**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.02** **ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

**программы подготовки специалистов среднего звена по специальности по специальности**

**10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**

(базовой подготовки)

Ростов-на-Дону

2024г.

| **ОДОБРЕНО**  На заседании цикловой комиссии  Информационной безопасности  Протокол № 11 от 29 июня 2024 года  Председатель ЦК ИБ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Копылова О.В. | **УТВЕРЖДАЮ**  Зам. директора по УиНМР  \_\_\_\_\_\_\_\_\_\_ Подцатова И.В.  «30» августа 2024 г. |
| --- | --- |

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации № 1553 от 9 декабря 2016г. (ред. от 03.07.2024 № 464) «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем», зарегистрированного Министерством юстиции зарегистрированного Министерством юстиции (рег. № 44938 от 26 декабря 2016 г).

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

Разработчики:

МДК.02.01 Программные и программно-аппаратные средства защиты информации, Копылова О.В.– преподаватель ГБПОУ РО «РКСИ»;

МДК.02.02 Криптографические средства защиты информации, Перевышина Е.А.– преподаватель ГБПОУ РО «РКСИ»

МДК.02.02 Криптографические средства защиты информации, Сафарьян О.А.– преподаватель ГБПОУ РО «РКСИ»

УП.02.01 Учебная практика Защита информации, Копылова О.В. - преподаватель ГБПОУ РО «РКСИ»

Производственная практика (по профилю специальности)

Рецензенты:

Фамилия, инициалы – Масютин А.Н. Начальник управления системных проектов Ростовского НТЦ ФГУП «НПП «Гамма»

**СОДЕРЖАНИЕ**

[**1 Паспорт рабочей программы профессионального модуля** 4](#_Toc175307536)

[**2 Структура и содержание профессионального модуля** 9](#_Toc175307537)

[**3 Условия реализации рабочей программы профессионального модуля** 19](#_Toc175307538)

[**4. Контроль и оценка результатов освоения профессионального модуля** 22](#_Toc175307539)

# **1 Паспорт рабочей программы профессионального модуля**

**1.1 Область применения рабочей программы**

Рабочая программа профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» является частью основной профессиональной образовательной программы по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» базового уровня подготовки в части освоения основного вида профессиональной деятельности (ВПД): Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующих профессиональных компетенций (ПК):

* ПК 2.1 Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
* ПК 2.2 Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
* ПК 2.3 Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
* ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа.
* ПК 2.5 Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
* ПК 2.6 Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Рабочая программа профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» предназначена для студентов 3-4 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, настройки программных средств защиты информации в автоматизированной системе;

− обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;

− тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ;

− решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

− применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных;

− учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;

− работы с подсистемами регистрации событий;

− выявления событий и инцидентов безопасности в автоматизированной системе.

**уметь:**

− устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

− устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

− диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

− применять программные и программно-аппаратные средства для защиты информации в базах данных;

− проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

− применять математический аппарат для выполнения криптографических преобразований;

− использовать типовые программные криптографические средства, в том числе электронную подпись;

− применять средства гарантированного уничтожения информации;

− устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

− осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

**знать:**

* особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
* методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;
* типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
* основные понятия криптографии и типовых криптографических методов и средств защиты информации;
* особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;
* типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

**1.3 Рекомендуемое количество часов на освоение рабочей программы профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»**

| Всего | **–** | 582 часа |
| --- | --- | --- |
| в том числе: |  |  |
| * максимальная учебная нагрузка обучающегося | **–** | 582 часа |
| включая: |  |  |
| - обязательную аудиторную учебную нагрузку обучающегося | **–** | 320 часов |
| - самостоятельную работу обучающегося | **–** | 24 часа |
| -Консультации | **-** | 2 часа |
| -Учебная практика | **–** | 72 часа |
| -Производственная практика | **-** | 144 часа |
| Промежуточная аттестация | **-** | 8 часов |
| Экзамен квалификационный | **-** | 12 часов |

Практическая подготовка при реализации профессионального модуля путем проведения практических и лабораторных занятий, учебной и производственной практики занимает **330 часов.**

Из вариативной части на профессиональный модуль ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» отведено **71 час**:

* на частично-вариативную учебную дисциплину МДК.02.01 «Программные и программно-аппаратные средства защиты информации» отведено **24 часа**;
* на частично-вариативную учебную дисциплину МДК 02.02 «Криптографические средства защиты информации» отведено **6 часов**;
* на учебную практику УП.02.01 **20 часов**;
* на производственную практику ПП.02.01 **21 час**.

| Наименование раздела | Наименование темы | Кол-во часов | Дополнительные умения | Дополнительные знания | Формируемые компетенции |
| --- | --- | --- | --- | --- | --- |
| МДК.02.01 | **Тема 1.7** Мониторинг систем защиты | 8 | * устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации | * основные методики реагирования на инциденты ИБ | ПК 2.1. -ПК 2.6  ОК 1– ОК 9 |
| МДК.02.01 | **Тема 1.8** Мониторинг безопасности и тестирование на проникновение | 10 | * устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации | * основные методики реагирования на инциденты ИБ |
| МДК.02.01 | **Тема 1.9** Построение системы безопасности ЛВС | 6 | * устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации | * основные методики реагирования на инциденты ИБ |
| МДК.02.02 | **Тема 2.11** Защита информации в электронных платежных | 6 | * применять математический аппарат для выполнения криптографических преобразований; | * основные понятия криптографии и типовых криптографических методов и средств защиты информации |
| УП 02.01 | **Тема 1**. VipNet | 20 | устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации | * особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; |
| ПП02.01 |  | 21 | устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации | * особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; |

**1.4 Результаты освоения профессионального модуля**

Результатом освоения профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» является овладение обучающимися видом профессиональной деятельности (ВПД) Защита информации в автоматизированных системах программными и программно-аппаратными средствами, в том числе профессиональными компетенциями (ПК), общими компетенциями (ОК).

| Код | Наименование результатов обучения |
| --- | --- |
| ПК 2.1 | Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации |
| ПК 2.2 | Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами |
| ПК 2.3 | Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации |
| ПК 2.4 | Осуществлять обработку, хранение и передачу информации ограниченного доступа |
| ПК 2.5 | Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. |
| ПК 2.6 | Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак |
| ОК 1. | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам |
| ОК 2. | Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности |
| ОК 3. | Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях |
| ОК 4. | Эффективно взаимодействовать и работать в коллективе и команде |
| ОК 5. | Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста |
| ОК 6. | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе духовно-нравственных традиционных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения |
| ОК 7. | Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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. | Пользоваться профессиональной документацией на государственном и иностранном языках |

# **2 Структура и содержание профессионального модуля**

**2.1Тематический план профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»**

| **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 | **Производственная**  **(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 2.1. -ПК 2.6**  **ОК 1– ОК 9** | **МДК 02.01** «**Программные и программно-аппаратные средства защиты информации»** | **204** | **186** | **64** | **40** | **8** | | - | | **-** | **-** |
| **ПК 2.1. -ПК 2.6**  **ОК 1– ОК 9** | **МДК 02.02 «Криптографические средства защиты информации»** | **150** | **134** | **50** | **-** | **16** | | **-** | | **-** | **-** |
| **ПК 2.1. -ПК 2.6**  **ОК 1– ОК 9** | **УП.02.01 Учебная практика** | **72** |  |  |  |  | |  | | **72** |  |
| **ПК 2.1. -ПК 2.6**  **ОК 1– ОК 9** | **Производственная практика (по профилю специальности)** | **144** |  | | | | | | | | **144** |
|  | **Экзамен по модулю** | **12** | - | - | - | - | - | | - | | **-** |
|  | **Всего:** | **582** | **320** | **114** | **40** | **24** | | **-** | | **72** | **144** |

**2.2 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 02.01«Программные и программно-аппаратные средства защиты информации»** | | | | **216** |  |
| **Тема 1.1** Основные понятия | **Содержание:** | | | **42** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
|  | Предмет и задачи программно-аппаратной защиты информации. Основные понятия. | | 2 |
|  | Классификация методов и средств ПАЗИ. Угрозы информационной безопасности | | 2 |
|  | Требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты) | | 2 |
|  | Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. | | 2 |
|  | Особенности автоматизированных систем в защищенном исполнении. Методы создания безопасных систем | | 2 |
|  | Политика безопасности. Управление рисками. Механизмы и службы защиты. | | 2 |
|  | Функциональные возможности программно-аппаратных средств защиты. Учет, обработка, хранение и передача информации в АИС | | 2 |
|  | Принципы программно-аппаратной защиты информации от несанкционированного доступа | | 2 |
|  | Понятие АМДЗ (доверенная загрузка). Средства замыкания программной среды | | 2 |
|  | Методы управления ключевой информации. Криптографическая защита данных. | | 2 |
|  | Методы контроля целостности данных. Уничтожение остаточной информации. | | 2 |
|  | Защита программ и данных от несанкционированного копирования | | 2 |
|  | Защита программ от изучения | | 2 |
|  | Защита информации на машинных носителях | | 2 |
|  | Защита от вредоносного программного обеспечения | | 2 |
|  | Основы построения защищенных сетей | | 2 |
|  | Средства организации VPN | | 2 |
|  | Обеспечение безопасности межсетевого взаимодействия | | 2 |
|  | Защита информации в базах данных | | 2 |
|  | Мониторинг систем защиты | | 2 |
|  | Системы резервного копирования и восстановления данных с защитой от вирусов | | 2 |
| **Тема 1.2.** Обеспечение безопасности операционных систем | **Практические занятия:** | | | **26** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
|  | **Практическое занятие № 1.** Работа с учетными записями пользователей и группами (AstraLinux) | | 2 |
|  | **Практическое занятие № 2.** Настройка параметров мандатного управления доступом и мандатного контроля целостности (AstraLinux) | | 2 |
|  | **Практическое занятие № 3.** Организация файловой системы ОССН для работы пользователей в рамках мандатного управления доступом и мандатного контроля целостности (AstraLinux) | | 2 |
|  | **Практическое занятие № 4.** Администрирование ОССН в рамках реализации мандатного контроля целостности (AstraLinux) | | 2 |
|  | **Практическое занятие № 5.** Настройка механизмов организации ЗПС. Контроль целостности КСЗ (AstraLinux) | | 2 |
|  | **Практическое занятие № 6.** Настройка сетевого взаимодействия (AstraLinux) | | 2 |
|  | **Практическое занятие № 7.** Конфигурирование службы ALD (AstraLinux) | | 2 |
|  | **Практическое занятие № 8.** Управление программными пакетами. Настройка системных служб (AstraLinux) | | 2 |
|  | **Практическое занятие № 9.** Настройка защищенного режима работы ОССН в соответствии с Astra Linux Red-Book (AstraLinux) | | 2 |
|  | **Практическое занятие № 10.** Настройка защищенного режима работы ОССН в соответствии с Astra Linux Red-Book (AstraLinux) | | 2 |
|  | **Практическое занятие № 11.** Настройка домена Windows | | 2 |
|  | **Практическое занятие № 12.** Управление доменными пользователями (Windows) | | 2 |
|  | **Практическое занятие № 13.** Настройка доменных групповых политик (Windows) | | 2 |
| **Тема 1.3** Защита конечных точек | **Практические занятия:** | | | **16** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
|  | **Практическое занятие № 14** Установка SNS, настройка политик безопасности. | | 2 |
|  | **Практическое занятие № 15** Настройка полномочного управления доступом SNS | | 2 |
|  | **Практическое занятие № 16** Настройка аудита операционной системы и событий SNS. Работа с журналом событий | | 2 |
|  | **Практическое занятие № 17** Настройка механизма дискреционного управления доступом | | 2 |
|  | **Практическое занятие № 18** Управление доступом к съемным носителям информации | | 2 |
|  | **Практическое занятие № 19** Настройка механизма замкнутой программной среды SNS | | 2 |
|  | **Практическое занятие № 20** Настройка механизма контроля целостности | | 2 |
|  | **Практическое занятие № 21** Настройка антивируса и СОВ. Персональный межсетевой экран | | 2 |
| **Промежуточная аттестация по МДК.02.01** | | | | | |
| **Тема 1.4** Защита программ от изучения | **Содержание:** | | | **6** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
|  | Изучение и обратное проектирование ПО | | 2 |
|  | Способы изучения ПО: статическое и динамическое изучение. Задачи защиты от изучения и способы их решения | | 2 |
|  | Защита от отладки. Защита от дизассемблирования. Защита от трассировки по прерываниям. | | 2 |
| **Тема 1.5** Вредоносное программное обеспечение | **Содержание:** | | | **8** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9ПК 2.6  ОК 1– ОК 10 |
|  | Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения | | 2 |
|  | Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch. | | 2 |
|  | Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме" | | 2 |
|  | Основные концепции построения систем антивирусной защиты на предприятии | | 2 |
| **Тема 1.6** Защита информации в локальных сетях | **Содержание:** | | | **8** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
|  | Основы построения защищенных сетей. Средства организации VPN | | 2 |
|  | Обеспечение безопасности межсетевого взаимодействия. Требования по сертификации межсетевых экранов | | 2 |
|  | Уровень 1. Пакетные фильтры. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. | | 2 |
|  | Уровень 3. Proxy-сервера прикладного уровня | | 2 |
| **Тема 1.7** Мониторинг систем защиты | **Содержание:** | | | **8** |
|  | Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации. Классификация отслеживаемых событий. Особенности построения систем мониторинга | | 2 |
|  | Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке. | | 2 |
|  | Проведение аудита ЛВС сетевым сканером. Классификация сетевых мониторов. | | 2 |
|  | DLP системы примеры и принцип работы. | | 2 |
| **Тема 1.8** Мониторинг безопасности и тестирование на проникновение | **Содержание:** | | | **10** |
|  | Цифровая техническая экспертиза | | 2 |
|  | Модели реагирования на инциденты. Обработка инцидентов. Методология тестирования на проникновение | | 2 |
|  | Получение отпечатка и сбор информации. Методы сканирования и уклонения. Сканирование уязвимостей | | 2 |
|  | Социальная инженерия. Целевая эксплуатация. Повышение привилегий и поддержание доступа | | 2 |
|  | Тестирование web-приложений. Тестирование беспроводных сетей на проникновение. Мобильное тестирование | | 2 |
| **Тема 1.9** Построение системы безопасности ЛВС | **Практические занятия:** | | | **20** |
|  | **Практическое занятие №22**. Установка и настройка файлового сервера. Настройка систем безопасности | | 2 |
|  | **Практическое занятие №23**. Установка и настройка веб-сервера. Настройка систем безопасности | | 2 |
|  | **Практическое занятие №24**. Установка и настройка Почтового сервера. Настройка систем безопасности | | 2 |
|  | **Практическое занятие №25**. Установка и настройка базы данных. Настройка систем безопасности | | 2 |
|  | **Практическое занятие №26**. Установка и настройка программного маршрутизатора. Настройка межсетевого экрана | | 2 |
|  | **Практическое занятие №27.** Установка и настройка системы резервного копирования для серверов. Проверка работоспособности | | 2 |
|  | **Практическое занятие №28.** Установка и настройка DLP-сервера и сервера агентского мониторинга | | 2 |
|  | **Практическое занятие №29.** Настройка правил и политик DLP. | | 2 |
|  | **Практическое занятие №30.** Установка и настройка сканера безопасности | | 2 |
|  | **Практическое занятие №31.** Эксплуатация сканера безопасности | | 2 |
|  | **Практическое занятие №32.** Перехват трафика и его анализ | | 2 |
| **Курсовой проект** |  | Актуальность темы. Постановка целей и задач | | **40** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
|  | Разработка политики безопасности предприятия | | 2 |
|  | Обзор стандартов ИБ регламентирующих деятельность предприятия | | 2 |
|  | Описание возможных угроз ИБ | | 2 |
|  | Обзор возможностей DLP-системы | | 2 |
|  | Установка DLP-системы | | 2 |
|  | Конфигурация DLP-системы | | 8 |
|  | Настройка правил агентского мониторинга | | 8 |
|  | Настройка политик DLP-системы | | 8 |
|  | Тестирование средств ИБ. Проверка эффективности реализации защиты от возможных угроз | | 2 |
|  | Разработка нормативно-правовой документации для пользователей | | 2 |
|  | Защита курсового проекта | | 2 |
| Экзамен | | | | **12** |  |
| **Примерная тематика курсовых работ**   1. Разработка предложений по внедрению DLP-системы в сеть предприятия | | | |  |  |
| **Самостоятельная учебная работа при изучении МДК.02.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты»** | | | | **10** |  |
| **Рекомендуемая тематика самостоятельной работы:**   1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему 4. Обзор современных программных и программно-аппаратных средств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты | | | |  |  |
| **МДК 02.02 «Криптографические средства защиты информации»** | | | | **144** |  |
| **Тема 2.1** Математические основы криптографии | **Содержание:** | | | **24** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Предмет и задачи криптографии. История криптографии. Основные термины | 2 |
| 2 | | Элементы теории множеств. Группы, кольца, поля. | 2 |
| 3 | | Делимость чисел. Простые и составные числа. | 2 |
| 4 | | НОД. Алгоритм Евклида. | 2 |
| 5 | | Отношения сравнимости. Модулярная арифметика | 2 |
| 6 | | Функция Эйлера. Алгоритм быстрого возведения в степень | 2 |
| 7 | | Расширенный алгоритм Евклида | 2 |
| 8 | | Китайская теорема об остатках | 2 |
| 9 | | Проверка чисел на простоту. Алгоритмы генерации простых чисел. | 2 |
| 10 | | Разложение числа на множители. Алгоритмы факторизации. | 2 |
| 11 | | Алгоритмы дискретного логарифмирования. | 2 |
| 12 | | Арифметические операции над большими числами. Первообразный корень | 2 |
| **Практические занятия:** | | | **10** |
| 1 | | Практическое занятие №1. Проверка чисел на простоту | 2 |
| 2 | | Практическое занятие №2 Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений | 2 |
| 3 | | Практическое занятие №3 Модульная арифметика | 2 |
| 4 | | Практическое занятие №4 Нахождение мультипликативного обратного, используя расширенный алгоритм Евклида | 2 |
| 5 | | Практическое занятие №5 Китайская теорема об остатках | 2 |
| **Промежуточная аттестация по МДК.02.02** | | | | | |
| **Тема 2.2** Методы криптографического защиты информации | **Содержание:** | | | **8** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Классификация основных методов криптографической защиты. Методы симметричного шифрования | 2 |
| 2 | | Шифры замены | 2 |
| 3 | | Методы перестановки | 2 |
| 4 | | Методы гаммирования | 2 |
| **Практические занятия:** | | | **6** |
| 1 | | Практическое занятие №6. Применение классических шифров замены | 2 |
| 2 | | Практическое занятие №7. Применение классических шифров перестановки | 2 |
| 3 | | Практическое занятие №8. Применение метода гаммирования | 2 |
| **Тема 2.3.** Криптоанализ | **Содержание:** | | | **6** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Основные методы криптоанализа. Криптографические атаки. | 2 |
| 2 | | Криптографическая стойкость | 2 |
| 3 | | Перспективные направления криптоанализа, | 2 |
| **Практические занятия:** | | | **6** |
| 1 | | Практическое занятие №9. Криптоанализ шифра простой замены | 2 |
| 2 | | Практическое занятие №10. Криптоанализ шифров методом полного перебора ключей | 2 |
| 3 | | Практическое занятие №11. Криптоанализ шифра Вижинера | 2 |
| **Тема 2. 4.** Кодирование информации. Компьютеризация шифрования | **Содержание:** | | | **2** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Кодирование информации. | 2 |
| **Практические занятия:** | | | **6** |
| 1 | | Практическое занятие №12 Кодирование информации | 2 |
| 2 | | Практическое занятие №13 Программная реализация классических шифров | 2 |
| 3 | | Практическое занятие №14 Изучение реализации классических шифров замены и перестановки в программе CRYPTOOL | 2 |
| **Тема 2.5.** Симметричные системы шифрования | **Содержание:** | | | **14** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Симметричное шифрование. Алгоритм DES | 2 |
| 2 | | ГОСТ 28147-89 в режиме простой замены | 2 |
| 3 | | ГОСТ 28147-89 в режиме гаммирования | 2 |
| 4 | | ГОСТ 28147-89 гаммирование с обратной связью | 2 |
| 5 | | ГОСТ 28147-89 выработка имитовставки | 2 |
| 6 | | Алгоритм AES | 2 |
| 7 | | Отечественные алгоритмы Магма и Кузнечик | 2 |
| **Практические занятия:** | | | **4** |
| 1 | | Практическое занятие №15 Упрощенный алгоритм шифрования DES (S-DES) | 2 |
| 2 | | Практическое занятие №16 Алгоритм шифрования S-AES | 2 |
| **Тема 2.6.** Поточные шифры и генераторы псевдослучайных чисел | **Содержание:** | | | **2** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Поточное шифрование. Псевдослучайные последовательности. RC4, MD5 | 2 |
| **Практические занятия:** | | | **4** |
| 1 | | Практическое занятие №17 Методы генерации ПСЧ | 2 |
| 2 | | Практическое занятие №18 Регистры сдвига с обратной линейной связью | 2 |
| **Тема 2.7.** Асимметричные системы шифрования | **Содержание:** | | | **8** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Асимметричное шифрование. | 2 |
| 2 | | Схема шифрования RSA. Электронная цифровая подпись (ЭЦП) RSA. | 2 |
| 3 | | Система Диффи и Хеллмана. Схема шифрования Эль Гамаля | 2 |
| 4 | | ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. | 2 |
| **Практические занятия:** | | | **6** |
| 1 | | Практическая работа №19 Система Диффи и Хеллмана | 2 |
| 2 | | Практическое занятие №20 Применение асимметричного алгоритма RSA | 2 |
| 3 | | Практическая работа №21 Алгоритм Эль-Гамаля | 2 |
| **Тема 2.8.** Аутентификация данных. Электронная подпись | **Содержание:** | | | **6** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Аутентификация данных | 2 |
| 2 | | ЭП. Однонаправленные хэш-функции. | 2 |
| 3 | | Применение различных функций хэширования, анализ особенностей хешей | 2 |
| **Тема 2.9.** Алгоритмы обмена ключей и протоколы аутентификации | **Содержание:** | | | **4** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Алгоритмы распределения ключей с применением симметричных и асимметричных схем | 2 |
| 2 | | Протоколы аутентификации. Протокол KERBEROS | 2 |
| **Тема 2.10.** Криптозащита информации в сетях передачи данных | **Содержание:** | | | **2** | ПК 2.1.  -ПК 2.6  ОК 1– ОК 10 |
| 1 | | Криптографическая защита беспроводных соединений | 2 |
| **Тема 2.11** Защита информации в электронных платежных системах | **Содержание:** | | | **8** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 10 |
| 1 | | Принципы функционирования электронных платежных систем. | 2 |
| 2 | | Применение криптографических протоколов для обеспечения безопасности электронной коммерции. | 2 |
| 3 | | Технология блокчейн | 2 |
| 4 | | Вопросы безопасности блокчейн | 2 |
| **Тема 2.12.** OpenSSL | **Практические занятия:** | | | **8** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Практическая работа №22 Использование алгоритмов шифрования для сокрытия содержимого файла с применением OpenSSL | 2 |
| 2 | | Практическая работа №23 Использование алгоритмов хеширования для подтверждения неизменности файла с применением OpenSSL | 2 |
| 3 | | Практическая работа №24 Создание цифровых сертификатов Х.509 и преобразование их форматов с применением пакета OpenSSL. Создание центра сертификации | 2 |
| 4 | | Практическая работа №25.Применение электронной цифровой подписи для проверки авторства и неизменности файла | 2 |
| Дифференцированный зачет | | | | 2 |
| **Самостоятельная учебная работа при изучении МДК.02.02 «Криптографические средства защиты информации»** | | | | **8** |  |
| **Рекомендуемая тематика самостоятельной работы:**  1. История развития криптографии  2. Программная реализация классических шифров  3. Оптимизация методов частотного анализа моноалфавитных шифров.  4. Программная реализация классических шифров  5. Методы механизации шифрования  6. Цифровое представление различных форм информации  7. Анализ современных симметричных криптоалгоритмов  8. Анализ современных асимметричных криптоалгоритмов  9. Программная реализация современных криптоалгоритмов  10. Сравнительный анализ функций хеширования  11. Аутентификация сообщений  12. Законодательство в области криптографической защиты информации  13. Перспективные направления криптографии. | | | |  |  |
| **УП.02.01 Учебная практика** | | | | **72** |  |
| Тема 1. VipNet | **Практические занятия:** | | | **72** | ПК 2.1. -  ПК 2.6  ОК 1– ОК 9 |
| 1 | | Планирование схемы защищённой сети | 2 |
| 2 | | Установка программного комплекса vipnet administrator 4, | 2 |
| 3 | | Создание структуры защищённой сети, | 2 |
| 4 | | Настройка резервного копирования данных и восстановление данных в по vipnet administrator | 2 |
| 5 | | Модификация защищённой сети | 2 |
| 6 | | Компрометация | 2 |
| 7 | | Настройка политик безопасности в vipnet policy manager | 2 |
| 8 | | Установка vipnet Coordinator в качестве межсетевого шлюза | 2 |
| 9 | | Первоначальная настройка межсетевого взаимодействия | 2 |
| 10 | | Модификация межсетевого взаимодействия | 2 |
| 11 | | Coordinator linux 4. Firewall. Фильтры по умолчанию | 2 |
| 12 | | Coordinator linux 4. Firewall. | 2 |
| 13 | | Coordinator linux 4. Настройка трансляции сетевых адресов | 2 |
| 14 | | Coordinator linux 4. Туннелирование незащищенных узлов | 2 |
| 15 | | Coordinator linux 4.Сохранение настроек | 2 |
| 16 | | Coordinator linux 4.Кластер горячего резервирования | 2 |
| 17 | | Coordinator VA 4.x. Первичная настройка | 2 |
| 18 | | Coordinator VA 4.x.DHCP и маршрутизация | 2 |
| 19 | | Coordinator VA 4.x. Фильтрация трафика | 2 |
| 20 | | Coordinator VA 4.x. NAT и тунеллирование | 2 |
| 21 | | Coordinator VA 4.x. Агрегация каналов | 2 |
| 22 | | Coordinator VA 4.x. Сохранение настроек | 2 |
| 23 | | Установка ViPNet IDS NS VA, ViPNet IDS MC VA, ViPNet IDS HS, ViPNet TIAS VA | 2 |
| 24 | | Подготовка к работе и настройка ViPNet IDS NS VA в роли Главного администратора (Администратора системы) | 2 |
| 25 | | настройка подключения ViPNet IDS HS Server и ViPNet IDS NS на Терминале управления ViPNet IDS MC | 2 |
| 26 | | Подготовка к работе и настройка ViPNet TIAS VA в роли Системного администратора | 2 |
| 27 | | Обновление ViPNet IDS MC | 2 |
| 28 | | Обновление программного обеспечения ViPNet IDS NS через ViPNet IDS MC | 2 |
| 29 | | Добавление ViPNet TIAS в ViPNet IDS MC | 2 |
| 30 | | Сканирование сети виртуальной машиной AttackImitator IDS | 2 |
| 31 | | Мониторинг и анализ состояния системы и устройств ViPNet IDS HS в роли Администратора | 2 |
| 32 | | Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority | 2 |
| 33 | | Установка и настройка ПО RegistrationPoint | 2 |
| 34 | | Установка и настройка ПО CA Informing | 2 |
| 35 | | Выполнение комплексного задания |  |
| 36 | | Выполнение комплексного задания. Зачет | 2 |
| **Производственная практика (по профилю специальности)** | | | | **144** |  |
| Анализ принципов построения систем информационной защиты производственных подразделений.  Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.  Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;  Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении  Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации  Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. | | | |  |  |
| **Максимальная учебная нагрузка:** | | | | **562** |  |
| **в том числе:** | | | |  |  |
| ***Лекции*** | | | | **166** |  |
| ***Лабораторные и практические занятия*** | | | | **114** |  |
| ***Курсовое проектирование*** | | | | **40** |  |
| ***Учебная практика/Учебная практика (производственное обучение)*** | | | | **72** |  |
| ***Производственная практика*** | | | | **144** |  |
| ***Самостоятельная работа*** | | | | **24** |  |
| ***Консультации*** | | | | **2** |  |
| **Промежуточная аттестация** | | | | **20** |  |
| **Всего** | | | | **582** |  |

# **3 Условия реализации рабочей программы профессионального модуля**

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

Реализация программы профессионального модуля требует наличия учебных кабинетов, лабораторий:

* лаборатория «Программных и программно-аппаратных средств защиты информации».

Технические средства обучения:

− компьютеры, объединенные в локальную вычислительную сеть;

− мультимедиа проектор;

Лаборатория должна быть оснащена;

* антивирусными программными комплексами;
* аппаратными средствами аутентификации пользователя;
* программно-аппаратными средствами управления доступом к данным и защиты (шифрования) информации;

- средствами защиты информации от НСД, блокирования доступа и нарушения целостности (дистрибутивы Secret Net Studio, дистрибутивы Secret Net LSP и ПАК "Соболь", АПКШ "Континент", дистрибутивы программного комплекса Vipnet, дистрибутивы программного комплекса InfoWatch TrafficMonitor, дистрибутивы Linux операционных систем, дистрибутивы антивирусных программных комплексов; ПО Oracle VirtualBox);

* программными средствами криптографической защиты информации;
* программными средствами выявления уязвимостей и оценки защищенности ИТКС,
* анализа сетевого трафика;
* системы разграничения доступа;
* межсетевые экраны;
* средство криптографической защиты информации, реализующее функции удостоверяющего центра и создания виртуальных сетей;

− прикладное программное обеспечение, бесплатное ПО: LibreOffice - офисный пакет или Microsoft Office.

**3.2. Информационное обеспечение обучения**

**3.2.1 Основные источники/основная литература:**

1. Шива Парарасрам, Алекс Замм, Kali Linux Тестирование на проникновение и безопасность. Изд. Питер, 2020, 441 стр.
2. А.П. Душкин. Программно-аппаратные средства обеспечения информационной безопасности. Изд.: Москва Горячая линия- Телеком, 2020, 242стр.
3. Маршаков Д. В., Фатхи Д. В. Программно-аппаратные средства защиты информации: учебное пособие. Изд.: Донской государственный технический университет, 2021, 228 стр.
4. П.Б. Хорев. Программно-аппаратная защита информации. Учебное пособие. Изд.: Форум, 2021, 352 стр.
5. Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации. Изд.: URSS, 2021, 464 стр.
6. Казарин О.В., Забабурин А.С. Программно-аппаратные средства защиты информации. Защита программного обеспечения. Учебник и практикум для ВУЗов. Изд.: Юрайт, 2022, 312 стр.

**3.2.2. Периодические издания:**

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: <http://bit.mephi.ru/>

**3.2.3. Электронные источники:**

1. Информационно-справочная система по документам в области технической защиты информации [www.fstec.ru](http://www.fstec.ru)
2. Информационный портал по безопасности [www.SecurityLab.ru](http://www.securitylab.ru).
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал [www.biometrics.ru](http://www.biometrics.ru)
5. Сайт журнала Информационная безопасность http://www.itsec.ru –
6. Сайт Научной электронной библиотеки [www.elibrary.ru](http://www.elibrary.ru)
7. Справочно-правовая система «Гарант» » [www.garant.ru](http://www.garant.ru)
8. Справочно-правовая система «Консультант Плюс» [www.consultant.ru](http://www.consultant.ru)
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru)
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\[:www.ict.edu.ru](http://www.ict.edu.ru/)
11. Федеральный портал «Российское образование [www.edu.ru](http://www.edu.ru/)

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

Перед изучением профессионального модуля обучающиеся изучают следующие учебные дисциплины:

ОП. 04 «Основы информационной безопасности»

* ОП.02«Электротехника»,
* ОП.03«Электроника и схемотехника»,
* ОП.05 «Основы алгоритмизации и программирования»;
* ОП.08 «Организационное и правовое обеспечение информационной безопасности»

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. 02 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты» является освоение соответствующих междисциплинарных курсов.

**3.4. Кадровое обеспечение образовательного процесса**

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

# **4. Контроль и оценка результатов освоения профессионального модуля**

| Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля | Критерии оценки | Методы оценки |
| --- | --- | --- |
| ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. | Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации | тестирование,  экзамен квалификационный,  экспертное наблюдение выполнения лабораторных работ,  экспертное наблюдение выполнения практических работ,  оценка решения ситуационных задач,  оценка процесса и результатов выполнения видов работ на практике |
| ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. | Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами |
| ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. | Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации |
| ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. | Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа |
| ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. | Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств |
| ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. | Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак |

| **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  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии 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  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях | - 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.  Курсовой проект.  Экзамен.  Отчет по производственной практике  Экзамен по модулю |
| ОК 04. Эффективно взаимодействовать и работать в коллективе и команде | * 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  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации 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  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе духовно-нравственных традиционных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения | - демонстрация своей позиции, при обосновании выбора методов и способов решения профессиональных задач с учетом общечеловеческих ценностей,  - демонстрирование сформированности российской гражданской идентичности, патриотизма, уважения к своему народу, уважение к государственным символам. | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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,  - осуществление деятельности по сбережению ресурсов и сохранения окружающей среды. | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| 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,  - соблюдение норм здорового образа жизни, осознанное выполнение правил безопасности жизнедеятельности. | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках | * изучение нормативно-правовой документации, технической профессиональной документации на государственном и иностранном языке, * применение необходимого лексического и грамматического минимума для чтения и перевода иностранных текстов профессиональной направленности, * владение современной научной и профессиональной терминологией, * владение навыками технического перевода текста, понимание содержание инструкций и графической документации на иностранном языке в области профессиональной деятельности. | Оценка результатов выполнения практических занятий. Оценка результатов внеаудиторной самостоятельной работы обучающихся, ответов на устные вопросы по темам  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |

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