** Виброакустический канал утечки информации.Акустоэлектрический канал утечки информации | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.72-99 |
| **4** | **Оптический канал утечки информации.** Оптико-электронный канал утечки информации | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.39-55 |
| **5** | **Радиоэлектронный канал утечки информации** | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.15-26 |
| **6** | Радиоэлектронный беспроводной канал утечки информации | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 26-27 |
| **7** | **Радиоэлектронный проводной канал утечки информации** Индукционный канал утечки информации | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.30-34 |
| **8** | **Параметрический канал утечки информации** Емкостной канал утечки информации | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.34-36 |
| **9** | **Вещественный канал утечки информации** | **2** |
| **Домашнее задание:** чтение и анализ литературы [2] стр.242-253 |
| **10** | **Методы и средства технической разведки** Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства дистанционного съема информации. | **2** |
| Домашнее задание: чтение и анализ литературы [1] стр.99-127 |
| **Практические занятия** | **12** |
| **22** | Измерение уровня акустических сигналов шумомером |
| **23** | Радиоэлектронный канал. Измерение уровня ЭМ-поля АТТ 2592 |
| **24 -25** | Радиоэлектронный канал. Сканирование сигналов анализатором поля. |
| **26** | Радиоэлектронный канал. Детектор ЗУ. |
| **27** | Опасные сигналы. Измерение параметров колебательного контураQ-метром |
| **Самостоятельная работа** | **2** |
| Подготовить презентацию на тему «Современная мобильная операционная система: инструкция пользователя» |
| **Тема 1.3 Физические основы утечки информации, методы и средства защиты** | **Содержание** | **36** |
| **1** | **Физические основы побочных электромагнитных излучений и наводок.** Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.30-34 |  |
| **2** | **Физические явления, вызывающие утечку информации** Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.34-39 |  |
| **3** | **Физические процессы при подавлении опасных сигналов** Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление. | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.205-248 |  |
| **4** | **Системы защиты от утечки информации по акустическому каналу** Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу. | **2** |
| **Домашнее задание:** чтение и анализ литературы [1] стр.318-330 |  |
| **5** | **Системы защиты от утечки информации по оптическому каналу** Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу. | **2** |
| Домашнее задание: чтение и анализ литературы [1] стр.166-181 |  |
| **6** | **Системы защиты от утечки информации по радиоэлектронному каналу**  | **2** |
| Домашнее задание: чтение и анализ литературы [1] стр.205-248 |  |
| **Практические занятия** | **18** |
| **28** | Применение генераторов белого шума |
| **29** | Применение виброакустической защиты |
| **30** | Применение тепловизора |
| **31** | Линейное зашумление сети 220 В |
| **32** | Зашумление диапазона ПЭМИН. ЛГШ. Паутина |
| **33** | Зашумление диапазона ЗУ. ЛГШ.  |
| **34** | Поиск видеокамер |
| **35** | Линейное зашумление телефонной сети |
| **36** | Экранирование помещений |
| **Самостоятельная работа** |
| Подготовить презентацию на тему: «Звукоизоляция помещений» | **6** |
|  |
| Подготовить презентацию на тему: «Защита по оптическому каналу УИ» |
| Подготовить презентацию на тему: «Экранирование кабелей» |
| **Тема 1.4****Эксплуатация технических средств защиты информации** | **Содержание** | **20** |
| **1** | **Этапы эксплуатации технических средств защиты информации.** Виды, содержание и порядок проведения технического обслуживания средств защиты информации. | **2** |
| Домашнее задание: чтение и анализ литературы [2] стр.330-349 |  |
| **2** | **Установка и настройка технических средств защиты информации.** Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. | **2** |
| Домашнее задание: чтение и анализ литературы [2] стр.330-349 |  |
| **3** | **Проведение аттестации объектов информатизации.** | **2** |
| Домашнее задание: чтение и анализ литературы [8]  |  |
| **4** | **Категорирование КИИ** | **2** |
| Домашнее задание: чтение и анализ литературы [8]  |  |
| **Практические занятия** | **12** |
| **37** | Регламентные работы по эксплуатации |
| **38** | ППР  |
| **39-40** | Аттестация объектов информатизации. Акт аттестации. |
| **41-42** | Категорирование КИИ. Акт категорирования |
| **Промежуточная аттестация (экзамен)** | **6** |

|  |  |
| --- | --- |
| **Раздел 2.** Организация физической защиты линий связи информационно-телекоммуникационных систем и сетей |  |
| **МДК 2.2 Физическая защита линий связи информационно-телекоммуникационных систем и сетей** | **113** |
| **Тема 2.1****Физическая защита объектов информатизации** | **Содержание** | **84** |
| 1 | **Цели и задачи физической защиты объектов информатизации** 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. | 6 |
|  | Домашнее задание: чтение и анализ литературы [1] стр.100-109 |  |
| 2 | **Общие 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 |
|  | Домашнее задание: чтение и анализ литературы [1] стр.110-120 |  |
| 3 | **Система обнаружения комплекса инженерно-технических средств физической защиты** 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 | 6 |
|  | Домашнее задание: чтение и анализ литературы [1] стр.120-131 |  |
| 4 | **Система контроля и управления доступом** 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. | 6 |
|  | Домашнее задание: чтение и анализ литературы [1] стр.131-137 |  |
| 5 | **Система телевизионного наблюдения** Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения. | 6 |
|  | Домашнее задание: чтение и анализ литературы [1] стр.137-149 |  |
| 6 | **Система сбора, обработки, отображения и документирования информации** 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 |
|  | Домашнее задание: чтение и анализ литературы [1] стр.149-153 |  |
| 7 | **Система воздействия** Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия. | 6 |
|  | Домашнее задание: чтение и анализ литературы [1] стр.154-159 |  |
| **Практические задания** | **42** |
| 1 | Монтаж датчиков пожарной и охранной сигнализации | 4 |
| 2 | Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя | 4 |
| 3 | Рассмотрение принципов устройства, работы и применения средств контроля доступа | 4 |
| 4 | Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. | 4 |
| 5 | Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. | 2 |
| 6 | Администрирование СКУД. Электронные ключи Touch-Memory | 2 |
| 7 | Администрирование СКУД. Электронные ключи Proximity-card | 2 |
| 8 | Изучение извещателей «Астра-6131» | 2 |
| 9 | Изучение извещателей «Астра-4511», «Астра-3321» | 2 |
| 10 | Изучение извещателей «Астра-421» | 2 |
| 11 | Изучение извещателей «Астра-5121» | 2 |
| 12 | Изучение «Астра-РПДК» | 2 |
| 13 | Настройка «Астра-РПУ» | 2 |
| 14 | Настройка «Астра-812 ППКОП» | 2 |
| 15 | Администрирование системы видеорегистрации  | 2 |
| 16 | Система видеонаблюдения. Подключение и настройка видеокамер | 2 |
| 17 | Биометрические системы СКУД по отпечатку пальца. видеообразу. Система штрих-кодирования.QR- коды. | 2 |
| **Тема 2.2** **Применение инженерно-технических средств физической защиты** | **Содержание** | **24** |
| 1 | **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 |
|  | Домашнее задание: Чтение и анализ литературы: [1] c.265-288 |  |
| 2 | **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. | 6 |
|  | Домашнее задание: Чтение и анализ литературы: [1] c.288-299 |  |
| **Практические задания** | **12** |
| 1 | Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты | 6 |
| 2 | Организация пропускного режима | 6 |
| **Самостоятельная работа при изучении раздела ПМ 3.** Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя.Оформление практических работ, отчетов и подготовка к их защите. | **5** |
| **Примерная тематика домашних заданий** |  |
| 1 | 1.Чтение и анализ литературы: [1] c.34-472Чтение и анализ литературы: [1] c.47-493Чтение и анализ литературы: [1] c.53-644Чтение и анализ литературы: [1] c.65-785Чтение и анализ литературы: [1] c.79-906Чтение и анализ литературы: [1] c.92-1127Чтение и анализ литературы: [1] c.113-128 |  |
| 2 | 1Чтение и анализ литературы: [1] c.231-245 |  |
| **Промежуточная аттестация (экзамен)**  | **6** |

|  |  |
| --- | --- |
|  |  |
| **Учебная практика****Виды работ** | **108** |
| 1 | Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике. Разработка маркетингового плана продвижения услуг связи. Выявление конкурентного преимущества на рынке. Проведение маркетингового исследования рынка услуг связи/ Анализ внешней микросреды маркетинга | 6 |
| 2 | Монтаж различных типов датчиков. | 6 |
| 3 | Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. | 6 |
| 4 | Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. | 6 |
| 5 |  Рассмотрение системы контроля и управления доступом. | 6 |
| 6 | Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. | 6 |
| 7 | Рассмотрение датчиков периметра, их принципов работы. | 6 |
| 8 | Выполнение звукоизоляции помещений системы зашумления. | 6 |
| 9 | Реализация защиты от утечки по цепям электропитания и заземления. | 6 |
| 10 | Разработка организационных и технических мероприятий по заданию преподавателя; | 6 |
| 11 | Разработка основной документации по инженерно-технической защите информации. | 6 |
| 12 | Монтаж различных типов датчиков. | 6 |
| 13 | Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. | 6 |
| 14 | Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. | 6 |
| 15 |  Рассмотрение системы контроля и управления доступом. | 6 |
| 16 | Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. | 6 |
| 17 | Рассмотрение датчиков периметра, их принципов работы. | 6 |
| 18 | Оформление отчета. Участие в зачет-конференции по учебной практике | 6 |
| **Производственная практика (по профилю специальности)****Виды работ** | **144** |
| 1 | Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Получение заданий по тематике. | 6 |
| 2 | Участие в монтаже технических средств защиты информации; | 6 |
| 3 | Участие в монтаже средств охраны и безопасности, инженерной защиты  | 6 |
| 4 | Участие в монтаже средств защиты информации от несанкционированного съёма и утечки по техническим каналам; | 6 |
| 5 | Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. | 6 |
| 6 | Участие в обслуживании технических средств защиты информации; | 6 |
| 7 | Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; | 6 |
| 8 | Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам; | 6 |
| 9 | Участие в эксплуатации технических средств защиты информации; | 6 |
| 10 | Участие в эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; | 6 |
| 11 | Участие в эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; | 6 |
| 12 | Участие в монтаже технических средств защиты информации; | 6 |
| 13 | Участие в монтаже средств охраны и безопасности, технической охраны объектов. | 6 |
| 14 | Участие в монтаже средств защиты информации от несанкционированного съёма и утечки по техническим каналам; | 6 |
| 15 | Участие в монтаже технических средств защиты информации; | 6 |
| 16 | Участие в монтаже средств охраны и безопасности и систем видеонаблюдения; | 6 |
| 17 | Участие в монтаже средств защиты информации от утечки по техническим каналам; | 6 |
| 18 | Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; | 6 |
| 19 | Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам; | 6 |
| 20 | Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; | 6 |
| 21 | Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам; | 6 |
| 22 | Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; | 6 |
| 23 | Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам; | 6 |
| 24 | Оформление отчета. Участие в зачет- конференции по производственной практике | 6 |
| **Промежуточная аттестация (экзамен (квалификационный))** | **5** |
| **Всего:** |  |

# **3. условия реализации программы ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

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

Реализация программы модуля предполагает наличие 1. Лаборатория защиты информации от утечки по техническим каналам (ОИБТкС+) 2. Лаборатория технической защиты информации

**Оборудование лаборатории:**

 - стол ученическией 9шт;

 - стол стендовый 2 шт;

 - стул 22 шт;

- стенд 14 шт;

**Технические средства обучения:**

- персональные компьютеры студентов 7 шт,

- система видеонаблюдения (6 видеомониторов);

- ЛГШ-720 Многозонная система обнаружения и блокирования мобильных средств связи для образовательных учреждений (IMT-MC-450, GSM900/1800, DECT1800, IMT-2000/UMTS (3G), Bluetooth, WiFi, 4G (WiMAX, LTE));

- ЛГШ-503 Генератор шума по цепям электропитания, заземления и ПЭМИ;

- Анализатор телефонных линий;

- Устройство обнаружения скрытых видеокамер;

- ЛГШ-404 Двухканальный генератор;

- ЛАГ-103 Акустический сейф;

- ЛГШ-304 Генератор акустического шума;

- ЛГШ-402 Система постановки виброакустических помех;

- ЛВП-10 Электромагнитный вибропреобразователь к ЛГШ-404 (для окон, стен, труб); ЛГШ-504 Программно-аппаратный комплекс защиты объектов информационных технологий от разведки ПЭМИ, 0,009 - 1000 МГц;

- Гранит-8 Абонентское устройство защиты информации.

# **3.2. Информационное обеспечение обучения**

Основные источники:

1.Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2020.

2.Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2021.

3.Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2022.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

4.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспеч-е информац. безопасности – М.: МИЭТ, 2019. – 184 с.

5.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информац. безопасности: учеб.пособие. – М.: МИЭТ, 2019. – 172 с.

6.Е.Б. Белов, В.Н. Пржегорлинский Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/. – М.: ИЦ «Академия», 2019. -336с

7. Ю.Ю. Коваленко. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / – М.: Горячая линия – Телеком, 2022.

8. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2021. — 416 с. — (СПО) https://znanium.com/catalog/product/1189327

Дополнительные источники:

1.Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование): https://znanium.com/catalog/product/1189327 (дата обращения: 10.02.2022).

2.Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с. — (Высшее образование: Бакалавриат). -: https://znanium.com/catalog/product/

Интернет ресурсы:

1. Федеральная служба по техническому и экспортному контролю [Электронный ресурс] – режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty

2. ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ [Электронный ресурс] – режим доступа: https://rkn.gov.ru/it/

3. ФГУП «ГРЧЦ», отраслевой экспертный центр, обеспечивающий выполнение задач и функций, возложенных на радиочастотную службу[Электронный ресурс] – режим доступа: https://grfc.ru/grfc/

# **4. Контроль и оценка результатов освоения профессионального модуля (пО РАЗДЕЛАМ)**

|  |  |  |
| --- | --- | --- |
| **Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля** | **Критерии оценки** | **Методы оценки** |
| **Раздел модуля 1. Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты** |
| ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в ИТКС. | Оценка «**отлично**» - проводит установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;- применяет нормативные правовые акты и нормативные методические документы в области защиты информации;Оценка «**хорошо**» - проводит установку, монтаж, настройку технических средств защиты информации от утечки по техническим каналам;- применяет нормативные методические документы в области защиты информации;Оценка «**удовлетворительно**» - проводит установку, монтаж технических средств защиты информации от утечки по техническим каналам; | Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам |
| ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в | Оценка «отлично» - проводит установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;- проводит техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;- применяет нормативные правовые акты и нормативные методические документы в области защиты информации;Оценка «хорошо» - проводит установку, монтаж, настройку технических средств защиты информации от утечки по техническим каналам;- проводит техническое обслуживание, устранение неисправностей технических средств защиты информации от утечки по техническим каналам;- применяет нормативные методические документы в области защиты информации;Оценка «удовлетворительно» - проводить установку технических средств защиты информации от утечки по техническим каналам;- проводит техническое обслуживание, технических средств защиты информации от утечки по техническим каналам; | Экзамен/зачет в форме собеседования: практическое задание по разработке программного модуля в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работамИнтерпретация резуль­татов наблюдений за деятельностью обучающегося в процессе практики |
| ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями. | Оценка «отлично» - проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС;- проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;- применяет нормативные правовые акты и нормативные методические документы в области защиты информации;Оценка «хорошо» - проводит измерение параметров фоновых шумов создаваемых оборудованием ИТКС;- проводит измерение параметров электромагнитных излучений, создаваемых техническими средствами защиты информации от утечки по техническим каналам;- применяет нормативные методические документы в области защиты информации;Оценка «удовлетворительно» - проводить измерение параметров фоновых шумов, создаваемых оборудованием ИТКС; | Экзамен/зачет в форме собеседования: практическое задание по разработке программного модуля в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работамИнтерпретация резуль­татов наблюдений за деятельностью обучающегося в процессе практики |
| ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС. | Оценка «отлично» - выявляет и оценивает угрозы безопасности информации в ИТКС;настраивает и применяет средства защиты информации в операционных системах, в том числе средства антивирусной защиты;проводит конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защитыОценка «хорошо» - настраивает и применяет средства защиты информации в операционных системах, в том числе средства антивирусной защиты;проводит конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защитыОценка «удовлетворительно» - проводит конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты | Экзамен/зачет в форме собеседования: практическое задание по разработке программного модуля в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работамИнтерпретация резуль­татов наблюдений за деятельностью обучающегося в процессе практики |
| **Раздел модуля 2.**  |
|  |  |  |
| ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. | * распознавание задач и/или проблем в профессиональном и/или социальном контексте;
* анализ задач и/или проблем и выделение её составных частей;
* определение этапов решения задач
 | Экспертное наблюдение за выполнением работ |
| ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. | - определение задач поиска информации;- планирование процесса поиска; - оформление результатов поиска |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. | - определение актуальности нормативно-правовой документации в профессиональной деятельности;- выстраивание траектории профессионального и личностного развития |
| ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. | - организация работы коллектива и команды;- взаимодействование с коллегами, руководством, клиентами |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. | - изложение своих мыслей на государственном языке;- оформление документов |
| ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей. | - описание значимости своей профессии;- презентация структуры профессиональной деятельности по профессии (специальности) |
| ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. | - соблюдение норм экологической безопасности; - определение направлений ресурсосбережения в рамках профессиональной деятельности по профессии (специальности). |
| ОК 09. Использовать информационные технологии в профессиональной деятельности. | - применение средств информационных технологий для решения профессиональных задач; использовать современное программное обеспечение |

Приложение 1

Обязательное

**КОНКРЕТИЗАЦИЯ ДОСТИЖЕНИЯ ЛИЧНОСТНЫХ РЕЗУЛЬТАТОВ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Личностные результаты** | **Содержание урока (тема, тип урока, воспитательные задачи)** | **Способ организации деятельности** | **Продукт деятельности** | **Оценка процесса формирования ЛР** |
| ЛР 17 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты ЛР 18 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты  | Тема:«Проблемы информационной безопасности» (4 ч.)Тип урока:комплексного применения знаний и способов деятельности – деловая играВоспитательная задача:- закрепление и углубление имеющихся навыков и умений;- развитие ответственного отношения к организации и ходу продуктивной деятельности при выполнении проектных работ | Викторина по информационной безопасности и информационным технологиям с использование электронных средств и проектов. Состоит из 2 частей, теоретическая игра Quiz и защита проектов по ИБ | День специалиста ИТВыступление и проекты по ИБ студентов, а так же комплексноезакрепление и применение знаний. | - эмоциональное отношение к своей будущей профессии- умение работать и выполнять требования трудовой дисциплины |

1. \*Раздел профессионального модуля – часть программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний. [↑](#footnote-ref-1)