**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 информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты**

программы подготовки специалистов среднего звена по специальности по специальности

**10.02.04 «Обеспечение информационной безопасности телекоммуникационных 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 НМР  \_\_\_\_\_\_\_\_\_\_ Подцатова И.В.  «30» августа 2024 г. |
| --- | --- |

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерства образования и науки Российской Федерации № 1551 от 9 декабря 2016г (ред. от 03.07.2024 №464) «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем», зарегистрированного Министерством юстиции (рег. № 44944 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 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты, Копылова О.В.– преподаватель ГБПОУ РО «РКСИ»

МДК.02.02 Криптографическая защита информации, Сафарьян О.А.. – преподаватель ГБПОУ РО «РКСИ»

МДК.02.02 Криптографическая защита информации, Перевышина Е.А.. – преподаватель ГБПОУ РО «РКСИ»

МДК.02.03 Разработка и администрирование удаленных баз данных, Бондаренко О.О. преподаватель ГБПОУ РО «РКСИ»

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

Производственная практика (по профилю специальности)

Рецензенты:

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

**СОДЕРЖАНИЕ**

[1. Паспорт рабочей программы профессионального модуля 4](#_Toc176177443)

[2. Результаты освоения профессионального модуля 8](#_Toc176177444)

[3.структура и содержание профессионального модуля 10](#_Toc176177445)

[4. Условия реализации рабочей программы профессионального модуля 22](#_Toc176177446)

[5. Контроль и оценка результатов освоения профессионального модуля 26](#_Toc176177447)

# **1. Паспорт рабочей программы профессионального модуля**

* 1. **Область применения рабочей программы**

Рабочая программа 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 частью основной профессиональной образовательной программы по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» базового уровня подготовки в части освоения основного вида профессиональной деятельности (ВПД): Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защитыи соответствующих профессиональных компетенций (ПК):

* ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
* ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
* ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

Рабочая программа профессионального модуля ПМ.02 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты» предназначена для студентов 3-4 курсов очной формы обучения.

* 1. **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, испытаний и конфигурирования программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей;
* поддержания бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях;
* защиты информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

уметь:

* выявлять и оценивать угрозы безопасности информации в ИТКС;
* настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
* проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
* проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
* проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
* проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
* проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации.

#### *знать:*

* возможные угрозы безопасности информации в ИТКС;
* способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее;
* типовые программные и программно-аппаратные средства
* защиты информации в информационно-телекоммуникационных системах и сетях;
* криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;
* порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;
* организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;
* порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации.

**1.3 Рекомендуемое количество часов на освоение рабочей программы профессионального модуля ПМ.02 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты»**

|  |  |  |
| --- | --- | --- |
| Всего | **–** | 690 часов |
| в том числе: |  |  |
| * максимальная учебная нагрузка обучающегося | **–** | 466 часов |
| включая: |  |  |
| - обязательную аудиторную учебную нагрузку обучающегося | **–** | 440 часов |
| - самостоятельную работу обучающегося:  Написание реферата.  Написание конспекта первоисточника.  Подготовка информационного сообщения.  Создание презентации.  Составление опорного конспекта.  Подготовка к практическим занятиям.  Другие виды самостоятельной работы | **–** | 16 часов |
| -Консультации | **-** | 2 часа |
| -Учебная практика | **–** | 36 часов |
| -Производственная практика | **-** | 180 часов |
| Промежуточная аттестация | **-** | 8 часов |
| Экзамен квалификационный | **-** | 8 часов |

Практическая подготовка при реализации профессионального модуля путем проведения практических и лабораторных занятий, учебной и производственной практики занимает **368 часов.**

Из вариативной части на профессиональный модуль ПМ.02 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты» отведено **167** часов:

* на частично-вариативную учебную дисциплину МДК.02.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты» отведено **36** часов;
* на частично-вариативную учебную дисциплину МДК 02.02 «Криптографическая защита информации» отведено **20** часов;
* на вариативную дисциплину МДК.02.03 «Разработка и администрирование удаленных баз данных» отведено **70** часов;
* на частично-вариативную УП.02.01 Учебную практику отведено **18** часов;
* на производственную практику ПП.02.01 (по профилю специальности) отведено **23** часа.

**1.4 Результаты освоения профессионального модуля**

Результатом освоения 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 овладение обучающимися видом профессиональной деятельности (ВПД) Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты, в том числе профессиональными компетенциями (ПК), общими компетенциями (ОК).

|  |  |
| --- | --- |
| Код | Наименование результатов обучения |
| ПК 2.1 | Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей |
| ПК 2.2 | Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях. |
| ПК 2.3 | Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями |
| 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**

**2.1 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 2.2**  **ПК 2.3**  **ОК 1– ОК 9** | **МДК 02.01** **Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты** | **240** | **220** | **64** | **30** | **10** | | - | | **-** | **-** |
| **ПК 2.1.**  **ПК 2.2**  **ПК 2.3**  **ОК 1– ОК 9** | **МДК 02.02 «Криптографическая защита информации»** | **156** | **150** | **54** | **-** | **6** | | **-** | | **-** | **-** |
| **ПК 2.1.**  **ПК 2.2**  **ПК 2.3**  **ОК 1– ОК 9** | **МДК.02.03 «Разработка и администрирование удаленных баз данных»** | **70** | **70** | **34** | **-** | **-** | | **-** | | **-** | **-** |
|  | **УП.02.01 «Учебная практика»** | **36** |  |  |  |  | |  | | **36** |  |
|  | **Производственная практика (по профилю специальности)** | **180** |  | | | | | | | | **180** |
|  | **Экзамен по профессиональному модулю** | **8** | - | - | - | - | - | | - | | **-** |
|  | **Всего:** | **690** | **440** | **152** | **-** | **16** | | **-** | | **36** | **180** |

**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»** | | | | **194** |  |
| **Тема 1.1** Основные понятия | **Содержание:** | | | **42** | ПК 2.1.  ПК 2.2  ПК 2.3  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:** | | | **24** |
|  | **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). Конфигурирование службы ALD (AstraLinux) | | 2 |
| **Тема 1.3** Защита конечных точек | **Практические занятия:** | | | **12** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
|  | **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 | | 2 |
| **Тема 1.4** Защита программ от изучения | **Содержание:** | | | **6** | ПК 2.1.  ПК 2.2  ПК 2.3  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 2.2  ПК 2.3  ОК 1– ОК 9 |
|  | 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 2.2  ПК 2.3  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** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
|  | 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** Установка и базовая настройка программного комплекса InfoWatch | **Содержание:** | | | **10** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
|  | Теоретические основы корпоративной защиты т внутренних угроз. | | 2 |
|  | Административно-организационные аспекты корпоративной защиты от внутренних угроз | | 2 |
|  | Лицензирование InfoWatch Trafic Monitor | | 2 |
|  | Политики в InfoWatch Trafic Monitor. Создание категорий и терминов в InfoWatch Traffic Monitor | | 2 |
|  | Создание правил защиты данных в InfoWatch Device Monitor | | 2 |
| **Промежуточная аттестация по МДК.02.01** | | | | | |
| **Тема 1.9**Мониторинг безопасности и тестирование на проникновение | **Содержание:** | | | **30** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
|  | Мониторинг общих ресурсов. Технологии обеспечения безопасности | | 2 |
|  | Файлы журналов оконечных устройств, сетевые журналы | | 2 |
|  | Источники предупреждений. Работа с данными безопасности сети. | | 2 |
|  | Цифровая техническая экспертиза | | 2 |
|  | Модели реагирования на инциденты | | 2 |
|  | Обработка инцидентов | | 2 |
|  | Методология тестирования на проникновение | | 2 |
|  | Получение отпечатка и сбор информации | |  |  |
|  | Методы сканирования и уклонения | |  |  |
|  | Сканирование уязвимостей | |  |  |
|  | Социальная инженерия | |  |  |
|  | Целевая эксплуатация | |  |  |
|  | Повышение привилегий и поддержание доступа | |  |  |
|  | Тестирование web-приложений | |  |  |
|  | Тестирование беспроводных сетей на проникновение | |  |  |
| **Тема 1.10.** VipNet | **Содержание:** | | | **14** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
|  | Обзор VipNet Administrator | | 2 |
|  | Обзор VipNet Client | | 2 |
|  | Обзор VipNet Coordinator | | 2 |
|  | Обзор VipNet Cluster | | 2 |
|  | Обзор VipNet Watcher | | 2 |
|  | Обзор VipNet Policy Manager | | 2 |
|  | Сценарии использования VipNet | | 2 |
| **Практические занятия:** | | | **40** |
|  | Планирование схемы защищённой сети | | 2 |
|  | Установка программного комплекса vipnet administrator 4, | | 2 |
|  | Создание структуры защищённой сети, | | 2 |
|  | Настройка резервного копирования данных и восстановление данных в по vipnet administrator | | 2 |
|  | Модификация защищённой сети | | 2 |
|  | Компрометация | | 2 |
|  | Настройка политик безопасности в vipnet policy manager | | 2 |
|  | Установка vipnet Coordinator в качестве межсетевого шлюза | | 2 |
|  | Первоначальная настройка межсетевого взаимодействия | | 2 |
|  | Модификация межсетевого взаимодействия | | 2 |
|  | Coordinator linux 4. Firewall. Фильтры по умолчанию | | 2 |
|  | Coordinator linux 4. Firewall. | | 2 |
|  | Coordinator linux 4. Настройка трансляции сетевых адресов | | 2 |
|  | Coordinator linux 4. Туннелирование незащищенных узлов | | 2 |
|  | Coordinator linux 4.Сохранение настроек | | 2 |
|  | Coordinator linux 4.Кластер горячего резервирования | | 2 |
|  | Установка ViPNet IDS NS VA, ViPNet IDS MC VA, ViPNet IDS HS, ViPNet TIAS VA | | 2 |
|  | Подготовка к работе и настройка ViPNet IDS NS VA | | 2 |
|  | Подготовка к работе и настройка ViPNet TIAS VA в роли Системного администратора | | 2 |
|  | Обновление ViPNet IDS MC | | 2 |
| **Курсовой проект** | **Практические занятия:** | | |  | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
|  | Актуальность темы. Постановка целей и задач | | **30** |
|  | 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 | | 4 |
|  | Настройка правил агентского мониторинга | | 4 |
|  | Настройка политик DLP-системы | | 6 |
|  | Тестирование средств ИБ. Проверка эффективности реализации защиты от возможных угроз | | 2 |
|  | Разработка нормативно-правовой документации для пользователей | | 2 |
|  | Защита курсового проекта | | 2 |
| Экзамен | | | | **8** |  |
| **Самостоятельная учебная работа при изучении МДК.02.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты»** | | | | **2** |  |
| **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. | | | |  |  |
| **МДК 02.02 «Криптографическая защита информации»** | | | | **150** |  |
| **Тема 2.1** Математические основы криптографии | **Содержание:** | | | **30** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
| 1 | | Элементы теории множеств. Группы, кольца, поля. | 2 |
| 2 | | Делимость чисел. Простые и составные числа. | 2 |
| 3 | | НОД. Алгоритм Евклида. | 2 |
| 4 | | Отношения сравнимости. | 2 |
| 5 | | Модулярная арифметика | 2 |
| 6 | | Функция Эйлера. | 2 |
| 7 | | Алгоритм быстрого возведения в степень | 2 |
| 8 | | Расширенный алгоритм Евклида | 2 |
| 9 | | Китайская теорема об остатках | 2 |
| 10 | | Проверка чисел на простоту. | 2 |
| 11 | | Алгоритмы генерации простых чисел. | 2 |
| 12 | | Разложение числа на множители. | 2 |
| 13 | | Алгоритмы факторизации. | 2 |
| 14 | | Алгоритмы дискретного логарифмирования. | 2 |
| 15 | | 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 |
| **Тема 2.2** Методы криптографического защиты информации | **Содержание:** | | | **10** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
| 1 | | Классификация основных методов криптографической защиты. | 2 |
| 2 | | Методы симметричного шифрования | 2 |
| 3 | | Шифры замены | 2 |
| 4 | | Методы перестановки | 2 |
| 5 | | Методы гаммирования | 2 |
| **Практические занятия:** | | | **8** |
| 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 | 4 |
| **Тема 2.3.** Криптоанализ | **Содержание:** | | | **10** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
| 1 | | Основные методы криптоанализа. | 2 |
| 2 | | Криптографические атаки. | 2 |
| 3 | | Криптографическая стойкость | 2 |
| 4 | | Перспективные направления криптоанализа, | 2 |
| 5 | | Инструменты криптоанализа | 2 |
| **Практические занятия:** | | | **12** |
| 1 | | Практическое занятие №9. Криптоанализ шифра простой замены | 4 |
| 2 | | Практическое занятие №10. Криптоанализ шифров методом полного перебора ключей | 4 |
| 3 | | Практическое занятие №11. Криптоанализ шифра Вижинера | 4 |
| **Конец 6 семестра** | | | | | |
| **Тема 2.4.** Кодирование информации. Компьютеризация шифрования | **Содержание:** | | | **2** | ПК 2.1.  ПК 2.2  ПК 2.3  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:** | | | **16** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
| 1 | | Симметричное шифрование | 2 |
| 2 | | Алгоритм DES | 2 |
| 3 | | ГОСТ 28147-89 в режиме простой замены | 2 |
| 4 | | ГОСТ 28147-89 в режиме гаммирования | 2 |
| 5 | | ГОСТ 28147-89 гаммирование с обратной связью | 2 |
| 6 | | ГОСТ 28147-89 выработка имитовставки | 2 |
| 7 | | Алгоритм AES | 2 |
| 8 | | 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:** | | | **4** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
| 1 | | Поточное шифрование. Псевдослучайные последовательности | 2 |
| 2 | | 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 2.2  ПК 2.3  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:** | | | **8** |
| 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:** | | | **8** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
| 1 | | Аутентификация данных | 2 |
| 2 | | ЭП. Однонаправленные хэш-функции. | 2 |
| 3 | | Применение различных функций хэширования, анализ особенностей хешей | 2 |
| 4 | | Применение криптографических атак на хеш-функции | 2 |
| **Практические занятия:** | | | **4** |
| 1 | | Практическая работа №22 Применение различных функций хэширования, анализ особенностей хешей | 2 |
| 2 | | Практическая работа №23 Применение криптографических атак на хеш-функции | 2 |
| **Тема 2.9.** Алгоритмы обмена ключей и протоколы аутентификации | **Содержание:** | | | **6** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК9 |
| 1 | | Алгоритмы распределения ключей с применением симметричных и асимметричных схем | 2 |
| 2 | | Протоколы аутентификации | 2 |
| 3 | | Протокол KERBEROS | 2 |
| Дифференцированный зачет | | | | 2 |  |
| **Самостоятельная учебная работа при изучении МДК.02.02 «Криптографическая защита информации»** | | | | **6** |  |
| **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.  6. Криптографические методы.  7. Шифрование. Кодирование. Стеганография. Сжатие.  8. Традиционные шифры перестановки. Одно и двух направленные. Поточные и блочные шифры.  9.Традиционные шифры замены. Шифры многоалфавитной замены. Частотность символов.  10. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста.  11. Компьютерное шифрование.  12. Стандарт шифрования данных DES. Структура DES. Безопасность DES. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015.  13. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos.  14. Асимметричное шифрование. Криптографическая система Эль-Гамаля. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012.  15. Модель угроз безопасности ИС персональных данных на предприятии  16. Комплексная модель защиты информации на предприятии.  17. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)  18. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)  19. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)  20. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)  21. Проблема защиты информации в облачных хранилищах данных и ЦОДах  22 Защита сред виртуализации. | | | |  | ПК 2.1.  -ПК 2.3  ОК 1– ОК 9 |
| **МДК.02.03 «Разработка и администрирование удаленных баз данных»** | | | | **72** |  |
| **Тема 3.1.** Основные теории баз данных. Модели данных | **Содержание:** | | | **4** | ОК1-4, 9  ПК 1.1 |
| 1 | | Основные понятия теории баз данных. Реляционные и не реляционные базы данных (отличии, примеры). | 2 |
| 2 | | ОбъектыSQL и NoSQLбаз данных и классы объектов. Отношения. Атрибут. Типы данных. Домен. Понятия реляционной базы данных (база данных, таблица, ключи, связи, индексы). | 2 |
| **Тема 3.2** Модели данных | **Содержание:** | | | **2** | ОК1-4, 9  ПК 1.1 |
| 1 | | Модели и структуры информационных систем.  Логическая и физическая независимость данных. Типы моделей данных(иерархические, сетевые, реляционные и постреляционные модели организации данных). | 2 |
| **Тема 3.3.** Проектирование баз данных | **Содержание:** | | | **6** | ОК1-4, 9  ПК 1.1 |
| 1 | | Информационные модели реляционных баз данных | 2 |
| 2 | | Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами. | 2 |
| 3 | | Средства автоматизации проектирования | 2 |
| **Практические занятия:** | | | **6** |
| 1 | | **Практическое занятие 1**. Проектирование инфологической модели данных | 2 |
| 2 | | **Практическое занятие 2**. Проектирование структуры базы данных | 2 |
| 3 | | **Практическое занятие 3.**  Проектирование базы данных с использованием CASE-средств | 2 |
| **Тема 3.4.** Создание базы данных и работа с ней в СУБД | **Содержание:** | | | **4** | ОК1-4, 9  ПК 1.1 |
| 1 | | Создание базы данных. Манипулирование данными. | 2 |
| 2 | | Индексы. Связи между таблицами. Объединение таблиц | 2 |
| **Практические занятия:** | | | **8** |
| 1 | | **Практическое занятие 4.** Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям | 2 |
| 2 | | **Практическое занятие 5.** Создание взаимосвязей | 2 |
| 3 | | **Практическое занятие 6.** Сортировка, поиск и фильтрация данных | 2 |
| 4 | | **Практическое занятие 7.** Способы объединения таблиц | 2 |
| **Тема 3.5.** Структурированный язык запросов SQL.  Реализация запросов к базе данных. | **Содержание:** | | | **6** | ОК1-4, 9  ПК 1.1ОК 9 |
| 1 | | Общая характеристика языка структурированных запросов SQL. | 2 |
| 2 | | Структуры и типы данных. Стандарты языка SQL. | 2 |
| 3 | | Команды определения данных и манипулирования данными | 2 |
| **Практические занятия:** | | | **8** |
| 1 | | **Практическое занятие 8**. Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL | 2 |
| 2 | | **Практическое занятие 9.** Создание и использование запросов. Группировка и агрегирование данных | 2 |
| 3 | | **Практическое занятие 10.** Коррелированные вложенные запросы | 2 |
| 4 | | **Практическое занятие 11.** Создание в запросах вычисляемых полей. Использование условий | 2 |
| **Тема 3.6.** Организация распределённых баз данных | **Содержание:** | | | **6** | ОК1-4, 9  ПК 1.1 |
| 1 | | Архитектуры распределенных баз данных | 2 |
| 2 | | Серверная часть распределенной базы данных | 2 |
| 3 | | Клиентская часть распределенной базы данных | 2 |
| **Практические занятия:** | | | **2** |
| 1 | | **Практическое занятие 12.** Управление доступом к объектам базы данных | 2 |
| **Тема 3.7** Администрирование базы данных | **Содержание:** | | | **8** | ОК1-4, 9  ПК 1.1 |
| 1 | | Обеспечение целостности, достоверности и непротиворечивости данных | 2 |
| 2 | | Перехват исключительных ситуаций и обработка ошибок | 2 |
| 3 | | Механизмы защиты информации в системах управления базами данных | 2 |
| 4 | | Копирование и перенос данных. Восстановление данных | 2 |
| **Практические занятия:** | | | 10 |
| 1 | | **Практическое занятие 13.** Установка СУБД. Настройка компонентов СУБД.. | 2 |
| 2 | | **Практическое занятие 14**. Создание форм и отчетов | 2 |
| 3 | | **Практическое занятие 15.**  Создание меню. Генерация, запуск. | 2 |
| 4 | | **Практическое занятие №16** Профилирование запросов клиентских приложений | 2 |
| 5 | | **Практическое занятие №17**Управление правами доступа к базам данных | 2 |
| **УП.02.01 Учебная практика** | | | | **36** |  |
| Тема 1. Корпоративная защита от внутренних угроз | **Практические занятия:** | | | **36** | ПК 2.1.  ПК 2.2  ПК 2.3  ОК 1– ОК 9 |
| 1 | | Установка VipNet Administrator | 2 |
| 2 | | Создание структуры защищенной сети VipNet. | 2 |
| 3 | | Настройка резервного копирования и восстановления данных в VipNet Administrator | 2 |
| 4 | | Модификация защищенной сети | 2 |
| 5 | | Компрометация в VipNet и настройка политик безопасности | 2 |
| 6 | | Установка VipNet Coordinator в качестве межсетевого шлюза | 2 |
| 7 | | Модификация межсетевого взаимодействия | 2 |
| 8 | | **.** VipNet Coordinator Linux установка | 2 |
| 9 | | Coordinator Linux Firewall | 2 |
| 10 | | VipNet Coordinator Linux туннелирование | 2 |
| 11 | | Установка VipNet Administrator | 2 |
| 12 | | **.** Создание структуры защищенной сети VipNet. | 2 |
| 13 | | Настройка резервного копирования и восстановления данных в VipNet Administrator | 2 |
| 14 | | Подготовка к работе и настройка ViPNet IDS NS VA | 2 |
| 15 | | Подготовка к работе и настройка ViPNet TIAS VA | 2 |
| 16 | | Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority | 2 |
| 17 | | Установка и настройка ПО RegistrationPoint | 2 |
| 18 | | Установка и настройка ПО CA Informing | 2 |
| **Производственная практика (по профилю специальности)** | | | | **180** |  |
| Участие в организации работ по защите персональных компьютеров на предприятии  Участие в организации работ по защите локальных сетей на предприятии  Участие в организации работ по защите работ в глобальной сети интернет на предприятии  Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети.  Администрирование систем безопасности проводной защищенной локальной сети.  Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети.  Администрирование систем безопасности беспроводной защищенной локальной сети.  Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей.  Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей  Подключение, установка драйверов, настройка программных средств абонентского шифрования  Администрирование внедренных средств  Настройка средств электронной подписи  Администрирование средств электронной подписи  Администрирование средств PKI | | | |  |  |
| **Максимальная учебная нагрузка:** | | | | **440** |  |
| **в том числе:** | | | |  |  |
| ***Лекции*** | | | | **258** |  |
| ***Лабораторные и практические занятия*** | | | | **152** |  |
| ***Учебная практика/Учебная практика (производственное обучение)*** | | | | **36** |  |
| ***Производственная практика*** | | | | **180** |  |
| ***Самостоятельная работа*** | | | | **16** |  |
| ***Консультации*** | | | | **2** |  |
| **Промежуточная аттестация** | | | | **16** |  |
| **Всего** | | | | **690** |  |

# **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. Федорова Г.Н. Основы проектирования баз данных. –М.: ОИЦ «Академия» 2020.
2. Шива Парарасрам, Алекс Замм, Kali Linux Тестирование на проникновение и безопасность. Изд. Питер, 2020, 441 стр.
3. А.П. Душкин. Программно-аппаратные средства обеспечения информационной безопасности. Изд.: Москва Горячая линия- Телеком, 2020, 242мтр.
4. А.О. Чефранова, Технология построения VPN VipNet: курс лекций. Тзд.: Москва Горячая линия – Телекос, 2023. 334 стр.
5. Букатов Александр Алексеевич, Гуда Сергей Александрович. Компьютерные сети. Расширенный начальный курс. Спб. : Питер, 2022.
6. Л.Г. Гагарина. Разработка и эксплуатация автоматизированных информационных систем. ИД Форум 2021, 384 стр.
7. В.Б. Кравченко, П.В. Зиновьев, И.Н. Селютин. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении. ИЦ «Академия» 2018, 299 стр.
8. Таненбаум Эндрю, Бос Х. Современные операционные системы. Изд. – Спб.: Питер, 2018, 1120 стр.
9. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2014.
10. Костров Б. В., Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2016.
11. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. - 2-е изд.- М.: Горячая линия-Телеком, 2014.
12. Мельников Д. Информационная безопасность открытых систем. - М.: Форум, 2013.
13. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
14. Диго С.М. Базы данных: проектирование и использование:Учеб.для вузов. - М.: Финансы и статистика, 2021.
15. [Суэринг](http://www.ozon.ru/person/5317903/) С., [Конверс](http://www.ozon.ru/person/2708682/) Т., [Парк](http://www.ozon.ru/person/2708681/) Д. PHP и MySQL. Библия программиста. Перевод: [Птицын](http://www.ozon.ru/person/269439/) К. – Изд: [Вильямс](http://www.ozon.ru/brand/856490/), 2020.
16. Дунаев В. Базы данных. Язык SQL для студента. – Изд: БХВ-Петербург, 2022.
17. Рудаков А.В. Технология разработки программных продуктов: учеб.пособие для студ.сред.проф.образования/А.В.Рудаков.-5-е изд.,стер.- М.: Издательский центр «Академия», 2021.
18. Харрис Энди. PHP/MySQL для начинающих. – СПб: Питер, 2020

**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 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.

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

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

МДК.02.03 Разработка и администрирование удаленных баз данных, Бондаренко О.О.

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

УП.02.01 Учебная практика, Бороненкова С.Е.

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)

|  |  |  |
| --- | --- | --- |
| Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля | Критерии оценки | Методы оценки |
| ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей | - выявлять и оценивать угрозы безопасности информации в ИТКС;  - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;  - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) 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. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях | - выявлять и оценивать угрозы безопасности информации в ИТКС;  - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) 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 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями | - выявлять и оценивать угрозы безопасности информации в ИТКС;  - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;  - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; | 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 |

|  |  |  |
| --- | --- | --- |
| **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\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_