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

для специальности

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

(базовой подготовки)

Ростов-на-Дону

2023г.

|  |  |
| --- | --- |
| **ОДОБРЕНО**  На заседании цикловой комиссии  Информационной безопасности  Протокол № 10 от30июня 2023 года  Председатель ЦК ИБ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Копылова О.В. | **УТВЕРЖДАЮ**  Зам. директора по НМР  \_\_\_\_\_\_\_\_\_\_ Подцатова И.В.  «30» июня 2023 г. |

Рабочая программа частично вариативного и профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного приказом Минобрнауки России от 09.12.2016 №1553 (в ред. от 17.12.2020) «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Разработчики:

МДК.02.01Программные 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, СафарьянО.А.. – преподаватель ГБПОУ РО «РКСИ»

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

УП.02.01 Учебная практика Защита информации, Бороненкова С.Е. - преподаватель ГБПОУ РО «РКСИ»

УП.02.01 Учебная практика Защита информации, Купчинская Н.И. - преподаватель ГБПОУ РО «РКСИ»

Рецензенты:

Королькова О.В. зам директора по УР ГБПОУ РО «РКСИ»

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

СОДЕРЖАНИЕ

[1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ\_\_\_\_\_\_\_\_\_\_\_\_\_4](#_Toc64710525)

[2.РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_9](#_Toc64710526)

[3.СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_10](#_Toc64710527)

[4.УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_21](#_Toc64710528)

[5. КОНТРОЛЬ И УСВОЕНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ\_\_\_\_\_\_\_\_\_25](#_Toc64710529)

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

**1.1 Область применения рабочей программы**

Рабочая программа частично вариативного профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» разработана в соответствии с ФГОС СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного приказом Минобрнауки России от 09.12.2016 №1553 (в ред. от 17.12.2020).

Рабочая программа является частью профессионального цикла учебного плана и предназначена для студентов очной формы обучения.

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

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

ОК1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК3. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения, применять стандарты антикоррупционного поведения.

ОК7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях, применять стандарты антикоррупционного поведения.

ОК8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК9. Использовать информационные технологии в профессиональной деятельности.

ОК10. Пользоваться профессиональной документацией на государственном и иностранном языках.

профессиональные компетенции:

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.

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.

Из вариативной части на профессиональный модуль ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» отведено **93**часа:

* на частично-вариативную учебную дисциплину МДК.02.01 «Программные и программно-аппаратные средства защиты информации» отведено **30часов**;
* на частично-вариативную учебную дисциплину МДК 02.02 «Криптографические средства защиты информации» отведено**22часа**;
* на учебную практику УП.02.01 **20 часов**;
* на производственную практику ПП.02.01 **21 час.**

**Использование часов вариативной части**

Из вариативной части на учебный междисциплинарный МДК 02.01 «Программные и программно-аппаратные средства защиты информации» отведено **30** часов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Дополнительные умения, знания** | **№, наименование раздела/темы** | **Количество часов** | **Формируемые компетенции** | **Обоснование включения в рабочую программу** |
| ***умения:***  - применять штатные средства защиты и специализированные продукты для решения типовых задач;  - квалифицированно оценивать область применения конкретных механизмов защиты;  - грамотно использовать аппаратные средства защиты при решении практических задач.  ***знания:***  - возможные действия злоумышленника, направленные на нарушение политики безопасности информации;  - наиболее уязвимые для атак противника элементы компьютерных систем;  - механизмы решения типовых задач защиты информации. | **Тема 1.2.** Стандарты безопасности  **Тема 1.3.** Защищенная автоматизированная система  **Тема 1.4.** Дестабилизирующее воздействие на объекты защиты  **Тема 2.3.** Вредоносное программное обеспечение  **Тема 2.6**. Аппаратные средства идентификации и аутентификации пользователей  **Тема 3.1.** Основы построения защищенных сетей  **Тема 4.1.** Обеспечение безопасности межсетевого взаимодействия  **Тема 6.1.** Мониторинг систем защиты | **4**  **4**  **4**  **4**  **4**  **4**  **4**  **2** | **ПК 2.2**  **ПК 2.3**  **ОК 01**  **ОК 02**  **ОК 09** | Запрос работодателя на дополнительные результаты освоения ОПОП |

Из вариативной части на учебный междисциплинарный МДК 02.02 «Криптографические средства защиты информации» отведено **22** часов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Дополнительные умения, знания** | **№, наименование раздела/темы** | **Количество часов** | **Формируемые компетенции** | **Обоснование включения в рабочую программу** |
| ***уметь:***  - правильно выбирать тип шифра в соответствии с поставленной задачей;  - качественно реализовать алгоритм шифрования;  - реализовывать атаку на классические шифры (исторические и современные).  ***знать:***  - классические исторические шифры и методы атак на эти шифры, современные шифры - криптографические протоколы и электронную подпись;  - типичные слабости реализации криптографических систем (PGP, RC4, Windows и др.);  - теоретические основы "хорошего" шифра по Шеннону;  - теоретические основы "хорошей" криптосистемы (правила Кирхгоффа) | **Тема 1.1.** Математические основы криптографии  **Тема 2.1.** Методы криптографического защиты информации  **Тема 2.2.** Криптоанализ  **Тема 2.3.** Поточные шифры и генераторы псевдослучайных чисел  **Тема 3.1.** Кодирование информации. Компьютеризация шифрования.  **Тема 3.2.** Симметричные системы шифрования  **Тема 3.4.** Аутентификация данных. Электронная подпись  **Тема 3.5.** Алгоритмы обмена ключей и протоколы аутентификации | **2**  **2**  **2**  **2**  **4**  **2**  **2**  **4** | **ПК 2.2**  **ПК 2.3**  **ПК 3.3.**  **ОК 02**  **ОК 04** | Запрос работодателя на дополнительные результаты освоения ОПОП |

**Формирование личностных результатов:**

|  |  |
| --- | --- |
| **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 (в студенческом самоуправлении, добровольчестве, экологических, природоохранных, военнопатриотических и др. объединениях, акциях, программах). Принимающий роль избирателя и участника общественных отношений, связанных с взаимодействием с народными избранниками | **ЛР 2** |
| Демонстрирующий приверженность традиционным духовнонравственным ценностям, культуре народов России, принципам честности, порядочности, открытости. Действующий и оценивающий свое поведение и поступки, поведение и поступки других людей с позиций традиционных российских духовнонравственных, 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 бе-режливое и чуткое отношение к религиозной принадлежности каж-дого 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** |
| Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры. Критически оценивающий и деятельно проявляющий понимание эмоционального воздействия искусства, его влияния на душевное состояние и поведение людей. Бережливо относящийся к культуре как средству коммуникации ЛР 11 и самовыражения в обществе, выражающий сопричастность к нравственным нормам, традициям в искусстве. Ориентированный на собственное самовыражение в разных видах искусства, художественном творчестве с учётом российских традиционных духовно-нравственных ценностей, эстетическом обустройстве собственного быта. Разделяющий ценности отечественного и мирового художественного наследия, роли народных традиций и народного творчества в искусстве. Выражающий ценностное отношение к технической и промышленной эстетике | **ЛР 11** |
| 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 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** |

**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 часов |
| включая: |  |  |
| - обязательную аудиторную учебную нагрузку обучающегося | **–** | 320часов |
| - самостоятельную работу обучающегося | **–** | 24часов |
| -Консультации | **-** | 12часов |
| -Учебная практика | **–** | 72часа |
| -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

1. **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 | **Практический опыт:**  установка, настройка программных средств защиты информации в автоматизированной системе  **Умения:**  устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;  **Знания:**  особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных |
| ПК 2.2 | **Практический опыт:**  обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами;  использование программных и программно-аппаратных средств для защиты информации в сети  **Умения:**  устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;  устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;  **Знания:**  особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных |
| ПК 2.3 | **Практический опыт:**  тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации  **Умения:**  диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации  **Знания:**  методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации |
| ПК 2.4 | **Практический опыт:**  решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;  применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных  **Умения:**  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  **Знания:**  особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;  типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;  основные понятия криптографии и типовых криптографических методов и средств защиты информации |
| ПК 2.5 | **Практический опыт:**  учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности  **Умения:**  применять средства гарантированного уничтожения информации  **Знания:**  особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации |
| ПК 2.6. | **Практический опыт:**  работа с подсистемами регистрации событий;  выявление событий и инцидентов безопасности в автоматизированной системе  **Умения:**  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  **Знания:**  типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа |
| ОК 1. | **Умения:**  распознавать задачу и/или проблему в профессиональном и/или социальном контексте;  анализировать задачу и/или проблему и выделять её составные части;  определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;  составить план действия;  определить необходимые ресурсы;  владеть актуальными методами работы в профессиональной и смежных сферах;  реализовать составленный план;  оценивать результат и последствия своих действий (самостоятельно или с помощью наставника).  **Знания:**  актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте.  алгоритмы выполнения работ в профессиональной и смежных областях;  методы работы в профессиональной и смежных сферах;  структуру плана для решения задач;  порядок оценки результатов решения задач профессиональной деятельности. |
| ОК 2. | **Умения:**  определять задачи поиска информации;  определять необходимые источники информации;  планировать процесс поиска;  структурировать получаемую информацию;  выделять наиболее значимое в перечне информации;  оценивать практическую значимость результатов поиска;  оформлять результаты поиска.  **Знания:**  номенклатура информационных источников, применяемых в профессиональной деятельности;  приемы структурирования информации;  формат оформления результатов поиска информации |
| ОК 3. | **Умения:**  определять актуальность нормативно-правовой документации в профессиональной деятельности;  выстраивать траектории профессионального и личностного развития  **Знания**:  содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология;  возможные траектории профессионального развития и самообразования |
| ОК 4. | **Умения:**  организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами  **Знания:**  психология коллектива; психология личности; основы проектной деятельности |
| ОК 5. | **Умения**:  излагать свои мысли на государственном языке; оформлять документы.  **Знания:**  особенности социального и культурного контекста; правила оформления документов. |
| ОК 6. | **Умения:**  описывать значимость своей профессии;  Презентовать структуру профессиональной деятельности по специальности;  **Знания:**  сущность гражданско-патриотической позиции;  Общечеловеческие ценности;  Правила поведения в ходе выполнения профессиональной деятельности |
| ОК 7. | **Умения:**  соблюдать нормы экологической безопасности;  определять направления ресурсосбережения в рамках профессиональной деятельности по специальности.  **Знания:**  правила экологической безопасности при ведении профессиональной деятельности;  основные ресурсы, задействованные в профессиональной деятельности;  пути обеспечения ресурсосбережения. |
| ОК 8. | **Умения:**  использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей;  применять рациональные приемы двигательных функций в профессиональной деятельности;  пользоваться средствами профилактики перенапряжения характерными для данной специальности  **Знания:**  роль физической культуры в общекультурном, профессиональном и социальном развитии человека;  основы здорового образа жизни;  условия профессиональной деятельности и зоны риска физического здоровья для специальности;  средства профилактики перенапряжения. |
| ОК 9. | **Умения:**  применять средства информационных технологий для решения профессиональных задач;  использовать современное программное обеспечение  **Знания:**  современные средства и устройства информатизации;  порядок их применения и программное обеспечение в профессиональной деятельности. |
| ОК 10 | **Умения:**  понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы;  участвовать в диалогах на знакомые общие и профессиональные темы;  строить простые высказывания о себе и о своей профессиональной деятельности;  кратко обосновывать и объяснить свои действия (текущие и планируемые);  писать простые связные сообщения на знакомые или интересующие профессиональные темы  **Знания:**  правила построения простых и сложных предложений на профессиональные темы;  основные общеупотребительные глаголы (бытовая и профессиональная лексика);  лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности;  особенности произношения;  правила чтения текстов профессиональной направленности |

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

**3.1 Тематический план профессионального модуля ПМ.02 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе криптографических) 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 2.1.-ПК 2.5  ОК 1– ОК 10 | МДК 02.01 «Программные и программно-аппаратные средства защиты информации» | 204 | 186 | 64 | 40 | 8 | | - | | - | - |
| ПК 2.1.-ПК 2.5  ОК 1– ОК 10 | МДК 02.02 «Криптографические средства защиты информации» | 150 | 134 | 50 | - | 16 | | - | | - | - |
|  | УП.02.01 «Учебная практика Защита информации» | 72 |  |  |  |  | |  | | 72 |  |
|  | Производственная практика (по профилю специальности) | 144 |  | | | | | | | | 144 |
|  | Экзамен по модулю | 12 | - | - | - | - | - | | - | | - |
|  | Всего: | 582 | 320 | 114 | 40 | 24 | | - | | 72 | 144 |

**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 02.01«Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты»** | | | | **216** |  |
| **Тема 1.1** Основные понятия | **Содержание:** | | | **16** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
|  | Основные понятия и определения. Угрозы информационной безопасности | | 2 |
|  | Функциональные возможности программно-аппаратных средств защиты. Концепция диспетчера доступа | | 2 |
|  | Политика безопасности. Управление рисками. Механизмы и службы защиты. | | 2 |
|  | Методы обеспечения идентификации и аутентификации, криптографической защиты, хранение ключевой информации | | 2 |
|  | Методы ограничения доступа к компонентам вычислительных систем. Методы привязки ПО к АО и физическим носителям | | 2 |
|  | Методы аудита безопасности. Методы обеспечения доступа к системе защиты и управления безопасностью | | 2 |
|  | Методы обеспечения целостности системы защиты. Классификация аппаратных и программных компонентов средств защиты программ | | 2 |
|  | Методы защиты программ от изучения кода. Принципы обеспечения безопасности программ | | 2 |
| **Практические занятия:** | | | **12** |
|  | **Практическое занятие №1**. Определение выполняемых процессов. Изучение процессов, потоков, дескрипторов и реестра Windows. Создание учетных записей пользователей | | 2 |
|  | **Практическое занятие №2**. Создание учетных записей пользователей. Использование Windows PowerShell. | | 2 |
|  | **Практическое занятие №3**. Диспетчер задач Windows. Мониторинг системных ресурсов в Windows и управление ими. | | 2 |
|  | **Практическое занятие №4**. Использование командной строки Linux. Основные команды. | | 2 |
|  | **Практическое занятие №5**. Службы Linux. Журналы Linux. | | 2 |
|  | **Практическое занятие №6**. Файловая система. Управление правами доступа | | 2 |
| **Тема 1.2.** Защищенная автоматизированная система | **Содержание:** | | | **8** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
|  | Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. | | 2 |
|  | Методология проектирования гарантированно защищенных КС. Дискреционные/мандатные модели | | 2 |
|  | SecretNetStudio Функциональные возможности. Принцип работы | | 2 |
|  | Электронные замки. Соболь | | 2 |
| **Практические занятия:** | | | **14** |
|  | **Практическое занятие № 7** Установка SNS, настройка политик безопасности. | | 2 |
|  | **Практическое занятие № 8** Настройка полномочного управления доступом SNS | | 2 |
|  | **Практическое занятие № 9** Настройка аудита операционной системы и событий SNS. Работа с журналом событий | | 2 |
|  | **Практическое занятие № 10** Настройка механизма дискреционного управления доступом | | 2 |
|  | **Практическое занятие № 11** Управление доступом к съемным носителям информации | | 2 |
|  | **Практическое занятие № 12** Настройка механизма замкнутой программной среды SNS | |  |
|  | **Практическое занятие № 13** Настройка механизма контроля целостности | |  |
| **Тема 1.3** Программно-аппаратные средства защиты автономных автоматизированных систем | **Содержание:** | | | **18** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
|  | Дестабилизирующее воздействие на объекты защиты | | 2 |
|  | Вредоносные программы. Элементы защиты от вредоносного ПО. | | 2 |
|  | Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме | | 2 |
|  | Защита от вторжений на уровне хоста | | 2 |
|  | Безопасность приложений | | 2 |
|  | Оценка уязвимостей хостов. Безопасное управление устройствами | | 2 |
|  | Понятие несанкционированного доступа к информации | | 2 |
|  | Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам | | 2 |
|  | Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды | | 2 |
| **Практические занятия:** | | | **16** |
|  | **Практическое занятие №14**. Установка и настройка антивирусного ПО | | 2 |
|  | **Практическое занятие №15**. Создание дискреционной модели безопасности. Создание скрытой информации. Установка паролей | | 2 |
|  | **Практическое занятие №16**. Разграничение прав доступа для пользователей локального  компьютера и локальной сетиWindows | | 2 |
|  | **Практическое занятие №17**. Настройка параметров политики аудита | | 2 |
|  | **Практическое занятие №18.** Настройка параметров политики безопасности операционной системы Windows | | 2 |
|  | **Практическое занятие №19**. Архивация и восстановление данных Windows | | 2 |
|  | **Практическое занятие №20**. Предотвращение и исправление ошибок жесткого диска CrystalDiskInfo | | 2 |
|  | **Практическое занятие №21**. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint) | | 2 |
| **Промежуточная аттестация по МДК.02.01** | | | | | |
| **Тема 1.4** Защита программ от изучения | **Содержание:** | | | **10** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1.-  ПК 2.5  ОК 1– ОК 10 |
|  | Задачи защиты ПО от изучения и способы их решения. | | 2 |
|  | Защита ПО от отладки/дизассемблирования/трассировки по прерываниям | | 2 |
|  | Несанкционированное копирование программ как тип НСД. Привязка ПО к аппаратному окружению и носителям. | | 2 |
|  | Методы защиты информации на отчуждаемых носителях. Шифрование. Безвозвратное удаление данных. Принципы и алгоритмы. | | 2 |
|  | Аппаратные средства идентификации и аутентификации пользователей. Устройства Touch Memory | | 2 |
| **Тема 1.5**Мониторинг безопасности и тестирование на проникновение | **Содержание:** | | | **26** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
|  | Цифровая техническая экспертиза | | 2 |
|  | Модели реагирования на инциденты | | 2 |
|  | Обработка инцидентов | | 2 |
|  | Методология тестирования на проникновение | | 2 |
|  | Получение отпечатка и сбор информации | | 2 |
|  | Методы сканирования и уклонения | | 2 |
|  | Сканирование уязвимостей | | 2 |
|  | Социальная инженерия | | 2 |
|  | Целевая эксплуатация | | 2 |
|  | Повышение привилегий и поддержание доступа | | 2 |
|  | Тестирование web-приложений | | 2 |
|  | Тестирование беспроводных сетей на проникновение | | 2 |
|  | Мобильное тестирование | | 2 |
| **Практические занятия:** | | | **14** |
|  | **Практическое занятие №22**. Правила Snort и правила межсетевого экрана | | 2 |
|  | **Практическое занятие №23**. Преобразование данных в универсальный формат | | 2 |
|  | **Практическое занятие №24**. Использовать регулярные выражения для поиска необходимых текстовых строк данных | | 2 |
|  | **Практическое занятие №25**. Извлечение исполняемого файла. Анализ предварительно записанных журналов и перехватов трафика | | 2 |
|  | **Практическое занятие №26**. Интерпретация данных HTTP и DNS для изоляции злоумышленника | | 2 |
|  | **Практическое занятие №27.**Изучение атаки на основе внедрения вредоносного кода SQL | | 2 |
|  | **Практическое занятие №28.** Изучение журналов для определения скомпрометированных узлов и файлов | | 2 |
| **Тема 1.5** WindowsServer | **Содержание:** | | | **4** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
|  | ActiveDirectory. Контролер домена | | 2 |
|  | Службы сетевой инфраструктуры в Windows Server | | 2 |
| **Практические занятия:** | | | **8** |
|  | **Практическое занятие №29.** Начальное конфигурирование WindowsServer. Настройка контроллера домена | | 2 |
|  | **Практическое занятие №30.** DHCP, DNS, IIS | | 2 |
|  | **Практическое занятие №31.** Групповые политики. Настройка хранилища и создание кластера | | 2 |
|  | **Практическое занятие №32.** WindowsServerBackup. Настройка журналирования | | 2 |
| **Курсовой проект** |  | Актуальность темы. Постановка целей и задач | | **40** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
|  | 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 |
|  | Защитакурсового проекта | | 2 |
| Экзамен | | | | **8** |  |
| **Примерная тематика курсовых работ**   1. Внедрение DLP-системы в сеть предприятия 2. Изучение средств тестирования на проникновение | | | |  |  |
| **Самостоятельная учебная работа при изучении МДК.02.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты»** | | | | **6** |  |
| **Рекомендуемая тематика самостоятельной работы:**  1. Проблемы обеспечения безопасности операционных систем. Windows, Linux.  2.Технологии аутентификации.  3.Аутентификация, авторизация и администрирование действий пользователя.  4.Пароли. PIN-коды. Методы надежного составления паролей.  5.Токены. Смарт-карты. Виртуальные ключи.  6.Программно-аппаратные модули доверенной загрузки.  7.АПМДЗ Криптон – Замок системный администратор.  8.Изучение настроек системного администратора АПМДЗ.  9.Сектор НЖМД. Область памяти. Файл, папка, каталог.  10.Разграничение доступа к объектам операционной системы.  11.Комплексная система организации управления доступом. Инсталяция. Настройка.  12.Аудит безопасности операционной системы.  13.Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика.  14.Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ.  15.Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ.  16.Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.  17.Концепция построения виртуальных защищенных сетей;  18.Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура защищенного пакета. Варианты построения защищенных каналов.  19.Защита на канальном уровне. Протоколы PPTP, L2F, L2TP.  20.Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS.  21.Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP.  22.Защита на прикладном уровне. Протоколы PAP, CHAP, Kerberos.  23.Функционирование системы управления средствами защиты.  24.Аудит безопасности информационной системы.  25. Изучение новых технологий хранения информации  26. Статистика и анализ крупных утечек информации за год  27. Поиск информации о новых видах атак на информационную систему  28. Обзор современных программных и программно-аппаратных средств защиты  29. Сравнительный анализ современных программных и программно-аппаратных средств защиты | | | |  |  |
| **МДК 02.02 «Криптографическая защита информации»** | | | | **144** |  |
| **Тема 2.1**Математические основы криптографии | **Содержание:** | | | **24** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1.-  ПК 2.5  ОК 1– ОК 10 |
| 1 | | Предмет и задачи криптографии. История криптографии. Основные термины | 2 |
| 2 | | Элементы теории множеств. Группы, кольца, поля. |  |
| 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** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
| 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** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
| 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** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
| 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** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
| 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 №15Упрощенный 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** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1.-  ПК 2.5  ОК 1– ОК 10 |
| 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** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1. -  ПК 2.5  ОК 1– ОК 10 |
| 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** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1.-  ПК 2.5  ОК 1– ОК 10 |
| 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** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1.2-  ПК 2.5  ОК 1– ОК 10 |
| 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** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1.  -ПК 2.5  ОК 1– ОК 10 |
| 1 | | Криптографическая защита беспроводных соединений | 2 |
| **Тема 2.11** Защита информации в электронных платежных системах | **Содержание:** | | | **4** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1.  -ПК 2.5  ОК 1– ОК 10 |
| 1 | | Принципы функционирования электронных платежных систем. | 2 |
| 2 | | Применение криптографических протоколов для обеспечения безопасности электронной коммерции. | 2 |
| **Тема 2.12.** OpenSSL | **Практические занятия:** | | | **8** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1.  -ПК 2.5  ОК 1– ОК 10 |
| 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 «Криптографическая защита 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. 1 SNS | **Практические занятия:** | | | **72** | ЛР1-ЛР4, ЛР7, ЛР10, ЛР12-ЛР20  ПК 2.1.-ПК2.5  ОК 1– ОК 10 |
| 1 | | Настройка контроллера домена | 2 |
| 2 | | Введение в домен устройств | 2 |
| 3 | | Применение групповых политик | 2 |
| 4 | | Установка компонентов Secret Net Studio в сетевом варианте | 2 |
| 5 | | Локальная настройка Secret Net Studio в соответствии с заданными параметрами | 2 |
| 6 | | Настройка механизма контроля целостности | 2 |
| 7 | | Централизованное ведение журналов в SecretNetStudio" | 2 |
| 8 | | Управление подчинением защищаемых компьютеров серверу безопасности SNS | 2 |
| 9 | | Работа с электронными идентификаторами | 2 |
| 10 | | Настройка полномочного управления доступом | 2 |
| 11 | | Настройка механизма дискреционного управления доступом | 2 |
| 12 | | Управление доступом к съемным носителям информации" | 2 |
| 13 | | Настройка механизма замкнутой программной среды | 2 |
| 14 | | Использование криптоконтейнеров | 2 |
| 15 | | Настройка теневого копирования и маркировки при контроле печати | 2 |
| 16 | | Формирование отчетов в Secret Net Studio | 2 |
| 17 | | Персональный межсетевой экран | 2 |
| 18 | | Авторизация сетевых соединений | 2 |
| 19 | | Настройка антивируса и СОВ | 2 |
| 20 | | Построение закрытого контура | 2 |
| 21 | | Организация защиты средствами Secret Net Studio согласно требованиям регуляторов | 2 |
| Тема 1.2 Secret Net LSP | 22 | | Настройка стенда | 2 |
| 23 | | Установка Secret Net LSP | 2 |
| 24 | | Управление учетными записями пользователей | 2 |
| 25 | | Настройка параметров работы Secret Net LSP | 2 |
| 26 | | Настройка механизма контроля целостности | 2 |
| 27 | | Настройка механизма дискреционного управления доступом | 2 |
| 28 | | Управление доступом к съемным носителям информации | 2 |
| 29 | | Настройка механизма замкнутой программной среды | 2 |
| 30 | | Настройка персонального межсетевого экрана | 2 |
| 31 | | Построение закрытого контура | 2 |
| Тема 1.3 Континент 4 | 32 | | Развертывание центра управления сетью Континент и регистрация главного администратора | 2 |
| 33 | | Подготовка рабочего места главного администратора | 2 |
| 34 | | Развертывание подчиненных узлов безопасности | 2 |
| 35 | | Настройка правил фильтрации | 2 |
| 36 | | Настройка СОВ в составе UTM-узла безопасности | 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:** | | | | **582** |  |
| **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** |  |

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

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

Реализация программы профессионального модуля требует наличия

* учебных кабинетов, лабораторий:
* Лаборатория «Программных и программно-аппаратных средств защиты информации».

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;
* 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;
* комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

**4.2. Информационное обеспечение обучения**

**4.2.1 Основные источники/основная литература:**

1. Шива Парарасрам, Алекс Замм, KaliLinux 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, 242мтр.
3. А.О. Чефранова, Технология построения VPNVipNet: курс лекций. Тзд.: Москва Горячая линия – Телекос, 2018. 334 стр.
4. Букатов Александр Алексеевич, Гуда Сергей Александрович. Компьютерные сети. Расширенный начальный курс. Спб.: Питер, 2019.
5. Олифер, В.Г. Компьютерные сети: Принципы, технологии, протоколы: Учеб. пособие для вузов / В. Г. Олифер, Н.А. Олифер.Спб.: Питер, 2019.
6. Таненбаум, Э. Компьютерные сети/ Э. Таненбаум, Д. Уэзеролл– 5-е изд. –Спб.: Питер, 2017.
7. Куроуз, Дж.Компьютерные сети: Нисходящий подход / Дж. Куроуз; К.Росс. – М.: Э, 2016.
8. Л.Г. Гагарина. Разработка и эксплуатация автоматизированных информационных систем. ИД Форум 2021, 384 стр.
9. В.Б. Кравченко, П.В. Зиновьев, И.Н. Селютин. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении. ИЦ «Академия» 2018, 299 стр.
10. Таненбаум Эндрю, Бос Х. Современные операционные системы. Изд. – Спб.: Питер, 2018, 1120 стр.
11. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2014.
12. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2016.
13. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. - 2-е изд.- М.: Горячая линия-Телеком, 2014.
14. Мельников Д. Информационная безопасность открытых систем. - М.: Форум, 2013.
15. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

**4.2.2. 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/>

**4.2.3. 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/)

**4.3. 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 производственнойпрактике (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.

**4.4. Кадровое обеспечение образовательного процесса**

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

МДК.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты, Копылова О.В

МДК.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты, Перевышина Е.А.

МДК.02.02 – Криптографическая защита информации, Перевышина Е.А,

МДК.02.02 – Криптографическая защита информации, Сафарьян О.А.

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

УП.02.01 Учебная практика, Бороненкова С.Е.

УП.02.01 Учебная практика, Купчинская Н.И.

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

# **5. Контроль и оценка результатов освоения ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

(ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

|  |  |  |
| --- | --- | --- |
| **Результаты обучения** | **Критерии оценки** | **Формы и методы**  **контроля и оценки**  **результатов обучения** |
| **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 правдуо 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 (в студенческом самоуправлении, добровольчестве, экологических, природоохранных, военнопатриотических и др. объединениях, акциях, программах). Принимающий роль избирателя и участника общественных отношений, связанных с взаимодействием с народными избранниками  **ЛР 3**  Демонстрирующий приверженность традиционным духовнонравственным ценностям, культуре народов России, принципам честности, порядочности, открытости. Действующий и оценивающий свое поведение и поступки, поведение и поступки других людей с позиций традиционных российских духовнонравственных, 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 | 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;  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;  проявление правовой активности и навыков правомерного поведения, уважения к Закону;  отсутствие фактов проявления идеологии терроризма и экстремизма среди обучающихся;  проявление культуры потребления информации, умений и навыков пользования компьютерной техникой, навыков отбора и критического анализа информации, умения ориентироваться в информационном пространстве;  проявление экономической и финансовой культуры, экономической грамотности, а также собственной адекватной позиции по отношению к социально-экономической действительности. | 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. |
| 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. 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  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| 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.  Курсовой проект.  Экзамен.  Отчет по производственной практике  Экзамен по модулю |
| 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  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| 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  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. | - 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  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| 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  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 | 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. 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  Курсовой проект.  Экзамен.  Дифференцированный зачет.  Отчет по производственной практике  Экзамен по модулю |
| 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  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\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_