**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА» (СПбГУТ)**

**Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля**

СПбГУТ))) Документ подписан простой электронной подписью

Сертификат: 009b47d8b89b08d0f6
Владелец: Киричек Руслан Валентинович
Действителен с 13.02.2023 по 12.02.2028

УТВЕРЖДАЮ
Первый проректор – проректор по учебной работе
_____ А.В. Абилов
_____ 2023 г.

Регистрационный № 11.09.23/247

# РАБОЧАЯ ПРОГРАММА

# ПМ.03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ РАДИОСВЯЗИ, МОБИЛЬНОЙ СВЯЗИ И ТЕЛЕРАДИОВЕЩАНИЯ

(наименование профессионального модуля)

по специальности

11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания
(код и наименование специальности)

квалификация
специалист по системам радиосвязи, мобильной связи и телерадиовещания

Санкт-Петербург

2023

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена (индекс – ПМ.03) среднего профессионального образования по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 30 марта 2023 г., протокол №3.

СОГЛАСОВАНО

Директор филиала РТРС
Санкт-Петербургский РЦ» Р.Н. Евсеев

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена (индекс – ПМ.03) по специальности 11.02.18 системы радиосвязи, мобильной связи и телерадиовещания, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 30 марта 2023 г., протокол № 3.

Составитель:

Преподаватель _____ Н.В. Кривоносова
(подпись)

СОГЛАСОВАНО
Главный специалист НТБ УИОР _____ Р.Х. Ахтреева
(подпись)

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 9 (информационной безопасности телекоммуникационных систем)
1 февраля 2023 г., протокол № 6

Председатель предметной (цикловой) комиссии: _____ Н.В. Кривоносова
(подпись)

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля
8 февраля 2023 г., протокол № 3

Заместитель директора по учебной работе колледжа СПб ГУТ
_____ Н.В. Калинина
(подпись)

СОГЛАСОВАНО

Директор колледжа СПб ГУТ
_____ Т.Н. Сиротская
(подпись)

СОГЛАСОВАНО

Директор департамента ОКОД
_____ С.И. Ивасишин
(подпись)

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ. 03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ РАДИОСВЯЗИ, МОБИЛЬНОЙ СВЯЗИ И ТЕЛЕРАДИОВЕЩАНИЯ

## 1.1 Область применения рабочей программы

Рабочая программа профессионального модуля – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания.

## 1.2 Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности «Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания» и соответствующие ему общие компетенции и профессиональные компетенции:

1.2.1 Перечень общих компетенций и личностных результатов реализации программы воспитания

| | |
|---|---|
| ОК 01 | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам |
| ОК 02 | Использование современных средств 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 |
| ОК 05 | Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста |
| ОК 06 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения |
| ОК 07 | Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях |
| ОК 08 | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности |
| ОК 09 | Пользоваться профессиональной документацией на государственном и иностранном языках |
| ЛР1–ЛР4, ЛР9, ЛР10, ЛР13-ЛР15, ЛР20, ЛР23–ЛР28 | |

1.1.2 Перечень профессиональных компетенций

| Код | Наименование профессиональных компетенций |
|---|---|
| ПК 3.1 | Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. |

| | |
|---|---|
| ПК 3.2 | Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. |
| ПК 3.3 | Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. |

1.1.3. В результате освоения профессионального модуля студент должен:

| | |
|---|---|
| Иметь практический опыт | – анализе сетевой инфраструктуры;<br>– выявлении угроз и уязвимости в сетевой инфраструктуре;<br>– разработке комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;<br>– осуществлении текущего администрирования для защиты инфокоммуникационных сетей и систем связи;<br>– использовании специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи. |
| уметь | – классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;<br>– определять оптимальные способы обеспечения информационной безопасности;<br>– осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;<br>– выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;<br>– выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;<br>– защищать базы данных при помощи специализированных программных продуктов. |
| знать | – принципы построения систем радиосвязи, мобильной связи и телерадиовещания;<br>– международные стандарты информационной безопасности;<br>– акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;<br>– технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;<br>– классификацию угроз сетевой безопасности;<br>– методы и способы защиты информации, передаваемой по кабельным направляющим системам;<br>– правила проведения возможных проверок согласно нормативным документам ФСТЭК;<br>– средства защиты различных операционных систем и среды передачи информации |

**1.2. Количество часов, отводимое на освоение профессионального модуля**

Всего часов: **376 часов.**
Из них на освоение МДК:

**МДК.03.01.** Технология обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания- **196 часов.**

на практики учебную и производственную - **162 часа.**

## 2. СТРУКТУРА и содержание профессионального модуля

### 2.1. Структура профессионального модуля

| Коды профессиональных компетенций | Наименования разделов профессионального модуля | Суммарный объем нагрузки, час. | В т.ч. в форме практической подготовки | **Объем профессионального модуля, час.** | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Работа обучающихся во взаимодействии с преподавателем | | | | | | |
| | | | | Обучение по МДК, в час. | | | Практики | | Самостоятельная работа, часов | Промежуточная аттестация, часов |
| | | | | Всего, часов | Лабораторные работы и практические занятия, часов | в т.ч., курсовая работа (проект), часов | Учебная, часов | Производственная | | |
| ПК 3.1, ПК 3.2, ПК 3.3 ОК 01 – ОК 09 | Раздел 1. Обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания | **196** | 76 | **196** | 76 | - | 72 | | **36** | |
| Учебная практика | | **72** | 72 | | | | | | | |
| Производственная практика | | **90** | 90 | | | | | | | |
| Промежуточная аттестация | | **18** | | | | | | | | 18 |
| **Всего:** | | **376** | 238 | **196** | 76 | - | **72** | **90** | **36** | **18** |

**2.2 Тематический план и содержание профессионального модуля**

| Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем | Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) | | Объем часов |
|---|---|---|---|
| **Раздел 1. Обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания** | | | |
| **МДК.03.01. Технология обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания** | | | 196 |
| Тема 1.1. Основы безопасности информационных технологий | **Содержание учебного материала** | | |
| | **1** | **Занятие 1.** Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем. Основные причины обострения проблемы обеспечения безопасности информационных технологий. | 18 |
| | **2** | **Занятие 2.** Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. | |
| | **3** | **Занятие 3.** Идентификация и аутентификация пользователей. | |
| | **4** | **Занятие 4.** Угрозы безопасности информационных технологий. Классификация угроз безопасности. | |
| | **5** | **Занятие 5.** Принципы обеспечения безопасности информационных технологий. | |
| | **6** | **Занятие 6.** Принципы построения системы обеспечения безопасности информации в автоматизированной системе. | |
| | **7** | **Занятие 7.** Стандарты информационной безопасности систем мобильной связи | |
| | **8** | **Занятие 8.** Особенности решений по информационной безопасности в беспроводных стандартах IEEE 802.11, IEEE 802.16, DECT. | |
| | **9** | **Занятие 9.** Особенности решений по информационной безопасности в системах сотовой связи GSM, CDMA | |
| | **Лабораторные работы** | | |
| | **1** | **Занятие 10.** Анализ современных угроз информационной безопасности (часть 1). | 16 |
| | **2** | **Занятие 11.** Анализ современных угроз информационной безопасности (часть 2). | |
| | **3** | **Занятие 12.** Проектирование границ защиты (часть 1). | |
| | **4** | **Занятие 13.** Проектирование границ защиты (часть 2). | |
| | **5** | **Занятие 14.** Применение сертификатов для аутентификации (часть 1). | |
| | **6** | **Занятие 15.** Применение сертификатов для аутентификации (часть 2). | |
| | **7** | **Занятие 16.** Применение сертификатов для авторизации (часть 1). | |
| | **8** | **Занятие 17.** Применение сертификатов для авторизации (часть 1). | |
| | **Самостоятельная работа обучающихся** | | |

| | | | |
|---|---|---|---|
| | Составление доклада по перспективе и направлению развития программно-аппаратных средств защиты информации на основе публикаций в периодической специализированной аппаратуре | | 7 |
| Тема 1.2. Обеспечение безопасности информационных технологи | **Содержание учебного материала** | | |
| | **1** | **Занятие 18.** Особенности обеспечения информационной безопасности в компьютерных сетях. | 24 |
| | **2** | **Занятие 19.** Спецификация средств защиты в компьютерных сетях. | |
| | **3** | **Занятие 20.** Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Структура пакета. Шифрование. | |
| | **4** | **Занятие 21.** Типовые удаленные атаки и их характеристика. | |
| | **5** | **Занятие 22.** Принципы защиты распределенных вычислительных сетей. | |
| | **6** | **Занятие 23.** Принципы построения защищенных вычислительных сетей. | |
| | **7** | **Занятие 24.** Безопасность операционных систем | |
| | **8** | **Занятие 25.** Проблемы обеспечения безопасности операционных систем, угрозы безопасности, защищенная операционная система | |
| | **9** | **Занятие 26.** Архитектура подсистемы защиты операционных систем | |
| | **10** | **Занятие 27.** Функции подсистемы идентификация и аутентификация | |
| | **11** | **Занятие 28.** Функции подсистемы авторизации доступа в операционные системы з | |
| | **12** | **Занятие 29.** Функции подсистемы разграничения доступа и аудит | |
| | **Лабораторные работы** | | |
| | **9** | **Занятие 30.** Установка СЗИ (на примере IWTM) (часть 1) | 24 |
| | **10** | **Занятие 31.** Установка СЗИ (на примере IWTM) (часть 2) | |
| | **11** | **Занятие 32.** Установка СЗИ (на примере IWTM) (часть 3) | |
| | **12** | **Занятие 33.** Установка межсетевого экрана (часть 1) | |
| | **13** | **Занятие 34**. Установка межсетевого экрана (часть 2) | |
| | **14** | **Занятие 35.** Установка межсетевого экрана (часть 3) | |
| | **15** | **Занятие 36.** Настройка правил фильтрации траффика DLP системой (часть 1) | |
| | **16** | **Занятие 37.** Настройка правил фильтрации траффика DLP системой (часть 2) | |
| | **17** | **Занятие 38.** Настройка правил фильтрации траффика DLP системой (часть 3) | |
| | **18** | **Занятие 39.** Настройка уровней доступа к различным подсетям (часть 1) | |
| | **19** | **Занятие 40.** Настройка уровней доступа к различным подсетям (часть 2) | |
| | **20** | **Занятие 41.** Настройка уровней доступа к различным подсетям (часть 3) | |
| | **Самостоятельная работа обучающихся** | | |

| | | | |
|---|---|---|---|
| | Практическое применение антивирусных программ для защиты информации от несанкционированного доступа | | 12 |
| Тема 1.3. Обеспечение безопасности стандартными средствами защиты | **Содержание учебного материала** | | |
| | **1** | **Занятие 42.** Локальные политики безопасности. | 16 |
| | **2** | **Занятие 43.** Особенности локальных политик безопасности различных операционных систем. | |
| | **3** | **Занятие 44.** Пользователи, типы пользователей, создание и ограничение пользователей (windows, unix-подобные ОС) | |
| | **4** | **Занятие 45.** Построение виртуальных защищенных сетей (VPN) | |
| | **5** | **Занятие 46.** Основные понятия, классификация и функции сетей VPN | |
| | **6** | **Занятие 47.** Средства обеспечения безопасности VPN | |
| | **7** | **Занятие 48.** Варианты архитектуры и принципы построения виртуальных защищенных каналов | |
| | **8** | **Занятие 49.** Достоинства применения технологий VPN | |
| | **Лабораторные работы** | | |
| | **21** | **Занятие 50.** Настройка локальных политик (часть 1) | 16 |
| | **22** | **Занятие 51.** Настройка локальных политик (часть 2) | |
| | **23** | **Занятие 52.** Создание пользователей, административная, пользовательская, гостевая учетные записи (windows системы) | |
| | **24** | **Занятие 53.** Сознание пользователей, права суперпользователя, ограничения пользователей, права доступа (часть 1) | |
| | **25** | **Занятие 54.** Сознание пользователей, права суперпользователя, ограничения пользователей, права доступа (часть 2) | |
| | **26** | **Занятие 55.** Сознание пользователей, права суперпользователя, ограничения пользователей, права доступа (часть 3) | |
| | **27** | **Занятие 56.** Сознание пользователей, права суперпользователя, ограничения пользователей, права доступа (часть 4) | |
| | **28** | **Занятие 57.** Построение фрагмента виртуальной защищенной сети | |
| | **Самостоятельная работа обучающихся** | | |
| | Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа. | | 7 |
| Тема 1.4 Технологии межсетевых экранов | **Содержание учебного материала** | | 10 |
| | **1** | **Занятие 58.** Функции межсетевых экранов | |
| | **2** | **Занятие 59.** Фильтрация трафика, выполнение функций посредничества, дополнительные возможности межсетевых экранов | |

| | | | |
|---|---|---|---|
| | **3** | **Занятие 60.** Особенности функционирования межсетевых экранов сетей связи Прикладной шлюз, варианты исполнения межсетевых экранов, формирование политики межсетевого взаимодействия, , | |
| | **4** | **Занятие 61.** Схемы подключения межсетевых экранов, персональные и распределенные межсетевые экраны | |
| | **5** | **Занятие 62.** Проблемы безопасности межсетевых экранов | |
| | **Лабораторные работы** | | |
| | **29** | **Занятие 63.** Установка и настройка межсетевых экранов | 6 |
| | **30** | **Занятие 64.** Выявление возможных атак на автоматизированные системы и применение различных функций межсетевых экранов | |
| | **31** | **Занятие 65.** Конфигурирование операционной системы | |
| Тема 1.5. Криптографическая защита информации. | **Содержание учебного материала** | | |
| | **1** | **Занятие 66.** Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных. | |
| | **2** | **Занятие 67.** Симметричные криптосистемы. Ассимметричные криптосистемы. | |
| | **3** | **Занятие 68.** Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом. | |
| | **4** | **Занятие 69.** Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. | 10 |
| | **5** | **Занятие 70.** Контрольное значение циклического избыточного кода CRC. | |
| | **6** | **Занятие 71.** Цифровые сертификаты. | |
| | **7** | **Занятие 72.** Отечественный стандарт цифровой подписи. | |
| | **8** | **Занятие 73.** Понятие криптоанализа. | |
| | **Лабораторные работы** | | |
| | **32** | **Занятие 74.** Шифрование данных симметричными алгоритмами. | |
| | **33** | **Занятие 75.** Шифрование данных ассимметричными алгоритмами. | |
| | **34** | **Занятие 76.** Криптоанализ (часть 1). | |
| | **35** | **Занятие 77.** Криптоанализ (часть 2). | 14 |
| | **36** | **Занятие 78.** Шифрование траффика. | |
| | **37** | **Занятие 79.** Шифрование данных (часть 1). | |
| | **38** | **Занятие 80.** Шифрование данных (часть 2). | |
| | **Самостоятельная работа обучающихся** | | |
| | Самостоятельная разработка предложений по программно-аппаратной защите информации на определенном объекте. | | 10 |

| | | | |
|---|---|---|---|
| Учебная практика | **Виды работ** | | |
| | **1** | Установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов. | 72 |
| | **2** | Установка и настройка типовых программно-аппаратных средств защиты информации. | |
| | **3** | Использование программно-аппаратных и инженерно-технических средств. | |
| | **4** | Настройка, регулировка и ремонт оборудования средств защиты. | |
| | **5** | Выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой. | |
| | **6** | Проведение типовых операции настройки средств защиты операционных систем. | |
| | **7** | Проведение аттестации объектов защиты. | |
| | **8** | Определение источников несанкционированного доступа, исходя из модели угроз. | |
| | **9** | Определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта. | |
| | **10** | Обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств. | |
| | **11** | Защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК. | |
| | **12** | Защита информации организационными методами в соответствии с инструкциями на объекте. | |
| **Промежуточная аттестация в форме дифференцированного зачета** | | | **2** |
| **Производственная практика** | **Виды работ** | | |
| | **1** | Ознакомление со структурой предприятия, вводный инструктаж по технике безопасности и охране труда | 90 |
| | **2** | Участие в создании комплексной системы защиты на предприятии. | |
| | **3** | Применение программно-аппаратных средств защиты информации на предприятии. | |
| | **4** | Применение инженерно-технических средств защиты информации на предприятии. | |
| | **5** | Применение криптографических средств защиты информации на предприятии. | |
| | **6** | Обобщение материала, оформление отчета, сдача зачета. | |
| **Самостоятельная работа при подготовке к экзамену по профессиональному модулю** | | | **8** |
| **Консультации** | | | **2** |
| **Промежуточная аттестация в форме экзамена по профессиональному модулю** | | | **8** |

| | |
|---|---|
| **Всего по ПМ** | **376** |

## 3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 3.1 Для реализации программы предусмотрены следующие специальные помещения

Лаборатории «Информационной безопасности телекоммуникационных систем», оснащенная оборудованием: стойки с сетевым оборудованием: CISCO1941/K9 – 12 шт., ASA5505-50-BUN-K8 – 4 шт., ASA5520-AIP10-K8 – 4 шт., IPS-4240-K9 – 4 шт., WS-C3560G-24PS-E -4 шт., Cisco Catalyst 2960 – 8 шт., Cisco ISR G1 2801 – 6 шт., CISCO2911/K9, AIR-CT2504-15-K9, MSE-3310-K9, Digi port server - 4 шт., Nexus 2248, Nexus 5548, Milrotik CRS 125 – 24g – 1s - rm, сервер Fujitsu - 3 шт.,NAC - 3315 -2 шт.и 2 сервера supermicro.

### 3.2 Информационное обеспечение реализации программы

**3.2.1. Основные электронные издания:**


1. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А.Бузов. - Москва: Горячая линия-Телеком, 2018. - 586 с. - ISBN 978-5-9912-0424-8. - URL: https://ibooks.ru/products/354357 (дата обращения: 22.02.2023).
2. Васильков, А.В. Безопасность и управление доступом в информационных системах: учебное пособие для СПО /А.В.Васильков, И.А.Васильков. - Москва: ФОРУМ, 2022. — 368 с. — ISBN 978-5-91134-360-6. - URL: https://znanium.com/catalog/product/1836631 (дата обращения: 22.02.2023).
3. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2021. — 400 с. —- ISBN 978-5-369-01759-3. - URL: https://znanium.com/catalog/product/1210523(дата обращения: 22.02.2023).
4. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А.П.Зайцев, Р.В.Мещеряков, А.А.Шелупанов. – 7-е изд., испр. – Москва: Горячая Линия–Телеком, 2018. - 442 с. - ISBN 978-5-9912-0233-6. - URL: https://ibooks.ru/bookshelf/333981/reading (дата обращения: 22.02.2023).
5. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО /В.Я.Ищейнов, М.В.Мецатунян. - Москва: Форум: ИНФРА-М, 2021. — 208 с. — ISBN 978-5-00091-489-2. - URL: https://znanium.com/catalog/product/1189337(дата обращения: 22.02.2023).
6. Партыка, Т.Л. Информационная безопасность: учебное пособие для студ. учрежд. СПО /Т.Л.Партыка, И.И.Попов. - Москва: Форум, 2020. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - URL: https://znanium.com/catalog/product/1081318 (дата обращения: 22.02.2023).
7. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учрежд. СПО. - Москва: ФОРУМ: ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - - URL: https://znanium.com/catalog/product/1189327 (дата обращения: 22.02.2023).
8. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА-М, 2022. — 592 с. — ISBN 978-5-8199-0730-6. - URL: https://znanium.com/catalog/product/1843022 (дата обращения: 22.02.2023). .


**Электронные ресурсы:**


1. Стандарты и регламенты//РОССТАНДАРТ. Федеральное агентство по техническому регулированию и метрологии: официальный сайт. - URL: https://www.rst.gov.ru/portal/gost//home/standarts (дата обращения: 22.02.2023)
2. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. - URL: www.fstec.ru (дата обращения: 22.02.2023)
3. Электронный фонд правовой и нормативно-технической документации/АО «Кодекс»: Профессиональные справочные системы: официальный сайт. – URL: http://docs.cntd.ru (дата обращения: 22.02.2023).
4. Elibrary.ru. Научная электронная библиотека: официальный сайт. – URL: www.elibrary.ru(дата обращения: 22.02.2023).

5. Глобус – Телеком: официальный сайт. – URL: http:/www.globus-telecom.com (дата обращения: 22.02.2023).
6. Морион. Российский разработчик и производитель оборудования связи. –URL: http://www.morion.ru/ (дата обращения: 22.02.2023).
7. НАТЕКС: официальный сайт. – URL: http://www.nateks.ru/. (дата обращения: 22.02.2023).
8. ISKRATEL: официальный сайт. – URL: http://www.iskratel.com/. (дата обращения: 22.02.2023).
9. Промсвязь: официальный сайт. – URL: http://www.ps-ufa.ru/.(дата обращения: 22.02.2023).
10. 3М. Наука, воплощенная в жизнь: [сайт]. – URL: http://3m.com/ (дата обращения: 22.02.2023).
11. ОАО «Ферроприбор»: официальный сайт. – URL: http://www.rusgates.ru/index/php (дата обращения: 22.02.2023).
12. SecurityLab. Защита информации и информационная безопасность: информационный портал/ООО "Positive Technologies". – URL: http://www.securitylab.ru (дата обращения: 22.02.2023).
13. Безопасность информационных технологий: рецензируемый научный журнал НИЯУ МИФИ: официальный сайт. - URL: http://bit.mephi.ru/ (дата обращения: 22.02.2023).
14. Вопросы кибербезопасности: научный, периодический, информационно-методический журнал: официальный сайт. - URL: http://cyberrus.com/ (дата обращения: 22.02.2023).
15. Астахова, Л.В. Теория информационной безопасности и методология защиты информации: учебное пособие / Л.В. Астахова. – Челябинск: Издательский центр ЮУрГУ, 2014. – URL: https://lib.susu.ru/ftd?base=SUSU_METHOD&key=000540003&dtype=F&etype=.pdf (дата обращения: 22.02.2023).
16. Волхонский, В.В. Устройства охранной сигнализации/В.В.Волхонский; НИУ ИТМО. – Санкт-Петербург: Университет ИТМО, 2015. – URL: https://books.ifmo.ru/book/1633/ustroystva_ohrannoy_signalizacii.htm (дата обращения: 22.02.2023).
17. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. - Екатеринбург: Изд-во Урал. ун-та, 2019. – URL: http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf (дата обращения: 22.02.2023).
18. Горбунов, А.В. Волоконно-оптический ответвитель-прищепка для съёма информации в волоконно-оптических линиях связи: учебное пособие /А.В.Горбунов. - Таганрог: Изд-во ТТИ ЮФУ, 2009. – URL: http://ntb.tgn.sfedu.ru/UML/UML_4399.pdf (дата обращения: 22.02.2023).
19. Гуляев, В.П. Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации: учебно-методический комплект / В. П. Гуляев. – Екатеринбург: Изд-во Урал. ун-та, 2014. – URL: http://elar.urfu.ru/bitstream/10995/28779/1/978-5-7996-1120-0_2014.pdf (дата обращения: 22.02.2023).
20. Защита информации в оптоволоконных локальных сетях: методические указания по выполнению лабораторных работ / ФГАУ ВО Северо-Кавказский федеральный университет. - Пятигорск, 2020. – URL: https://www.ncfu.ru/NCFU_PYATIGORSK/.doc/obrazovanie/OP/2020/bakalavriat/10.03.01/MD-10.03.01/Metod_ZIvOLS_SR_10.03.01_2020.pdf (дата обращения: 22.02.2023).
21. Каторин, Ю.Ф. Защита информации техническими средствами: учебное пособие / Ю.Ф.Каторин, А.В.Разумовский, А.И.Спивак; под редакцией Ю.Ф. Каторина. – С.-Петербург: НИУ ИТМО, 2012. – URL: https://books.ifmo.ru/file/pdf/975.pdf (дата обращения: 22.02.2023).
22. Меньшаков, Ю.К. Теоретические основы технических разведок: учебное пособие / Ю.К.Меньшаков; под ред. Ю.Н. Лаврухина. – Москва: Изд-во МГТУ им. Н.Э. Баумана, 2008. – URL: https://rusneb.ru/catalog/000199_000009_02000010254/ (дата обращения: 22.02.2023).
23. Руководство по применению адресно-аналоговых систем пожарной сигнализации/ С.М. Щипицын, А. Н. Членов, И. В. Павлов, А. Е. Атаманов. - Москва: Систем Сенсор Фаир

Детекторс, 2012// СИГМА: группа компаний: официальный сайт. – URL: http://www.sigma-is.ru/files/education/Rukovodstvo_AASPS_2012.pdf (дата обращения: 22.02.2023).
24. Рыжова, В.А. Проектирование и исследование комплексных систем безопасности/В.А.Рыжова; НИУ ИТМО. – С.-Петербург: НИУ ИТМО, 2013. – URL: https://books.ifmo.ru/file/pdf/1018.pdf (дата обращения: 22.02.2023).
25. Теория информационной безопасности и методология защиты информации /Ю.А.Гатчин, В.В.Сухостат, А.С.Куракин, Ю.В.Донецкая. – 2-е изд., испр. и доп. – С.-Петербург: Университет ИТМО, 2018. – URL: https://books.ifmo.ru/file/pdf/2372.pdf (дата обращения: 22.02.2023).

**3.2.2. Дополнительные источники:**

1. Бубнов, А. А. Техническая защита информации в объектах информационной инфраструктуры: учебник для среднего проф. образования/А.А. Бубнов, В.Н.Пржегорлинский, К.Ю.Фомина. – Москва: Академия, 2019. – 272 с.
2. Бурькова, Е. В. Системы охранно-пожарной сигнализации: учебное пособие / Е. В. Бурькова. — Оренбург: ОГУ, 2019. — 134 с. — ISBN 978-5-7410-2303-7. —— URL: https://e.lanbook.com/book/159903 (дата обращения: 22.02.2023). - URL: https://e.lanbook.com/book/159903 (дата обращения: 22.02.2023).
3. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - Москва: Форум: ИНФРА-М, 2022. — 239 с. —ISBN 978-5-00091-545-5. - URL: https://znanium.com/catalog/product/1846437 (дата обращения: 22.02.2023).
4. Груба, И.И. Системы охранной сигнализации. Технические средства обнаружения: справочное пособие / И.И.Груба. - Москва: СОЛОН-Пресс, 2020. - 220 с. - ISBN 978-5-91359-103-6. - URL: https://znanium.com/catalog/product/1858802 (дата обращения: 22.02.2023).
5. Инженерно-технические методы защиты объектов: учебное пособие / Е. Ю. Герлинг, М. М. Ковцур, Г. А. Орлов, П. В. Карельский. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2021. — 50 с. — URL: https://e.lanbook.com/book/279602 (дата обращения: 20.02.2023).
6. Инфокоммуникационные системы специального назначения: учебное пособие / сост. А. В. Паринов, Л. В. Степанов, О. В. Исаев. - Воронеж: Научная книга, 2021. - 144 с. - URL: https://znanium.com/catalog/product/1996335 (дата обращения: 14.02.2022).
7. Кирпичникова, М. Ю. Системы видеонаблюдения и контроля доступа: учебное пособие / М. Ю. Кирпичникова. — Самара: ПГУТИ, 2020. — 129 с. — URL: https://e.lanbook.com/book/255452 (дата обращения: 14.02.2022).
8. Особенности функционирования, подключения и настройки средств обнаружения и контроля: практикум / сост. А. В. Паринов, О. В. Исаев, О. А. Андреева. - Иваново: ПресСто, 2022. - 112 с. - URL: https://znanium.com/catalog/product/1998968 (дата обращения: 15.02.2023).
9. Новикова, Е.Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи: учебник для среднего проф. образования /Е.Л.Новикова. – Москва: Академия, 2018.- 189 с.
10. Поликанин, А. Н. Технические средства охраны и видеонаблюдения. Системы видеонаблюдения и тепловизионного контроля: учебное пособие / А. Н. Поликанин. — Новосибирск: СГУГиТ, 2021. — 46 с. — ISBN 978-5-907320-92-5. — URL: https://e.lanbook.com/book/222380 (дата обращения: 11.02.2023).
11. Технические средства защиты объектов. Часть 1: Основные понятия. Принципы построения средств инженерно-технической защиты объектов: учебное пособие / Б. Г. Ануфриев, О. В. Трубиенко, В. В. Филатов, А. А. Худяков. — Москва: РТУ МИРЭА, 2020. — 144 с. — URL: https://e.lanbook.com/book/256700 (дата обращения: 11.02.2023).
12. Шейдаков, Н. Е. Физические основы защиты информации: учеб. пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. - Москва: РИОР: ИНФРА-М, 2019. — 204 с. — ISBN 978-5-369-01603-9. - URL: https://znanium.com/catalog/product/916070 (дата обращения: 11.02.2023).

13. Ярочкина, Г.В. Монтаж и эксплуатация систем видеонаблюдения и систем безопасности: учебник для среднего проф. образования/Г.В.Ярочкина. – Москва: Академия, 2020. – 256 с.

**Нормативные документы:**

1. Кодекс Российской Федерации об административных правонарушениях//Гарант: справочно-правовая система. – URL: https://base.garant.ru/12125267/
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12148555/
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12148567/
4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12129354/
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12185475/
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12136635/
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/10200083/
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/192944/
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608//Гарант: справочно-правовая система. – URL: https://base.garant.ru/102670/
10. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г. //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/en/component/attachments/download/288
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21 //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 17 июля 2017 г. N 134// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/administrativnye-reglamenty/1362-prikaz-fstek-rossii-ot-17-iyulya-2017-g-n-134-2
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/administrativnye-reglamenty/478-

prikaz-fstek-rossii-ot-12-iyulya-2012-g-n-84
15. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702
16. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/370
17. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». – URL: https://base.garant.ru/187947/
18. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: https://docs.cntd.ru/document/1200095034
19. ГОСТ Р 34-11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200095035
20. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. –URL: http://docs.cntd.ru/document/1200058320
21. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/gost-r-51275-2006
22. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200108858
23. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. – URL: http://docs.cntd.ru/document/1200102287
24. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200044725
25. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200113006
26. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200113336
27. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий//Электронный фонд правовых и

нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: https://docs.cntd.ru/document/1200048398
28. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс». – URL: https://docs.cntd.ru/document/1200101777
29. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200105710
30. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: https://docs.cntd.ru/document/1200105711
31. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. - URL: http://docs.cntd.ru/document/1200103619
32. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010
33. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200048416
34. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380

**Периодические издания:**

1. Information Security/Информационная безопасность: официальный сайт. - URL: https://lib.itsec.ru/imag/
2. Защита информации Inside.
3. Электросвязь.

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

| Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля | Критерии оценки | Методы оценки |
|---|---|---|
| **ПК 3.1** Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности | – проведение анализа сетевой инфраструктуры;<br>– выявление угроз и уязвимости в сетевой инфраструктуре;<br>– определение оптимальные способы обеспечения информационной безопасности | - ассесмеит-центр,<br>- выполнение лабораторных и самостоятельных работ,<br>- результаты тестирования,<br>- отчет по практике |
| **ПК 3.2** Разрабатывать комплекс методов и средств защиты информации в системах радиосвязи, мобильной связи и телерадиовещания | – разработка комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах радиосвязи, мобильной связи и телерадиовещания;<br>– выявление недостатков систем защиты в системах и сетях связи с использованием специализированных программных продуктов | |
| **ПК 3.3** Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием специализированного программного обеспечения и оборудования | – осуществление текущего администрирования для защиты инфокоммуникационных сетей и систем радиосвязи, мобильной связи и телерадиовещания;<br>– работа с использованием специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи;<br>– выполнение расчетов и установки специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;<br>– -защита базы данных при помощи специализированных программных продуктов | |
| **ОК 01.** Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам | – умение распознавать задачу и/или проблему в профессиональном и/или социальном контексте;<br>– анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи;<br>– выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;<br>– составлять план действия;<br>– определять необходимые ресурсы;<br>– владение актуальными методами работы в профессиональной и смежных сферах;<br>– реализовывать составленный план; оценивать результат и последствия своих | |

| | | |
|---|---|---|
| | действий (самостоятельно или с помощью наставника) | |
| **ОК 02.** Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности | – быстрое определение сути задачи для поиска информации, необходимых источников информации;<br>– планирование процесса поиска;<br>– структурирование получаемой информации;<br>– оценивание практической значимости результатов поиска;<br>– применение средств информационных технологий для решения профессиональных задач;<br>– использование современного программного обеспечения;<br>– различных цифровых средств 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 | – работа в рамках актуальной нормативно-правовой документации;<br>– применение современной научной профессиональной терминологии;<br>– определение инвестиционной привлекательности коммерческих идей в рамках профессиональной деятельности; | |
| **ОК 04.** Эффективно взаимодействовать и работать в коллективе и команде | – организация работы коллектива и команды;<br>– взаимодействие с коллегами, руководством, клиентами в ходе профессиональной деятельности | |
| **ОК 05.** Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста | – -грамотное изложение своих мыслей и оформление документов по профессиональной тематике на государственном языке, проявление толерантности в рабочем коллективе | |
| **ОК 06.** Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных | – -определение значимости своей специальности;<br>– применение стандартов антикоррупционного поведения | |

| | | |
|---|---|---|
| ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения | | |
| **ОК 07.** Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях | – соблюдение нормы экологической безопасности;<br>– определение направления ресурсосбережения в рамках профессиональной деятельности по специальности, осуществление работы с соблюдением принципов бережливого производства;<br>– организация профессиональной деятельности с учетом знаний об изменении климатических условий региона | |
| **ОК 08.** Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности | – использование средств профилактики перенапряжения, характерных для данной специальности | |
| **ОК 09.** Пользоваться профессиональной документацией на государственном и иностранном языках | – понимание текста на базовые профессиональные темы | |
| ЛР1–ЛР4, ЛР9, ЛР10, ЛР13-ЛР15, ЛР20, ЛР23–ЛР28 | | |