МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯРОСТОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

РОСТОВСКОЙ ОБЛАСТИ

**«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ СВЯЗИ И ИНФОРМАТИКИ»**

**РАБОЧАЯ ПРОГРАММА**

профессионального модуля

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

программы подготовки специалистов среднего звена

для специальности

**10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»**

(базовой подготовки)

г. Ростов-на-Дону

2023 г.

|  |  |
| --- | --- |
| **ОДОБРЕНО**  На заседании цикловой комиссии  «Информационная безопасность»  Протокол № 11 от 30 июня 2023 года  Председатель ЦК ИБ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Копылова О.В. | **УТВЕРЖДАЮ**  Зам. директора по НМР  \_\_\_\_\_\_\_\_\_\_ Подцатова И.В.  «30» июня 2023 г. |

Рабочая программа профессионального модуля ПМ.03 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Минобрнауки России от 09.12.2016 №1551 (в ред. от 17.12.2020) «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования» по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем.

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж связи и информатики»

Разработчики:

МДК.03.01Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, Шлюпкина А.И.– преподаватель ГБПОУ РО «РКСИ»

МДК.03.02Физическая защита линий связи информационно-телекоммуникационных систем и сетей, Копылова О.В.– преподаватель ГБПОУ РО «РКСИ»

УП.03.01 Учебная практика "Экономическое обоснование проекта по защите информации", Ревнивцева О.А. - преподаватель ГБПОУ РО «РКСИ»

УП.03.02Учебная практика "Защита информации", Копылова О.В.– преподаватель ГБПОУ РО «РКСИ»

Производственная практика (по профилю специальности)

Рецензенты:

Комова О.В. – председатель цикловой комиссии «Информационная безопасность» ГБПОУ РО «РКСИ»

Масютин А.Н. - Начальник управления системных проектов Ростовского НТЦ ФГУП «НПП «Гамма»

**СОДЕРЖАНИЕ**

[1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 4](#_Toc64663216)

[2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 13](#_Toc64663217)

[3.СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 15](#_Toc64663218)

[4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 36](#_Toc64663219)

[5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 40](#_Toc64663220)

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

**1.1 Область применения рабочей программы**

Рабочая программа профессионального модуля ПМ.03 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» разработана на основе ФГОС СПО по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», утвержденного приказом Минобрнауки России от 09.12.2016 №1551 (в ред. от 17.12.2020).

Рабочая программа предназначена для студентов очной формы обучения.

В процессе освоения ПМ у обучающегося формируются соответствующие общие компетенции и профессиональные компетенции (ПК):

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

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

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

* 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 ПМ.03«Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты «предназначена для студентов 4 курсов очной формы обучения.

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

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

**иметь практический опыт:**

* установки, монтажа, настройки и испытания технических средств защиты информации от утечки по техническим каналам;
* защиты информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
* проведения отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей;
* *применение основных типов технических средств защиты информации;*
* *выявление технических каналов утечки информации;*
* *участие в мониторинге эффективности технических средств защиты информации;*
* *диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации;*
* *проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации;*
* *проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;*
* *установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты.*

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;
* *производить установку и монтаж технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами;*
* *производить настройку и испытания технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов;*
* *применять технические средства для уничтожения информации и носителей информации;*
* *применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;*
* *применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;*
* *применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;*
* *применять инженерно-технические средства физической защиты объектов информатизации.*

#### *знать:*

* 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;
* технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах;
* технические средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок;
* методы и методики контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок;
* методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
* номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
* номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации
* номенклатуру применяемых средств физической защиты объектов информатизации;
* физические основы формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
* структуру и условия формирования технических каналов утечки информации;
* порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;
* основные способы физической защиты информации.

**Вариативная часть.**

**Использование часов вариативной части**

Из вариативной части на профессиональный модуль ПМ.03 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» отведено **116** часов:

на частично-вариативную учебную дисциплину МДК 03.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» отведено **31** часов;

на частично-вариативную учебную дисциплину МДК 03.02 «Физическая защита линий связи информационно-телекоммуникационных систем и сетей» отведено **22** часа;

на вариативную учебную дисциплину МДК 03.03 «Экономическое обоснование проекта по защите информации» отведено **50** часов.

на квалификационный экзамен по ПМ 03 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» отведено **8** часов.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Дополнительные умения, знания** | **№, наименование раздела/темы** | **Количество часов** | **Формируемые компетенции** | **Обоснование включения в рабочую программу** |
| 1 | уметь:  ­ производить установку и монтаж технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами;  ­ производить настройку и испытания технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов;  ­ применять технические средства для уничтожения информации и носителей информации;  ­ применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;  ­ применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;  ­ применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;  ­ применять инженерно-технические средства физической защиты объектов информатизации.  знать:  ­ технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом "высокочастотного облучения" основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах;  ­ технические средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок;  ­ методы и методики контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок;  ­ методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;  ­ номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;  ­ номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации  ­ номенклатуру применяемых средств физической защиты объектов информатизации;  ­ физические основы формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;  ­ структуру и условия формирования технических каналов утечки информации;  ­ порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;  основные способы физической защиты информации. | МДК 03.01.  Тема 1.6  Экранирование электромагнитных волн  Устройства контроля и защиты слаботочных линий связи, оптоволоконных, электрических сетей, цепей заземления  Скрытие и защита от утечки информации по акустическому и виброакустическому каналам  Скрытие речевой информации в телефонных системах  Технические средства для уничтожения информации и носителей информации, порядок применения | 10 | ПК. 3.1  ПК. 3.2  ПК. 3.3  ПК. 3.4  ОК. 1  ОК. 2  ОК. 3  ОК. 4  ОК. 5  ОК. 6  ОК. 7  ОК. 8  ОК. 9  ОК. 10  ОК. 11 | Запрос работодателя на дополнительные результаты освоения ОПОП |
| МДК 03.01.  Тема 1.7  Порядок проведения проверки технических средств  Выполнение поисковых мероприятия  Специальные исследования в области защиты речевой и цифровой информации  Практическое занятие 20. Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации  Практическое занятие 21. Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, использующих силовые линии сети переменного тока и линии систем охранной (пожарной) сигнализации  Практическое занятие 22. Контроль эффективности защиты речевой информации с помощью программно-аппаратного комплекса  Практическое занятие 23. Поиск и измерение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса  Практическое занятие 24. Поиск каналов утечки речевой информации  Практическое занятие 25. Блокировка виброакустических каналов утечки информации  Практическое занятие 26. Блокировка сотовых телефонов  Практическое занятие 27. Поиск и обнаружение ИК-закладок | 30 |
| 2 | МДК 03.01.  Тема 1.8  Алгоритм проектирования системы защиты информации  Моделирование объектов защиты  Моделирование угроз информации  Рекомендации по организации физической защиты источников информации  Рекомендации по предотвращению утечки информации  Общие сведения об аттестации объектов информатизации  Специальные проверки, обследования, исследования  Практическое занятие 28. Описание объекта защиты. Характеристика защищаемой информации  Практическое занятие 29. Моделирование угроз на объекте защиты  Практическое занятие 30. Разработка мер по защите информации | 20 |
| 3 | МДК 03.01.  Тема 1.9  Цели и задачи технического контроля эффективности мер защиты информации  Порядок проведения контроля защищенности информации на объекта ВТ от утечки по каналу ПЭМИ  Методы испытаний ПЭВМ. Порядок проведения контроля защищенности АС от НСД  Методы контроля побочных электромагнитных излучений генераторов технических средств  Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации. Общие положения  Выбор контрольных точек и размещение элементов измерительных комплексов. Калибровка передающего измерительного комплекса  Измерение отношений «сигнал/шум» Контроль технических средств и систем на наличие акустоэлектрических преобразований | 14 |
| 4 | МДК 03.02  Тема 2.5  Практическое занятие 6. Определение питающих напряжений извещателей  Практическое занятие 7. Определение токов потребления извещателей.  Практическое занятие 8. Определение сопротивления участка цепи "заземление прибор - шина заземления"  Практическое занятие 9. Измерение нагрузочных резисторов.  Практическое занятие 10. Монтаж различных охранных систем.  Практическое занятие 11. Определение и устранение ошибок рабочей системы.  Практическое занятие. 12 Программирование приборов и оборудования.  Практическое занятие. 13 Наладка приборов и оборудования.  Практическое занятие 14. Основы работы оператора охранных систем.  Практическое занятие 15. Работа с электроизмерительными приборами. | 20 |
| 5 | МДК 03.02  Тема 2.10  Практическое занятие 29. Подключение датчиков  Практическое занятие 30. Отображение показателей  Практическое занятие 31. Управление исполнительными устройствами  Практическое занятие 32. Создание будильников для запуска исполнительных устройств по расписанию  Практическое занятие 32. Организация подключения к сети Интернет | 24 |

**В рамках образовательной программы у обучающихся формируются личностные результаты:**

|  |  |
| --- | --- |
| **Личностные результаты**  **реализации программы воспитания**  *(дескрипторы)* | **Код личностных результатов  реализации  программы  воспитания** |
| Осознающий себя гражданином России и защитником Отечества, выражающий свою российскую идентичность в поликультурном  и многоконфессиональном российском обществе и современном мировом сообществе. Сознающий свое единство с народом России,  с Российским государством, демонстрирующий ответственность  за развитие страны. Проявляющий готовность к защите Родины, способный аргументированно отстаивать суверенитет и достоинство народа России, сохранять и защищать историческую правду  о Российском государстве. | **ЛР 1** |
| Проявляющий активную гражданскую позицию на основе уважения закона и правопорядка, прав и свобод сограждан, уважения  к историческому и культурному наследию России. Осознанно  и деятельно выражающий неприятие дискриминации в обществе  по социальным, национальным, религиозным признакам; экстремизма, терроризма, коррупции, антигосударственной деятельности. Обладающий опытом гражданской социально значимой деятельности. | **ЛР 2** |
| Демонстрирующий приверженность традиционным духовно-нравственным ценностям, культуре народов России, принципам честности, порядочности, открытости. Действующий  и оценивающий свое поведение и поступки, поведение и поступки других людей с позиций традиционных российских духовно-нравственных, социокультурных ценностей и норм с учетом осознания последствий поступков. Готовый к деловому взаимодействию и неформальному общению с представителями разных народов, национальностей, вероисповеданий, отличающий их от участников групп с деструктивным и девиантным поведением. Демонстрирующий неприятие социально опасного поведения окружающих и предупреждающий его. Проявляющий уважение  к людям старшего поколения, готовность к участию в социальной поддержке нуждающихся в ней. | **ЛР 3** |
| Проявляющий и демонстрирующий уважение к труду человека, осознающий ценность собственного труда и труда других людей. Экономически активный, ориентированный на осознанный выбор сферы профессиональной деятельности с учетом личных жизненных планов, потребностей своей семьи, российского общества. Выражающий осознанную готовность к получению профессионального образования, к непрерывному образованию  в течение жизни Демонстрирующий позитивное отношение  к регулированию трудовых отношений. Ориентированный  на самообразование и профессиональную переподготовку  в условиях смены технологического уклада и сопутствующих социальных перемен. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа». | **ЛР 4** |
| Осознающий и деятельно выражающий приоритетную ценность каждой человеческой жизни, уважающий достоинство личности каждого человека, собственную и чужую уникальность, свободу мировоззренческого выбора, самоопределения.  Проявляющий бережливое и чуткое отношение к религиозной принадлежности каждого человека, предупредительный  в отношении выражения прав и законных интересов других людей. | **ЛР 7** |
| Бережливо относящийся к природному наследию страны и мира, проявляющий сформированность экологической культуры на основе понимания влияния социальных, экономических  и профессионально-производственных процессов на окружающую среду. Выражающий деятельное неприятие действий, приносящих вред природе, распознающий опасности среды обитания, предупреждающий рискованное поведение других граждан, популяризирующий способы сохранения памятников природы страны, региона, территории, поселения, включенный  в общественные инициативы, направленные на заботу о них. | **ЛР 10** |
| Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания | **ЛР 12** |
| 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 13** |
| Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности | **ЛР 14** |
| Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем | **ЛР 15** |
| Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению | **ЛР16** |
| Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение | **ЛР17** |
| Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве | **ЛР18** |
| Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации | **ЛР19** |
| Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики | **ЛР20** |
| Демонстрирующий уровень подготовки, соответствующий современным стандартам и передовым технологиям, потребностям регионального рынка и цифровой экономики, в том числе требованиям стандартов Ворлдскиллс | **ЛР 22** |
| Способный использовать различные цифровые средства и умения, позволяющие во взаимодействии с другими людьми достигать поставленных целейв цифровой среде | **ЛР 23** |
| Способный работать в мультикультурных и мультиязычных средах, владетьнавыками междисциплинарного общения в условиях постепенного формирования глобального рынка труда посредством развития международных стандартов найма и повышения мобильности трудовых ресурсов | **ЛР 24** |

**1.3 Рекомендуемое количество часов на освоение рабочей программы профессионального модуля ПМ.03 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты»**

|  |  |  |
| --- | --- | --- |
| Всего | **–** | **552 часа** |
| в том числе: |  |  |
| - обязательную аудиторную учебную нагрузку обучающегося | **–** | **336 часов** |
| теоретическое обучение |  | 150 часов |
| практические занятия |  | 156 часов |
| - самостоятельную работу обучающегося:   * Написание реферата. * Написание конспекта первоисточника. * Подготовка информационного сообщения. * Создание презентации. * Составление опорного конспекта. * Подготовка к практическим занятиям.   Другие виды самостоятельной работы | **–** | **28 часа** |
| Промежуточная аттестация |  | **8 часов** |
| - Учебную практику | **–** | **72 час** |
| - Производственную практику | **–** | **108 часов** |
| Экзамен квалификационный | **-** | 8 часов |

Практическая подготовка при реализации профессионального модуля путем проведения практических и лабораторных занятий, учебной и производственной практики занимает **336** часов.

# **РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

Результатом освоения профессионального модуля ПМ.03 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» является овладение обучающимися видом профессиональной деятельности (ВПД) Защита информации в информационно-телекоммуникационных системах и сетях сиспользованием технических средств защиты, в том числе профессиональными компетенциями (ПК), общими компетенциями (ОК).

|  |  |
| --- | --- |
| Код | Наименование результатов обучения |
| 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 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 поддержания необходимого уровня физической подготовленности. |
| ОК 9. | Использовать информационные технологии в профессиональной деятельности. |
| ОК 10. | Пользоваться профессиональной документацией на государственном и иностранном языке |

# **3.СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**3.1 Тематический план профессионального модуля ПМ.03«Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты»**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Код профессиональной компетенции** | **Наименования МДК профессионального модуля** | **Всего (максимальное количество), часов** | **Объем времени, отведенный на освоение  междисциплинарного курса** | | | | | | **Практика** | |
| **Обязательная аудиторная учебная нагрузка обучающегося** | | | **Самостоятельная работа обучающегося** | | | **Учебная,** часов | **Производ ственная**  **(по профилю специальности и преддипломная),** часов |
| **Всего (обязательная аудиторная нагрузка),** часов | **В том числе** | | **Всего,** часов | **курсовая работа (проект),** часов | |
| **лаб.работы и практич. занятия,**  часов | **курсовая работа (проект),** часов |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | | **9** | **10** |
| **ПК 3.1-ПК3.3** | **МДК 03.01«Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты»** | **182** | **160** | 62 | 30 | 22 | - | | **-** | **-** |
| **ПК 3.4** | **МДК 03.02«Физическая защита линий связи информационно-телекоммуникационных систем и сетей»** | **132** | **126** | 70 | **-** | 6 | **-** | | **-** | **-** |
| **ПК 3.1-ПК3.4** | **МДК 03.03 «Экономическое обоснование проекта по защите информации»** | **50** | **50** | 26 | **24** |  |  | |  |  |
|  | **УП.03.01 «Экономическое обоснование проекта по защите информации»** | **36** | **-** | - | **-** | - | **-** | | **36** | **-** |
| **ПК 3.1-ПК3.4** | **УП.03.02 «Защита информации»** | **36** | **-** | - | **-** | - | **-** | | **36** | **-** |
| **ПК 3.1-ПК3.4** | **Производственная практика (по профилю специальности)** | **108** |  | | | | | | | **108** |
|  | **Всего:** | **464** | **286** | **132** | **30** | **28** | **-** | **72** | | **108** |

**3.2 Содержание обучения по профессиональному модулю**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Наименование разделов профессионального модуля (разделов - междисциплинарных курсов) и тем** | **Содержание учебного материала, лабораторные работы, практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)** | | | | **Объем часов** | **Осваиваемые элементы компетенций** |
| **1** | **2** | | | | **3** | **4** |
| **Раздел 1. МДК 03.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты»** | | | | | **114** |  |
| **Тема 1.1** Предмет и задачи технической защиты информации | **Содержание:** | | | | **4** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12 – ЛР20, ЛР22-ЛР24  ПК 3.1  ПК 3.2  ПК 3.3  ПК 3.4  ОК1-10 |
|  | Предмет и задачи технической защиты информации | | | 2 |
|  | Принципы системного анализа проблем инженерно-технической защиты информации. | | | 2 |
| **Тема 1.2** Теоретические основы инженерно-технической защиты информации | **Содержание:** | | | | **6** |
|  | | Свойства информации. Виды, источники и носители защищаемой информации | | 2 |
|  | | Демаскирующие признаки объектов наблюдения, сигналов и веществ | | 2 |
|  | | Характеристики угроз безопасности информации | | 2 |
| **Тема 1.3** Технические каналы утечки информации обрабатываемой ТСПИ и при передачи ее по каналам связи | **Содержание:** | | | | **8** |
|  | | Преобразование акустических сигналов в электрические сигналы | | 2 |
|  | | Низкочастотные и высокочастотные излучения ТС. Электромагнитные излучения | | 2 |
|  | | Утечки 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 |
| **Тема 1.4** Технические каналы утечки речевой и видовой информации | **Содержание:** | | | | **4** |
|  | | Основные характеристики каналов утечки речевой информации | | 2 |
|  | | Основные характеристики каналов утечки видовой информации | | 2 |
| **Тема 1.5** Средства выявления каналов утечки информации | **Содержание:** | | | | **2** |
|  | | Индикаторы ЭМП, сканирующие радиоприемники, анализаторы спектра, нелинейные локаторы | | 2 |
| **Практические занятия:** | | | | **18** |
|  | | **Практическое занятие 1.** Селективный индикатор поля RAKSA-120 | | 2 |
|  | | **Практическое занятие 2.** ST 131 ПИРАНЬЯ-II многофункциональное поисковое устройство каналов утечки информации | | 2 |
|  | | **Практическое занятие 3.**  Универсальный поисковый прибор D 008 | | 2 |
|  | | **Практическое занятие 4.**  ЛОРНЕТ 24 нелинейный локатор | | 2 |
|  | | **Практическое занятие 5.**  Обнаружитель видеокамер Оптик-2 | | 2 |
|  | | **Практическое занятие 6.**  Обнаружитель видеокамер "АРКАМ" С-200 | | 2 |
|  | | **Практическое занятие 7.** Устройство обнаружения оптических устройств "Алмаз" | | 2 |
|  | | **Практическое занятие 8** Магнитный томограф Дозор1 | | 2 |
|  | | **Практическое занятие 9** Имитатор сигналов ST-121 | | 2 |
| **Тема 1.6.** Скрытие и защита информации от утечки по техническим каналам | **Содержание:** | | | | **12** |
|  | | | |  |
|  | | Концепция и методы инженерно-технической защиты информации | | 2 |
|  | | Экранирование электромагнитных волн | | 2 |
|  | | Устройства контроля и защиты слаботочных линий связи, оптоволоконных, электрических сетей, цепей заземления | | 2 |
|  | | Скрытие и защита от утечки информации по акустическому и виброакустическому каналам | | 2 |
|  | | Скрытие речевой информации в телефонных системах | | 2 |
|  | | Технические средства для уничтожения информации и носителей информации, порядок применения | | 2 |
| **Практические занятия:** | | | | **28** |
|  | | **Практическое занятие 10.** Шумогенератор "Гром-ЗИ-4" | | 2 |
|  | | **Практическое занятие 11.** Блокиратор сотовой связи ЛГШ-719 | | 2 |
|  | | **Практическое занятие 12.** Подавитель сотовых телефонов "Мозаика" | | 2 |
|  | | **Практическое занятие 13.** Генератор радиошума переносной ПРП-2500 | | 2 |
|  | | **Практическое занятие 14.** Подавитель диктофонов "Барсетка" | | 2 |
|  | | **Практическое занятие 15.** Подавитель диктофонов Завеса-Аудио Максимум 7 | | 2 |
|  | | **Практическое занятие 16.** Система виброакустической защиты "Соната-АВ-1М" | | 4 |
|  | | **Практическое занятие 17.** Обнаружение каналов утечки речевой информации | | 4 |
|  | | **Практическое занятие 18.** Исследование свойств каналов утечки речевой информаци | | 4 |
|  | | **Практическое занятие 19.** Исследование способов виброакустической защиты информации от утечки | | 4 |
| **Конец 7 семестра** | | | | | | |
| **Тема 1.7.** Мероприятия по выявлению каналов утечки информации | **Содержание:** | | | | **6** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12 – ЛР20, ЛР22-ЛР24  ПК 3.1  ПК 3.2  ПК 3.3  ПК 3.4  ОК1-10 |
| 1. | Порядок проведения проверки технических средств | | | 2 |
| 2. | Выполнение поисковых мероприятия | | | 2 |
| 3. | Специальные исследования в области защиты речевой и цифровой информации | | | 2 |
| **Практические занятия:** | | | | **24** |
| 1. | **Практическое занятие 20.** Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации | | | 4 |
| 2. | **Практическое занятие 21.** Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, использующих силовые линии сети переменного тока и линии систем охранной (пожарной) сигнализации | | | 4 |
| 3. | **Практическое занятие 22.** Контроль эффективности защиты речевой информации с помощью программно-аппаратного комплекса | | | 4 |
| 4. | **Практическое занятие 23.** Поиск и измерение побочных электромагнитных излучений и наводок с помощью программно-аппаратного комплекса | | | 4 |
| 5. | **Практическое занятие 24.** Поиск каналов утечки речевой информации | | | 2 |
| 6. | **Практическое занятие 25.** Блокировка виброакустических каналов утечки информации | | | 2 |
| 7. | **Практическое занятие 26.** Блокировка сотовых телефонов | | | 2 |
| 8. | **Практическое занятие 27.** Поиск и обнаружение ИК-закладок | | | 2 |
| **Тема 1.8.** Аттестация объектов информатизации по требованиям безопасности информации | **Содержание:** | | | | **14** |
|  | | Алгоритм проектирования системы защиты информации | | 2 |
|  | | Моделирование объектов защиты | | 2 |
|  | | Моделирование угроз информации | | 2 |
|  | | Рекомендации по организации физической защиты источников информации | | 2 |
|  | | Рекомендации по предотвращению утечки информации | | 2 |
|  | | Общие сведения об аттестации объектов информатизации | | 2 |
|  | | Специальные проверки, обследования, исследования | | 2 |
| **Практические занятия:** | | | | **6** |
|  | | **Практическое занятие 28.** Описание объекта защиты. Характеристика защищаемой информации | | 2 |
|  | | **Практическое занятие 29.** Моделирование угроз на объекте защиты | | 2 |
|  | | **Практическое занятие 30.** Разработка мер по защите информации | | 2 |
| **Тема 1.9.** Технический контроль эффективности мер защиты информации | **Содержание:** | | | | **12** |
|  | | Цели и задачи технического контроля эффективности мер защиты информации Порядок проведения контроля защищенности информации на объекта ВТ от утечки по каналу ПЭМИ | | 2 |
|  | | Методы испытаний ПЭВМ. Порядок проведения контроля защищенности АС от НСД | | 2 |
|  | | Методы контроля побочных электромагнитных излучений генераторов технических средств | | 2 |
|  | | Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации. Общие положения | | 2 |
|  | | Выбор контрольных точек и размещение элементов измерительных комплексов. Калибровка передающего измерительного комплекса | | 2 |
|  | | Измерение отношений «сигнал/шум» Контроль технических средств и систем на наличие акустоэлектрических преобразований | | 2 |
| Курсовой проект | **Содержание:** | | | | **30** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12 – ЛР20, ЛР22-ЛР24  ПК 3.1  ПК 3.2  ПК 3.3  ПК 3.4  ОК1-10 |
|  | | Актуальность исследования. Цель исследования. | | 2 |
|  | | Определение целей и задач защиты информации на исследуемом объекте, основных объектов защиты, предмет защиты. | | 2 |
|  | | Определение факторов, влияющих на защиту информации на исследуемом объекте, выявление возможных угроз защищаемой информации и их структуру | | 2 |
|  | | Выявление источников, видов и способов дестабилизирующего воздействия на защищаемую информацию на исследуемом объекте, выявление причин их дестабилизирующего воздействия | | 2 |
|  | | Выявление каналов и методов несанкционированного доступа к защищаемой информации на исследуемом объекте. | | 2 |
|  | | Выявление и оценка свойств каналов утечки информации | | 2 |
|  | | Определение основных направлений, методов и средств защиты информации | | 2 |
|  | | Разработка методов защиты объекта | | 2 |
|  | | Описание основных методов и средств инженерной защиты, выбранных для защиты объекта | | 2 |
|  | | Описание места расположения и требуемые параметры средств инженерной защиты | | 2 |
|  | | Реализация информационной безопасности объекта | | 2 |
|  | | Разработка методики технического контроля эффективности мер защиты информации | | 2 |
|  | | Описание порядка проведения контроля защищенности информации | | 2 |
|  | | Разработка пакета организационно - правовых документов, обеспечивающих систему информационной безопасности на предприятии | | 2 |
|  | | Защита курсового проекта | | 2 |
| Дифференцированный зачет | | | | | **2** |  |
| **Самостоятельная учебная работа при изучении МДК.03.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты»** | | | | | **24** |  |
| **Рекомендуемая тематика самостоятельной работы:**  1. Классификация способов и средств защиты информации.  2. Основные и вспомогательные технические средства и системы.  3. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации.  4. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.  5. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.  6. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.  7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.  8. Технические средства для уничтожения информации и носителей информации, порядок применения. | | | | |  |  |
| **Тематика курсовых проектов по МДК.03.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты»**   1. Оптимизация защиты персональных данных работников предприятия 2. Изучение и оптимизация защиты коммерческой тайны. 3. Интеграция охранно-пожарной сигнализации, СКУД и системы видеонаблюдения в комплексную систему безопасности. 4. Разработка политики информационной безопасности для организации 5. Организация безопасного удаленного доступа к ЛВС. 6. Проектирование и модернизация комплексной системы защиты информации (КСЗИ). 7. Обоснование и модернизация мер организационной защиты. конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями. 8. Проектирование и модернизация методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации. 9. Проектирование систем видеонаблюдения и СКУД для обеспечения защиты информации. 10. Проектирование и модернизация системы защиты информации конфиденциального характера от утечки по техническим каналам. 11. Проектирование и модернизация комплексной системы защиты информации в кабинете руководителя предприятия. 12. Защита акустической информации в организации. 13. Проектирование и модернизация систем видеонаблюдения и контроля ОПС к объектам информатизации. 14. Обеспечение безопасной работы в выделенном помещении при обмене данными со сторонними организациями. 15. . Модель угроз НСД на предприятии 16. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии 17. Проведение классификации ПО по требованиям ФСТЭК на предприятии 18. Проведение классификации МЭ по требованиям ФСТЭК на предприятии 19. Построение модели нарушителя по требованиям ФСТЭК на предприятии 20. Построение модели нарушителя по требованиям ФСБ на предприятии 21. Модель угроз безопасности ИС персональных данных на предприятии 22. Комплексная модель защиты информации на предприятии. 23. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 24. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)   Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание). | | | | |  |  |
| **МДК 03.02 «Инженерно-технические средства физической защиты объектов информатизации»** | | | | | **76** |  |
| **Тема 2.1.** Цели и задачи физической защиты объектов информатизации | **Содержание:** | | | | **6** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12 – ЛР20, ЛР22-ЛР24  ПК 3.5  ОК1-10 |
| 1 | | | Цели и задачи физической защиты объектов информатизации. | 2 |
| 2 | | | Общие сведения о комплексах инженерно-технических средств физической защиты | 2 |
| 3 | | | Модель нарушителя и возможные пути проникновения на охраняемый объект | 2 |
| **Тема 2.2.** Концепция инженерно-технической защиты информации | **Содержание:** | | | | **4** |
| 1 | | | Системный подход к инженерно-технической защите информации | 2 |
| 2 | | | Основные положения концепции инженерно-технической защиты информации | 2 |
| **Тема 2.3.** Теоретические основы инженерно-технической защиты информации | **Содержание:** | | | | **10** |
| 1 | | | Характеристики защищаемой информации | 2 |
| 2 | | | Характеристики угроз безопасности информации | 2 |
| 3 | | | Методы инженерно-технической защиты информации | 2 |
| 4 | | | Методы физической защиты информации | 2 |
| 5 | | | Система инженерно-технической защиты информации | 2 |
| **Тема 2.4.**Система телевизионного наблюдения | **Содержание:** | | | | **6** |
| 1 | | | Назначение, принципы построения СТН | 2 |
| 2 | | | Технические средства СТН | 2 |
| 3 | | | Пост наблюдения и управления СТН | 2 |
| **Практические занятия:** | | | | **6** |
| 1 | | | **Практическое занятие 1**. Типовое решение «Квартира» | 2 |
| 2 | | | **Практическое занятие 2.** Типовое решение «Офис» | 2 |
| 3 | | | **Практическое занятие** **3**. Типовое решение «Парковка» | 2 |
| **Тема 2.5.** Охранно-пожарная система | **Содержание:** | | | | **4** |
| 1 | | | Принципы построения ОПС | 2 |
| 2 | | | Требования к ОПС | 2 |
| **Практические занятия:** | | | | **24** |
| 1 | | | **Практическое занятие 4**. Анализ объекта защиты и использования оборудования. | 2 |
| 2 | | | **Практическое занятие 5.** Построение рабочей системы. | 2 |
|  | | | **Практическое занятие 6.** Определение питающих напряжений извещателей | 2 |
|  | | | **Практическое занятие 7.** Определение токов потребления извещателей. | 2 |
|  | | | **Практическое занятие 8.** Определение сопротивления участка цепи "заземление прибор - шина заземления" | 2 |
|  | | | **Практическое занятие 9.** Измерение нагрузочных резисторов**.** | 2 |
| 3 | | | **Практическое занятие 10**. Монтаж различных охранных систем. | 2 |
| 4 | | | **Практическое занятие 11.** Определение и устранение ошибок рабочей системы. | 2 |
|  | | | **Практическое занятие. 12** Программирование приборов и оборудования. | 2 |
| 5 | | | **Практическое занятие. 13** Наладка приборов и оборудования. | 2 |
| 6 | | | **Практическое занятие 14**. Основы работы оператора охранных систем. | 2 |
| 7 | | | **Практическое занятие 15**. Работа с электроизмерительными приборами. | 2 |
| **Конец 7 семестра** | | | | | | |
| **Тема 2.6.** Система контроля и управления доступом | **Содержание:** | | | | **4** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12 – ЛР20, ЛР22-ЛР24  ПК 3.5  ОК1-10 |
| 1 | | | Принципы построения СКУД | 2 |
| 2 | | | Требования к СКУД | 2 |
| **Практические занятия:** | | | | **18** |
| 1 | | | **Практическое занятие 16**. Виды штрих-кодов, их генерация и считывание | 2 |
| 2 | | | **Практическое занятие** **17**. Построение системы контроля управления доступом (СКУД) на базе контактных смарт-карт | 2 |
| 3 | | | **Практическое занятие 18**. Построение СКУД на базе бесконтактных RFID смарт-карт | 2 |
| 4 | | | **Практическое занятие 19**. Построение СКУД на базе биометрических систем | 2 |
| 5 | | | **Практическое занятие 20**. Построение СКУД на базе ключей eToken | 2 |
| 6 | | | **Практическое занятие 21**. Построение домофонной системы | 2 |
| 7 | | | **Практическое занятие 22**. Система аутентификации на основе цифровых сертификатов. | 2 |
| 8 | | | **Практическое занятие 23**. Настройка и работа с сервером RADIUS. | 2 |
| 9 | | | **Практическое занятие 24**. Использование протокола 802.1X для авторизации пользователей сети. | 2 |
| **Тема 2.7**. Система сбора, обработки, отображения и документирования информации | **Содержание:** | | | | **4** |
| 1 | | | Схема функционирования ССОИ | 2 |
| 2 | | | Структура средств сбора и отображения информации и информационных сетей в современных системах ТСО | 2 |
| **Практические занятия:** | | | | **4** |
| 1 | | | **Практическое занятие 25**. Разработка системы ССОИ для частного домовладения | 2 |
| 2 | | | **Практическое занятие 26.** Разработка системы ССОИ для офисного здания | 2 |
| **Тема 2.8**. Прочие системы | **Содержание:** | | | | **6** |
| 1 | | | Периметровые и объектовые средства обнаружения, порядок применения. | 2 |
| 2 | | | Назначение и классификация технических средств воздействия | 2 |
| **Тема 2.9.** Эксплуатация инженерно-технических средств физической защиты | **Содержание:** | | | | **12** |
| 1 | | | Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. | 2 |
| 2 | | | Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. | 2 |
| 3 | | | Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. | 2 |
| 4 | | | Организация ремонта технических средств физической защиты. | 2 |
| 5 | | | Эксплуатационное тестирование систем ТСЗ | 2 |
| 6 | | | Методики инструментального контроля эффективности защиты информации, | 2 |
| 7 | | | Технические средства для уничтожения информации и носителей информации | 2 |
| **Практические занятия:** | | | | **4** |
| 1. | | | **Практическое занятие 27**. Диагностика кабельных трасс | 2 |
| 2. | | | **Практическое занятие 28**. Обслуживание объектов инженерно-технических средств физической защиты | 2 |
| **Тема 2.10.** Интернет вещей | **Практические занятия:** | | | | **24** |
| 1. | | | **Практическое занятие 29**. Подключение датчиков | 6 |
| 2. | | | **Практическое занятие 30**. Отображение показателей | 6 |
| 3. | | | **Практическое занятие 31**. Управление исполнительными устройствами | 4 |
| 4. | | | **Практическое занятие 32**. Создание будильников для запуска исполнительных устройств по расписанию | 4 |
| 5. | | | **Практическое занятие 32**. Организация подключения к сети Интернет | 4 |
| **Дифференцированный зачет** | | | | | 2 |  |
| **Самостоятельная учебная работа при изучении МДК.03.02 «Физическая защита линий связи информационно-телекоммуникационных систем и сетей»** | | | | | **10** |  |
| **Рекомендуемая тематика самостоятельной работы:**  1. Классификация инженерно-технических систем.  2. Подбор оборудования по заданной теме | | | | |  |  |
| **МДК 03.03 Экономическое обоснование проекта по защите информации** | | | | | **24** |  |
| **УП.03.01 Учебная практика "Экономическое обоснование проекта по защите информации"** | | | | |  |  |
| Тема 1. Расчёт затрат на создание системы обеспечения информационной безопасности на предприятии и на разработку методических рекомендации по созданию системы обеспечения информационной безопасности на предприятии | **Практические занятия:** | | | | **36** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12 – ЛР20, ЛР22-ЛР24  ОК1-10 |
| 1 | | | Определение состава и расчёт необходимой численности работников | 2 |
| 2 | | | Определение состава и расчёт необходимой численности работников | 2 |
| 3 | | | Определение трудоёмкости работ по обеспечению информационной безопасности | 2 |
| 4 | | | Определение трудоёмкости работ по обеспечению информационной безопасности | 2 |
| 5 | | | Расчёт стоимости материалов, используемых для реализации комплексной защиты информации | 2 |
| 6 | | | Расчёт стоимости материалов, используемых для реализации комплексной защиты информации | 2 |
| 7 | | | Расчёт оплаты труда работников | 2 |
| 8 | | | Расчёт оплаты труда работников | 2 |
| 9 | | | Определение суммы страховых взносов от оплаты труда | 2 |
| 10 | | | Определение суммы страховых взносов от оплаты труда | 2 |
| 11 | | | Расчет суммы амортизационных отчислений | 2 |
| 12 | | | Расчет суммы амортизационных отчислений | 2 |
| 13 | | | Определение затрат на электроэнергию | 2 |
| 14 | | | Расчет общей суммы расходов на реализацию проекта | 2 |
| 15 | | | Расчет затрат на оплату труда и отчисления на социальные нужды | 2 |
| 16 | | | Расчет амортизационных отчисления. | 2 |
| 17 | | | Определение суммы материальны расходов. Расчет общей суммы затрат на разработку методических рекомендаций. | 2 |
| 18 | | | Подготовка и оформление отчета по практике в соответствии с правилами оформления текстовых документов | 2 |
| **УП.03.02 «Защита информации»** | | | | | **36** |  |
| **Тема 2.1.** Инженерно-технические средства защиты информации | **Практические занятия:** | | | | **36** |  |
| 1 | | | Практическое занятие 1. Описание объекта информатизации. | 2 |  |
| 2 | | | Практическое занятие 2. Построение модели нарушителя. | 2 |
| 3 | | | Практическое занятие 3. Изучение проекта типового комплекса инженерно-технических средств физической защиты | 2 |
| 4 | | | Практическое занятие 4. Оценка уязвимости объектов комплекса инженерно-технических средств физической защиты | 2 |
| 5 | | | Практическое занятие 5. Изучение типового проекта системы охранной сигнализации | 2 |
| 6 | | | Практическое занятие 6. Оценка уязвимости объектов системы охранной сигнализации | 2 |
| 7 | | | Практическое занятие 7. Изучение типового проекта системы пожарной сигнализации | 2 |
| 8 | | | Практическое занятие 8. Оценка уязвимости объектов системы пожарной сигнализации | 2 |
| 9 | | | Практическое занятие 9. Изучение типового проекта системы контроля и управления доступом | 2 |
| 10 | | | Практическое занятие 10. Оценка уязвимости объектов системы контроля и управления доступом | 2 |
| 11 | | | Практическое занятие 11. Изучение типового проекта системы аналогового видеонаблюдения | 2 |
| 12 | | | Практическое занятие 12. Изучение типового проекта системы цифрового видеонаблюдения | 2 |
| 13 | | | Практическое занятие 13. Оценка уязвимости объектов системы видеонаблюдения | 2 |
| 14 | | | Практическое занятие 14. Изучение типового проекта системы сбора, обработки, отображения и документирования информации | 2 |
| 15 | | | Практическое занятие 15. Оценка уязвимости объектов системы сбора, обработки, отображения и документирования информации | 2 |
| 16 | | | Практическое занятие 16. Изучение типового проекта системы воздействия | 2 |
| 17 | | | Практическое занятие 17. Оценка уязвимости объектов системы воздействия | 2 |
| 18 | | | Практическое занятие 18. Изучение типового проекта системы умного дома и оценка уязвимости объектов системы умного дома | 2 |
| **Производственная практика (по профилю специальности)** | | | | |  |  |
| * Принятие участия в выявлении технических каналов утечки информации; * Участие в техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, инженерно-технических средств физической защиты и технических средств защиты информации * Участие в установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; * Проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; * Проведение и измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. * Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; * Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; * Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; * Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. | | | | | **108** |  |
| **Объем ОП** | | | | | **552** |  |
| **в том числе:** | | | | |  |  |
| **Лекции** | | | | | **150** |  |
| **Лабораторные и практические занятия** | | | | | **156** |  |
| **Курсовое проектирование** | | | | | **30** |  |
| **Учебная практика/Учебная практика (производственное обучение)** | | | | | **72** |  |
| **Производственная практика** | | | | | **108** |  |
| **Самостоятельная работа** | | | | | **28** |  |

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

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

Реализация программы модуля предполагает наличия лаборатории «Защиты информации от утечки по техническим каналам»

Оборудование учебного кабинета:

* посадочные места по количеству обучающихся;
* рабочее место преподавателя;
* комплект учебно-наглядных пособий.

Технические средства обучения:

* компьютер с лицензионным программным обеспечением;
* мультимедиа проектор;
* образы программных продуктов;
* вспомогательные программные продукты;
* система аппаратной/программной виртуализации,
* выход в Internet;
* средствами защиты информации от утечки по акустическому (виброакустическому) каналу;
* средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок;
* средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок.

Реализация рабочей программы профессионального модуля предполагает наличие учебной и производственной (по профилю специальности) практики, которые могут проводиться концентрированно, то есть после всех МДК профессионального модуля, или рассредоточено, после каждого МДК.

**4.2. Информационное обеспечение обучения**

Основные источники/основная литература:

1. [Зайцев А.П.,](http://www.techbook.ru/book_list.php?str_author=Зайцев%20А.П.)[Мещеряков Р.В.,](http://www.techbook.ru/book_list.php?str_author=Мещеряков%20Р.В.)[Шелупанов А.А.](http://www.techbook.ru/book_list.php?str_author=Шелупанов%20А.А.) Технические средства и методы защиты информации. 7-е изд., испр. – М.: «Горячая линия» - Телеком, 2020. –444стр.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2018
3. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: «Горячая линия» - Телеком, 2020 – 586 стр.
4. Бузов Г. А.Выявление специальных технических средств несанкционированного получения информации. - М.: «Горячая линия» - Телеком, 2020 – 203 стр.
5. Карпухин Е.О. Технологии и методы защиты инфокоммуникационных систем и сетей. - М.: «Горячая линия» - Телеком, 2020 – 120 стр.
6. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. - М.: «Горячая линия» - Телеком, 2020 – 352стр.

Интернет- ресурсы:

* Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
* Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
* Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
* Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
* <http://www.morion.ru/>
* <http://www.nateks.ru/>
* <http://www.iskratel.com/>
* <http://www.ps-ufa.ru/>
* <http://3m.com/>
* <http://www.rusgates.ru/index/php> - Материалы сайта завода «Ферроприбор»

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

Перед изучением профессионального модуля обучающиеся изучают следующие учебные дисциплины:

* ОП.02«Электротехника»,
* ОП.03«Электроника и схемотехника»,
* ОП.04«Основы информационной безопасности»,
* ОП.06«Экономика и управление»,
* ОП.10«Маркетинг»,
* ПМ.01 «Эксплуатация информационно-телекоммуникационных систем и сетей»

Лекционно-практические занятия проводятся в специализированной аудитории.

Производственное обучение обучающихся, осваивающих образовательные программы СПО осуществляется в учебных лабораториях, а также на предприятиях, в учреждениях и организациях различных организационно-правовых форм на основе договоров, заключенных между предприятием и образовательным учреждением.

При подготовке к квалификационному экзамену с обучающимися проводятся консультации.

Во время самостоятельной подготовки обучающимся должен быть предоставлен доступ в Internet.

Требования к учебно-методической документации: наличие рекомендаций к выполнению практических и самостоятельных работ.

Обязательным условием допуска к производственной практике (по профилю специальности) в рамках профессионального модуля ПМ. 03 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» является освоение соответствующих междисциплинарных курсов.

**4.4. Кадровое обеспечение образовательного процесса**

1. Квалификация педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарным курсам:

МДК.03.01 – Шлюпкина Алла Ильинична,преподаватель высшей квалификационной категории

МДК.03.02 – Копылова Ольга Васильевна, преподаватель высшей квалификационной категории

1. Квалификация педагогических (инженерно-педагогических) кадров, осуществляющих руководство практикой:

УП.03.01 – Ревнивцева Оксана Александровна, преподаватель высшей квалификационной категории,

УП.03.01 – Дороганова Лилия Васильевна, преподаватель высшей квалификационной категории,

УП.03.02 – Копылова Ольга Васильевна, преподаватель высшей квалификационной категории

ПП.03.01 - Копылова Ольга Васильевна, преподаватель высшей квалификационной категории

Образование педагогических работников соответствует профилю преподаваемого профессионального модуля, а повышение квалификации - требованиям ФГОС СПО.

# **5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

|  |  |  |
| --- | --- | --- |
| **Результаты**  **(освоенные личностные результаты)** | **Основные показатели**  **оценки** | **Формы и методы контроля и оценки** |
| **ЛР 1**  Осознающий себя гражданином России и защитником Отечества, выражающий свою российскую идентичность в поликультурном  и многоконфессиональном российском обществе и современном мировом сообществе. Сознающий свое единство с народом России,  с Российским государством, демонстрирующий ответственность  за развитие страны. Проявляющий готовность к защите Родины, способный аргументированно отстаивать суверенитет и достоинство народа России, сохранять и защищать историческую правду  о Российском государстве  **ЛР 2**  Проявляющий активную гражданскую позицию на основе уважения закона и правопорядка, прав и свобод сограждан, уважения  к историческому и культурному наследию России. Осознанно  и деятельно выражающий неприятие дискриминации в обществе  по социальным, национальным, религиозным признакам; экстремизма, терроризма, коррупции, антигосударственной деятельности. Обладающий опытом гражданской социально значимой деятельности  **ЛР 3**  Демонстрирующий приверженность традиционным духовно-нравственным ценностям, культуре народов России, принципам честности, порядочности, открытости. Действующий  и оценивающий свое поведение и поступки, поведение и поступки других людей с позиций традиционных российских духовно-нравственных, социокультурных ценностей и норм с учетом осознания последствий поступков. Готовый к деловому взаимодействию и неформальному общению с представителями разных народов, национальностей, вероисповеданий, отличающий их от участников групп с деструктивным и девиантным поведением. Демонстрирующий неприятие социально опасного поведения окружающих и предупреждающий его. Проявляющий уважение  к людям старшего поколения, готовность к участию в социальной поддержке нуждающихся в ней  **ЛР 4**  Проявляющий и демонстрирующий уважение к труду человека, осознающий ценность собственного труда и труда других людей. Экономически активный, ориентированный на осознанный выбор сферы профессиональной деятельности с учетом личных жизненных планов, потребностей своей семьи, российского общества. Выражающий осознанную готовность к получению профессионального образования, к непрерывному образованию  в течение жизни Демонстрирующий позитивное отношение  к регулированию трудовых отношений. Ориентированный  на самообразование и профессиональную переподготовку  в условиях смены технологического уклада и сопутствующих социальных перемен. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»  **ЛР 7**  Осознающий и деятельно выражающий приоритетную ценность каждой человеческой жизни, уважающий достоинство личности каждого человека, собственную и чужую уникальность, свободу мировоззренческого выбора, самоопределения.  Проявляющий бережливое и чуткое отношение к религиозной принадлежности каждого человека, предупредительный  в отношении выражения прав и законных интересов других людей  **ЛР 10**  Бережливо относящийся к природному наследию страны и мира, проявляющий сформированность экологической культуры на основе понимания влияния социальных, экономических  и профессионально-производственных процессов на окружающую среду. Выражающий деятельное неприятие действий, приносящих вред природе, распознающий опасности среды обитания, предупреждающий рискованное поведение других граждан, популяризирующий способы сохранения памятников природы страны, региона, территории, поселения, включенный  в общественные инициативы, направленные на заботу о них  **ЛР 12**  Принимающий российские традиционные семейные ценности. Ориентированный на создание устойчивой многодетной семьи, понимание брака как союза мужчины и женщины для создания семьи, рождения и воспитания детей, неприятия насилия в семье, ухода от родительской ответственности, отказа от отношений  со своими детьми и их финансового содержания  **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  **ЛР16**  Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению  **ЛР17**  Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение  **ЛР18**  Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве  **ЛР19**  Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации  **ЛР20**  Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики  **ЛР 22**  Демонстрирующий уровень подготовки, соответствующий современным стандартам и передовым технологиям, потребностям регионального рынка и цифровой экономики, в том числе требованиям стандартов Ворлдскиллс  **ЛР 23**  Способный использовать различные цифровые средства и умения, позволяющие во взаимодействии с другими людьми достигать поставленных целейв цифровой среде  **ЛР 24**  Способный работать в мультикультурных и мультиязычных средах, владетьнавыками междисциплинарного общения в условиях постепенного формирования глобального рынка труда посредством развития международных стандартов найма и повышения мобильности трудовых ресурсов | * демонстрация интереса к будущей профессии; * оценка собственного продвижения, личностного развития; * положительная динамика в организации собственной учебной деятельности по результатам самооценки, самоанализа и коррекции ее результатов; * ответственность за результат учебной деятельности и подготовки к профессиональной деятельности; * проявление высокопрофессиональной трудовой активности; * участие в исследовательской и проектной работе; * участие в конкурсах профессионального мастерства, олимпиадах по профессии, викторинах, в предметных неделях; * соблюдение этических норм общения при взаимодействии с обучающимися, преподавателями, мастерами и руководителями практики; * конструктивное взаимодействие в учебном коллективе/бригаде; * готовность к общению и взаимодействию с людьми самого разного статуса, этнической, религиозной принадлежности и в многообразных обстоятельствах; * проявление мировоззренческих установок на готовность молодых людей к работе на благо Отечества; * отсутствие социальных конфликтов среди обучающихся, основанных на межнациональной, межрелигиозной почве; * демонстрация умений и навыков разумного природопользования, нетерпимого отношения к действиям, приносящим вред экологии; * проявление культуры потребления информации, умений и навыков пользования компьютерной техникой, навыков отбора и критического анализа информации, умения ориентироваться в информационном пространстве. | * анализ соблюдения норм и правил поведения, принятых в колледже, обществе, профессиональном сообществе; * анализ самооценки событий обучающимися; * педагогический и психологический мониторинг; * анализ проявления обучающимися качеств своей личности: оценка поступков, осознание своей жизненной позиции, культурного выбора, мотивов личностных целей; * анализ портфолио. |

|  |  |  |
| --- | --- | --- |
| **Результаты**  **(освоенные ПК)** | **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;  - применять нормативные правовые акты и нормативные методические документы в области защиты информации; | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| 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;  - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;  - применять нормативные правовые акты и нормативные методические документы в области защиты информации; | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| 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;  - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;  - применять нормативные правовые акты и нормативные методические документы в области защиты информации; | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей. | * выявлять и оценивать угрозы безопасности информации в ИТКС; * настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; * проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |

|  |  |  |
| --- | --- | --- |
| **Результаты**  **(освоенные общие компетенции)** | **Основные показатели**  **оценки** | **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;   - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач; | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| 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; | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. | - демонстрация ответственности за принятые решения;  - обоснованность самоанализа и коррекция результатов собственной работы; | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| 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; * обоснованность анализа работы членов команды (подчиненных); | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. | - демонстрация грамотной письменной и устной речи, при обосновании выбора методов и способов решения профессиональных задач | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей. | - демонстрация своей позиции, при обосновании выбора методов и способов решения профессиональных задач с учетом общечеловеческих ценностей. | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. | - обоснование методов и средств утилизации технических средств защиты информации;  - обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач в условиях ЧС | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности | - применение средств сохранения физического здоровья при осуществлении профессиональной деятельности | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| ОК 09. Использовать информационные технологии в профессиональной деятельности. | * эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту; | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке. | - эффективность использования профессиональной документации на государственном и иностранном языке при решении профессиональных задач | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Дифференцированный зачет.  Отчет по производственной практике  Квалификационный экзамен |

Лист согласования

**Дополнения и изменения к рабочей программе ПМ на учебный год**

Дополнения и изменения **к рабочей программе ПМ** на \_\_\_\_\_\_\_\_\_\_ учебный год по дисциплине Наименование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**В рабочую программу ПМ** внесены следующие изменения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дополнения и изменения в **рабочей программе ПМ** обсуждены на заседании ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Протокол № \_\_\_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_\_г.

Председатель ЦК\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_