

**ПРИЛОЖЕНИЕ 1**  
**к ОПОП-П по специальности**  
**10.02.05 Обеспечение информационной безопасности автоматизированных систем**

**РАБОЧИЕ ПРОГРАММЫ ПРОФЕССИОНАЛЬНЫХ МОДУЛЕЙ**

**СОДЕРЖАНИЕ**

|  |           |
|--|-----------|
| <b>ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ</b>                     | <b>2</b>  |
| <b>(ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ</b>           | <b>2</b>  |
| <b>ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ</b>     |           |
| <b>ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ</b>          | <b>29</b> |
| <b>ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ</b>           | <b>51</b> |
| <b>ПМ.04 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ</b> |           |
| <b>МАШИН</b>   | <b>71</b> |
| <b>ПМ.05 КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА</b>       |           |
| <b>ИНФОРМАТИЗАЦИИ</b>  | <b>82</b> |

**Приложение 1.1**  
к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

**Рабочая программа профессионального модуля**  
**«ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ**  
**(ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ»**

**2025 г.**

## СОДЕРЖАНИЕ

|   |           |
|---|-----------|
| <b>1. Общая характеристика .....</b>  | <b>4</b>  |
| 1.1. Цель и место профессионального модуля в структуре образовательной программы..... | 4         |
| 1.2. Планируемые результаты освоения профессионального модуля.....                    | 4         |
| <b>2. Структура и содержание профессионального модуля .....</b>                       | <b>5</b>  |
| 2.1. Трудоемкость освоения модуля .....   | 5         |
| 2.2. Структура профессионального модуля .....   | 5         |
| 2.3. Содержание профессионального модуля .....  | 7         |
| <b>3. Условия реализации профессионального модуля .....</b>                           | <b>27</b> |
| 3.1. Материально-техническое обеспечение.....   | 27        |
| 3.2. Учебно-методическое обеспечение .....  | 27        |
| <b>4. Контроль и оценка результатов освоения профессионального модуля .....</b>       | <b>28</b> |

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ»

## 1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «эксплуатация автоматизированных (информационных) систем в защищенном исполнении».

Профессиональный модуль включен в обязательную часть профессионального цикла образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

## 1.2. Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ОПОП-П).

В результате освоения профессионального модуля обучающийся должен:

| Код ОК, ПК | Уметь   | Знать  | Владеть навыками   |
|------------|---|--|--|
| ОК.05      | <ul style="list-style-type: none"> <li>– грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке</li> <li>– проявлять толерантность в рабочем коллективе</li> </ul>  | <ul style="list-style-type: none"> <li>– правила оформления документов</li> <li>– правила построения устных сообщений</li> <li>– особенности социального и культурного контекста</li> </ul>  |  |
| ПК 1.1.    | <ul style="list-style-type: none"> <li>– Выполнять конфигурирование</li> <li>– Настраивать автоматизированные системы в защищенном исполнении</li> <li>– Производить компонент систем защиты информации автоматизированных систем</li> </ul>  | <ul style="list-style-type: none"> <li>– Состав и принципы работы автоматизированных систем, операционных систем и сред</li> <li>– Принципы разработки алгоритмов программ, основных приемов программирования Модели баз данных</li> <li>– Принципы построения, физические основы работы периферийных устройств</li> </ul> | <ul style="list-style-type: none"> <li>– Устанавливать компоненты системы защиты информации автоматизированных (информационных) систем</li> <li>– Настраивать компоненты системы защиты информации автоматизированных (информационных) систем</li> </ul> |
| ПК 1.2.    | <ul style="list-style-type: none"> <li>– Организовывать, конфигурировать, производить монтаж диагностику и устранять неисправности КС</li> <li>– Работать с сетевыми протоколами разных уровней</li> <li>– Осуществлять конфигурирование</li> <li>– Выполнять настройку компонент систем защиты информации автоматизированных систем</li> <li>– Производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации АС</li> </ul> | <ul style="list-style-type: none"> <li>– Теоретические основы компьютерных сетей и их аппаратных</li> <li>– Сетевых моделей</li> <li>– Протоколов и принципов адресации</li> </ul>   | <ul style="list-style-type: none"> <li>– Администрировать автоматизированные система в защищенном исполнении</li> </ul>  |

|         |  |  |   |
|---------|--|--|---|
| ПК 1.3. | <ul style="list-style-type: none"> <li>– Настраивать неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным Правилам</li> <li>– Устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным Правилам</li> </ul> | <ul style="list-style-type: none"> <li>– Порядок установки средств защиты информации в компьютерных сетях</li> <li>– Ввод в эксплуатацию средств защиты информации в компьютерных сетях</li> </ul>           | <ul style="list-style-type: none"> <li>– Выполнять эксплуатацию компонентов систем защиты информации автоматизированных систем</li> </ul>   |
| ПК 1.4. | <ul style="list-style-type: none"> <li>– Обеспечивать работоспособность</li> <li>– Обнаруживать неисправности</li> <li>– Устранять неисправности</li> </ul>  | <ul style="list-style-type: none"> <li>– Принципы основных методов организации</li> <li>– Проведения технического обслуживания вычислительной техники и других технических средств информатизации</li> </ul> | <ul style="list-style-type: none"> <li>– Выполнять диагностику компонентов систем защиты информации автоматизированных систем</li> <li>– Устранять отказы работоспособности автоматизированных (информационных) систем в защищенном исполнении</li> <li>– Восстанавливать работоспособности автоматизированных (информационных) систем в защищенном исполнении</li> </ul> |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.1. Трудоемкость освоения модуля

| Наименование составных частей модуля   | Объем в часах | В т.ч. в форме практической подготовки |
|--|---------------|--|
| Учебные занятия                        | 424           | 316                                    |
| Курсовая работа (проект)               | -             | -                                      |
| Самостоятельная работа                 | 36            |  |
| Практика, в т.ч.:                      | 204           | 204                                    |
| учебная                                | 84            | 84                                     |
| производственная                       | 120           | 120                                    |
| Промежуточная аттестация, в том числе: |               |  |
| МДК 01.01 в форме экзамена             | 6             |  |
| МДК 01.02. в форме экзамена            | 6             |  |
| МДК 01.04. в форме экзамена            | 6             |  |
| МДК 01.05. в форме экзамена            | 6             |  |
| ПМ 01                                  | 12            |  |
| Всего                                  | <b>700</b>    | <b>528</b>                             |

### 2.2. Структура профессионального модуля

| Код ОК, ПК  | Наименования разделов профессионального модуля  | Всего, час. | В т.ч. в форме практической подготовки | Обучение по МДК, в т.ч.: | Учебные занятия | Курсовая работа (проект) | Самостоятельная работа | Промежуточная аттестация | Учебная практика | Производственная практика |
|---|---|-------------|--|--------------------------|-----------------|--------------------------|------------------------|--------------------------|------------------|---------------------------|
| 1   | 2   | 3           | 4                                      | 5                        | 6               | 7                        | 8                      |                          | 9                | 10                        |
| ОК 05; ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4. ПК 1.5 | <b>Раздел 1</b> Операционные системы  | <b>130</b>  | <b>80</b>                              | <b>130</b>               | 116             | -                        | 8                      | 6                        |                  |                           |
| ОК 05; ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4. ПК 1.5 | <b>Раздел 2</b> Базы данных   | <b>82</b>   | <b>48</b>                              | <b>82</b>                | 68              | -                        | 8                      | 6                        |                  |                           |
| ОК 05; ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4. ПК 1.5 | <b>Раздел 3</b> Сети и системы передачи информации  | <b>72</b>   | <b>48</b>                              | <b>72</b>                | 64              | -                        | 8                      |                          |                  |                           |
| ОК 05; ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4. ПК 1.5 | <b>Раздел 4</b> Эксплуатация автоматизированных (информационных) систем в защищенном исполнении | <b>100</b>  | <b>70</b>                              | <b>100</b>               | 88              | -                        | 6                      | 6                        |                  |                           |
| ОК 05; ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4. ПК 1.5 | <b>Раздел 5</b> Эксплуатация компьютерных сетей   | <b>100</b>  | <b>70</b>                              | <b>100</b>               | 88              | -                        | 6                      | 6                        |                  |                           |
|   | Учебная практика  | <b>84</b>   | <b>84</b>                              |                          |                 |                          |                        |                          | <b>84</b>        |                           |
|   | Производственная практика   | <b>120</b>  | <b>120</b>                             |                          |                 |                          |                        |                          |                  | <b>120</b>                |
|   | Промежуточная аттестация  | <b>12</b>   |  |                          |                 |                          |                        | <i>12</i>                |                  |                           |
|   | <b>Всего:</b>   | <b>700</b>  | <b>528</b>                             | <b>484</b>               | <b>424</b>      | <b>-</b>                 | <b>36</b>              | <b>36</b>                | <b>84</b>        | <b>120</b>                |

### 2.3. Содержание профессионального модуля

| Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК) | Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)                                    | Объем, акад. ч / в том числе в форме практической подготовки, акад. ч | Код ПК, ОК                                 |
|---|--|---|--|
| 1   | 2  | 3   | 4  |
| <b>Раздел 1 модуля. Операционные системы</b>  |  | <b>130/80</b>   |  |
| <b>МДК.01.01</b>  |  | <b>130/80</b>   |  |
| <b>Тема 1.1. Основы теории операционных систем</b>  | <b>Содержание</b>  | <b>8</b>  | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Определение операционной системы. Основные понятия. История развития операционных систем.  | 2   |  |
|   | Виды операционных систем. Классификация операционных систем по разным признакам. Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. | 2   |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>2</b>  |  |
|   | Исследование процесса загрузки ОС  | 2   |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Исследования в области операционных систем  | 2   |  |
| <b>Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем</b>     | <b>Содержание</b>  | <b>16</b>   | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС.   | 2   |  |
|   | Переносимость ОС. Машинно-зависимые модули ОС  |   |  |
|   | Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода.   | 2   |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>12</b>   |  |
|   | Виртуальные машины. Создание, модификация, работа  | 2   |  |
|   | Установка ОС   | 2   |  |
|   | Создание и изучение структуры разделов жесткого диска  | 2   |  |
|   | Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов   | 2   |  |
| <b>Тема 1.3. Модульная структура операционных систем, пространство пользователя</b>       | Файловые операции, контроль доступа к файлам   | 4   |  |
|   | <b>Содержание</b>  | <b>8</b>  | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Экзодро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.   | 2   |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>6</b>  |  |
|   | Настройка параметров рабочей среды пользователя  | 2   |  |

|  |   |           |  |
|--|---|-----------|--|
|  | Изучение основных команд для работы с файловой системой в консольном режиме                                     | 4         |  |
| <b>Тема 1.4.</b> Управление памятью  | <b>Содержание</b>   | <b>6</b>  |  |
|  | Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц                          | 2         | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>4</b>  |  |
|  | Мониторинг за использованием памяти   | 2         |  |
|  | Разработка систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти                     | 2         |  |
| <b>Тема 1.5.</b> Управление процессами, многопроцессорные системы              | <b>Содержание</b>   | <b>10</b> |  |
|  | Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. | 2         | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Межпроцессорное взаимодействие Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок                  | 2         |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>6</b>  |  |
|  | Управление процессами   | 2         |  |
|  | Наблюдение за использованием ресурсов системы   | 2         |  |
|  | Избегание взаимоблокировок. Предотвращение взаимоблокировок   | 2         |  |
| <b>Тема 1.6.</b> Виртуализация и облачные технологии                           | <b>Содержание</b>   | <b>15</b> |  |
|  | Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации                      | 2         | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства  | 2         |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>10</b> |  |
|  | Установка и настройка сетевых параметров VMware Workstation   | 2         |  |
|  | Создание и настройка виртуальной машины в VMware Workstation. Изменение конфигурации виртуально машины          | 2         |  |
|  | Установка, настройка и запуск Oracle VirtualBox   | 2         |  |
|  | Установка и запуск гостевой ОС в VM Oracle VirtualBox   | 2         |  |
|  | Использование облачных технологий. Преимущества использования облаков   | 2         |  |
|  | <b>В том числе самостоятельная работа обучающихся</b>   | <b>1</b>  |  |
|  | Создание виртуальной машины. Исследования в области виртуализации и облаков                                     |           |  |
| <b>Тема 1.7.</b> Принципы построения защиты информации в операционных системах | <b>Содержание</b>   | <b>19</b> |  |
|  | Понятие безопасности ОС. Классификация угроз ОС   | 2         | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Источники угроз информационной безопасности и объекты воздействия   | 2         |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>14</b> |  |
|  | Управление учетными записями пользователей и доступом к ресурсам  | 2         |  |



|  |   |           |  |
|--|---|-----------|--|
|  | Изучение способов аутентификации пользователей в ОС Windows. Настройка ОС Windows для реализации политики парольной защиты    | 2         |  |
|  | Планирование и настройка политики аудита ресурсов и событий в ОС Windows  | 2         |  |
|  | Управление журналом безопасности  | 2         |  |
|  | Изучение штатных средств защиты информации в операционных системах  | 2         |  |
|  | Архивация и восстановление данных   | 2         |  |
|  | Установка и настройка антивирусных программ. Изучение принципов диагностики антивирусной защиты                               | 2         |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Анализ журнала аудита ОС   | 1         |  |
| <b>Тема 1.8.</b> Операционные системы UNIX, Linux и MacOS, Android | <b>Содержание</b>   | <b>22</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX. | 2         |  |
|  | Операционные системы отечественных компаний: Astra Linux, Ред ОС  | 2         |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>16</b> |  |
|  | Настройка пользовательского интерфейса РЕД ОС   | 2         |  |
|  | Реализация системных настроек РЕД ОС  | 2         |  |
|  | Работа с папками и файлами, средствами мультимедиа и коммуникациями в РЕД ОС  | 2         |  |
|  | Работа в CLI ОС Linux   | 2         |  |
|  | Разграничение прав доступа  | 2         |  |
|  | Обеспечение целостности и доступности данных  | 4         |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Анализ возможностей отечественных операционных систем                | 2         |  |
| <b>Тема 1.9.</b> Операционная система Windows                      | <b>Содержание</b>   | <b>4</b>  | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.                                     | 2         |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>2</b>  |  |
|  | Установка и первичная настройка Windows.  | 2         |  |
| <b>Тема 1.10.</b> Серверные операционные системы                   | <b>Содержание</b>   | <b>12</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.                                  | 2         |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>8</b>  |  |
|  | Работа с сетевой файловой системой.   | 4         |  |
|  | Работа с серверной ОС, например, AltLinux.  | 4         |  |

|  |   |              |  |
|--|---|--------------|--|
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Изучение аналитических обзоров в области построения систем безопасности операционных систем  | 2            |  |
| <b>Обобщение тем МДК</b>   |   | <b>4</b>     |  |
| <b>Промежуточная аттестация по МДК.01.01</b>                                     |   | <b>6</b>     |  |
| <b>Раздел 2. Базы данных</b>   |   | <b>82/48</b> |  |
| <b>МДК.01.02 Базы данных</b>   |   | <b>82/48</b> |  |
| <b>Тема 2.1.</b> Основные понятия теории баз данных. Модели данных               | <b>Содержание</b>   | <b>2</b>     |  |
|  | Понятие базы данных. Компоненты системы БД: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. | 1            | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Модели данных. Иерархические, сетевые и реляционные модели организации данных. Терминология реляционных моделей. Классификация сущностей.   |              |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Централизованное управление данными, основные требования. Постреляционные модели данных. Двенадцать правил Кодда для определения концепции реляционной модели.                           | 1            |  |
| <b>Тема 2.2.</b> Основы реляционной алгебры                                      | <b>Содержание</b>   | <b>3</b>     |  |
|  | Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.   | 1            | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>2</b>     |  |
|  | Традиционные операции над отношениями   | 2            |  |
|  | Специальные операции над отношениями  |              |  |
| <b>Тема 2.3.</b> Базовые понятия и классификация систем управления базами данных | <b>Содержание</b>   | <b>1</b>     |  |
|  | Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД.  | 1            | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Знакомство с СУБД SQL Server Management Studio  |              |  |
| <b>Тема 2.4.</b><br>Целостность данных как ключевое понятие баз данных           | <b>Содержание</b>   | <b>2</b>     |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.   | 2            | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
| <b>Тема 2.5.</b><br>Информационные   | <b>Содержание</b>   | <b>3</b>     |  |
|  | Типы информационных моделей. Логические модели данных. Физические модели данных.  | 1            | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.           |

|   |   |          |  |
|---|---|----------|--|
| модели реляционных баз данных   | <b>В том числе практических занятий и лабораторных работ</b>  | <b>2</b> | ПК 1.4                                     |
|   | Проектирование инфологической модели данных   | 2        |  |
| <b>Тема 2.6.</b> Нормализация таблиц реляционной базы данных.<br>Проектирование связей между таблицами. | <b>Содержание</b>   | <b>7</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам.   | 1        |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>  | <b>4</b> |  |
|   | Проектирование структуры базы данных  | 2        |  |
|   | Приведение таблицы к первой, второй и третьей нормальным формам.  | 2        |  |
|   | <b>В том числе самостоятельная работа обучающихся</b>   |          |  |
|   | Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.   | 2        |  |
| <b>Тема 2.7.</b> Средства автоматизации проектирования  | <b>Содержание</b>   | <b>7</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML.   | 1        |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>  | <b>6</b> |  |
|   | Проектирование базы данных с использованием CASE-средств – диаграмма сущность-связь   | 2        |  |
|   | Проектирование диаграммы потоков данных   | 2        |  |
|   | Проектирование диаграммы прецедентов использования.   | 2        |  |
| <b>Тема 2.8.</b> Создание базы данных.<br>Манипулирование данными.                                      | <b>Содержание</b>   | <b>4</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными. Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных: восстановление и сжатие. Команды хранения, добавления, редактирования, удаления и восстановления данных. | 1        |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>  | <b>2</b> |  |
|   | Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.   | 2        |  |
|   | <b>В том числе самостоятельная работа обучающихся</b>   |          |  |
|   | Открытие и модификация данных. Навигация по набору данных.  | 1        |  |
| <b>Тема 2.9.</b> Индексы.<br>Связи между таблицами.<br>Объединение таблиц                               | <b>Содержание</b>   | <b>5</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.  | 1        |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>  | <b>4</b> |  |
|   | Создание взаимосвязей   | 2        |  |

|  |   |          |  |
|--|---|----------|--|
|  | Сортировка, поиск и фильтрация данных<br>Способы объединения таблиц   | 2        |  |
| <b>Тема 2.10.</b><br>Структурированный<br>язык запросов SQL        | <b>Содержание</b>   | <b>3</b> |  |
|  | Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.  | 1        | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>2</b> |  |
|  | Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL   | 2        |  |
| <b>Тема 2.11.</b> Операторы и<br>функции языка SQL                 | <b>Содержание</b>   | <b>7</b> |  |
|  | Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.   | 1        | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>6</b> |  |
|  | Создание и использование запросов   | 2        |  |
|  | Группировка и агрегирование данных  |          |  |
|  | Коррелированные вложенные запросы   | 2        |  |
|  | Создание в запросах вычисляемых полей. Использование условий  | 2        |  |
| <b>Тема 2.12.</b><br>Архитектуры<br>распределенных баз<br>данных   | <b>Содержание</b>   | <b>4</b> |  |
|  | Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных. | 1        | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>2</b> |  |
|  | Управление доступом к объектам базы данных  | 2        |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Отличия и преимущества удаленных баз данных от локальных баз данных. Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.  | 1        |  |
|  |   |          |  |
| <b>Тема 2.13.</b> Серверная<br>часть распределенной<br>базы данных | <b>Содержание</b>   | <b>3</b> |  |
|  | Планирование и развёртывание СУБД для работы с клиентскими приложениями   | 1        | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>2</b> |  |
|  | Установка СУБД. Настройка компонентов СУБД.   | 2        |  |
|  | <b>Содержание</b>   | <b>7</b> |  |

|  |   |          |  |
|--|---|----------|--|
| <b>Тема 2.14.</b> Клиентская часть распределенной базы данных                            | Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация.  | 1        | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>6</b> |  |
|  | Создание форм. Создание отчетов   | 2        |  |
|  | Создание меню. Генерация, запуск.   | 2        |  |
|  | Профилирование запросов клиентских приложений.  | 2        |  |
| <b>Тема 2.15.</b><br>Обеспечение целостности, достоверности и непротиворечивости данных. | <b>Содержание</b>   | <b>5</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.   | 1        |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>4</b> |  |
|  | Разработка хранимых процедур  | 2        |  |
|  | Разработка триггеров. Создание представлений  | 2        |  |
| <b>Тема 2.16.</b> Перехват исключительных ситуаций и обработка ошибок                    | <b>Содержание</b>   | <b>2</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.  | 1        |  |
| <b>Тема 2.17.</b> Механизмы защиты информации в системах управления базами данных        | <b>Содержание</b>   | <b>3</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. | 1        |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>2</b> |  |
|  | Управление правами доступа к базам данных. Средства защиты информации в базах данных  | 2        |  |
| <b>Тема 2.18.</b> Копирование и перенос данных. Восстановление данных                    | <b>Содержание</b>   | <b>5</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями.  |          |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>4</b> |  |

|  |  |              |  |
|--|--|--------------|--|
|  | Аудит данных с помощью средств СУБД и триггеров  | 2            |  |
|  | Резервное копирование и восстановление баз данных  | 2            |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Автоматизация процессов копирования. Восстановление данных                | 1            |  |
| <b>Обобщение тем МДК</b>   |  | <b>4</b>     |  |
| <b>Промежуточная аттестация по МДК.01.02</b>                           |  | <b>6</b>     |  |
| <b>Раздел 3. Сети и системы передачи информации</b>                    |  | <b>72/48</b> |  |
| <b>МДК.01.03 Сети и системы передачи информации</b>                    |  | <b>72/48</b> |  |
| <b>Тема 3.1. Основные понятия и определения</b>                        | <b>Содержание</b>  | <b>12</b>    |  |
|  | Классификация систем связи. Сообщения и сигналы.   | 2            | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Виды электронных сигналов. Спектральное представление сигналов.  | 2            |  |
|  | Параметры сигналов. Объем и информационная емкость сигнала.  |              |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>8</b>     |  |
|  | Особенности распространения ЭМВ, применение ЭМВ  | 2            |  |
|  | Изучение и расчет параметров сигнала   | 2            |  |
|  | Изучение видов модуляции сигналов  | 4            |  |
| <b>Тема 3.2. Принципы передачи информации в сетях и системах связи</b> | <b>Содержание</b>  | <b>6</b>     |  |
|  | Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход.   | 2            | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.  |              |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>2</b>     |  |
|  | Изучение принципов построения телекоммуникационных сетей   | 2            |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Семиуровневая модель OSI  | 2            |  |
| <b>Тема 3.3. Типовые каналы передачи и их характеристики</b>           | <b>Содержание</b>  | <b>8</b>     |  |
|  | Канал передачи. Сетевой тракт, групповой канал передачи.   | 2            | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>4</b>     |  |
|  | Расчет пропускной способности канала связи   | 2            |  |
|  | Изучение аппаратуры цифровых плезиохронных систем передачи   | 2            |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Упрощенная схема организации канала                                       | 2            |  |
| <b>Тема 3.4. Архитектура и принципы работы</b>                         | <b>Содержание</b>  | <b>26</b>    |  |
|  | Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов | 2            | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.           |

|  |   |               |  |
|--|---|---------------|--|
| современных сетей передачи данных  | Протоколы и интерфейсы управления каналами и сетью передачи данных.   |               | ПК 1.4                                     |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>22</b>     |  |
|  | Изучение структуры стандартов   | 2             |  |
|  | Конфигурирование сетевого интерфейса рабочей станции  | 2             |  |
|  | Маршрутизация и управление потоками в сетях связи   | 2             |  |
|  | Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP   | 2             |  |
|  | Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне  | 2             |  |
|  | Диагностика и разрешение проблем сетевого уровня  | 4             |  |
|  | Диагностика и разрешение проблем протоколов транспортного уровня  | 4             |  |
|  | Диагностика и разрешение проблем протоколов прикладного уровня  | 4             |  |
|  | <b>В том числе самостоятельная работа обучающихся</b>   | 2             |  |
|  | Переадресация пакетов   |               |  |
| <b>Тема 3.5.</b> Беспроводные системы передачи данных  | <b>Содержание</b>   | <b>6</b>      |  |
|  | Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения   | 2             | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Основные элементы беспроводных сетей.. Технология WIMAX   |               |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>4</b>      |  |
|  | Изучение стандартов беспроводных сетей  | 2             |  |
|  | Настройка Wi-Fi маршрутизатора  | 2             |  |
| <b>Тема 3.6.</b> Сотовые и спутниковые системы   | <b>Содержание</b>   | <b>12</b>     |  |
|  | Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA.   | 2             | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Спутниковые системы передачи данных.  |               |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | <b>8</b>      |  |
|  | Устройства сотовой связи  | 4             |  |
|  | Устройства спутниковой связи  | 4             |  |
|  | <b>В том числе самостоятельная работа обучающихся</b>   | 2             |  |
|  | Современные беспроводные системы  |               |  |
| <b>Промежуточная аттестация по МДК.01.03 (дифзачет)</b>  |   | <b>2</b>      |  |
| <b>Раздел 4. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении</b> |   | <b>100/70</b> |  |
| <b>МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении</b> |   | <b>100/70</b> |  |
| <b>Тема 4.1.</b> Основы информационных систем как объекта защиты.                                | <b>Содержание</b>   | <b>8</b>      |  |
|  | Понятие автоматизированной (информационной) системы. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру | 1             | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |

|   |  |          |  |
|---|--|----------|--|
|   | использования информации, по сфере применения. Требования к АИС: гибкость, надежность, эффективность, безопасность.  |          |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>6</b> |  |
|   | Изучение процессов в АИС: ввод, обработка, вывод, обратная связь   | 2        |  |
|   | Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)   | 4        |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Примеры областей применения АИС. Основные особенности современных проектов АИС. Электронный документооборот   | 1        |  |
| <b>Тема 4.2.</b> Жизненный цикл автоматизированных систем                     | <b>Содержание</b>  | <b>8</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС. | 1        |  |
|   | Требования по защите сведений о создаваемой автоматизированной системе.  |          |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>6</b> |  |
|   | Изучение требований к автоматизированной системе в защищенном исполнении   | 2        |  |
|   | Задачи и этапы проектирования АС в защищенном исполнении   | 2        |  |
|   | Разработка технического задания на проектирование автоматизированной системы   | 2        |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Методологии проектирования. Организация работ, функции заказчиков и разработчиков. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении.                             | 1        |  |
|   |  |          |  |
| <b>Тема 4.3.</b> Угрозы безопасности информации в автоматизированных системах | <b>Содержание</b>  | <b>7</b> | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз.  | 1        |  |
|   | Методы оценки опасности угроз. Банк данных угроз безопасности информации   |          |  |
|   | Понятие уязвимости угрозы. Классификация уязвимостей.  |          |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>6</b> |  |
|   | Категорирование информационных ресурсов  | 2        |  |
|   | Анализ угроз безопасности информации. Построение модели угроз  | 4        |  |
|   | <b>Содержание</b>  | <b>5</b> |  |



|   |   |            |  |
|---|---|------------|--|
| Тема 4.4. Основные меры защиты информации в автоматизированных системах   | В том числе практических занятий и лабораторных работ   | 4          | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Изучение нормативно-правовой базы для определения мер защиты информации в автоматизированных информационных системах и требований к ним   | 4          |  |
|   | В том числе самостоятельная работа обучающихся<br>Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.  | 1          |  |
| Тема 4.5. Содержание и порядок эксплуатации АС в защищенном исполнении  | Содержание  | 10         | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Защита машинных носителей информации. Регистрация событий безопасности<br>Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения.   | 2          |  |
|   | Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных. Резервное копирование и восстановление данных.   |            |  |
|   | В том числе практических занятий и лабораторных работ   | 8          |  |
|   | Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации  | 2          |  |
|   | Идентификация и аутентификация субъектов доступа и объектов доступа.<br>Управление доступом субъектов доступа к объектам доступа.   | 2          |  |
|   | Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.   | 2          |  |
|   | Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ. Обнаружение (предотвращение) вторжений   | 2          |  |
|   | Тема 4.6. Защита информации в распределенных автоматизированных системах  | Содержание |  |
| Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем. |   | 1          |  |
| Тема 4.7. Особенности разработки информационных систем персональных данных  | Содержание  | 7          | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности. | 1          |  |
|   | В том числе практических занятий и лабораторных работ   | 6          |  |

|  |  |   |  |
|--|--|---|--|
|  | Требования по защите персональных данных, в соответствии с уровнем защищенности  | 2 |  |
|  | Определения уровня защищенности ИСПДн  | 2 |  |
|  | Выбор мер по обеспечению безопасности ПДн  | 2 |  |
| Тема 4.8. Особенности эксплуатации автоматизированных систем в защищенном исполнении.                                | Содержание   | 6 |  |
|  | Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.   | 1 | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.  |   |  |
|  | В том числе практических занятий и лабораторных работ  | 4 |  |
|  | Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.   | 2 |  |
|  | Мониторинг и аудит, выявление угроз информационной безопасности автоматизированных систем  | 2 |  |
|  | В том числе самостоятельная работа обучающихся<br>Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении   | 1 |  |
| Тема 4.9. Администрирование автоматизированных систем  | Содержание   | 5 |  |
|  | Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем.   | 1 | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | В том числе практических занятий и лабораторных работ  | 4 |  |
|  | Управление, тестирование и эксплуатация автоматизированных систем  | 2 |  |
|  | Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем  | 2 |  |
| Тема 4.10. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении | Содержание   | 1 |  |
|  | Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем. | 1 | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
| Тема 4.11. Защита от несанкционированного доступа к информации   | Содержание   | 7 |  |
|  | Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД.  | 1 | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Требования защищенности СВТ от НСД к информации  |   |  |

|   |  |           |  |
|---|--|-----------|--|
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>6</b>  |  |
|   | Организация работ по защите от НСД   | 2         |  |
|   | Классификация автоматизированных систем. Требования по защите информации от НСД для АС   | 2         |  |
|   | Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ                                  | 2         |  |
| <b>Тема 4.12. СЗИ от НСД</b>                  | <b>Содержание</b>  | <b>14</b> | ОК 05   ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления.   | 1         |  |
|   | Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.   |           |  |
|   | Обеспечение целостности информационной системы и информации  |           |  |
|   | Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности   |           |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>12</b> |  |
|   | Установка и настройка СЗИ от НСД   | 2         |  |
|   | Защита входа в систему (идентификация и аутентификация пользователей)  | 2         |  |
|   | Разграничение доступа к устройствам. Управление доступом. Управление грифами конфиденциальности.   | 2         |  |
|   | Управление доступом и контроль печати конфиденциальной информации. Настройка механизма полномочного управления доступом. Использование принтеров для печати конфиденциальных документов. Контроль печати | 2         |  |
|   | Настройка регистрации событий. Управление режимом потоков.   | 2         |  |
|   | Настройка системы для задач аудита.  | 2         |  |
|   | Настройка контроля целостности и замкнутой программной среды. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности   | 2         |  |
|   | <b>В том числе самостоятельная работа обучающихся</b>  | 1         |  |
|   | Общие принципы управления. Основные механизмы защиты. Правила работы с конфиденциальными ресурсами.  |           |  |
| <b>Тема 4.13. Эксплуатация средств защиты</b> | <b>Содержание</b>  | <b>8</b>  | ОК 05   ПК 1.1.<br>ПК 1.2. ПК 1.3.           |
|   | Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.   | 1         |  |

|  |  |               |  |
|--|--|---------------|--|
| информации в компьютерных сетях  | Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении   |               | ПК 1.4                                     |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>6</b>      |  |
|  | Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем   | 2             |  |
|  | Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам   | 4             |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации   | 1             |  |
| <b>Тема 4.14.</b><br>Документация на защищаемую автоматизированную систему | <b>Содержание</b>  | <b>3</b>      | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему. | 1             |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>2</b>      |  |
|  | Оформление основных эксплуатационных документов на автоматизированную систему  | 2             |  |
| <b>Обобщение разделов (консультация)</b>                                   |  | <b>4</b>      |  |
| <b>Промежуточная аттестация по МДК.01.04 экзамен</b>                       |  | <b>6</b>      |  |
| <b>Раздел 5 Эксплуатация компьютерных сетей</b>                            |  | <b>100/70</b> |  |
| <b>МДК.01.05. Эксплуатация компьютерных сетей</b>                          |  | <b>100/70</b> |  |
| <b>Тема 5.1.</b><br>Модели сетевого взаимодействия                         | <b>Содержание</b>  | <b>3</b>      | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.  | 1             |  |
|  | Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.   |               |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>2</b>      |  |
|  | Изучение элементов кабельной системы.  | 2             |  |
| <b>Тема 5.2.</b><br>Физический уровень модели OSI                          | <b>Содержание</b>  | <b>4</b>      | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Понятие линии и канала связи. Сигналы. Основные характеристики канала связи. Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.  | 1             |  |
|  | Стандарты кабелей. Электрическая проводка. Оптоволоконные линии связи  |               |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>2</b>      |  |

|  |   |    |  |
|--|---|----|--|
|  | Создание сетевого кабеля на основе неэкранированной витой пары (UTP)  | 2  |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Беспроводная среда передачи                                      | 1  |  |
| <b>Тема 5.3.</b><br>Топология компьютерных сетей | <b>Содержание</b>   | 7  | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Понятие топологии сети. Обзор сетевых топологий.  | 1  |  |
|  | Сетевое оборудование в топологии.   |    |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | 6  |  |
|  | Построение одноранговой сети  | 2  |  |
|  | Разработка топологии сети небольшого предприятия  | 4  |  |
| <b>Тема 5.4.</b><br>Технологии Ethernet          | <b>Содержание</b>   | 3  | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Обзор технологий построения локальных сетей. Технология Ethernet.   | 1  |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | 2  |  |
|  | Изучение адресации канального уровня. MAC-адреса.   | 2  |  |
| <b>Тема 5.5.</b> Технологии коммутации           | <b>Содержание</b>   | 4  | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI. Конструктивное исполнение коммутаторов | 1  |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | 2  |  |
|  | Создание коммутируемой сети   | 2  |  |
|  | <b>В том числе самостоятельная работа обучающихся</b>   | 1  |  |
|  | Программное обеспечение коммутаторов. Общие принципы сетевого дизайна   |    |  |
| <b>Тема 5.6.</b> Сетевой протокол IPv4           | <b>Содержание</b>   | 10 |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | 10 |  |
|  | Изучение IP-адресации. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.         | 2  |  |
|  | Поиск ошибок адресации в IP-сетях   | 2  |  |
|  | Формирование подсетей с использованием масок переменной длины   | 2  |  |
|  | Маршрутизация пакетов IPv4. Изучение протоколов статической и динамической маршрутизации                                  | 4  |  |
|  |   |    |  |
| <b>Тема 5.7.</b> Скоростные и беспроводные сети  | <b>Содержание</b>   | 5  | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Сеть FDDI. Сеть 100VG-AnyLAN. Сверхвысокоскоростные сети. Беспроводные сети   | 1  |  |
|  | <b>В том числе практических занятий и лабораторных работ</b>  | 4  |  |
|  | Настройка беспроводного сетевого оборудования   | 4  |  |

|  |  |   |  |
|--|--|---|--|
| Тема 5.8. Основы коммутации                                  | Содержание   | 5 | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах. | 1 |  |
|  | В том числе практических занятий и лабораторных работ  | 2 |  |
|  | Работа с основными командами коммутатора.  | 2 |  |
|  | В том числе самостоятельная работа обучающихся<br>Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов    | 2 |  |
| Тема 5.9. Начальная настройка коммутатора                    | Содержание   | 8 | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Средства управления коммутаторами. Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор.                                   | 1 |  |
|  | В том числе практических занятий и лабораторных работ  | 6 |  |
|  | Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора   | 2 |  |
|  | Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов.   | 2 |  |
|  | Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы   | 2 |  |
|  | В том числе самостоятельная работа обучающихся<br>Загрузка и резервное копирование конфигурации коммутатора.   | 1 |  |
|  |  |   |  |
| Тема 5.10. Виртуальные локальные сети (VLAN)                 | Содержание   | 7 | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.  | 1 |  |
|  | В том числе практических занятий и лабораторных работ  | 6 |  |
|  | Настройка VLAN на основе стандарта IEEE 802.1Q.  | 2 |  |
|  | Настройка протокола GVRP.  | 2 |  |
|  | Настройка сегментации трафика без использования VLAN.  | 2 |  |
|  |  |   |  |
| Тема 5.11. Функции повышения надежности и производительности | Содержание   | 5 | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.   | 1 |  |
|  | Дополнительные функции защиты от петель. Агрегирование каналов связи.  |   |  |
|  | В том числе практических занятий и лабораторных работ  | 4 |  |
|  | Настройка протоколов связующего дерева STP, RSTP, MSTP.  | 2 |  |
|  | Настройка функции защиты от образования петель LoopBackDetection. Агрегирование каналов.   | 2 |  |
| Тема 5.12. Адресация сетевого уровня и маршрутизация         | Содержание   | 9 | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.           |
|  | Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса.   | 1 |  |

|  |  |          |  |
|--|--|----------|--|
|  | Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP. Протокол NDP.   |          | ПК 1.4                                     |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>8</b> |  |
|  | Основные и расширенные конфигурации маршрутизатора.  | 2        |  |
|  | Работа с протоколом CDP. Работа с протоколом TELNET. Работа с протоколом TFTP.   | 2        |  |
|  | Работа с протоколом RIP и OSPF.  | 2        |  |
|  | Конфигурирование функции маршрутизатора NAT/PAT. Конфигурирование PPP и CHAP.  | 2        |  |
| <b>Тема 5.13.</b><br>Качество обслуживания (QoS)                                   | <b>Содержание</b>  | <b>3</b> |  |
|  | Модели QoS. Приоритезация пакетов. Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок.  | 1        | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>2</b> |  |
|  | Настройка QoS. Приоритезация трафика. Управление полосой пропускания   | 2        |  |
| <b>Тема 5.14.</b><br>Функции обеспечения безопасности и ограничения доступа к сети | <b>Содержание</b>  | <b>5</b> |  |
|  | Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.  | 1        | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>4</b> |  |
|  | Списки управления доступом (AccessControlList). Контроль над подключением узлов к портам коммутатора. Функция PortSecurity.  | 2        |  |
|  | Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding  | 2        |  |
| <b>Тема 5.15.</b><br>Многоадресная рассылка  | <b>Содержание</b>  | <b>3</b> |  |
|  | Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.  | 1        | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>2</b> |  |
|  | Отслеживание трафика многоадресной рассылки. Отслеживание трафика Multicast.   | 2        |  |
| <b>Тема 5.16.</b><br>Функции управления коммутаторами                              | <b>Содержание</b>  | <b>3</b> |  |
|  | Управление множеством коммутаторов. Протокол SNMP. RMON (Remote Monitoring). Функция Port Mirroring.   | 1        | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|  | <b>В том числе практических занятий и лабораторных работ</b>   | <b>2</b> |  |
|  | Функции анализа сетевого трафика. Настройка протокола управления топологией сети LLDP.   | 2        |  |
| <b>Тема 5.17.</b><br>Основные принципы создания надежной и                         | <b>Содержание</b>  | <b>1</b> |  |
|  | Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры. Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности | 1        | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |

|   |  |           |  |
|---|--|-----------|--|
| безопасной ИТ-инфраструктуры  |  |           |  |
| <b>Тема 5.18.</b><br>Межсетевые экраны  | <b>Содержание</b>  | <b>4</b>  |  |
|   | Технологии межсетевых экранов. Политика межсетевого экрана.  | 1         | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Межсетевые экраны с возможностями NAT.   |           |  |
|   | Топология сети при использовании межсетевых экранов.   |           |  |
|   | Планирование и внедрение межсетевого экрана.   |           |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>2</b>  |  |
|   | Основы администрирования межсетевого экрана. Создание политик для традиционного (или исходящего) NAT.  | 2         |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Соединение двух локальных сетей межсетевыми экранами. Создание политики без проверки состояния. | <b>1</b>  |  |
| <b>Тема 5.19.</b><br>Системы обнаружения и предотвращения проникновений   | <b>Содержание</b>  | <b>5</b>  |  |
|   | Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS.  | 1         | ОК 05 ПК 1.1.<br>ПК 1.2. ПК 1.3.<br>ПК 1.4 |
|   | Дополнительные инструментальные средства.  |           |  |
|   | Требования организации к функционированию IDPS. Развертывание IDPS.  |           |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>4</b>  |  |
|   | Обнаружение и предотвращение вторжений.  | 2         |  |
|   | Возможности IDPS. Сильные стороны и ограниченность IDPS.   | 2         |  |
| <b>Тема 5.20.</b><br>Приоритизация трафика и создание альтернативных маршрутов  | <b>Содержание</b>  | <b>2</b>  |  |
|   | <b>В том числе практических занятий и лабораторных работ</b>   | <b>2</b>  |  |
|   | Создание альтернативных маршрутов с использованием статической маршрутизации   | 2         |  |
| <b>Обобщение разделов МДК.01.05</b>   |  | <b>4</b>  |  |
| <b>Промежуточная аттестация по МДК.01.05</b>  |  | <b>6</b>  |  |
| <ul style="list-style-type: none"> <li>– <b>Учебная практика</b></li> <li>– <b>Виды работ:</b></li> <li>– установка программного обеспечения в соответствии с технической документацией.</li> <li>– настройка параметров работы программного обеспечения, включая системы управления базами данных.</li> <li>– настройка компонентов подсистем защиты информации операционных систем.</li> <li>– управление учетными записями пользователей.</li> <li>– работа в операционных системах с соблюдением действующих требований по защите информации.</li> <li>– установка обновления программного обеспечения.</li> <li>– контроль целостность подсистем защиты информации операционных систем.</li> </ul> |  | <b>84</b> |  |



|   |            |  |
|---|------------|--|
| <ul style="list-style-type: none"> <li>– выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных</li> <li>– использование программных средств для архивирования информации.</li> <li>– проведение аудита защищенности автоматизированной системы.</li> <li>– установка, настройка и эксплуатация сетевых операционных систем.</li> <li>– диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.</li> <li>– организация работ с удаленными хранилищами данных и базами данных.</li> <li>– организация защищенной передачи данных в компьютерных сетях.</li> <li>– выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.</li> <li>– осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.</li> <li>– заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.</li> </ul>  |            |  |
| <p><b>Производственная практика</b><br/> <b>Виды работ:</b></p> <ul style="list-style-type: none"> <li>– участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации</li> <li>– обслуживание средств защиты информации прикладного и системного программного обеспечения</li> <li>– настройка программного обеспечения с соблюдением требований по защите информации</li> <li>– настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам</li> <li>– настройка встроенных средств защиты информации программного обеспечения</li> <li>– проверка функционирования встроенных средств защиты информации программного обеспечения</li> <li>– своевременное обнаружение признаков наличия вредоносного программного обеспечения</li> <li>– обслуживание средств защиты информации в компьютерных системах и сетях</li> <li>– обслуживание систем защиты информации в автоматизированных системах</li> <li>– участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем</li> <li>– проверка работоспособности системы защиты информации автоматизированной системы</li> <li>– контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации</li> <li>– контроль стабильности характеристик системы защиты информации автоматизированной системы</li> <li>– ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем</li> <li>– участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем</li> </ul> | <b>120</b> |  |
| <b>Экзамен по профессиональному модулю</b>  | <b>12</b>  |  |

|              |                |  |
|--------------|----------------|--|
| <i>Всего</i> | <b>700/528</b> |  |
|--------------|----------------|--|

**2.4. Курсовая работа.** Выполнение курсовой работы не предусмотрено

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

#### **3.1. Материально-техническое обеспечение**

Мастерская «Кибербезопасности», оснащена в соответствии с приложением 3 ОПОП-П. и с п. 3.1.2. образовательной программы

Базы практики (мастерские) оснащены в соответствии с приложением 3 ОПОП-П.

#### **3.2. Учебно-методическое обеспечение**

##### **3.2.1. Основные печатные и/или электронные издания**

1. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2018.

2. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2019

3. Заяц, А. М. Организация беспроводных Ad Hoc и Hot Spot сетей в среде ОС Windows : учебное пособие для спо / А. М. Заяц, С. П. Хабаров. — Санкт-Петербург : Лань, 2021. — 220 с. — ISBN 978-5-8114-6974-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/153938> — Режим доступа: для авториз. пользователей.

4. Кутузов, О. И. Инфокоммуникационные системы и сети : учебник для спо / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 244 с. — ISBN 978-5-8114-8488-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/176902> — Режим доступа: для авториз. пользователей.

5. Соснин, П. И. Архитектурное моделирование автоматизированных систем : учебник для спо / П. И. Соснин. — 3-е изд., стер. — Санкт-Петербург : Лань, 2023. — 180 с. — ISBN 978-5-507-46075-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/297017> — Режим доступа: для авториз. пользователей.

6. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для спо / А. Г. Уймин. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 480 с. — ISBN 978-5-8114-9255-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/189420> — Режим доступа: для авториз. пользователей.

#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

| Код ПК, ОК  | Критерии оценки результата<br>(показатели освоенности компетенций)   | Формы контроля и методы оценки  |
|---|--|---|
| ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.                                     | Демонстрирует умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации  | 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 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.  | Проявляет умения и практический опыт администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении   | 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 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.   | Проводит перечень работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации   | 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 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении. | Проявляет знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении | 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 |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.  | Грамотно владеет устной и письменной речью<br>Ясно формулирует и излагает мысли  |   |

**Приложение 1.2**  
**к ОПОП-П по специальности**

**10.02.05 Обеспечение информационной безопасности автоматизированных систем**

**Рабочая программа профессионального модуля**  
**«ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ**  
**ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ»**

2025 г.

## СОДЕРЖАНИЕ

|  |           |
|--|-----------|
| <b>1. Общая характеристика.....</b>  | <b>31</b> |
| <i>1.1. Цель и место профессионального модуля в структуре образовательной программы.....</i> | <i>31</i> |
| <i>1.2. Планируемые результаты освоения профессионального модуля.....</i>                    | <i>31</i> |
| <b>2. Структура и содержание профессионального модуля.....</b>                               | <b>33</b> |
| <i>2.1. Трудоемкость освоения модуля.....</i>  | <i>33</i> |
| <i>2.2. Структура профессионального модуля .....</i>   | <i>33</i> |
| <i>2.3. Содержание профессионального модуля .....</i>  | <i>34</i> |
| <i>2.4. Курсовая работа.....</i>   | <i>47</i> |
| <b>3. Условия реализации профессионального модуля .....</b>                                  | <b>48</b> |
| <i>3.1. Материально-техническое обеспечение .....</i>  | <i>48</i> |
| <i>3.2. Учебно-методическое обеспечение.....</i>   | <i>48</i> |
| <b>4. Контроль и оценка результатов освоения профессионального модуля .....</b>              | <b>49</b> |

## 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### «ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ»

#### 1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «защита информации в автоматизированных системах программными и программно-аппаратными средствами».

Профессиональный модуль включен в обязательную часть профессионального цикла образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

#### 1.2. Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ОПОП-П).

В результате освоения профессионального модуля обучающийся должен:

| Код ОК,<br>ПК | Уметь   | Знать  | Владеть навыками  |
|---------------|---|--|---|
| ОК 08         | <ul style="list-style-type: none"> <li>– использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей</li> <li>– применять рациональные приемы двигательных функций в профессиональной деятельности</li> <li>– пользоваться средствами профилактики перенапряжения, характерными для данной специальности</li> </ul> | <ul style="list-style-type: none"> <li>– роль физической культуры в общекультурном, профессиональном и социальном развитии человека</li> <li>– основы здорового образа жизни</li> <li>– условия профессиональной деятельности и зоны риска физического здоровья для специальности</li> <li>– средства профилактики перенапряжения</li> </ul> |   |
| ПК 2.1.       | <ul style="list-style-type: none"> <li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации</li> </ul>  | <ul style="list-style-type: none"> <li>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, Компьютерных сетях, базах данных</li> </ul>   | <ul style="list-style-type: none"> <li>– выполнять установку, настройку программных средств защиты информации в автоматизированной</li> </ul>   |
| ПК 2.2.       | <ul style="list-style-type: none"> <li>– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями</li> <li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации</li> </ul>   | <ul style="list-style-type: none"> <li>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных</li> </ul>   | <ul style="list-style-type: none"> <li>– обеспечивать защиту автономных автоматизированных систем программными и программно-аппаратными средствами</li> <li>– использовать программные и программно-аппаратные средства для защиты информации в сети</li> </ul> |

|         |   |   |   |
|---------|---|---|---|
| ПК 2.3. | <ul style="list-style-type: none"> <li>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации</li> </ul>   | <ul style="list-style-type: none"> <li>– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации</li> </ul>   | <ul style="list-style-type: none"> <li>– тестировать функций, диагностировать работоспособности программных и программно-аппаратных средств защиты информации</li> <li>– устранять отказы и восстанавливать работоспособности программных и программно-аппаратных средств защиты информации</li> </ul>                      |
| ПК 2.4. | <ul style="list-style-type: none"> <li>– применять программные и программно-аппаратные средства для защиты информации в базах данных</li> <li>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации</li> <li>– применять математический аппарат для выполнения криптографических преобразований</li> <li>– использовать типовые программные криптографические средства, в том числе электронную подпись</li> </ul> | <ul style="list-style-type: none"> <li>– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных</li> <li>– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации</li> <li>– основные понятия криптографии и типовых криптографических методов и Средств защиты информации</li> </ul> | <ul style="list-style-type: none"> <li>– решать задачи защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации</li> <li>– применять электронную подпись, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных</li> </ul> |
| ПК 2.5. | <ul style="list-style-type: none"> <li>– применять средства гарантированного уничтожения информации</li> </ul>  | <ul style="list-style-type: none"> <li>– особенности и способы применения программных уничтожения информации</li> <li>– особенности и способы применения программно-аппаратных средств гарантированного уничтожения информации</li> </ul>   | <ul style="list-style-type: none"> <li>– учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности</li> </ul>  |
| ПК 2.6  | <ul style="list-style-type: none"> <li>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации</li> <li>– 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</li> </ul>   | <ul style="list-style-type: none"> <li>– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа</li> </ul>   | <ul style="list-style-type: none"> <li>– выполнять работу с подсистемами регистрации событий</li> <li>– выявлять события и инцидентов безопасности в автоматизированной системе</li> </ul>  |



## 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.1. Трудоемкость освоения модуля

| Наименование составных частей модуля   | Объем в часах | В т.ч. в форме практической подготовки |
|--|---------------|--|
| Учебные занятия, в т.ч.:               | 274           | 168                                    |
| Курсовая работа (проект)               | 20            |  |
| Самостоятельная работа                 | 32            |  |
| Практика, в т.ч.:                      | 204           | 204                                    |
| учебная                                | 48            | 48                                     |
| производственная                       | 156           | 156                                    |
| Промежуточная аттестация, в том числе: |               |  |
| Промежуточная аттестация МДК 01        | 6             |  |
| Промежуточная аттестация МДК 02        | 6             |  |
| <i>ПМ 02</i>                           | 12            |  |
| Всего                                  | <b>534</b>    | <b>372</b>                             |

### 2.2. Структура профессионального модуля

| Код ОК, ПК   | Наименования разделов профессионального модуля                                 | Всего, час. | В т.ч. в форме практической подготовки | Обучение по МДК, в т.ч.: | Учебные занятия | Курсовая работа (проект) | Самостоятельная работа | Промежуточная аттестация | Учебная практика | Производственная практика |
|--|--|-------------|--|--------------------------|-----------------|--------------------------|------------------------|--------------------------|------------------|---------------------------|
| 1  | 2  | 3           | 4                                      | 5                        | 6               | 7                        | 8                      |                          | 9                | 10                        |
| ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5 ПК 2.6 | <b>Раздел 1</b> Программные и программно-аппаратные средства защиты информации | <b>178</b>  | <b>98</b>                              | <b>178</b>               | 138             | 20                       | 14                     | 6                        |                  |                           |
| ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5 ПК 2.6 | <b>Раздел 2</b> Криптографические средства защиты информации                   | <b>140</b>  | <b>70</b>                              | <b>146</b>               | 116             |                          | 18                     | 6                        |                  |                           |
|  | Учебная практика   | <b>48</b>   | <b>48</b>                              |                          |                 |                          |                        |                          | <b>48</b>        |                           |
|  | Производственная практика  | <b>156</b>  | <b>156</b>                             |                          |                 |                          |                        |                          |                  | <b>156</b>                |
|  | Промежуточная аттестация   | <b>12</b>   |  |                          |                 |                          |                        |                          |                  |                           |
|  | <b>Всего:</b>  | <b>554</b>  | <b>372</b>                             | <b>344</b>               | <b>274</b>      | <b>20</b>                | <b>32</b>              | <b>12</b>                | <b>48</b>        | <b>156</b>                |

### 2.3. Содержание профессионального модуля

| Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК) | Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)   | Объем, акад. ч / в том числе в форме практической подготовки, акад. ч | Код ПК, ОК   |
|---|---|---|--|
| 1   | 2   |   |  |
| <b>Раздел 1 Программные и программно-аппаратные средства защиты информации</b>            |   | <b>178/98</b>   |  |
| <b>МДК.02.01. Программные и программно-аппаратные средства защиты информации</b>          |   | <b>178/98</b>   |  |
| <b>Тема 1.1.</b> Предмет и задачи программно-аппаратной защиты информации                 | <b>Содержание</b>   | <b>2</b>  |  |
|   | Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации. Классификация методов и средств программно-аппаратной защиты информации   | 2   | ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6. |
| <b>Тема 1.2.</b> Стандарты безопасности   | <b>Содержание</b>   | <b>5</b>  |  |
|   | Нормативные правовые акты, нормативные методические документы, в состав которых входят 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   | ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6. |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>2</b>  |  |
|   | Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами   | 1   |  |
|   | Работа с содержанием нормативных правовых актов   | 1   |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.   | <b>1</b>  |  |

|  |   |            |   |
|--|---|------------|---|
| Тема 1.3. Защищенная автоматизированная система  | Содержание  | 21         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Автоматизация процесса обработки информации. Понятие автоматизированной системы   | 2          |   |
|  | Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Дискреционные модели. Мандатные модели                       | 2          |   |
|  | В том числе практических и лабораторных занятий   | 16         |   |
|  | Учет, обработка, хранение и передача информации в АИС   | 2          |   |
|  | Ограничение доступа на вход в систему. Разграничение доступа  | 2          |   |
|  | Идентификация и аутентификация пользователей  | 2          |   |
|  | Регистрация событий (аудит)   | 2          |   |
|  | Контроль целостности данных. Уничтожение остаточной информации  | 2          |   |
|  | Управление политикой безопасности. Шаблоны безопасности   | 2          |   |
|  | Криптографическая защита  | 2          |   |
|  | Обзор программ шифрования данных  | 2          |   |
|  | В том числе самостоятельная работа обучающихся  | 1          |   |
|  | Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС  |            |   |
|  | Тема 1.4. Дестабилизирующее воздействие на объекты защиты   | Содержание |   |
| Источники дестабилизирующего воздействия на объекты защиты                                 |   | 2          |   |
| Способы воздействия на информацию  |   |            |   |
| В том числе практических и лабораторных занятий  |   | 2          |   |
| Распределение каналов в соответствии с источниками воздействия на информацию               |   | 2          |   |
| В том числе самостоятельная работа обучающихся   |   | 1          |   |
| Причины и условия дестабилизирующего воздействия на информацию                             |   |            |   |
| Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа | Содержание  | 11         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД  | 2          |   |
|  | Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса | 2          |   |

|  |  |           |   |
|--|--|-----------|---|
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b>  |   |
|  | Организация доступа к файлам   | 2         |   |
|  | Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД   | 4         |   |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Особенности защиты данных от изменения. Шифрование  | <b>1</b>  |   |
| <b>Тема 1.6</b> Основы защиты автономных автоматизированных систем | <b>Содержание</b>  | <b>5</b>  | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды | 2         |   |
|  | Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)   | 2         |   |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Применение закладок, направленных на снижение эффективности средств, замыкающих среду             | <b>1</b>  |   |
| <b>Тема 1.7</b> Защита программ от изучения                        | <b>Содержание</b>  | <b>4</b>  | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Изучение и обратное проектирование ПО. 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         |   |
| <b>Тема 1.8</b> Вредоносное программное обеспечение                | <b>Содержание</b>  | <b>11</b> | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения                       | 2         |   |
|  | Бот-нет. Принцип функционирования. Методы обнаружения. Классификация антивирусных средств. Сигнатурный и эвристический анализ                              | 2         |   |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>4</b>  |   |
|  | Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО   | 2         |   |
|  | Основные концепции построения систем антивирусной защиты на предприятии  | 2         |   |
|  | <b>В том числе самостоятельная работа обучающихся</b>  | <b>3</b>  |   |

|   |  |           |  |
|---|--|-----------|--|
|   | Вредоносное программное обеспечение как особый вид разрушающих воздействий. Поиск следов активности вредоносного ПО. Реестр Windows. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch. Основные ветки, содержащие информацию о вредоносном ПО. Защита от вирусов в «ручном режиме» |           |  |
| <b>Тема 1.9</b><br>Защита программ и данных от несанкционированного копирования | <b>Содержание</b>  | <b>9</b>  |  |
|   | Несанкционированное копирование программ как тип НСД. Привязка ПО к аппаратному окружению и носителям  | 2         | ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6. |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b>  |  |
|   | Требования по защите персональных данных, в соответствии с уровнем защищенности  | 2         |  |
|   | Защитные механизмы в приложениях (на примере MSWord, MSeXcel, MSPowerPoint)  | 2         |  |
|   | Защитные механизмы от копирования современных операционных систем  | 2         |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования  | <b>1</b>  |  |
| <b>Тема 1.10</b> Защита информации на машинных носителях                        | <b>Содержание</b>  | <b>15</b> |  |
|   | Проблема защиты отчуждаемых компонентов ПЭВМ.  | 2         | ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6. |
|   | Средства восстановления остаточной информации. Создание посекторных образов НЖМД. Безвозвратное удаление данных. Принципы и алгоритмы  | 2         |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>10</b> |  |
|   | Применение средства восстановления остаточной информации на примере Foremost или аналога   | 2         |  |
|   | Применение специализированного программного средства для восстановления удаленных файлов   | 2         |  |
|   | Методы защиты информации на отчуждаемых носителях. Шифрование  | 2         |  |
|   | Применение программ для безвозвратного удаления данных   | 2         |  |
|   | Применение программ для шифрования данных на съемных носителях   | 2         |  |
|   | <b>В том числе самостоятельная работа обучающихся</b>  | <b>1</b>  |  |

|  |   |           |   |
|--|---|-----------|---|
|  | Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов.<br>Нормативная база, документирование результатов |           |   |
| <b>Тема 1.11</b><br>Аппаратные средства идентификации и аутентификации пользователей | <b>Содержание</b>   | <b>4</b>  |   |
|  | Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ  | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Устройства Touch Memory   |           |   |
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>2</b>  |   |
|  | Установка и настройка Touch Memory  | 2         |   |
| <b>Тема 1.12.</b><br>Системы обнаружения атак и вторжений                            | <b>Содержание</b>   | <b>11</b> |   |
|  | СОВ и СОА, отличия в функциях. Основные архитектуры СОВ. Использование сетевых снифферов в качестве СОВ   | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Аппаратный компонент СОВ. Программный компонент СОВ. Модели системы обнаружения вторжений.  | 2         |   |
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>6</b>  |   |
|  | Классификация систем обнаружения вторжений  | 2         |   |
|  | Моделирование проведения атаки  | 2         |   |
|  | Изучение инструментальных средств обнаружения вторжений   | 2         |   |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.   | <b>1</b>  |   |
| <b>Тема 1.13</b><br>Основы построения защищенных сетей                               | <b>Содержание</b>   | <b>6</b>  |   |
|  | Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации  | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Штатные средства защиты информации стека протоколов TCP/IP  | 2         |   |
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>2</b>  |   |
|  | Анализ средств идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения  | 2         |   |
| <b>Тема 1.14</b><br>Средства организации VPN   | <b>Содержание</b>   | <b>10</b> |   |
|  | Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN   | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.            |
|  | Устройства, образующие VPN. Криptomаршрутизатор и криптофильтр.   | 2         |   |

|   |  |           |   |
|---|--|-----------|---|
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b>  | ПК 2.6.   |
|   | Крипторouter. Принципы, архитектура, модель нарушителя, достоинства и недостатки   | 2         |   |
|   | Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки   | 2         |   |
|   | Развертывание VPN  | 2         |   |
| <b>Тема 1.15</b><br>Обеспечение безопасности межсетевого взаимодействия | <b>Содержание</b>  | <b>13</b> | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|   | Методы защиты информации при работе в сетях общего доступа. Основные типы firewall. Симметричные и несимметричные firewall   | 2         |   |
|   | Уровень 1. Пакетные фильтры  | 2         |   |
|   | Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне  |           |   |
|   | Уровень 3. Прoxy-сервера прикладного уровня  |           |   |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>8</b>  |   |
|   | Анализ межсетевых экранов типа firewall. Достоинства, недостатки, реализуемые политики безопасности  | 2         |   |
|   | Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.   | 2         |   |
|   | Изучение различных способов закрытия «опасных» портов  | 2         |   |
|   | Изучение требований по сертификации межсетевых экранов   | 2         |   |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций. | <b>1</b>  |   |
|   |  |           |   |
| <b>Тема 1.16</b><br>Защита информации в базах данных                    | <b>Содержание</b>  | <b>9</b>  | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|   | Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом. Средства контроля целостности информации в базах данных  | 2         |   |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b>  |   |
|   | Изучение механизмов защиты СУБД MS Access  | 2         |   |
|   | Изучение штатных средств защиты СУБД MSSQL Server  | 2         |   |
|   | Изучение механизмов защиты современных СУБД  | 2         |   |
|   | <b>В том числе самостоятельная работа обучающихся</b>  | <b>1</b>  |   |

|  |  |           |   |
|--|--|-----------|---|
|  | Средства аудита и контроля безопасности. Критерии защищенности баз данных. Применение криптографических средств защиты информации в базах данных   |           |   |
| <b>Тема 1.17</b><br>Мониторинг систем защиты                                 | <b>Содержание</b>  | <b>13</b> |   |
|  | Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25   | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов. Системы управления событиями информационной безопасности (SIEM) | 2         |   |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>8</b>  |   |
|  | Классификация отслеживаемых событий. Особенности построения систем мониторинга   | 2         |   |
|  | Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов   | 2         |   |
|  | Проведение аудита ЛВС сетевым сканером   | 2         |   |
|  | Обзор SIEM-систем на мировом и российском рынке  | 2         |   |
|  | <b>В том числе самостоятельная работа обучающихся</b>  |           |   |
|  | Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации   | <b>1</b>  |   |
| <b>Тема 1.18</b><br>Изучение мер защиты информации в информационных системах | <b>Содержание</b>  | <b>2</b>  |   |
|  | Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.   |           | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>2</b>  |   |
|  | Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.  | 2         |   |
| <b>Тема 1.19</b><br>Изучение современных программно-аппаратных               | <b>В том числе практических и лабораторных занятий</b>   | <b>10</b> |   |
|  | Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов  | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.                               |



|   |  |        |   |
|---|--|--------|---|
| комплексов.   | Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов | 2      | ПК 2.4. ПК 2.5.<br>ПК 2.6.                                      |
|   | Изучение типовых решений для построения VPN на примере VipNet или других аналогов  | 2      |   |
|   | Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов  | 2      |   |
|   | Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов   | 2      |   |
| Курсовая работа   |  | 20     |   |
| Промежуточная аттестация по МДК.02 дифференцированный зачет 3 семестр |  | 2      |   |
| Обобщение разделов (консультация)                                     |  | 4      |   |
| Промежуточная аттестация по МДК.02.01 экзамен 4 семестр               |  | 6      |   |
| Раздел 2. Криптографические средства защиты информации                |  | 140/70 |   |
| МДК.02.02. Криптографические средства защиты информации               |  | 140/70 |   |
| Тема 2.1.<br>Математические основы криптографии                       | Содержание   | 22     | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|   | Элементы теории множеств. Группы, кольца, поля.  | 2      |   |
|   | Делимость чисел. Признаки делимости. Простые и составные числа.  | 2      |   |
|   | Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.  |        |   |
|   | Отношения сравнимости. Свойства сравнений. Модулярная арифметика.  | 2      |   |
|   | Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.  |        |   |
|   | Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.   |        |   |
|   | Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.   | 2      |   |
|   | Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.   | 2      |   |
|   | В том числе практических и лабораторных занятий  | 8      |   |

|  |   |           |   |
|--|---|-----------|---|
|  | Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений   | 4         |   |
|  | Проверка чисел на простоту  | 2         |   |
|  | Решение задач с элементами теории чисел.  | 2         |   |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>История развития криптографии<br>Китайская теорема об остатках.<br>Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра<br>Арифметические операции над большими числами.<br>Эллиптические кривые и их приложения в криптографии | 4         |   |
|  |   |           |   |
| <b>Тема 2.2.</b> Методы криптографического защиты информации | <b>Содержание</b>   | <b>18</b> |   |
|  | Классификация основных методов криптографической защиты. Методы симметричного шифрования  | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр  | 2         |   |
|  | Методы перестановки. Табличная перестановка, маршрутная перестановка  | 2         |   |
|  | Гаммирование. Гаммирование с конечной и бесконечной гаммами   | 2         |   |
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>10</b> |   |
|  | Применение классических шифров замены   | 2         |   |
|  | Применение классических шифров перестановки   | 2         |   |
|  | Применение метода гаммирования  | 2         |   |
|  | Программная реализация классических шифров  | 4         |   |
| <b>Тема 2.3.</b> Криптоанализ                                | <b>Содержание</b>   | <b>14</b> |   |
|  | Основные методы криптоанализа. Криптографические атаки.   | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффа   |           |   |
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>10</b> |   |
|  | Криптоанализ шифра простой замены методом анализа частотности символов  | 2         |   |
|  | Криптоанализ классических шифров методом полного перебора ключей  | 4         |   |
|  | Криптоанализ шифра Вижинера   | 4         |   |

|  |  |           |   |
|--|--|-----------|---|
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Перспективные направления криптоанализа, квантовый криптоанализ<br>Оптимизация методов частотного анализа моноалфавитных шифров                             | <b>2</b>  |   |
| <b>Тема 2.4.</b> Поточные шифры и генераторы псевдослучайных чисел     | <b>Содержание учебного материала</b>   | <b>8</b>  |   |
|  | Основные принципы поточного шифрования.  | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод VBS.   |           |   |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>4</b>  |   |
|  | Применение методов генерации ПСЧ   | 4         |   |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Применение генераторов ПСЧ в криптографии   | <b>2</b>  |   |
| <b>Тема 2.5</b> Кодирование информации.<br>Компьютеризация шифрования. | <b>Содержание учебного материала</b>   | <b>12</b> |   |
|  | Кодирование информации. Символьное кодирование. Смысловое кодирование.   | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Компьютеризация шифрования. Аппаратное и программное шифрование<br>Стандартизация программно-аппаратных криптографических систем и средств.  |           |   |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>8</b>  |   |
|  | Кодирование информации   | 2         |   |
|  | Программная реализация классических шифров   | 2         |   |
|  | Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.  | 4         |   |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Механизация шифрования. Представление информации в двоичном коде.<br>Таблица ASCII. Изучение современных программных и аппаратных криптографических средств | <b>2</b>  |   |
| <b>Тема 2.6</b><br>Симметричные системы шифрования                     | <b>Содержание учебного материала</b>   | <b>8</b>  |   |
|  | Общие сведения. Структурная схема симметричных криптографических систем  | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|  | Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4  | 2         |   |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>4</b>  |   |
|  | Анализ современных симметричных криптоалгоритмов   | 2         |   |

|   |  |           |   |
|---|--|-----------|---|
|   | Изучение программной реализации современных симметричных шифров  | 2         |   |
| <b>Тема 2.7</b><br>Асимметричные системы шифрования                   | <b>Содержание учебного материала</b>   | <b>8</b>  |   |
|   | Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.                 | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|   | Элементы теории чисел в криптографии с открытым ключом.  |           |   |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b>  |   |
|   | Анализ современных асимметричных криптоалгоритмов  | 2         |   |
|   | Применение различных асимметричных алгоритмов  | 2         |   |
|   | Изучение программной реализации асимметричного алгоритма RSA   | 2         |   |
| <b>Тема 2.8</b><br>Аутентификация данных.<br>Электронная подпись      | <b>Содержание учебного материала</b>   | <b>10</b> |   |
|   | Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции.   | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|   | Алгоритмы цифровой подписи   |           |   |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>8</b>  |   |
|   | Применение различных функций хеширования, анализ особенностей хешей  | 2         |   |
|   | Применение криптографических атак на хеш-функции.  | 2         |   |
|   | Изучение программно-аппаратных средств, реализующих основные функции ЭП  | 4         |   |
| <b>Тема 2.9</b><br>Алгоритмы обмена ключей и протоколы аутентификации | <b>Содержание учебного материала</b>   | <b>8</b>  |   |
|   | Алгоритмы распределения ключей с применением симметричных и асимметричных схем. Протоколы аутентификации.              | 2         | ОК 08; ПК 2.1.<br>ПК 2.2. ПК 2.3.<br>ПК 2.4. ПК 2.5.<br>ПК 2.6. |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>4</b>  |   |
|   | Применение протокола Диффи-Хеллмана для обмена ключами шифрования.   | 2         |   |
|   | Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos. | 2         |   |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Взаимная аутентификация. Односторонняя аутентификация         | <b>2</b>  |   |
| <b>Тема 2.10</b>  | <b>Содержание учебного материала</b>   | <b>4</b>  |   |

|  |   |   |  |
|--|---|---|--|
| Криптозащита информации в сетях передачи данных                        | Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей.  | 2 | ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6. |
|  | Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.   |   |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Криптомаршрутизатор. Пакетный фильтр   | 2 |  |
| <b>Тема 2.11</b><br>Защита информации в электронных платежных системах | <b>Содержание учебного материала</b>  | 8 |  |
|  | Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер   | 2 | ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6. |
|  | Применение криптографических протоколов для обеспечения безопасности электронной коммерции.   |   |  |
|  | <b>В том числе практических и лабораторных занятий</b>  | 4 |  |
|  | Применение аутентификации по одноразовым паролям  | 2 |  |
|  | Реализация алгоритмов создания одноразовых паролей  | 2 |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Средства аутентификации в платежных системах   | 2 |  |
| <b>Тема 2.12</b><br>Компьютерная стеганография                         | <b>Содержание учебного материала</b>  | 8 |  |
|  | Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации  | 2 | ОК 08; ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6. |
|  | Методы компьютерной стеганографии. Цифровые водяные знаки.  |   |  |
|  | <b>В том числе практических и лабораторных занятий</b>  | 4 |  |
|  | Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ   | 2 |  |
|  | Реализация простейших стеганографических алгоритмов   | 2 |  |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Законодательство в области криптографической защиты информации<br>Защита авторских прав. Алгоритмы встраивания ЦВЗ | 2 |  |
| <b>Промежуточная аттестация по МДК.03.02</b> дифференцированный зачет  |   | 2 |  |
| <b>Обобщение разделов МДК</b>  |   | 4 |  |
| <b>Промежуточная аттестация по МДК.03.02</b> экзамен                   |   | 6 |  |

|  |            |  |
|--|------------|--|
| <p><b>Учебная практика</b><br/> <b>Виды работ:</b></p> <ul style="list-style-type: none"> <li>– Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах</li> <li>– Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности</li> <li>– Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности</li> <li>– Составление документации по учету, обработке, хранению и передаче конфиденциальной информации</li> <li>– Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации</li> <li>– Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.</li> <li>– Устранение замечаний по результатам проверки</li> <li>– Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.</li> <li>– Применение математических методов для оценки качества и выбора наилучшего программного средства</li> <li>– Применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных</li> <li>– Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи</li> </ul> | <b>48</b>  |  |
| <p><b>Производственная практика</b><br/> <b>Виды работ:</b></p> <ul style="list-style-type: none"> <li>– Участие в установке и настройку отдельных программных, программно-аппаратных средств защиты информации.</li> <li>– Участие в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.</li> <li>– Участие в тестировании функций отдельных программных и программно-аппаратных средств защиты информации.</li> <li>– Участие в обработке, хранении и передаче информации ограниченного доступа.</li> <li>– Участие в уничтожении информации и носителей информации с использованием программных и программно-аппаратных средств.</li> </ul>   | <b>156</b> |  |

|  |                |  |
|--|----------------|--|
| <ul style="list-style-type: none"> <li>– Участие в решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации</li> <li>– Осуществление регистрации основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.</li> <li>– Анализ принципов построения систем информационной защиты производственных подразделений.</li> <li>– Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.</li> <li>– Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности.</li> <li>– Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении.</li> <li>– Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики</li> </ul> |                |  |
| <b>Экзамен по профессиональному модулю</b>   | <b>12</b>      |  |
| <b>Всего:</b>  | <b>574/372</b> |  |

#### 2.4. Курсовая работа

Выполнение курсовой работы обязательно

Тематика курсовых работ:

- Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)
- Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)
- Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)
- Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)
- Проблема защиты информации в облачных хранилищах данных и ЦОДах
- Защита сред виртуализации

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

#### **3.1. Материально-техническое обеспечение**

Мастерская «Кибербезопасности», оснащена в соответствии с приложением 3 ОПОП-П.

Оснащенные базы практики (мастерские), оснащены в соответствии с приложением 3 ОПОП-П. и с п. 3.1.2. образовательной программы.

#### **3.2. Учебно-методическое обеспечение**

##### **3.2.1. Основные печатные и/или электронные издания**

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2020.- 175 с.

2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.: Горячая линия – Телеком, 2019.- 248 с.

3. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2020.- 400 с.

4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт].

5. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2021. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт].

##### **3.2.2 Дополнительные источники:**

1. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2019. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности

2. Федеральный образовательный портал «Информационно -коммуникационные технологии в образовании». [Электронный ресурс] – Режим доступа:  
<http://window.edu.ru/resource/832/7832>



#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

| Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля   | Критерии оценки  | Методы оценки   |
|--|--|---|
| ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.               | Демонстрирует умения и 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. | Демонстрирует знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами | 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 тестирование функций отдельных программных и программно-аппаратных средств защиты информации.               | Выполняет перечень работ по тестированию функций отдельных программных и 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 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.  | Проявляет знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа   | 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 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.  | Демонстрирует алгоритм проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств   | 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 2.6. 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. | Проявляет знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак | 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 |
| ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.  | Выполняет правила ТБ во время учебных занятий, при прохождении учебной и производственной практик   |   |

**Приложение 1.3**

к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

**Рабочая программа профессионального модуля**

**«ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ»**

2025 г.

## СОДЕРЖАНИЕ

|   |           |
|---|-----------|
| <b>1. Общая характеристика .....</b>  | <b>53</b> |
| 1.1. Цель и место профессионального модуля в структуре образовательной программы... | 53        |
| 1.2. Планируемые результаты освоения профессионального модуля.....                  | 53        |
| <b>2. Структура и содержание профессионального модуля .....</b>                     | <b>54</b> |
| 2.1. Трудоемкость освоения модуля .....   | 54        |
| 2.2. Структура профессионального модуля .....                                       | 55        |
| 2.3. Содержание профессионального модуля .....                                      | 56        |
| 2.4. Курсовая работа .....  | 66        |
| <b>3. Условия реализации профессионального модуля .....</b>                         | <b>68</b> |
| 3.1. Материально-техническое обеспечение.....                                       | 68        |
| 3.2. Учебно-методическое обеспечение .....  | 68        |
| <b>4. Контроль и оценка результатов освоения профессионального модуля.....</b>      | <b>69</b> |

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ»

## 1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «защита информации техническими средствами».

Профессиональный модуль включен в обязательную часть профессионального цикла образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

## 1.3. Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ОПОП-П).

В результате освоения профессионального модуля обучающийся должен:

| Код ОК, ПК | Уметь   | Знать  | Владеть навыками   |
|------------|---|--|--|
| ОК.09      | <ul style="list-style-type: none"> <li>– понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы</li> <li>– участвовать в диалогах на знакомые общие и профессиональные темы</li> <li>– строить простые высказывания о себе и о своей профессиональной деятельности</li> <li>– кратко обосновывать и объяснять свои действия (текущие и планируемые)</li> <li>– писать простые связные сообщения на знакомые или интересующие профессиональные темы</li> </ul> | <ul style="list-style-type: none"> <li>– правила построения простых и сложных предложений на профессиональные темы</li> <li>– основные общеупотребительные глаголы (бытовая и профессиональная лексика)</li> <li>– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности</li> <li>– особенности произношения</li> <li>– правила чтения текстов профессиональной направленности</li> </ul> | -  |
| ПК 3.1.    | <ul style="list-style-type: none"> <li>– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных</li> </ul>  | <ul style="list-style-type: none"> <li>– порядок технического обслуживания технических средств защиты информации</li> <li>– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам</li> </ul>   | <ul style="list-style-type: none"> <li>– установка, монтаж и настройка технических средств защиты информации</li> <li>– техническое обслуживание технических средств защиты информации</li> <li>– применение основных типов технических средств защиты информации</li> </ul> |
| ПК 3.2.    | <ul style="list-style-type: none"> <li>– применять технические средства для криптографической</li> </ul>  | <ul style="list-style-type: none"> <li>– физические основы, структуру и условия формирования технических каналов утечки</li> </ul>   | <ul style="list-style-type: none"> <li>– применять основные типы технических средств защиты информации</li> </ul>  |

|         |   |   |   |
|---------|---|---|---|
|         | защиты информации конфиденциального характера<br>– применять технические средства для уничтожения информации и носителей информации<br>– применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами | информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации<br>– порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации<br>– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации<br>– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам | – выявлять технические каналы утечки информации<br>– участвовать в мониторинге эффективности технических средств защиты информации<br>– диагностировать, устранять отказы и неисправности, восстанавливать работоспособности технических средств защиты информации    |
| ПК 3.3. | – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных  | – номенклатуру и характеристики аппаратуры, используемой для измерения параметров пэмин, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации<br>– структуру и условия формирования технических каналов утечки информации   | – проводить измерения параметров пэмин, созданные техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации |
| ПК 3.4. | – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных  | – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам   | – проводить измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации<br>– выявлять технические каналы утечки информации  |
| ПК 3.5. | – основные принципы действия и характеристики технических средств физической защиты<br>– основные способы физической защиты объектов информатизации<br>– номенклатуру применяемых средств физической защиты объектов информатизации                                       | – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом<br>– применять инженерно-технические средства физической защиты объектов информатизации   | – устанавливать, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей<br>– восстанавливать работоспособности инженерно-технических средств физической защиты  |

#### 1.4. Обоснование часов вариативной части ОПОП-П

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.1. Трудоемкость освоения модуля

| Наименование составных частей модуля   | Объем в часах | В т.ч. в форме практической подготовки |
|--|---------------|--|
| Учебные занятия, в т.ч.:   | 206           | 152                                    |
| Курсовая работа (проект)   | 20            |  |
| Самостоятельная работа   | 18            |  |
| Практика, в т.ч.:  | 234           | 234                                    |
| учебная  | 66            | 66                                     |
| производственная   | 168           | 168                                    |
| Промежуточная аттестация, в том числе:<br><i>МДК 03.02. в форме экзамена</i><br><i>ПМ 03</i> | 6<br>12       |  |
| Всего  | <b>476</b>    | <b>386</b>                             |

## 2.2. Структура профессионального модуля

| Код ОК, ПК  | Наименования разделов профессионального модуля   | Всего, час. | В т.ч. в форме практической подготовки | Обучение по МДК, в т.ч.: | Учебные занятия | Курсовая работа (проект) | Самостоятельная работа | Промежуточная аттестация | Учебная практика | Производственная практика |
|---|--|-------------|--|--------------------------|-----------------|--------------------------|------------------------|--------------------------|------------------|---------------------------|
| 1   | 2  | 3           | 4                                      | 5                        | 6               | 7                        | 8                      |                          | 9                | 10                        |
| ОК 09; ПК 3.1.<br>ПК 3.2. ПК 3.3.<br>ПК 3.4. ПК 3.5 | <b>Раздел 1</b> Техническая защита информации  | <b>122</b>  | <b>72</b>                              | <b>122</b>               | 106             | -                        | 16                     | -                        |                  |                           |
| ОК 09; ПК 3.1.<br>ПК 3.2. ПК 3.3.<br>ПК 3.4. ПК 3.5 | <b>Раздел 2</b> Инженерно-технические средства физической защиты объектов информатизации | <b>108</b>  | <b>80</b>                              | <b>108</b>               | 100             | 20                       | 2                      | 6                        |                  |                           |
|   | Учебная практика   | <b>66</b>   | <b>66</b>                              |                          |                 |                          |                        |                          | <b>66</b>        |                           |
|   | Производственная практика  | <b>168</b>  | <b>168</b>                             |                          |                 |                          |                        |                          |                  | <b>168</b>                |
|   | Промежуточная аттестация   | <b>12</b>   |  |                          |                 |                          |                        |                          |                  |                           |
|   | <b>Всего:</b>  | <b>476</b>  | <b>386</b>                             | <b>230</b>               | <b>206</b>      | <b>20</b>                | <b>18</b>              | <b>6</b>                 | <b>66</b>        | <b>168</b>                |

### 2.3. Содержание профессионального модуля

| Наименование разделов и тем  | Содержание учебного материала, практических и лабораторных занятия, курсовая работа (проект)  | Объем, ак. ч. /<br>в том числе<br>в форме<br>практической<br>подготовки,<br>ак. ч | Коды компетенций, формированию которых способствует элемент программы |
|--|---|---|---|
| 1  | 2   | 3   | 4   |
| <b>Раздел 1. Техническая защита информации</b>                             |   | <b>122/72</b>   |   |
| <b>МДК.03.01 Техническая защита информации</b>                             |   | <b>122/72</b>   |   |
| <b>Тема 1.1.</b> Предмет и задачи технической защиты информации            | <b>Содержание</b>   | <b>1</b>  |   |
|  | Входной контроль. Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.   | 1   | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5                |
| <b>Тема 1.2.</b> Общие положения защиты информации техническими средствами | <b>Содержание</b>   | <b>1</b>  | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5                |
|  | Задачи и требования к способам и средствам защиты информации техническими средствами. Классификация способов и средств защиты информации.   | 1   |   |
| <b>Тема 1.3.</b> Информация как предмет защиты                             | <b>Содержание</b>   | <b>10</b>   | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5                |
|  | Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства, и системы. Угрозы безопасности информации | 2   |   |
|  | Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.   | 2   |   |
|  | <i>В том числе практических и лабораторных занятий</i>  | <b>6</b>  |   |



|   |  |           |  |
|---|--|-----------|--|
|   | Изучение нормативной базы правового регулирования вопросов защиты информации   | 2         |  |
|   | Анализ стандартов информационной безопасности по вопросам технической защиты информации  | 2         |  |
|   | Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.   | 2         |  |
| <b>Тема 1.4.</b> Технические каналы утечки информации   | <b>Содержание</b>  | <b>12</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации.  | 2         |  |
|   | Характеристика каналов утечки информации. Оптические каналы утечки информации, их характеристика. Акустические, каналы утечки информации, их характеристика. Радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика | 2         |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b>  |  |
|   | Определение вариантов утечки информации по оптическим каналам для типовых контролируемых зон организации   | 2         |  |
|   | Изучение характеристик акустического канала утечки информации  | 2         |  |
|   | Изучение характеристик радиоэлектронного канала утечки информации  | 2         |  |
|   | <b>В том числе самостоятельная работа обучающихся</b>  | <b>2</b>  |  |
|   | Основные понятия в области акустики  |           |  |
| <b>Тема 1.5.</b> Методы и средства технической разведки | <b>Содержание</b>  | <b>4</b>  | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.                        | 2         |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>2</b>  |  |
|   | Изучение характеристик наземных средств дистанционного съема информации. Анализ современных средств перехвата сигналов   | 2         |  |
|   |  |           |  |
|   | <b>Содержание</b>  | <b>14</b> | ОК 09; ПК 3.1.   |

|   |  |          |  |
|---|--|----------|--|
| <b>Тема 1.6.</b> Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок | Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические основы побочных электромагнитных излучений и наводок.  | 2        | ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5                   |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b> |  |
|   | Измерение параметров физических полей  | 2        |  |
|   | Анализ современных средств перехвата сигналов  | 2        |  |
|   | Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей   | 2        |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Низкочастотные и высокочастотные излучения технических средств<br>Физические основы побочных излучений и наводок | <b>6</b> |  |
| <b>Тема 1.7.</b> Физические процессы при подавлении опасных сигналов  | <b>Содержание</b>  | <b>6</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.   | 2        |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>4</b> |  |
|   | Изучение пассивных методов подавления опасных сигналов акустоэлектрических преобразователей  | 2        |  |
|   | Изучение активных методов подавления опасных сигналов акустоэлектрических преобразователей   | 2        |  |
| <b>Тема 1.8.</b> Системы защиты от утечки информации по акустическому каналу                                  | <b>Содержание</b>  | <b>8</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу.  | 2        |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>4</b> |  |
|   | Анализ современных средств перехвата речевой информации. Защита от утечки по акустическому каналу  | 2        |  |
|   | Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу   | 2        |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Средства акустической разведки  | <b>2</b> |  |

|   |  |           |  |
|---|--|-----------|--|
| <b>Тема 1.9.</b> Системы защиты от утечки информации по проводному каналу         | <b>Содержание</b>  | <b>10</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов.              | 2         |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b>  |  |
|   | Анализ способов технического закрытия от утечки речевой информации   | 2         |  |
|   | Изучение сущности и параметров звукоизоляции   | 2         |  |
|   | Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу  | 2         |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Закладные устройства  | <b>2</b>  |  |
| <b>Тема 1.10.</b> Системы защиты от утечки информации по вибрационному каналу     | <b>Содержание</b>  | <b>4</b>  | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу                                   | 2         |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>2</b>  |  |
|   | Защита от утечки по виброакустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу                                  | 2         |  |
| <b>Тема 1.11.</b> Системы защиты от утечки информации по электромагнитному каналу | <b>Содержание</b>  | <b>12</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Системы защиты от утечки по электромагнитному каналу.                                     | 2         |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b>  |  |
|   | Определение каналов утечки ПЭМИН   | 2         |  |
|   | Защита от утечки по цепям электропитания и заземления  | 2         |  |
|   | Изучение принципов работы и основных характеристик обнаружителей электромагнитного поля  | 1         |  |
|   | Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу   | 1         |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации с пассивных закладок. | <b>4</b>  |  |

|   |   |          |  |
|---|---|----------|--|
| <b>Тема 1.12.</b> Системы защиты от утечки информации по телефонному каналу     | <b>Содержание</b>   | <b>6</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. | 2        |  |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>4</b> |  |
|   | Защита от утечки информации в средствах мобильной связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу   | 4        |  |
| <b>Тема 1.13.</b> Системы защиты от утечки информации по электросетевому каналу | <b>Содержание</b>   | <b>6</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.                                  | 2        |  |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>4</b> |  |
|   | Изучение требований по защите системы электропитания объектов информатизации  | 2        |  |
|   | Средства фильтрации опасных сигналов в цепях электропитания. Сетевые помехоподавляющие фильтры  | 2        |  |
| <b>Тема 1.14.</b> Системы защиты от утечки информации по оптическому каналу     | <b>Содержание</b>   | <b>6</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.   | 2        |  |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>4</b> |  |
|   | Изучение способов скрытого видеонаблюдения и съемки   | 2        |  |
|   | Изучение способов защиты информации от утечки по оптическому каналу   | 2        |  |
| <b>Тема 1.15.</b> Применение технических средств защиты информации              | <b>Содержание</b>   | <b>8</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>8</b> |  |
|   | Изучение характеристик технических средства для уничтожения информации и носителей информации   | 2        |  |
|   | Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных  | 2        |  |
|   | Изучение требований на комплексы и приборы, предназначенные для измерений характеристик побочных электромагнитных излучений и наводок   | 2        |  |

|   |   |               |  |
|---|---|---------------|--|
|   | Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов      | 1             |  |
|   | Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации   | 1             |  |
| <b>Тема 1.16. Эксплуатация технических средств защиты информации</b>                      | <b>Содержание</b>   | <b>10</b>     | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>10</b>     |  |
|   | Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации                           | 2             |  |
|   | Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации           | 2             |  |
|   | Оценка функционирования средств защиты информации от несанкционированного доступа   | 2             |  |
|   | Меры по защите информации на объекте информатизации   | 2             |  |
|   | Использование средств защиты информации. Реестр ФСТЭК России  | 2             |  |
| <b>Промежуточная аттестация по МДК.03.01 дифференцированный зачет</b>                     |   | <b>2</b>      |  |
| <b>Промежуточная аттестация по МДК.03.01 дифференцированный зачет (комплексный)</b>       |   | <b>2</b>      |  |
| <b>Раздел 2. Инженерно-технические средства физической защиты объектов информатизации</b> |   | <b>108/80</b> |  |
| <b>МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации</b> |   | <b>108/80</b> |  |
| <b>Тема 2.1. Цели и задачи физической защиты объектов информатизации</b>                  | <b>Содержание</b>   | <b>10</b>     | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты | 2             |  |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>8</b>      |  |
|   | Объект информатизации. Категорирование объектов информатизации  | 2             |  |
|   | Модель нарушителя и возможные пути, и способы его проникновения на охраняемый объект  | 2             |  |
|   | Типы охраны различных объектов и их обоснование при выборе помещения, как объекта защиты  | 4             |  |
|   | <b>Содержание</b>   | <b>12</b>     | ОК 09; ПК 3.1.   |

|   |   |           |  |
|---|---|-----------|--|
| <b>Тема 2.2.</b> Общие сведения о комплексах инженерно-технических средств физической защиты  | Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. | 2         | ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5                   |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>10</b> |  |
|   | Типовые инженерные конструкции применяемые на объектах информатизации   | 2         |  |
|   | Интегрированные системы обеспечения безопасности и их составляющие  | 2         |  |
|   | Этапы построения системы защиты объекта   | 4         |  |
|   | Требования к инженерным средствам физической защиты   | 2         |  |
| <b>Тема 2.3</b> Система обнаружения комплекса инженерно-технических средств физической защиты | <b>Содержание</b>   | <b>20</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.                                | 2         |  |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>18</b> |  |
|   | Характеристики систем защиты территории и помещений, примеры технической реализации – инфракрасные системы, системы защиты ИК-датчиков, оптоволоконные системы  | 2         |  |
|   | Характеристики систем защиты территории и помещений, примеры технической реализации – емкостные системы охраны периметров, вибрационные системы и вибрационно-сейсмические системы  | 2         |  |
|   | Характеристики систем защиты территории и помещений, примеры технической реализации – радиолучевые системы, системы «активной» охраны периметров  | 2         |  |
|   | Системы охранной, тревожной и пожарной сигнализации. Классификация извещателей охранных   | 2         |  |
|   | Функциональные особенности некоторых применяемых на практике охранных и пожарных извещателей  | 2         |  |
|   | Прибор приемно-контрольный (ППК) охранный (охранно-пожарный), классификация, параметры  | 2         |  |
|   | Анализ рынка современных систем защиты территории и помещений   | 2         |  |

|   |  |           |  |
|---|--|-----------|--|
|   | Построение систем обеспечения безопасности объекта   | 4         |  |
| <b>Тема 2.4.</b> Система контроля и управления доступом | <b>Содержание</b>  | <b>12</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Классификация средств управления доступом. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ. | 2         |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>10</b> |  |
|   | Изучение принципов устройства, работы и применения аппаратных средств аутентификации и идентификации пользователя  | 2         |  |
|   | Изучение принципов устройства, работы и применения средств контроля доступа  | 2         |  |
|   | Биометрические системы идентификации, классификация. Этапы работы биометрических систем  | 2         |  |
|   | Анализ рынка современных СКУД  | 4         |  |
| <b>Тема 2.5.</b> Система телевизионного наблюдения      | <b>Содержание</b>  | <b>12</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|   | Назначение системы телевизионного наблюдения. Аналоговые и цифровые системы видеонаблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.   | 2         |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>10</b> |  |
|   | Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.  | 2         |  |
|   | Изучение параметров видеокамер. Виды объективов.   | 2         |  |
|   | Требования к качеству изображения. Технические решения, направленные на улучшение характеристик видеокамер   | 2         |  |
|   | Варианты системы управления видеонаблюдением. Видеорегистраторы и их характеристики. Сетевое видеонаблюдение.  | 4         |  |
|   | <b>Содержание</b>  | <b>4</b>  | ОК 09; ПК 3.1.   |

|  |  |           |  |
|--|--|-----------|--|
| <b>Тема 2.6.</b> Система сбора, обработки, отображения и документирования информации | Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.                            | 2         | ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5                   |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>2</b>  |  |
|  | Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.   | 2         |  |
| <b>Тема 2.7</b> Система воздействия  | <b>Содержание</b>  | <b>4</b>  | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b>  |  |
|  | Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.   | 4         |  |
|  | Обзор современных технических средств воздействия  | 2         |  |
| <b>Тема 2.8</b> Применение инженерно-технических средств физической защиты           | <b>Содержание</b>  | <b>12</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|  | Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Управление системой воздействия. | 2         |  |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>8</b>  |  |
|  | Организация пропускного режима на КПП, система автоматического управления. Особенности организации пропускного режима на КПП   | 2         |  |
|  | Определение путей проникновения злоумышленника на объект информатизации  | 4         |  |
|  | Порядок применения устройств отображения и документирования информации   | 2         |  |
|  | <b>В том числе самостоятельная работа обучающихся</b>  | 2         |  |
|  | Внутриобъектовый режим. Интегрированные охранные системы   |           |  |
| <b>Тема 2.9.</b> Эксплуатация инженерно-технических средств физической защиты        | <b>Содержание</b>  | <b>10</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|  | Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Организация ремонта технических средств физической защиты.  | 2         |  |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>8</b>  |  |
|  | Установка и настройка периметровых и объектовых технических средств обнаружения  | 4         |  |



|   |   |            |  |
|---|---|------------|--|
|   | Изучение принципов диагностики, устранения отказов и восстановление работоспособности технических средств физической защиты | 4          |  |
| <b>Курсовая работа</b>  |   | <b>20</b>  |  |
| <b>Обобщение разделов МДК</b>   |   | <b>4</b>   |  |
| <b>Промежуточная аттестация по МДК.03.02 экзамен</b>  |   | <b>6</b>   |  |
| <b>Учебная практика</b><br><b>Виды работ:</b> <ul style="list-style-type: none"> <li>– Измерение параметров физических полей.</li> <li>– Определение каналов утечки ПЭМИН.</li> <li>– Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.</li> <li>– Установка и настройка технических средств защиты информации.</li> <li>– Проведение измерений параметров побочных электромагнитных излучений и наводок.</li> <li>– Проведение аттестации объектов информатизации.</li> <li>– Освоение методики выявления возможных угроз информационной безопасности объектов защиты.</li> <li>– Проектирование установки системы пожарно-охранной сигнализации по заданию.</li> <li>– Применение промышленных осциллографов, частотомеров и генераторов, и другого оборудования для защиты информации.</li> <li>– Рассмотрение системы контроля и управления доступом и её проектирование.</li> <li>– Рассмотрение принципов работы системы видеонаблюдения и её проектирование.</li> <li>– Рассмотрение датчиков периметра, их принципов работы.</li> <li>– Рассмотрение звукоизоляции помещений, обоснование шумления и его проектирование.</li> <li>– Реализация защиты от утечки по цепям электропитания и заземления.</li> <li>– Разработка организационных и технических мероприятий по заданию.</li> <li>– Разработка основной документации по инженерно-технической защите информации.</li> </ul> |   | <b>66</b>  |  |
| <b>Производственная практика</b><br><b>Виды работ:</b> <ul style="list-style-type: none"> <li>– Участие в монтаже, настройке, обслуживании и эксплуатации инженерной и технических средств защиты информации;</li> <li>– Участие в монтаже, настройке, обслуживании и эксплуатации средств охраны и безопасности;</li> <li>– Участие в монтаже, настройке, обслуживании и эксплуатации систем видеонаблюдения;</li> </ul>   |   | <b>168</b> |  |

|   |            |  |
|---|------------|--|
| <ul style="list-style-type: none"> <li>– Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам;</li> <li>– Участвовать в измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа;</li> <li>– Участвовать в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации;</li> <li>– Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами;</li> <li>– Освоение методики выявления возможных угрозы информационной безопасности объектов защиты;</li> <li>– Участие в организации отдельных работ по физической защите объектов информатизации</li> <li>– Разработка предложений по усовершенствованию технической защиты информации объекта информатизации.</li> </ul> |            |  |
| <b>Экзамен по профессиональному модулю</b>  | <b>12</b>  |  |
| <b>Всего</b>  | <b>476</b> |  |

## 2.4. Курсовая работа

Выполнение курсовой работы обязательно

Тематика курсовых работ

1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации.
2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации.
3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.
4. Моделирование объекта защиты и угроз безопасности информации для коммерческого предприятия
5. Разработка инженерно-технических мер по защите информации производственного объекта.
6. Разработка инженерно-технических мер по защите информации общественного учреждения
7. Разработка инженерно-технических мер по защите информации некоммерческой организации.
8. Разработка инженерно-технических мер по защите информации коммерческого предприятия
9. Разработка комплексной системы безопасности и мер по защите информации общественной организации
10. Комплексная система безопасности информации общественного здания

11. Расчет системы безопасности и контроля доступа коммерческой организации
12. Моделирование объекта защиты и угроз безопасности информации для некоммерческой организации
13. Расчет системы безопасности и контроля доступа производственного здания
14. Комплексная система безопасности информации коммерческой организации
15. Моделирование объекта защиты и угроз безопасности информации

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

#### **3.1. Материально-техническое обеспечение**

Мастерская «Кибербезопасности», оснащена в соответствии с приложением 3 ОПОП-П.

Базы практики (мастерские), оснащены в соответствии с приложением 3 ОПОП-П. и с п. 3.1.2. образовательной программы.

#### **3.2. Учебно-методическое обеспечение**

##### **3.2.1. Основные печатные и/или электронные издания**

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2019.

2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2020.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. — М.: МИЭТ, 2018. — 172 с.

4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. — М.: Издательский центр «Академия», 2018 — 336с.

5. Введение в теоретико-числовые методы криптографии : учебное пособие для спо / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 396 с. — ISBN 978-5-507-45348-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/265178> (дата обращения: 20.07.2023). — Режим доступа: для авториз. пользователей.

6. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум : учебное пособие для спо / Р. Н. Гилязова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 44 с. — ISBN 978-5-8114-9138-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/187645> (дата обращения: 20.07.2023). — Режим доступа: для авториз. пользователей.

6. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-47174-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/336200> (дата обращения: 20.07.2023). — Режим доступа: для авториз. пользователей.

##### **3.2.2. Дополнительные источники**

1. Котеров Д.В. РНР 5 в подлиннике. — СПб.: БХВ-Петербург, 2018. — 1104 с.

2. Федеральный образовательный портал «Информационно -коммуникационные технологии в образовании». [Электронный ресурс] — Режим доступа: <http://window.edu.ru/resource/832/7832>. Дата обращения 23.07.2022.

#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

| Код ПК, ОК  | Критерии оценки результата<br>(показатели освоённости компетенций)  | Формы контроля и методы оценки  |
|---|---|---|
| ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации   | Демонстрирует умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации | 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 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации  | Проявляет умения и практический опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации  | 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 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа | Проводит работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа                                       | 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 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации   | Проводит самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами 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 3.5 Организовывать отдельные работы по физической защите объектов информатизации       | Проявляет знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации   | 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 |
| ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках | Понимает тексты на базовые профессиональные темы, участвует в диалогах на профессиональные темы обосновывает и объясняет свои действия, пишет простые связные сообщения на профессиональные темы | 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 |

**Рабочая программа профессионального модуля**

**«ПМ.04 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И  
ВЫЧИСЛИТЕЛЬНЫХ МАШИН»**

## СОДЕРЖАНИЕ

|   |           |
|---|-----------|
| <b>1. Общая характеристика.....</b>   | <b>73</b> |
| 1.1. Цель и место профессионального модуля в структуре образовательной программы .. | 73        |
| 1.2. Планируемые результаты освоения профессионального модуля .....                 | 73        |
| <b>2. Структура и содержание профессионального модуля.....</b>                      | <b>75</b> |
| 2.1. Трудоемкость освоения модуля.....  | 75        |
| 2.2. Структура профессионального модуля.....  | 75        |
| 2.3. Содержание профессионального модуля.....                                       | 76        |
| <b>3. Условия реализации профессионального модуля .....</b>                         | <b>80</b> |
| 3.1. Материально-техническое обеспечение .....                                      | 80        |
| 3.2. Учебно-методическое обеспечение .....  | 80        |
| 4. Контроль и оценка результатов освоения профессионального модуля.....             | 81        |



# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## ПМ.04 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН

### 1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «Оператор электронно-вычислительных и вычислительных машин».

Профессиональный модуль включен в обязательную часть профессионального цикла образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

### 1.2 Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ОПОП-П).

В результате освоения профессионального модуля обучающийся должен:

| <b>Код ОК,<br/>ПК</b> | <b>Уметь</b>   | <b>Знать</b>  | <b>Владеть навыками</b>  |
|-----------------------|--|---|--|
| ПК 4.1                | <ul style="list-style-type: none"><li>– Выполнять требования техники безопасности при работе с вычислительной техникой</li><li>– Производить подключение блоков персонального компьютера и периферийных устройств</li><li>– Производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники</li><li>– Диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники</li><li>– Выполнять установку системного и прикладного программного обеспечения</li></ul> | <ul style="list-style-type: none"><li>– Требования техники безопасности при работе с вычислительной техникой</li><li>– Основные принципы устройства и работы компьютерных систем и периферийных устройств</li></ul> | <ul style="list-style-type: none"><li>– выполнять требования техники безопасности при работе с вычислительной техникой,</li><li>– организовывать рабочее место оператора электронно-вычислительных и вычислительных машин,</li><li>– подготовки оборудования компьютерной системы к работе</li></ul> |
| ПК 4.2                | <ul style="list-style-type: none"><li>– Создавать и управлять содержимым документов с помощью текстовых процессоров</li><li>– Создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц</li><li>– Создавать и управлять содержимым презентаций с</li></ul>   | <ul style="list-style-type: none"><li>– Классификацию и назначение компьютерных сетей</li><li>– Виды носителей информации</li></ul>   | <ul style="list-style-type: none"><li>– Инсталлировать, настраивать и обслуживать программное обеспечение компьютерной системы</li><li>– Управлять файлами</li><li>– Применять офисное программное обеспечение в соответствии с прикладной задачей</li></ul>   |

|        |   |   |  |
|--------|---|---|--|
|        | <p>помощью редакторов презентаций</p> <ul style="list-style-type: none"> <li>– Использовать мультимедиа проектор для демонстрации презентаций</li> <li>– Вводить, редактировать и удалять записи в базе данных</li> <li>– Эффективно пользоваться запросами базы данных</li> <li>– Создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики</li> <li>– Производить сканирование документов и их распознавание</li> <li>– Производить распечатку, копирование и тиражирование документов на принтере и других устройствах</li> </ul> |   |  |
| ПК 4.3 | <ul style="list-style-type: none"> <li>– Управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете</li> <li>– Осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера</li> <li>– Осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет-сайтов</li> </ul>  | – Программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета   | <ul style="list-style-type: none"> <li>– Использовать ресурсы локальной вычислительной сети</li> <li>– Использовать ресурсы, технологии и сервисов Интернет</li> </ul> |
| ПК 4.4 | <ul style="list-style-type: none"> <li>– Осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ</li> <li>– Осуществлять резервное копирование и восстановление данных</li> </ul>   | – Основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы | – Применять средства защиты информации в компьютерной системе  |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.1. Трудоемкость освоения модуля

| Наименование составных частей модуля   | Объем в часах | В т.ч. в форме практической подготовки |
|--|---------------|--|
| Учебные занятия  | 94            | 94                                     |
| Курсовая работа (проект)   |               |  |
| Самостоятельная работа   | 8             |  |
| Практика, в т.ч.:  | 240           | 240                                    |
| учебная  | 156           | 156                                    |
| производственная   | 84            | 84                                     |
| Промежуточная аттестация, в том числе:<br><i>МДК 04.01 в форме диф. зачета</i><br><i>УП 04</i><br><i>ПП 04</i><br><i>ПМ 04 экзамен</i> | 12            |  |
| Всего  | 354           | 334                                    |

### 2.2. Структура профессионального модуля

| Код ОК, ПК      | Наименования разделов профессионального модуля                | Всего, час. | В т.ч. в форме практической подготовки | Обучение по МДК, в т.ч.: | Учебные занятия | Курсовая работа (проект) | Самостоятельная работа | Учебная практика | Производственная практика |
|-----------------|---|-------------|--|--------------------------|-----------------|--------------------------|------------------------|------------------|---------------------------|
| 1               | 2   | 3           | 4                                      | 5                        | 6               | 7                        | 8                      | 9                | 10                        |
| ПК 4.1 - ПК 4.4 | Раздел 1. Технология создания и обработки цифровой информации | 102         | 94                                     |                          | 94              |                          | 8                      |                  |                           |
| ПК 4.1- ПК 4.4  | Учебная практика  | 156         | 156                                    |                          |                 |                          |                        | 156              |                           |
| ПК 4.1- ПК 4.4  | Производственная практика                                     | 84          | 84                                     |                          |                 |                          |                        |                  | 84                        |
| ПК 4.1- ПК 4.4  | Промежуточная аттестация                                      | 12          |  |                          |                 |                          |                        |                  |                           |
|                 | <b>Всего:</b>   | <b>354</b>  | <b>334</b>                             |                          | <b>94</b>       |                          | <b>8</b>               | <b>156</b>       | <b>84</b>                 |

### 2.3. Содержание профессионального модуля

| Наименование разделов и тем  | Содержание учебного материала, практических и лабораторных занятия   | Объем, ак. ч.<br>/<br>в том числе<br>в форме<br>практической<br>подготовки | Коды компетенций, формированию которых способствует элемент программы |
|--|--|--|---|
| <b>МДК 04.01 Технология создания и обработки цифровой информации</b>   |  |  |   |
| <b>Раздел 1. Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения</b>                                       |  | <b>20</b>  |   |
| <b>Тема 1.1.</b><br>Работа с устройствами компьютерной системы   | <b>Содержание</b>  | <b>6</b>   |   |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>6</b>   |   |
|  | Изучение охраны труда и техники безопасности Оператора ЭВМ. Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ      | 2  |   |
|  | Подключение, настройка и подготовка к работе периферийного оборудования  | 2  |   |
|  | Установка и замена расходных материалов для принтеров, ксерокса, сканера   | 2  |   |
| <b>Тема 1.2.</b><br>Работа с программным обеспечением компьютерной системы   | <b>Содержание</b>  | <b>8</b>   | ПК 4.1 -ПК 4.4  |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>8</b>   |   |
|  | Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в Интернете | 2  |   |
|  | Изучение процесса установки операционной среды, настройка интерфейса ОС  | 2  |   |
|  | Установка прикладных программ  | 4  |   |
| <b>Тема 1.3.</b><br>Диагностика неисправностей системы, ведение документации   | <b>Содержание</b>  | <b>6</b>   | ПК 4.1 -ПК 4.4  |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>4</b>   |   |
|  | Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ                     | 2  |   |
|  | Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники                 | 2  |   |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Оформление отчетной документации  | <b>2</b>   |   |
| <b>Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах</b> |  | <b>62</b>  |   |
| <b>Тема 2.1.</b>   | <b>Содержание</b>  | <b>14</b>  |   |

|   |  |           |  |
|---|--|-----------|--|
| Работа в текстовом процессоре   | <b>В том числе практических и лабораторных занятий</b>   | <b>14</b> |  |
|   | Изучение текстовых процессоры. Требования по оформлению технической документации   | 2         |  |
|   | Форматирование и редактирование шрифтов, абзацев и формул  | 2         |  |
|   | Форматирование и редактирование списков  | 2         |  |
|   | Работа с таблицами в текстовом процессоре  | 2         |  |
|   | Работа с графическими объектами в текстовом процессоре   | 4         |  |
|   | Форматирование документа в целом. Способы вывода документа на печать   | 2         |  |
| <b>Тема 2.2.</b><br>Работа в редакторе электронных таблиц                 | <b>Содержание</b>  | <b>12</b> |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>12</b> |  |
|   | Ввод и редактирование данных в табличном процессоре. Основы вычислений. Использование функций различных видов                              | 2         |  |
|   | Создание и форматирование таблицы в редакторе электронных таблиц   | 2         |  |
|   | Вычисление с помощью формул в электронной таблице. Работа со встроенными функциями в электронной таблице.                                  | 4         |  |
|   | Создание и работа с диаграммами и графиками. Обмен данными между текстовым процессором и электронной таблицей                              | 4         |  |
| <b>Тема 2.3.</b><br>Работа в программе подготовки и просмотра презентаций | <b>Содержание</b>  | <b>10</b> |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>10</b> |  |
|   | Изучение компьютерная презентации PowerPoint: основные и дополнительные возможности. Поэтапная разработка и настройка эффектов презентации | 2         |  |
|   | Основы работы со слайдом. Работа в презентации со шрифтом и текстом. Понятие темы слайда   | 2         |  |
|   | Добавление в слайды рисунков, звуковых эффектов, таблиц и диаграмм   | 2         |  |
|   | Настройка анимации объектов.   | 2         |  |
|   | Настройка показа и демонстрация результатов работы средствами мультимедиа  | 2         |  |
| <b>Тема 2.4.</b><br>Работа в системе управления базами данных             | <b>Содержание</b>  | <b>10</b> |  |
|   | <b>В том числе практических и лабораторных занятий</b>   | <b>10</b> |  |
|   | Проектирование БД и разработка ее компонентов  | 2         |  |
|   | Ввод данных в таблицы базы данных  | 2         |  |

|   |   |           |  |
|---|---|-----------|--|
|   | Создание простых запросов и форм.   | 2         |  |
|   | Создание и форматирование главной кнопочной формы.  | 2         |  |
|   | Создание отчетов  | 2         |  |
| <b>Тема 2.5.</b><br>Работа в графических редакторах                     | <b>Содержание</b>   | <b>16</b> |  |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>14</b> |  |
|   | Анализ системы автоматизированного проектирования. Компьютерная графика. Основы работы в Adobe Photoshop                    | 2         |  |
|   | Вставка и редактирование готового изображения с использованием программ растровой графики                                   | 2         |  |
|   | Работа с цветом с использованием программ растровой графики   | 2         |  |
|   | Работа со слоями с использованием программ растровой графики  | 2         |  |
|   | Работа со спецэффектами с использованием программ растровой графики   | 2         |  |
|   | Разработка проекта  | 4         |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Векторная графика  | 2         |  |
| <b>Раздел 3. Использование ресурсов технологий и сервисов Интернета</b> |   | <b>8</b>  |  |
| <b>Тема 3.1.</b><br>Работа с ресурсами Интернета                        | <b>Содержание</b>   | <b>8</b>  |  |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>6</b>  |  |
|   | Создание и обмен письмами электронной почты. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера           | 2         |  |
|   | Поиск, сортировка и анализ информации с помощью поисковых интернет-сайтов. Пересылка и публикация файлов данных в Интернете | 4         |  |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>СПС  | 2         |  |
| <b>Раздел 4. Обеспечение защиты информации в компьютерной системе</b>   |   | <b>10</b> |  |
| <b>Тема 4.1.</b> Защита информации при работе с офисными приложениями   | <b>Содержание</b>   | <b>10</b> |  |
|   | <b>В том числе практических и лабораторных занятий</b>  | <b>8</b>  |  |
|   | Использование штатных средств защиты информации в прикладных программах. Обеспечение безопасности в приложениях             | 2         |  |
|   | Настройка парольной защиты на открытие и запись файла   | 2         |  |

|  |   |                                 |          |
|--|---|---------------------------------|----------|
|  | Настройка защиты документа с помощью прав доступа   | 2                               |          |
|  | Защита информации в приложениях   | 2                               |          |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Методы защиты информации в приложениях | 2                               |          |
| <b>Промежуточная аттестация по МДК.04.01</b>   |   | <b>дифференцированный зачет</b> | <b>2</b> |
| <b>Учебная практика</b><br><b>Виды работ</b><br>Подключение периферийных устройств к разъемам системного блока.<br>Настройка и подготовка к работе принтера, сканера.<br>Создание схем, таблиц и формул в программе Microsoft Word.<br>Создание буклетов в программе Microsoft Publisher.<br>Ведение расчетов и построение диаграмм в программе Microsoft Excel.<br>Создание таблиц, форм, запросов и отчетов в программе Microsoft Access.<br>Создание презентации в программе PowerPoint.<br>Обработка графических объектов в Corel и PhotoShop.<br>Настройка локальной вычислительной сети.<br>Поиск информации в сети Интернет.<br>Обработка графической информации<br>Создание комплексного документа с использованием информации различных типов |   | <b>156</b>                      |          |
| <b>Производственная практика</b><br><b>Виды работ</b><br>Подготовка оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения.<br>Создание и управление текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах.<br>Использование ресурсов локальных вычислительных сетей и Интернета.<br>Обеспечение защиты информации в компьютерной системе.  |   | <b>84</b>                       |          |
| <b>Промежуточная аттестация</b>  |   | <b>12</b>                       |          |
| <b>Всего</b>   |   | <b>352</b>                      |          |

### 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1. Материально-техническое обеспечение

Кабинет «Информационных технологий» оснащен в соответствии с приложением 3 ОПОП-П.

Мастерская, необходимая для реализации модуля, оснащена в соответствии с приложением 3 ОПОП-П.

#### 3.2. Учебно-методическое обеспечение

##### 3.2.1. Основные печатные и/или электронные издания

1. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2018. – 172 с.

2. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2018 – 336с.

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-fed-eralnyj-zakon-ot-26-iyulya-2017-g-n-187-fz>.

4. Постановление Правительства РФ № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_291398](http://www.consultant.ru/document/cons_doc_LAW_291398).

5. Приказ Федеральной службы по техническому и экспортному контролю № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: <https://rg.ru/2018/02/13/fstek-prikaz-227-site-dok.html>.

6. Давыдова, Е. М. Организация защиты объектов критической информационной инфраструктуры: Учебно-методическое пособие [Электронный ресурс] / Е. М. Давыдова, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 20 с. [Электронный ресурс]: — Режим доступа: <https://edu.tusur.ru/publications/10003>.

##### 3.2.2. Дополнительные источники:

1. Киселев С.В. Оператор ЭВМ: учеб. пособие для студ. учреждений сред. проф. образования /. – 7-е изд., испр. – М.: Издательский центр «Академия», 2014.

2. Коньков, К. А. Устройство и функционирование ОС Windows. Практикум к курсу Операционные системы. /Учебное пособие // К.А. Коньков. М.: Бином, Лаборатория знаний Интуит, 2013.

3. Струмпэ Н.В. Оператор ЭВМ. Практические работы: учеб. пособие для нач. проф. образования / – 6-е изд., стер. – М.: Издательский центр «Академия», 2013.



#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

| Код ПК, ОК   | Критерии оценки результата<br>(показатели освоённости<br>компетенций)  | Формы контроля и методы<br>оценки   |
|--|--|---|
| ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить установку, настройку и обслуживание программного обеспечения                 | Демонстрировать умения и практические навыки в подготовке оборудования компьютерной системы к работе, производить установку, настройку и обслуживание программного обеспечения | 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 4.2 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах | Проявление умения и практического опыта в работе с текстовыми документами, таблицами и презентациями, а также базами данных  |   |
| ПК 4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета  | Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации  |   |
| ПК 4.4 Обеспечивать применение средств защиты информации в компьютерной системе  | Применение средств защиты информации в компьютерной системе  |   |

**Приложение 1.5**

к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

**Рабочая программа профессионального модуля**

**«ПМ.05 КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА**

**ИНФОРМАТИЗАЦИИ»**

## СОДЕРЖАНИЕ

|  |           |
|--|-----------|
| <b>1. Общая характеристика .....</b>   | <b>84</b> |
| 1.1. Цель и место профессионального модуля в структуре образовательной программы | 84        |
| 1.2. Планируемые результаты освоения профессионального модуля .....              | 84        |
| 1.3. Обоснование часов вариативной части ОПОП-П.....                             | 85        |
| <b>2. Структура и содержание профессионального модуля .....</b>                  | <b>86</b> |
| 2.1. Трудоемкость освоения модуля .....  | 86        |
| 2.2. Структура профессионального модуля .....                                    | 86        |
| 2.3. Содержание профессионального модуля .....                                   | 88        |
| <b>3. Условия реализации профессионального модуля .....</b>                      | <b>94</b> |
| 3.1. Материально-техническое обеспечение .....                                   | 94        |
| 3.2. Учебно-методическое обеспечение .....                                       | 94        |
| <b>4. Контроль и оценка результатов освоения профессионального модуля.....</b>   | <b>95</b> |

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ « ПМ.05 КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ»

## 1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: обеспечение комплексной системы защиты информации объекта информатизации.

Профессиональный модуль включен в вариативную часть профессионального цикла образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

## 1.2. Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ОПОП-П).

В результате освоения профессионального модуля обучающийся должен:

| Код ОК, ПК | Уметь   | Знать  | Владеть навыками   |
|------------|---|--|--|
| ОК.09      | <ul style="list-style-type: none"> <li>– понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы</li> <li>– участвовать в диалогах на знакомые общие и профессиональные темы</li> <li>– строить простые высказывания о себе и о своей профессиональной деятельности</li> <li>– кратко обосновывать и объяснять свои действия (текущие и планируемые)</li> <li>– писать простые связные сообщения на знакомые или интересующие профессиональные темы</li> </ul> | <ul style="list-style-type: none"> <li>– правила построения простых и сложных предложений на профессиональные темы</li> <li>– основные общеупотребительные глаголы (бытовая и профессиональная лексика)</li> <li>– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности</li> <li>– особенности произношения</li> <li>– правила чтения текстов профессиональной направленности</li> </ul> | -  |
| ПК 5.1.    | <ul style="list-style-type: none"> <li>– управлять защитой информации на объектах информатизации</li> <li>– проводить аудит защищенности информации на объекте информатизации</li> <li>– внедрять организационные меры по</li> </ul>  | <ul style="list-style-type: none"> <li>– направления деятельности по организационной защите информации</li> <li>– требования по обеспечению информационной безопасности на объектах критической информационной инфраструктуры (КИИ), в отношении которых отсутствует необходимость присвоения им категорий</li> </ul>  | <ul style="list-style-type: none"> <li>– внедрять программы и методики защиты на объектах</li> <li>– участвовать в оценке качества защиты объекта</li> </ul> |

|         |   |  |  |
|---------|---|--|--|
|         | защите информации на объекте информатизации   | значимости, в процессе их эксплуатации   |  |
| ПК 5.2. | <ul style="list-style-type: none"> <li>– вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации</li> <li>– разработка организационно-распорядительных документов по защите информации на объектах защиты</li> </ul> | <ul style="list-style-type: none"> <li>– документы, определяющие регулирование отношений в области обеспечения безопасности КИИ</li> <li>– требования по обеспечению безопасности объектов информатизации, в том числе значимых объектов критической информационной инфраструктуры</li> <li>– виды носителей конфиденциальной безопасности информации</li> </ul> | <ul style="list-style-type: none"> <li>– готовить организационные документы, регламентирующие работу по защите информации</li> <li>– вести учет работ и объектов, подлежащих защите</li> </ul> |
| ПК 5.3. | <ul style="list-style-type: none"> <li>– находить уязвимости системы защиты информации</li> <li>– разрабатывать модели угроз модели угроз объекта информатизации</li> </ul>   | <ul style="list-style-type: none"> <li>– модели угроз и выбор мер защиты объектов защиты в том числе объектов КИИ</li> <li>– требования к созданию систем безопасности объектов информатизации</li> </ul>  | <ul style="list-style-type: none"> <li>– анализировать уязвимости системы защиты информации</li> <li>– определять причины возникновения угроз безопасности</li> </ul>                          |

### 1.3. Обоснование часов вариативной части ОПОП-П

| №№ п/п | Дополнительные профессиональные компетенции  | Дополнительные знания, умения, навыки   | №, наименование темы | Объем часов | Обоснование включения в рабочую программу |
|--------|--|---|----------------------|-------------|---|
| ПК 5.1 | Участвовать в разработке и внедрении программ и методик организации защиты информации на объекте | <b>Навыки:</b> <ul style="list-style-type: none"> <li>– Внедрять программы и методики защиты на объектах</li> <li>– Участвовать в оценке качества защиты объекта</li> </ul> <b>Умения:</b> <ul style="list-style-type: none"> <li>– Управлять защитой информации на объектах информатизации</li> <li>– Проводить аудит защищенности информации на объекте информатизации</li> <li>– Внедрять организационные меры по защите информации на объекте информатизации</li> </ul> <b>Знания:</b> <ul style="list-style-type: none"> <li>– Направления деятельности по организационной защите информации</li> <li>– Требования по обеспечению информационной безопасности на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости, в процессе их эксплуатации</li> </ul> |                      |             |   |
| ПК 5.2 | Осуществлять планирование и организацию выполнения мероприятий по защите информации              | <b>Навыки:</b> <ul style="list-style-type: none"> <li>– Готовить организационные документы, регламентирующие работу по защите информации</li> <li>– Вести учет работ и объектов, подлежащих защите</li> </ul> <b>Умения:</b> <ul style="list-style-type: none"> <li>– Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации</li> <li>– Разработка организационно-распорядительных документов по</li> </ul>   |                      |             |   |

|        |  |   |  |  |  |
|--------|--|---|--|--|--|
|        |  | защите информации на объектах защиты<br><b>Знания:</b><br>– Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ<br>– Требования по обеспечению безопасности объектов информатизации, в том числе значимых объектов критической информационной инфраструктуры<br>– Виды носителей конфиденциальной безопасности информации  |  |  |  |
| ПК 5.3 | Выявлять и анализировать возможные угрозы информационной безопасности объектов | <b>Навыки:</b><br>– Анализировать уязвимости системы защиты информации<br>– Определять причины возникновения угроз безопасности<br><b>Умения:</b><br>– Находить уязвимости системы защиты информации<br>– Разрабатывать модели угроз модели угроз объекта информатизации<br><b>Знания:</b><br>– Модели угроз и выбор мер защиты объектов защиты в том числе объектов КИИ<br>– Требования к созданию систем безопасности объектов информатизации |  |  |  |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.1. Трудоемкость освоения модуля

| Наименование составных частей модуля  | Объем в часах | В т.ч. в форме практической подготовки |
|---|---------------|--|
| Учебные занятия   | 152           | 112                                    |
| Курсовая работа (проект)  | -             | -                                      |
| Самостоятельная работа  | 22            |  |
| Практика, в т.ч.:   | 96            | 96                                     |
| учебная   | 12            | 12                                     |
| производственная  | 84            | 84                                     |
| Промежуточная аттестация, в том числе:<br>МДК 05.01 в форме дифзачета<br>МДК 05.02. в форме дифзачета<br>МДК 05.03 в форме дифзачета<br>ПМ 05 | 12            |  |
| Всего   | 282           | 208                                    |

### 2.2. Структура профессионального модуля

| Код ОК, ПК                     | Наименования разделов профессионального модуля                                 | Всего, час. | В т.ч. в форме практической подготовки | Обучение по МДК, в т.ч.: | Учебные занятия | Курсовая работа (проект) | Самостоятельная работа | Промежуточная аттестация | Учебная практика | Производственная практика |
|--------------------------------|--|-------------|--|--------------------------|-----------------|--------------------------|------------------------|--------------------------|------------------|---------------------------|
| 1                              | 2  | 3           | 4                                      | 5                        | 6               | 7                        | 8                      |                          | 9                | 10                        |
| ОК 05; ПК 5.1. ПК 5.2. ПК 5.3. | <b>Раздел 1</b> Обеспечение безопасности ИТ-инфраструктуры объекта защиты      | <b>66</b>   | <b>40</b>                              | <b>66</b>                | 60              | -                        | 6                      |                          |                  |                           |
| ОК 05; ПК 5.1. ПК 5.2. ПК 5.3. | <b>Раздел 2</b> Организация и технология работы с конфиденциальной информацией | <b>52</b>   | <b>32</b>                              | <b>52</b>                | 44              | -                        | 8                      |                          |                  |                           |
| ОК 05; ПК 5.1. ПК 5.2. ПК 5.3. | <b>Раздел 3</b> Комплексная системы защиты объекта                             | <b>56</b>   | <b>40</b>                              | <b>56</b>                | 48              | -                        | 8                      |                          |                  |                           |
|                                | Учебная практика   | <b>12</b>   | <b>12</b>                              |                          |                 |                          |                        |                          | <b>12</b>        |                           |
|                                | Производственная практика  | <b>84</b>   | <b>84</b>                              |                          |                 |                          |                        |                          |                  | <b>84</b>                 |
|                                | Промежуточная аттестация   | <b>12</b>   |  |                          |                 |                          |                        | <i>12</i>                |                  |                           |
|                                | <b>Всего:</b>  | <b>282</b>  | <b>208</b>                             | <b>174</b>               | <b>152</b>      | <b>-</b>                 | <b>22</b>              | <b>12</b>                | <b>12</b>        | <b>84</b>                 |

### 2.3. Содержание профессионального модуля

| Наименование разделов и тем  | Содержание учебного материала, практических и лабораторных занятия, курсовая работа (проект)                                 | Объем, ак. ч. / в том числе в форме практической подготовки, ак. ч | Коды компетенций, формированию которых способствует элемент программы |
|--|--|--|---|
| 1  | 2  | 3  | 4   |
| <b>Раздел 1. Обеспечение безопасности ИТ- инфраструктуры объекта защиты</b>  |  | <b>66/40</b>   |   |
| <b>МДК.05.01 Обеспечение безопасности ИТ- инфраструктуры объекта защиты</b>  |  | <b>66/40</b>   |   |
| <b>Тема 1.1.</b><br>Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети объекта защиты | <b>Содержание</b>  | <b>14</b>  | ОК 05, ПК 5.1, ПК 5.2, ПК 5.3   |
|  | Принципы построения комплексных систем защиты информации   | 2  |   |
|  | Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети                    | 2  |   |
|  | Основные механизмы защиты  | 2  |   |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>8</b>   |   |
|  | Изучение руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации | 4  |   |
|  | Изучение порядка деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации      | 2  |   |
|  | Изучение принципов построения комплексных систем защиты информации   | 2  |   |
| <b>Тема 1.2.</b> Основные механизмы защиты. Мониторинг и оперативное управление  | <b>Содержание</b>  | <b>14</b>  | ОК 05, ПК 5.1, ПК 5.2, ПК 5.3   |
|  | Мониторинг и оперативное управление; полномочное управление доступом   | 2  |   |
|  | Централизованная инвентаризация ресурсов локальной сети  |  |   |
|  | Удаленный контроль работоспособности средств защиты информации на рабочих станциях   | 2  |   |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>10</b>  |   |
|  | Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети                    | 2  |   |
|  | Централизованная инвентаризация ресурсов локальной сети  | 2  |   |
|  | Разграничение доступа к данным. Разграничение доступа к устройствам  | 2  |   |
|  | Аудит событий информационной безопасности в КСЗИ   | 2  |   |



|  |  |           |                               |
|--|--|-----------|-------------------------------|
|  | Замкнутая программная среда. Контроль целостности  | 2         |                               |
| <b>Тема 1.3.</b> Управление системой безопасности ИТ-инфраструктуры объекта защиты | <b>Содержание</b>  | <b>19</b> | ОК 05, ПК 5.1, ПК 5.2, ПК 5.3 |
|  | Управление серверами администрирования, управление группами администрирования  | 2         |                               |
|  | Управление клиентскими компьютерами, работа с отчетами, статистикой. Централизованный учет и управление программно-аппаратными средствами защиты информации              | 2         |                               |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>12</b> |                               |
|  | Проведение инспекций и учет изменений конфигурации защищаемых рабочих станций  | 2         |                               |
|  | Работа со сведениями в журнале регистрации событий. Теневое копирование  | 2         |                               |
|  | Администрирование системы антивирусной защиты в локальной сети   | 2         |                               |
|  | Управление жизненным циклом средств аутентификации   | 2         |                               |
|  | Анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств | 4         |                               |
|  | <b>В том числе самостоятельная работа обучающихся</b>  | <b>3</b>  |                               |
|  | Управление жизненным циклом и аудит средств аутентификации   |           |                               |
| <b>Тема 1.4.</b> Нормативные требования по управлению средствами защиты информации | <b>Содержание</b>  | <b>17</b> | ОК 05, ПК 5.1, ПК 5.2, ПК 5.3 |
|  | Нормативные требования ФСТЭК при обеспечении мер безопасности персональных данных, в государственных информационных системах   | 2         |                               |
|  | Требования безопасности к автоматизированным системам управления технологическими процессами   | 2         |                               |
|  | <b>В том числе практических и лабораторных занятий</b>   | <b>10</b> |                               |
|  | Разработка политики безопасности информации автоматизированных систем  | 4         |                               |
|  | Разработка организационных мероприятий по обеспечению безопасности информации в автоматизированных системах  | 4         |                               |
|  | Оценка защищенности автоматизированных систем с помощью типовых программных средств  | 2         |                               |
|  | <b>В том числе самостоятельная работа обучающихся</b>  | <b>3</b>  |                               |
|  | Контроль работоспособности средств защиты информации на рабочих станциях   |           |                               |
| <b>Промежуточная аттестация по МДК.05.01</b>                                       |  | <b>2</b>  |                               |
| <b>дифференцированный зачет</b>  |  |           |                               |

|  |   |              |                               |
|--|---|--------------|-------------------------------|
| <b>Раздел 2. Организация и технология работы с конфиденциальной информацией</b>                |   | <b>52/32</b> |                               |
| <b>МДК.05.02 Организация и технология работы с конфиденциальной информацией</b>                |   | <b>52/32</b> |                               |
| <b>Тема 2.1.</b><br>Организационные меры безопасности объектов защиты в том числе объектов КИИ | <b>Содержание</b>   | <b>17</b>    | ОК 05, ПК 5.1, ПК 5.2, ПК 5.3 |
|  | Характеристики потенциально опасных объектов. Понятие критической информационной инфраструктуры. Документы, определяющие регулирование отношений в области обеспечения безопасности КИИ | 2            |                               |
|  | Категорирование объектов информатизации. Критерии значимости объектов КИИ РФ и их значения  | 2            |                               |
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>10</b>    |                               |
|  | Анализ документов, определяющих регулирование отношений в области обеспечения безопасности КИИ  | 2            |                               |
|  | Оценка безопасности объекта информатизации  | 2            |                               |
|  | Анализ Постановления от 8 февраля 2018 года №127. О порядке категорирования объектов критической информационной инфраструктуры  | 2            |                               |
|  | Анализ Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»   | 2            |                               |
|  | Классификация АСУТП по сфере функционирования, по виду системы, по Приказу ФСТЭК России №31   | 2            |                               |
|  | <b>В том числе самостоятельная работа обучающихся</b>   | <b>3</b>     |                               |
|  | Виды злоумышленников и их возможностей  |              |                               |
| <b>Тема 2.2.</b> Модели угроз и выбор мер защиты объектов защиты в том числе объектов КИИ      | <b>Содержание</b>   | <b>18</b>    | ОК 05, ПК 5.1, ПК 5.2, ПК 5.3 |
|  | Классификация уязвимостей информационной системы, причины возникновения угроз безопасности. Нарушители ИБ объектов КИИ  | 2            |                               |
|  | Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Анализ угроз и разработка модели угроз  | 2            |                               |
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>12</b>    |                               |
|  | Классификация АСУТП по сфере функционирования, по виду системы, по Приказу ФСТЭК России №31   | 2            |                               |
|  | Определение требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры  | 2            |                               |

|  |   |              |                               |
|--|---|--------------|-------------------------------|
|  | Анализ приказа № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»       | 2            |                               |
|  | Классификация уязвимостей информационной системы, модель угроз  | 2            |                               |
|  | Проектирование системы безопасности значимого объекта КИИ   | 4            |                               |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Состав системы безопасности значимых объектов  | <b>2</b>     |                               |
| <b>Тема 2.3</b><br>Организационно-распорядительные документы по обеспечению безопасности объектов в том числе объектов КИИ | <b>Содержание</b>   | <b>15</b>    | ОК 05, ПК 5.1, ПК 5.2, ПК 5.3 |
|  | Государственный контроль в области обеспечения безопасности значимых объектов КИИ. Правила выбора средств защиты информации для реализации организационных и технических мер  | 2            |                               |
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>10</b>    |                               |
|  | Анализ организационно-распорядительных документов по безопасности значимых объектов   | 2            |                               |
|  | Формирование технического задания на создание или модификацию системы защиты объекта критической информационной инфраструктуры  | 2            |                               |
|  | Изучение порядка и правил функционирования системы безопасности значимых объектов КИИ   | 2            |                               |
|  | Анализ приказа Федеральной службы по техническому и экспортному контролю № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» | 2            |                               |
|  | Разработка рабочей и эксплуатационной документации.   | 2            |                               |
|  | <b>В том числе самостоятельная работа обучающихся</b><br>Определение порядка и правил обеспечения безопасности объектов   | <b>3</b>     |                               |
| <b>Промежуточная аттестация по МДК.05.02 дифференцированный зачет</b>  |   | <b>2</b>     |                               |
| <b>Раздел 3. Обеспечение системы безопасности объекта защиты</b>   |   | <b>56/40</b> |                               |
| <b>МДК.05.03 Обеспечение системы безопасности объекта защиты</b>   |   | <b>56/40</b> |                               |
| <b>Тема 3.1.</b> Структура комплексной системы безопасности  | <b>Содержание</b>   | <b>16</b>    | ОК 05, ПК 5.1, ПК 5.2, ПК 5.3 |
|  | Основные подходы и требования к организации комплексной системы защиты информации. Управление безопасностью. Оценка уязвимостей системы безопасности.   | 2            |                               |

|  |   |           |  |
|--|---|-----------|--|
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>10</b> |  |
|  | Составление организационной структуры организации и определение ее сферы деятельности   | 2         |  |
|  | Выявление информационных активов организации  | 2         |  |
|  | Выявление структурных единиц, работающих с конфиденциальной информацией   | 2         |  |
|  | Анализ информационной системы объекта защиты  | 4         |  |
|  | <b>В том числе самостоятельная работа обучающихся</b>   | 4         |  |
|  | Проведение аудита информационной безопасности виртуального предприятия  |           |  |
| <b>Тема 3.2.</b> Состав и структура системы безопасности | <b>Содержание</b>   | <b>6</b>  | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|  | Состав и структура системы безопасности. Направления защиты объекта информатизации. Средства и способы защиты. Организации работы в чрезвычайной ситуации. Состав службы безопасности.  | 2         |  |
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>4</b>  |  |
|  | Разработка структуры системы безопасности организации   | 4         |  |
| <b>Тема 3.3</b> Построение системы защиты информации     | <b>Содержание</b>   | <b>32</b> | ОК 09; ПК 3.1.<br>ПК 3.2.<br>ПК 3.3.<br>ПК 3.4. ПК 3.5 |
|  | Планирование мероприятий по защите конфиденциальной информации. Формирование политики информационной безопасности на предприятии. Построение системы защиты информации объекта информатизации. Анализ рисков системы безопасности | 2         |  |
|  | <b>В том числе практических и лабораторных занятий</b>  | <b>26</b> |  |
|  | Характеристика информации ограниченного доступа, циркулирующей на объекте защиты  | 4         |  |
|  | Характеристика организационного обеспечения информационной безопасности   | 2         |  |
|  | Характеристика системы контроля управления доступом объекта защиты  | 2         |  |
|  | Характеристика инженерно-технического обеспечения системы защиты информации   | 2         |  |
|  | Характеристика программно-аппаратного обеспечения системы защиты информации   | 2         |  |
|  | Определение угроз информационной безопасности   | 4         |  |
|  | Выделение недостатки существующей КСЗИ. Анализ рисков КСЗИ.   | 2         |  |
|  | Усовершенствование организационного обеспечения и СКУД объекта защиты   | 2         |  |
|  | Усовершенствование инженерно-технического обеспечение комплексной системы защиты информации   | 2         |  |

|   |  |                                 |          |
|---|--|---------------------------------|----------|
|   | Усовершенствование программно-аппаратного обеспечения комплексной системы защиты информации                              | 2                               |          |
|   | Анализ рисков разработанной КСЗИ   | 2                               |          |
|   | <b>В том числе самостоятельная работа обучающихся</b><br>Политика информационной безопасности в отечественных стандартах | 4                               |          |
| <b>Промежуточная аттестация по МДК.05.03</b>  |  | <b>дифференцированный зачет</b> | <b>2</b> |
| <b>Учебная практика</b><br><b>Виды работ:</b> <ul style="list-style-type: none"> <li>– Разработка мер обеспечения информационной безопасности»</li> <li>– Разработка основных принципов построения системы информационной безопасности</li> <li>– Выявление требований к аппаратным и программным средствам</li> <li>– Подбор антивирусного средства для конкретного объекта</li> <li>– Подготовка документа Политики информационной безопасности</li> <li>–</li> </ul>   |  | <b>12</b>                       |          |
| <b>Производственная практика</b><br><b>Виды работ:</b> <ul style="list-style-type: none"> <li>– Анализ структуры организации и информационных процессов</li> <li>– Выявление опасностей и угроз объекта информатизации</li> <li>– Анализ структуры и типов защищаемой информации, по видам тайны и степеням конфиденциальности</li> <li>– Определение категории информационных ресурсов, подлежащих защите</li> <li>– Анализ существующей системы защиты объекта</li> <li>– Оценка степени защищенности объекта</li> <li>– Разработка нормативных документов необходимых для организации работы с персоналом, имеющим доступ к конфиденциальной информации</li> <li>– Разработка политики информационной безопасности</li> <li>– Разработка модели угроз информационной безопасности</li> </ul> |  | <b>84</b>                       |          |
| <b>Экзамен по профессиональному модулю</b>  |  | <b>12</b>                       |          |
| <b>Всего</b>  |  | <b>282</b>                      |          |

### 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1. Материально-техническое обеспечение

Мастерская «Кибербезопасности», оснащена в соответствии с приложением 3 ОПОП-П.

Базы практики (мастерские), оснащены в соответствии с приложением 3 ОПОП-П. и с п. 3.1.2. образовательной программы.

#### 3.2. Учебно-методическое обеспечение

##### 3.2.1. Основные печатные и/или электронные издания

1. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2018. – 172 с.

2. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2018 – 336с.

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kii/285-zakony/1610-fed-eralnyj-zakon-ot-26-iyulya-2017-g-n-187-fz>.

4. Постановление Правительства РФ № 162 от 17.02.2018 г. «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_291398](http://www.consultant.ru/document/cons_doc_LAW_291398).

5. Приказ Федеральной службы по техническому и экспортному контролю № 227 от 06.12.2017 г. «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]: — Режим доступа: <https://rg.ru/2018/02/13/fstek-prikaz-227-site-dok.html>.

6. Давыдова, Е. М. Организация защиты объектов критической информационной инфраструктуры: Учебно-методическое пособие [Электронный ресурс] / Е. М. Давыдова, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 20 с. [Электронный ресурс]: — Режим доступа: <https://edu.tusur.ru/publications/10003>.

#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

| Код ПК, ОК  | Критерии оценки<br>результата<br>(показатели освоенности<br>компетенций)   | Формы контроля и методы<br>оценки   |
|---|--|---|
| ПК 5.1 Участвовать в разработке и внедрении программ и методик организации защиты информации на объекте | Участвует в оценке качества защиты объекта<br>Управляет защитой информации на объектах информатизации<br>Проводит аудит защищенности информации на объекте информатизации<br>Внедряет организационные меры по защите информации на объекте информатизации                                      | 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 5.2 Осуществлять планирование и организацию выполнения мероприятий по защите информации              | Готовит организационные документы, регламентирующие работу по защите информации<br>Ведёт учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации<br>Разрабатывает организационно-распорядительные документы по защите информации на объектах защиты | 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 5.3 Выявлять и анализировать возможные угрозы информационной безопасности объектов                   | Проводит анализ уязвимостей системы защиты информации<br>Определяет причины возникновения угроз безопасности<br>Находит уязвимости системы защиты информации<br>Разрабатывает модели угроз модели угроз объекта информатизации   | 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 |

|   |  |   |
|---|--|---|
| ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках | Понимает тексты на базовые профессиональные темы, участвует в диалогах на профессиональные темы обосновывает и объясняет свои действия, пишет простые связные сообщения на профессиональные темы | 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 |
|---|--|---|