Смоленский колледж телекоммуникаций (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

УТВЕРЖДАЮ

Зам. директора по учебной работе

_____ И.А. Овчинникова

«14» 05 2025 г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00F35A15D2181C25968B35D1B1F78BE7DA
Владелец: Овчинникова Ирина Александровна
Действителен: с 09.04.2026 до 03.07.2027

# РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА МДК 02.02 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

в составе

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

среднего профессионального образования

для специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

г. Смоленск, 2025

РАССМОТРЕНО
на заседании методической комиссии
дисциплин сетей связи
Председатель _____ Е.Н. Кожекина
Протокол №11 от «14» 05 2025 г.

СОГЛАСОВАНО
Инженер ООО «Арсенал 67»
_____ Р.Н. Михайлов.
14.05.2025г.

СОГЛАСОВАНО
Методист _____ О.Г. Ряска
«14» 05 2025 г.

СОГЛАСОВАНО
на заседании методической комиссии
информационной безопасности и сетевого
администрирования
Председатель _____ О.Г.Ряска
Протокол №11 от «14» 05 2025 г.

Составитель: Королев Е.В. – преподаватель первой квалификационной категории СКТ(ф)СПбГУТ.

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерства образования и науки РФ от 09.12.2016 г. №1551 (ред.03.07.2024),
с учетом примерной основной образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, разработанной ФУМО в системе СПО по УГС 10.00.00 «Информационная безопасность».

СОДЕРЖАНИЕ

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА

## 1.1. Область применения программы

Рабочая программа междисциплинарного курса МДК 02.02 Криптографическая защита информации (далее программа МДК) – является частью рабочей программы профессионального модуля ПМ 02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты подготовки специалистов среднего звена в соответствии с ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

## 1.2. Цели и задачи, требования к результатам освоения МДК

В ходе освоения междисциплинарного курса студент должен овладеть следующими общими и профессиональными компетенциями:

| Код | Наименование видов деятельности и компетенций |
|---|---|
| ОК 01 | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. |
| ОК 02 | Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности. |
| ОК 03 | Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях. |
| ОК 04 | Эффективно взаимодействовать и работать в коллективе и команде. |
| ВД 2. | Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты |
| ПК 2.1 | Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей. |
| ПК 2.2 | Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях. |
| ПК 2.3 | Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями. |

В результате освоения междисциплинарного курса студент должен:

| | |
|---|---|
| Иметь практический опыт | в ПО 1- установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей;<br>в ПО2 - поддержании бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях;<br>в ПО3 - защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями |

| | |
|---|---|
| уметь | У 1 -выявлять и оценивать угрозы безопасности информации в ИТКС;<br>У 2 -настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;<br>У 3 - проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;<br>У 4- проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;<br>У 5 - проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;<br>У 6-проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;<br>У 7- проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации. |
| знать | З 1- возможные угрозы безопасности информации в ИТКС;<br>З 2 - способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее;<br>З 3 - типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;<br>З 5 - порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;<br>З 6 - организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;<br>З 7 - порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации. |

Вариативная часть

| | |
|---|---|
| уметь | У 8 - определять рациональные методы и средства защиты на объектах и оценивать их эффективность; |
| знать | З 9 - основные протоколы идентификации и аутентификации в телекоммуникационных системах;<br>З 10 - особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; |

## 2. СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА

2.1 Виды учебной деятельности и количество часов, отводимое на освоение МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

| **Вид учебной работы** | **Объём часов** | | |
|---|---|---|---|
| | **Обязательная часть** | **Вариативная часть** | **Всего** |
| Максимальная учебная нагрузка (всего) | 128 | 50 | **178** |
| Обязательная аудиторная учебная нагрузка (всего) | 120 | 28 | **148** |
| в том числе: | | | |
| теоретическое обучение | 76* | 28 | **104*** |
| практические занятия | 24 | - | **24** |
| лабораторные занятия | 20 | - | **20** |
| курсовое проектирование | - | - | **-** |
| консультации | | - | **2** |
| *Самостоятельная работа* | - | 22 | **22** |
| Промежуточная аттестация - другие формы (6 семестр) | - | - | **2*** |
| Промежуточная аттестация Экзамен (7 семестр) | - | - | **6** |

*Промежуточная аттестация в 6 семестре проводится за счет часов лекционной нагрузки

**2.2. Тематический план и содержание МДК 02.02 Криптографическая защита информации**

| **Разделы** | **Код ПК** | **Всего часов (макс. учебная нагрузка и практики)** | **Объём времени** | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Обязательная аудиторная учебная нагрузка студента, (часов) | | | | Самостоятельная работа студента, часов | |
| | | | Всего | В том числе | | | Всего часов | В том числе |
| | | | | Лекции | Лаборат. занятия и практич. занятия | Курсовая работа (проект) | | Курсовая работа (проект) |
| | ***1*** | ***2*** | ***3*** | ***4*** | ***5*** | ***6*** | ***7*** | ***8*** |
| **Тема 2.1. Основы криптографических методов защиты информации** | ПК 2.1 - 2.3 | 40 | 32 | 30 | 2 | | 8 | - |
| **Тема 2.2. Современные стандарты шифрования** | ПК 2.1 - 2.3 | 41 | 34 | 30 | 4 | - | 7 | - |
| **Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий** | ПК 2.1 - 2.3 | 87 | 80 | 42 | 38 | | 7 | - |
| Промежуточная аттестация | | 8 | 2 | 2 | - | - | - | - |
| Консультации | | 2 | - | - | - | - | - | - |
| **Всего** | | **178** | **148** | **104** | **44** | | **22** | **-** |

| Наименование разделов междисциплинарного курса (МДК) и тем | Содержание учебного материала, лабораторных и практических занятий, самостоятельной работы обучающихся, курсового проекта | Объем часов | |
|---|---|---|---|
| | | Обяз. часть | Вар. часть |
| 1 | 2 | 3 | 4 |
| **ПМ.02.Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты**<br>**Раздел 2. Криптографическая защита информации**<br>**МДК 02.02.Криптографическая защита информации** | | | |
| **Тема 2.1. Основы криптографических методов защиты информации**<br><br>**40 ч** | Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. | 2 | - |
| | Криптографические методы. | 2 | - |
| | Шифрование. Кодирование. Стеганография. Сжатие. | 2 | - |
| | Математика криптографии. | 2 | - |
| | Бинарные операции. Арифметика целых чисел. | 2 | |
| | Модульная арифметика. Матрицы. Линейное сравнение. | - | 2 |
| | Традиционные шифры перестановки. | 2 | - |
| | Шифры перестановки. | - | 2 |
| | Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования. | 2 | |
| | Традиционные шифры замены. | - | 2 |
| | Шифры замены. Шифры многоалфавитной замены. Частотность символов. | 2 | - |
| | Криптоанализ. | - | 2 |
| | Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста . | 2 | - |
| | Компьютерное шифрование. | - | 2 |
| | Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей. | 2 | - |
| | **Практические занятия** | **2** | |
| | ПЗ№1 Использование алгоритмов шифрования для сокрытия содержимого файла с применением OpenSSL | 2 | - |
| | **Самостоятельная работа студентов:**<br>составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - | - | 8 |

| | | | |
|---|---|---|---|
| | ресурсами | | |
| **Тема 2.2. Современные стандарты шифрования 41ч** | Симметричное шифрование. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. | 2 | - |
| | Анализ DES. Многократное применение DES. Безопасность DES. | 2 | - |
| | Усовершенствованный стандарт шифрования AES. | 2 | - |
| | Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES. | 2 | - |
| | Российские стандарты симметричного шифрования . | - | 2 |
| | Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. | 2 | - |
| | Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. | 2 | - |
| | Проблема распределения ключей симметричного шифрования. | 2 | - |
| | Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. | 2 | - |
| | Асимметричное шифрование. | - | 2 |
| | Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы. | 2 | - |
| | Криптографическая система Эль-Гамаля. | 2 | - |
| | Криптосистемы на основе метода эллиптических кривых. ЭЦП. | - | 2 |
| | Российские стандарты асимметричного шифрования. | - | 2 |
| | ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов. | 2 | - |
| | **Практические занятия** | **4** | |
| | ПЗ№2 Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа. | 2 | - |
| | ПЗ№3Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители | 2 | - |
| | **Самостоятельная работа студентов:**<br>составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет – ресурсами | - | **7** |
| **Тема 2.3. Криптографические методы обеспечения безопасности** | Целостность сообщения. | 2 | - |
| | Случайная модель Orac1e. Установление подлинности сообщения. Криптографические хэш-функции. | 2 | - |
| | MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. | 2 | - |
| | Атаки на хэш-функции. | - | 2 |
| | Электронная цифровая подпись. | 2 | - |

| | | | |
|---|---|---|---|
| **сетевых технологий**<br><br>**87 ч** | Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. | 2 | - |
| | Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2012. | 2 | - |
| | Установление подлинности объекта. | 2 | - |
| | Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. | - | 2 |
| | Биометрические средства идентификации. Электронные ключи и карты. Токены. | 2 | - |
| | Проблемы распределения открытого ключа асимметричного шифрования.<br>Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI. | 2 | - |
| | Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне. | 2 | - |
| | Электронная почта. Архитектура e-mail. PGP. S/M1ME . | - | 2 |
| | Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне. | 2 | - |
| | Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети | - | 2 |
| | Защита информации в сетях организованных по технологии беспроводного доступа.<br>IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16. | 2 | - |
| | Защита информации в сетях сотовой связи. | - | 2 |
| | A3. A8.A5/3. Атаки на алгоритмы. | 2 | - |
| | Перспективы развития беспроводной мобильной связи.<br>Криптовалюты.<br>Биткоин. Блокчейн-системы Ethereum. | 2 | - |
| | Перспективы развития криптографии. | 2 | - |
| | Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов. | 2 | - |
| | **Практические занятия** | 18 | |
| | ПЗ №4 Использование алгоритмов хеширования для подтверждения неизменности файла с применением OpenSSL. | 2 | - |
| | ПЗ№5 Создание цифровых сертификатов X.509 и преобразование их форматов с применением пакета OpenSSL. | 2 | - |

| | | | |
|---|---|---|---|
| | ПЗ№6 Создание центра сертификации с поддержкой списков отозванных сертификатов с применением пакета OpenSSL. | 2 | - |
| | ПЗ№7 Создание центра сертификации с поддержкой протокола OCSP с применением пакета OpenSSL. | 2 | - |
| | ПЗ№8 Применение «сетей доверия» для распространения сертификатов. | 2 | - |
| | ПЗ№9 Применение электронной цифровой подписи для проверки авторства и неизменности файла. | 2 | - |
| | ПЗ№10 Изучение каркаса обеспечения безопасности ISAKMP на примере протокола туннелированияIPSec. | 2 | - |
| | ПЗ№11 Безопасное хранение файлов с применением криптоконтейнеров. | 2 | - |
| | ПЗ№12Создание файловой системы с поддержкой прозрачного шифрования. | 2 | - |
| | **Лабораторные занятия** | 20 | |
| | ЛЗ№1 Система обнаружения руткитов tripwire. | 2 | - |
| | ЛЗ№2 Применение stunnel для шифрования данных, передаваемых с помощью протокола telnet. | 2 | - |
| | ЛЗ№3Хеширование по алгоритмам MD5, SHA-1, SHA-256, SHA-512. Оценка криптостойкости. | 2 | - |
| | ЛЗ№ 4Перехват и расшифровка трафика. Определение типа шифрования. | 2 | - |
| | ЛЗ№5 Знакомство с действующим криптографическим ПО. | 2 | - |
| | ЛЗ№6Обзор инструментов KaliLinux. | 2 | - |
| | ЛЗ№7 Стресс-тесты сети. | 2 | - |
| | ЛЗ№8 Анализ уязвимостей в операционных системах и серверном ПО. | 2 | - |
| | ЛЗ№ 9Сканирование сетей. Перехват данных по сетям. | 2 | - |
| | ЛЗ№10 Атаки на пароли. Брутфорсинг. | 2 | - |
| | **Самостоятельная работа студентов:**<br>составление презентации, подготовка реферата, работа с дополнительной литературой и Интернет - ресурсами | - | 7 |
| **Всего** | | 118 | 50 |
| **Консультация** | | 2 | |
| **Промежуточная аттестация(6 семестр) - другая форма в виде тестирования** | | 2 | |
| **Промежуточная аттестация экзамен (7 семестр)** | | 6 | |
| **ВСЕГО** | | 178 | |

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МДК 02.02

**3.1. Для реализации программы междисциплинарного курса предусмотрены следующие специальное помещение:**

Лаборатория программных и программно-аппаратных средств защиты информации (Ауд.315)
Типовой комплект учебного оборудования «Сетевая безопасность» - 1 шт.;
Виртуальный тренажёр «Программные средства криптографии» - 1 шт.;
Учебно-практический стенд «Системы контроля и управления доступом» – 1 шт.;
Учебный стенд «Программные средства криптографии»– 1 шт.;
Набор программного обеспечения для развёртывания стенда «Программные средства криптографии» - 1 шт.;
Учебный стенд «Системы доверенной загрузки» – 1 шт.;
Учебный стенд «Программные средства защиты информации от несанкционированного доступа» – 1 шт.
Системный блок в комплекте с клавиатурой и мышью: процессор 6 ядер/12 потоков, оперативная память 16 Гб, твердотельный накопитель 1 480 Гб, твердотельный накопитель 2 1000 Гб – 13 шт.;
Локальная сеть с выходом в Интернет топологии «звезда», 1 Гб/сек.
Свободные дистрибутивы операционных систем Linux (Ubuntu, Debian, CentOS).

**3.2. Информационное обеспечение реализации программы**

**Электронные издания (электронные ресурсы)**

**Электронные издания (электронные ресурсы)**

ОИ.1 Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие / А. В. Бабаш. — 2-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 413 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215714

ОИ.2 Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563

ОИ.3 Маршаков, Д. В. Методы и средства криптографической защиты информации. Практический курс : учебное пособие / Д.В. Маршаков, Д.В. Фахти. — Москва : ИНФРА-М, 2022. — 76 с. — (Высшее образование). - ISBN 978-5-16-110842-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1891129

ОИ.4 Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 352 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-557-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189341

ОИ5. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022

Интернет ресурсы и источники:

Интернет ресурсы и источники:

1. Электронно-библиотечная система издательства «Лань» [Электронный ресурс]. – Режим доступа: e.lanbook.com
2. Электронно-библиотечная система «Ibooks.ru» [Электронный ресурс]. – Режим доступа: ibooks.ru
3. Электронно-библиотечная система «IPRbook» [Электронный ресурс]. – Режим доступа: iprbookshop.ru

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ МДК 02.02

| Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля | Критерии оценки | Методы оценки |
|---|---|---|
| ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей. | - выявлять и оценивать угрозы безопасности информации в ИТКС;<br>- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;<br>- проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;<br>- проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; | Дифференцированный зачет в форме тестирования<br>Защита отчетов по лабораторным занятиям и практическим занятиям |
| ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях. | - выявлять и оценивать угрозы безопасности информации в ИТКС;<br>- проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;<br>- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;<br>- проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации | Дифференцированный зачет в форме тестирования<br>Защита отчетов по лабораторным занятиям и практическим занятиям |

| | | |
|---|---|---|
| ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями. | - выявлять и оценивать угрозы безопасности информации в ИТКС;<br>- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;<br>- проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации; | Дифференцированный зачет в форме тестирования<br>Защита отчетов по лабораторным занятиям и практическим занятиям |

| | | |
|---|---|---|
| ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. | - обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;<br>- адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы<br><br>Экспертное наблюдение и оценка на лабораторных занятиях, при выполнении работ практической подготовки по учебной и производственной практикам<br><br>Экзамен квалификационный |
| ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности | - использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач | |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях | - демонстрация ответственности за принятые решения;<br>- обоснованность самоанализа и коррекция результатов собственной работы | |
| ОК 04. Эффективно взаимодействовать и работать в коллективе и команде | - обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;<br>- адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач | |

**Приложение 1**

## Лист изменений рабочей программы

| Содержание изменения, страница рабочей программы | Дата и номер протокола заседания МК | Основание для внесения изменения |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |