**СОДЕРЖАНИЕ**

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

**1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ**

**ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

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

1.1.1.В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации в автоматизированных системах программными и программно-аппаратными средствами* и соответствующие ему профессиональные компетенции:

|  |  |
| --- | --- |
| Код | Наименование видов деятельности и профессиональных компетенций |
| 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. **Общие компетенции и личностные результаты**

|  |  |
| --- | --- |
| Код | Наименование видов деятельности и профессиональных компетенций |
| ОК 1. | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. |
| ОК 2. | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. |
| ОК 3. | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 4. | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. |
| ОК 5. | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 6. | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей. |
| ОК 7. | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 8. | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. |
| ОК 9. | Использовать информационные технологии в профессиональной деятельности. |
| ОК 10. | Пользоваться профессиональной документацией на государственном и иностранном языках. |
| ЛР 1 | Осознающий себя гражданином и защитником великой страны |
| ЛР 3 | Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих |
| ЛР 6 | Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях |
| ЛР 7 | Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности. |
| ЛР 8 | Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства |
| ЛР 10 | Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой |
| ЛР 13 | Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности |
| ЛР 14 | Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности |
| ЛР 15 | Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем |

1.1.3. В результате освоения профессионального модуля студент должен:

|  |  |
| --- | --- |
| **Иметь практический опыт** | * выявлении технических каналов утечки информации; * применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; * проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; * проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. |
| **уметь** | * применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; * применять технические средства для криптографической защиты информации конфиденциального характера; * применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; * применять инженерно-технические средства физической защиты объектов информатизации. |
| **знать** | * 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; * номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; * основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; * основные способы физической защиты объектов информатизации; * методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; * номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации. |

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

Всего 580 час, из них

на освоение МДК – 352 часов, в том числе

на промежуточную аттестацию по МДК – 12 часов,

на практики – 216 часов

**2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**2.1. Структура профессионального модуля** ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Коды профессиональных общих компетенций | Наименования разделов профессионального модуля | Объем образова-тельной программы, час. | **Объем профессионального модуля, час.** | | | | | |
| Обучение по МДК, в час. | | | Практики | | Самостоя-тельная работа |
| всего,  часов | в том числе | | учебная практика, часов | производственная практика,  часов |
| лабораторных и практических занятий | курсовая работа (проект),  часов |
| ОК 1– ОК 10  ПК.3.1- ПК.3.5  ЛР 7, 10, 14 | **МДК.03.01** Техническая защита информации | **172** | **158** | 78 | – | **-** | – | *–* |
| ОК 1– ОК 10  ПК.3.1- ПК.3.5  ЛР 1, 10, 15 | **МДК.03.02** Инженерно-технические средства физической защиты объектов информатизации | **180** | **174** | 80 | 30 | **-** | – | *–* |
| ОК 1– ОК 10  ПК.3.1- ПК.3.5  ЛР 6, 8, 13 | Учебная практика (Защита информации техническими средствами) | **72** | **-** | - | - | **72** | – | *–* |
| ОК 1– ОК 10  ПК.3.1- ПК.3.5  ЛР 1, 3, 14 | Производственная практика (Защита информации техническими средствами) | **144** |  | | | | **144** | – |
|  | **Всего:** | **584** | **332** | 136 | 30 | **72** | **144** | – |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)** | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)** | | **Объем часов** |
| 1 | 2 | | 3 |
| **Раздел 1 модуля. Техническая защита информации** | | | **176** |
| **МДК.03.01 Техническая защита информации** | | | **158** |
| **Раздел 1. Концепция инженерно-технической защиты информации** | | |  |
| **Тема 1.1.** Предмет и задачи технической защиты информации | | **Содержание** | **2** |
| Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации. | **2** |
| **Тема 1.2.** Общие положения защиты информации техническими средствами | | **Содержание** | **4** |
| Задачи и требования к способам и средствам защиты информации техническими средствами. | **2**  **2** |
| Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации. |
| **Раздел 2. Теоретические основы инженерно-технической защиты информации** | | |  |
| **Тема 2.1.** Информация как предмет защиты | | **Содержание** | **8** |
| Особенности информации как предмета защиты. | **2** |
| Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. | **2** |
| Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. | **2** |
| Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке. | **2** |
| **Тематика практических занятий и лабораторных работ** | **8** |
| Практическая работа №1 Автономный регистратор сотовых разговоров SpRecord SpGate MR | **2** |
| Практическая работа №2 Видеоглазок беспроводной Radio DVR | **2** |
| Практическая работа №3 Видеоэндоскоп MaxiVideo MV208 | **2** |
| Практическая работа №4 Микрофон усиливающий «Супер Ухо SD» | **2** |
| **Тема 2.2.** Технические каналы утечки информации | | **Содержание** | **8** |
| Понятие и особенности утечки информации. | **2** |
| Структура канала утечки информации. | **2** |
| Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. | **2** |
| Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. | **2** |
| **Тематика практических занятий и лабораторных работ** | **6** |
| Практическая работа №5 Видеорегистратор LawMate PV-550SE с камерой 618СА | **2** |
| Практическая работа №6 Подавитель диктофонов Бубен-ультра | **2** |
| Практическая работа №7 Беспроводная IP-камера для помещений Link 128 МИНИ | **2** |
| **Тема 2.3.** Методы и средства технической разведки | | **Содержание** | **8** |
| Классификация технических средств разведки. | **2** |
| Методы и средства технической разведки. | **2** |
| Средства несанкционированного доступа к информации. | **2** |
| Средства и возможности оптической разведки. Средства дистанционного съема информации. | **2** |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Практическая работа №8 Адаптер записи с телефонной линии ICON TRX1 | **2** |
| Практическая работа№9 Законодательство РФ в области информационной безопасности | **2** |
| **Раздел 3. Физические основы технической защиты информации** | | |  |
| **Тема 3.1.** Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок | | **Содержание** | **6** |
| Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. | **2** |
| Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. | **2** |
| Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей | **2** |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Практическая работа№10 Изучение положений о государственном лицензировании деятельности в области защиты информации | **2** |
| Практическая работа№11 Изучение положений о сертификации средств защиты информации по требованиям безопасности информации | **2** |
| **Тема 3.2.** Физические процессы при подавлении опасных сигналов | | **Содержание** | **2** |
| Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление. | **2** |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Практическая работа№12 Система сертификации средств криптографической защиты информации | **2** |
| Практическая работа№13 Изучение положения о сертификации средств вычислительной техники и связи | **2** |
| **Раздел 4. Системы защиты от утечки информации** | | |  |
| **Тема 4.1.** Системы защиты от утечки информации по акустическому каналу | | **Содержание** | **4** |
| Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. | **2** |
| Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу. | **2** |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Практическая работа №14 Изучение положения по аттестации объектов информатизации по требованиям безопасности информации | **2** |
| Практическая работа№15 Изучение особенностей аттестации помещений по требованиям безопасности информации | **2** |
| **Тема 4.2.** Системы защиты от утечки информации по проводному каналу | | **Содержание** | **8** |
| Принцип работы микрофона и телефона. | **2** |
| Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. | **2** |
| Системы защиты от диктофонов. | **2** |
| Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу. | **2** |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Практическая работа№16 Изучение положения об аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации | **2** |
| Практическое занятие 1. Угрозы безопасности информации на предприятии | **2** |
| **Тема 4.3.** Системы защиты от утечки информации по вибрационному каналу | | **Содержание** | **4** |
| Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. | **2** |
| Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу. | **2** |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Практическое занятие 2. Защита информации от традиционного шпионажа и диверсий | **2** |
| Практическое занятие 3. Защита информации от случайных угроз | **2** |
| **Тема 4.4.** Системы защиты от утечки информации по электромагнитному каналу | | **Содержание** | **4** |
| Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. | **2** |
| Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу. | **2** |
| **Тематика практических занятий и лабораторных работ** | **8** |
| Практическое занятие 4. Основные этапы проектирования системы защиты информации | **2** |
| Практическое занятие 5. Специфика персонала предприятия как объекта защиты | **2** |
| Практическое занятие 6. Разработка моделей объектов защиты | **2** |
| Практическое занятие 7. Электронно-цифровая подпись | **2** |
| **Тема 4.5.** Системы защиты от утечки информации по телефонному каналу | | **Содержание** | **4** |
| Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. | **2** |
| Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу. | **2** |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Практическое занятие 8. Методы аутентификации и способы управления доступом | **2** |
| Практическое занятие 9. Защита информации от электромагнитных излучений и наводок | **2** |
| **Тема 4.6.** Системы защиты от утечки информации по электросетевому каналу | | **Содержание** | **4** |
| Низкочастотное устройство съема информации. | **2** |
| Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу. | **2** |
| **Тематика практических занятий и лабораторных работ** | **4** |
| Практическое занятие 10. Исследование протокола IPSec | **2** |
| Практическое занятие 11. Изучение средств IP-безопасности, обеспечиваемых протоколом Ipsec | **2** |
| **Тема 4.7.** Системы защиты от утечки информации по оптическому каналу | | **Содержание** | **2** |
| Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу. | **2** |
| **Тематика практических занятий и лабораторных работ** | **2** |
| Тематика учебных занятий формируется образовательной организацией самостоятельно | ***2*** |
| **Раздел 5. Применение и эксплуатация технических средств защиты информации** | | |  |
| **Тема 5.1.** Применение технических средств защиты информации | | **Содержание** | **6** |
| 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. | ***2*** |
| Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. | ***2*** |
| Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. | ***2*** |
| **Тематика практических занятий и лабораторных работ** | **10** |
| Практическое занятие 12. Организация комплексной системы защиты информации объекта | **2** |
| Практическое занятие 13. Защита информации правовыми и организационными методами | **2** |
| Практическое занятие 14. Моделирование технических каналов утечки информации | **2** |
| Практическое занятие 15. Анализ рисков безопасности информации | **2** |
| Практическое занятие 16. Изучение правовых основ защиты информации и информационной безопасности (Федеральный закон РФ «Об информации, информационных технологиях и о защите информации») | **2** |
| **Тема 5.2.** Эксплуатация технических средств защиты информации | | **Содержание** | **8** |
| Этапы эксплуатации технических средств защиты информации. | **2** |
| Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. | **2** |
| Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. | **2** |
| Проведение аттестации объектов информатизации. | **2** |
| **Тематика практических занятий и лабораторных работ** | **16** |
| Тематика учебных занятий формируется образовательной организацией самостоятельно | **2** |
| Практическое занятие 17. Аппаратно-программные средства контроля доступа | **2** |
| Практическое занятие 18. Настройка аутентификации пользователейс помощью электронного замка «СОБОЛЬ-PCI | **2** |
| Практическое занятие 19. Управление ключами криптографической защиты электронной почты в комплексе программных средств | **2** |
| Практическое занятие 20. Изменение политики контроля устройств | **2** |
| Практическое занятие 21. Настройка средств криптографической защиты сетевого трафика стандартного протокола IPSec в операционной системе Microsoft Windows | **2** |
| Практическое занятие 22. Управление средствами информационной безопасности сервера приложений Internet Information Server | **2** |
| Практическое занятие 23. Настройка средств защиты информации сервера приложений Apache HTTPD | **2** |
| **Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации** | | | **169** |
| **МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации** | | | **174** |
| **Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты** | | |  |
| **Тема 1.1.** Цели и задачи физической защиты объектов информатизации | **Содержание** | | **10** |
| Характеристики потенциально опасных объектов. | | **2** |
| Содержание и задачи физической защиты объектов информатизации. | | **2** |
| Основные понятия инженерно-технических средств физической защиты | | **2** |
| Категорирование объектов информатизации. | | **2** |
| Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов. | | **2** |
| **Тематика практических занятий и лабораторных работ** | | **10** |
| Практическая работа № 1. Теоретические основы информационной безопасности | | **2** |
| Практическая работа № 2. Принципы построения системы защиты информации | | **2** |
| Практическая работа №3. Классификация угроз информационной безопасности | | **2** |
| Практическая работа №4. Методы и средства обеспечения информационной безопасности | | **2** |
| Практическая работа №5. Организация системы защиты информации | | ***2*** |
| **Тема 1.2.** Общие сведения о комплексах инженерно-технических средств физической защиты | **Содержание** | | **10** |
| Общие принципы обеспечения безопасности объектов. | | **2** |
| Жизненный цикл системы физической защиты. | | **2** |
| Принципы построения интегрированных систем охраны. | | **2** |
| Классификация и состав интегрированных систем охраны. | | **2** |
| Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. | | **2** |
| **Тематика практических занятий и лабораторных работ** | | **10** |
| Практическая работа №6. Информационная безопасность отдельных экономических систем | | **2** |
| Практическая работа № 7. Обнаружение и локализация радиоизлучающих технических средств с помощью детектора поля ST 111. | | **2** |
| Практическая работа №8. Поиск и локализация скрытых видеокамер с использованием обнаружителя скрытых видеокамер «Оптик-2». | | **2** |
| Практическая работа №9. Обнаружение скрытых проводных и беспроводных видеокамер с помощью оптического обнаружителя видеокамер BugHunter Dvideo. | | **2** |
| Практическая работа №10. Исследование помещений на предмет обнаружения в ближней зоне скрытых радиопередатчиков с помощью индикатора поля Expert BugHunter BH-03 | | 2 |
| **Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты** | | |  |
| **Тема 2.1** Система обнаружения комплекса инженерно-технических средств физической защиты | **Содержание** | | **10** |
| Информационные основы построения системы охранной сигнализации. | | 2 |
| Назначение, классификация технических средств обнаружения. | | 2 |
| Построение систем обеспечения безопасности объекта. | | 2 |
| Периметровые средства обнаружения: назначение, устройство, принцип действия. | | 2 |
| Объектовые средства обнаружения: назначение, устройство, принцип действия. | | 2 |
| **Тематика практических занятий и лабораторных работ** | | **10** |
| Практическая работа №11Автономный регистратор сотовых разговоров SpRecord SpGate MR | | **2** |
| Практическая работа №13 Видеоэндоскоп MaxiVideo MV208 | | **2** |
| Практическая работа №14 Микрофон усиливающий «Супер Ухо SD» | | **2** |
| Практическая работа №15 Видеорегистратор LawMate PV-550SE с камерой 618СА | | **2** |
| Практическая работа №16 Подавитель диктофонов Бубен-ультра | | 2 |
| **Тема 2.2.** Система контроля и управления доступом | **Содержание** | | **8** |
| Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. | | 2 |
| Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. | | 2 |
| Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. | | 2 |
| Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ. | | 2 |
| **Тематика практических занятий и лабораторных работ** | | **10** |
| Практическая работа № 1 Шифрование информации методом простой подстановки | | 2 |
| Практическая работа № 2 Шифрование информации методом «Решетки Кардано» | | 2 |
| Практическая работа № 3 Шифрование информации методом усложненной перестановки по таблице | | 2 |
| Практическая работа № 4 Шифрование информации методом сложной подстановки | | 2 |
| Практическая работа № 5 Шифрование информации методом «Линейного регистра с обратными связями» | | 2 |
| **Тема 2.3.** Система телевизионного наблюдения | **Содержание** | | **8** |
| Аналоговые и цифровые системы видеонаблюдения | | **2** |
| Назначение системы телевизионного наблюдения. | | **2** |
| Состав системы телевизионного наблюдения. Видеокамеры. Объективы. | | **2** |
| Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения. | | **2** |
|  | **Тематика практических занятий и лабораторных работ** | | **10** |
| Практическая работа № 6 Изучение CRC | | **2** |
| Практическая работа № 7 Изучение алгоритма шифрования RSA | | **2** |
| Практическая работа № 8 Количественная оценка стойкости парольной защиты | | **2** |
| Практическое занятие 9. Исследование типов вредоносного ПО | | **2** |
| Практическое занятие 10. Пути заражения ПК вредоносным ПО | | 2 |
| **Тема 2.4.** Система сбора, обработки, отображения и документирования информации | **Содержание** | | **8** |
| Классификация системы сбора и обработки информации. | | **2** |
| Схема функционирования системы сбора и обработки информации. | | **2** |
| Варианты структур построения системы сбора и обработки информации. | | **2** |
| Устройства отображения и документирования информации. | | **2** |
| **Тематика практических занятий и лабораторных работ** | | **10** |
| Практическое занятие 11. Изучение форм проявления компьютерных вирусов | | **2** |
| Практическое занятие 12. Изучение работы COM-вируса | | **2** |
| Практическое занятие 13. Изучение работы вируса, замещающего программный код | | **2** |
| Практическое занятие 14. Профилактика проникновения вредоносного программного обеспечения посредством исследования Реестра ОС Windows | | **2** |
| Практическое занятие 15. Профилактика проникновения вредоносного программного обеспечения посредством организации защиты от макровирусов средствами Microsoft Word | | 2 |
| **Тема 2.5** Система воздействия | **Содержание** | | **2** |
| Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия. | | **2** |
| **Тематика практических занятий и лабораторных работ** | | **10** |
| Практическое занятие 16. Исследование уязвимостей Интернет браузеров в контексте новых веб технологий | | **2** |
| Практическая работа 17. Изучение работы программы AVZ | | **2** |
| Практическая работа 18. Основные признаки присутствия вредоносных программ и методы по устранению последствий вирусных заражений компьютерной системы | | **2** |
| Практическая работа 19. Сравнительный анализ анализ антивирусных программ | | **2** |
| Практическая работа 20. Мониторинг подозрительных процессов с помощью специальных программ | | 2 |
| **Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты** | | |  |
| **Тема 3.1** Применение инженерно-технических средств физической защиты | **Содержание** | | **6** |
| Периметровые и объектовые средства обнаружения, порядок применения. | | 2 |
| Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. | | 2 |
| Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия. | | 2 |
| **Тематика практических занятий и лабораторных работ** | | **4** |
| Практическая работа 21. Скрипты управления программы AVZ | | **2** |
| Практическая работа 22. Работа скриптов программы AVZ | | 2 |
| **Тема 3.2.** Эксплуатация инженерно-технических средств физической защиты | **Содержание** | | **2** |
| 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. | | 2 |
| **Тематика практических занятий и лабораторных работ** | | **6** |
| Практическая работа 23. Установка и предварительная настройка Антивируса Касперского | | **2** |
| Практическая работа 24. Работа с Антивирусом Касперского Часть 1 | | **2** |
| Практическая работа 24. Работа с Антивирусом Касперского Часть 2 | | **2** |
| **Курсовой проект (работа)** | | | **30** |
| **Примерная тематика курсового проекта (работы)**   1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества. | | |
| **Учебная практика по разделу 2 модуля**   1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы зашумления. 8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации. | | | ***72*** |
| **Производственная практика профессионального модуля**  **Виды работ**   1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. | | | ***144*** |
| ***Экзамен по профессиональному модулю*** | | |  |
| ***Всего*** | | | ***584*** |

1. **УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

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

Лаборатория электроники и схемотехники; сетей и систем передачи информации; программных и программно-аппаратных средств защиты информации; технических средств защиты информации. Полигоны вычислительной техники; учебных баз практик. Кабинет для самостоятельной работы

**Наименование оборудования:**

1. Учебно-лабораторные стенды для освоения типовых схемотехнических решений -2;

2. Контрольно-измерительная аппаратура для измерения временных характеристик, амплитуды и формы сигналов -1;

3. Генераторы сигналов с заданными параметрами - 1.

4. Рабочие места на базе вычислительной техники -9;

5. Программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности - Программно-аппаратный комплекc ViPNet IDS1000 2.x– 1шт

6. Аппаратные средства аутентификации пользователя Идентификатор iButton DS1995 – 1 шт ;

7. Средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок - подавитель диктофонов Бубен-ультра – 1 шт;

8. Средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.); Детектор поля ST 111 - 2 шт. Обнаружители скрытых видеокамер «Оптик-2» - 1 шт.

9. Стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов - программное обеспечение сетевого оборудования Cisco Packet Tracer -1

10. Доска 1

11. Стенды 3

12. Плакаты 10

13. Монитор 9

14.Системный блок 9

15.Клавиатура 9

16.Мышь компьютерная 9

**Программное обеспечение общего и профессионального назначения:**

Microsoft Office, Kaspersky Endpoint Security,Cisco Packet Tracer, Eraser -1, Windows Vulnerability Scanner -1; Про CSP-1;

**4.2 Информационное обеспечение обучения:**

**Перечень рекомендуемых учебных изданий, дополнительной литературы**

**Основная литература:**

1.Белов Е.Б., Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для СПО/ Е.Б. Белов, В.Н. Пржегорлинский .-М.: ИЦ «Академия», 2017.- 336с.

2.Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 416 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт 7БЦ) ISBN 978-5-8199-0331-5 - Режим доступа: <http://znanium.com/catalog/product/549989>

3. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2018. — 416 с. — (Среднее профессиональное образование). - Режим доступа: <http://znanium.com/catalog/product/945331>

**Дополнительная литература:**

* 1. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.: 60x90 1/16. - (Профессиональное образование) (Обложка) ISBN 978-5-00091-079-5 - Режим доступа: <http://znanium.com/catalog/product/508381>
  2. Безопасность и управление доступом в информационных системах : учеб. пособие / А.В. Васильков, И.А. Васильков. — М. : ФОРУМ : ИНФРА-М, 2017. — 368 с. — (Среднее профессиональное образование). - Режим доступа: <http://znanium.com/catalog/product/537054>

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

Профессиональный модуль изучается параллельно с учебными дисциплинами общепрофессионального цикла.

Выполнение практических занятий предполагает деление группы по числу рабочих мест, оборудованных персональными компьютерами.

Учебная практики рассчитана на 36 часов в неделю и проводится в аудиториях учебного заведения. Производственная практика проходит в организациях города и края любой формы собственности.

Обязательным условием допуска к производственной практике в рамках профессионального модуля является освоение учебной практики с целью получения первичных профессиональных навыков.

Итоговая аттестация по профессиональному модулю проводится в форме экзамена (квалификационного).

**4.4. Кадровое обеспечение образовательного процесса**

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): наличие высшего профессионального образования, соответствующего профилю преподаваемого модуля, обязательная стажировка в профильных организациях не реже 1-го раза в 3 года.