**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
«3» апреля 2023 г.

Регистрационный № 11.09.23/209

# РАБОЧАЯ ПРОГРАММА

# ПМ.03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

(наименование профессионального модуля)

по специальности

11.02.15 Инфокоммуникационные сети и системы связи
(код и наименование специальности)

квалификация
специалист по монтажу и обслуживанию телекоммуникаций

Санкт-Петербург

2023

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена (индекс – ПМ.03) по специальности 11.02.15 инфокоммуникационные сети и системы связи, 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)

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 11.02.15 Инфокоммуникационные сети и системы связи, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 30 марта 2023 г., протокол №3.

СОГЛАСОВАНО

Заместитель директора
по развитию бизнеса ООО «Т8» К.В. Марченко

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ. 03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

## 1.1 Область применения рабочей программы

Рабочая программа профессионального модуля – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 11.02.15 Инфокоммуникационные сети и системы связи.

## 1.2 Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» 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 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 общечеловеческих 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:

| | |
|---|---|
| Владеть навыками | – анализировать сетевую инфраструктуру;<br>– выявлять угрозы и уязвимости в сетевой инфраструктуре;<br>– разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи;<br>– осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи;<br>– использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи. |
| уметь | – классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;<br>– проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;<br>– определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;<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 продукты;<br>– выполнять тестирование систем с целью определения уровня защищенности;<br>– определять оптимальные способы обеспечения информационной безопасности;<br>– проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;<br>– проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;<br>– разрабатывать политику безопасности сетевых элементов и логических сетей;<br>– выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;<br>– производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;<br>– конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;<br>– защищать базы данных при помощи специализированных программных продуктов;<br>– защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами |
| знать | – принципы построения информационно-коммуникационных сетей;<br>– международные стандарты информационной безопасности для проводных и беспроводных сетей;<br>– нормативно - правовые и законодательные акты в области |

| | |
|---|---|
| | 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>– способы и методы обнаружения средств съёма информации в радиоканале;<br>– классификацию угроз сетевой безопасности;<br>– характерные особенности сетевых атак;<br>– возможные способы несанкционированного доступа к системам связи;<br>– правила проведения возможных проверок согласно нормативным документам ФСТЭК;<br>– этапы определения конфиденциальности документов объекта защиты;<br>– назначение, классификацию и принципы работы специализированного оборудования;<br>– методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;<br>– методы и средства защиты информации в телекоммуникациях от вредоносных программ;<br>– технологии применения программных продуктов;<br>– возможные способы, места установки и настройки программных продуктов;<br>– методы и способы защиты информации, передаваемой по кабельным направляющим системам;<br>– конфигурации защищаемых сетей;<br>– алгоритмы работы тестовых программ;<br>– средства защиты различных операционных систем и среды передачи информации;<br>– способы и методы шифрования (кодирование и декодирование) информации |

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

Всего часов: **296 часов.**
Из них на освоение МДК:

**МДК.03.01.** Защита информации в инфокоммуникационных системах и сетях связи- **116 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<br>ОК 01 – ОК 09 | Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи | **116** | 58 | **116** | 58 | - | 72 | | **20** | |
| Учебная практика | | **72** | 72 | | | | | | | |
| Производственная практика | | **90** | 90 | | | | | | | |
| Промежуточная аттестация | | **18** | | | | | | | | 18 |
| **Всего:** | | **296** | 220 | **116** | 58 | - | **72** | **90** | **20** | **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. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи** | | | |
| **МДК.03.01. Защита информации в инфокоммуникационных системах и сетях связи** | | | 116 |
| 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. | 12 |
| | **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. | |
| | **Лабораторные работы** | | |
| | **1** | **Занятие 7.** Анализ современных угроз информационной безопасности. | 8 |
| | **2** | **Занятие 8.** Проектирование границ защиты. | |
| | **3** | **Занятие 9.** Применение сертификатов для аутентификации. | |
| | **4** | **Занятие 10.** Применение сертификатов для авторизации. | |
| | **Самостоятельная работа обучающихся** | | |
| | Составление доклада по перспективе и направлению развития программно-аппаратных средств защиты информации на основе публикаций в периодической специализированной аппаратуре | | 5 |
| Тема 1.2. Обеспечение безопасности информационных технологи | **Содержание учебного материала** | | |
| | **1** | **Занятие 11.** Особенности обеспечения информационной безопасности в компьютерных сетях. | 12 |
| | **2** | **Занятие 12.** Спецификация средств защиты в компьютерных сетях. | |
| | **3** | **Занятие 13.** Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Структура пакета. Шифрование. | |
| | **4** | **Занятие 14.** Типовые удаленные атаки и их характеристика. | |

| | | | |
|---|---|---|---|
| | **5** | **Занятие 15.** Принципы защиты распределенных вычислительных сетей. | |
| | **6** | **Занятие 16.** Принципы построения защищенных вычислительных сетей. | |
| | **Лабораторные работы** | | |
| | **5** | **Занятие 17.** Установка СЗИ (на примере IWTM) (часть 1) | 24 |
| | **6** | **Занятие 18.** Установка СЗИ (на примере IWTM) (часть 2) | |
| | **7** | **Занятие 19.** Установка СЗИ (на примере IWTM) (часть 3) | |
| | **8** | **Занятие 20.** Установка межсетевого экрана (часть 1) | |
| | **9** | **Занятие 21**. Установка межсетевого экрана (часть 2) | |
| | **10** | **Занятие 22.** Установка межсетевого экрана (часть 3) | |
| | **11** | **Занятие 23.** Настройка правил фильтрации траффика DLP системой (часть 1) | |
| | **12** | **Занятие 24.** Настройка правил фильтрации траффика DLP системой (часть 2) | |
| | **13** | **Занятие 25.** Настройка правил фильтрации траффика DLP системой (часть 3) | |
| | **14** | **Занятие 26.** Настройка уровней доступа к различным подсетям (часть 1) | |
| | **15** | **Занятие 27.** Настройка уровней доступа к различным подсетям (часть 2) | |
| | **16** | **Занятие 28.** Настройка уровней доступа к различным подсетям (часть 3) | |
| | **Самостоятельная работа обучающихся** | | |
| | Практическое применение антивирусных программ для защиты информации от несанкционированного доступа | | 5 |
| Тема 1.3. Обеспечение безопасности стандартными средствами защиты | **Содержание учебного материала** | | |
| | **1** | **Занятие 29.** Локальные политики безопасности. | 4 |
| | **2** | **Занятие 30.** Особенности локальных политик безопасности различных операционных систем. | |
| | **Лабораторные работы** | | |
| | **17** | **Занятие 31.** Настройка локальных политик (часть 1) | 14 |
| | **18** | **Занятие 32.** Настройка локальных политик (часть 2) | |
| | **19** | **Занятие 33.** Создание пользователей, административная, пользовательская, гостевая учетные записи (windows системы) | |
| | **20** | **Занятие 34.** Сознание пользователей, права суперпользователя, ограничения пользователей, права доступа (часть 1) | |
| | **21** | **Занятие 35.** Сознание пользователей, права суперпользователя, ограничения пользователей, права доступа (часть 2) | |
| | **22** | **Занятие 36.** Сознание пользователей, права суперпользователя, ограничения пользователей, права доступа (часть 3) | |
| | **23** | **Занятие 37.** Сознание пользователей, права суперпользователя, ограничения пользователей, права доступа (часть 4) | |

| | | | |
|---|---|---|---|
| | **Самостоятельная работа обучающихся** | | |
| | Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа. | | 5 |
| Тема 1.4. Криптографическая защита информации. | **Содержание учебного материала** | | |
| | **1** | **Занятие 38.** Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных. | 10 |
| | **2** | **Занятие 39.** Симметричные криптосистемы. Ассимметричные криптосистемы. | |
| | **3** | **Занятие 40.** 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 41.** Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. | |
| | **5** | **Занятие 42.** Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа. | |
| | **Лабораторные работы** | | |
| | **24** | **Занятие 43.** Шифрование данных симметричными алгоритмами. | 12 |
| | **25** | **Занятие 44.** Шифрование данных ассимметричными алгоритмами. | |
| | **26** | **Занятие 45.** Криптоанализ (часть 1). | |
| | **27** | **Занятие 46.** Криптоанализ (часть 2). | |
| | **28** | **Занятие 47.** Шифрование траффика. | |
| | **29** | **Занятие 48.** Шифрование данных. | |
| | **Самостоятельная работа обучающихся** | | |
| | Самостоятельная разработка предложений по программно-аппаратной защите информации на определенном объекте. | | 5 |
| 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** | | | **296** |

## 3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 3.1 Для реализации программы предусмотрены следующие специальные помещения

Кабинет «Компьютерного моделирования», оснащенный оборудованием: рабочее место преподавателя - ПК 1 шт., рабочие места обучающихся (25), экран, доска школьная, мультимедийный проектор, учебно-методические и демонстрационные пособия в электронном/печатном виде.

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.

Лаборатория «Телекоммуникационных систем», оснащенная оборудованием: рабочее место преподавателя – ноутбук 1 шт., рабочие места обучающихся - ноутбуки 13 шт., мобильное демонстрационное оборудование (ноутбук, мультимедиапроектор), доска школьная, стенды Связьстройдеталь, стенды для монтажа абонентского оптического доступа; участок распределительной сети GPON, стенд оптического доступа GPON на 3 абонента, макет «Изучение передатчиков и приёмников DTMFсигналов», макет «Изучения электронных телефонных аппаратов»; системные телефонные аппараты, кросс высокой плотности, стойки телекоммуникационные, шкаф, сервер Asterisk, сервер Middleware Stalker, кросс ШКОС-Л, кросс ШКОН-КПВ, кросс ШКОН-П, кросс ШКОН-ПА, коммутатор 2-го уровня D-Link DES, коммутатор 3-го уровня D-Link DGS, IP-телефоны, шлюзы D-Link, оптический тестер, оптический источник излучения, оптический сетевой терминал ONT HUAWEI, приставка телевизионная, набор монтажного инструмента для медного кабеля, терминал LLX, NEC УПАТС NEAX, ALCATEL-4100, радиотелефоны стандарта DECT различной модификации, антенные системы, эмуляторы сетевого оборудования, учебно-методические и демонстрационные пособия.

### 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 / Г.А.Бузов. - Москва: Горячая линия-Телеком, 2018. - 586 с. — 978-5-9912-0424-8. — URL: https://ibooks.ru/bookshelf/354357 (дата обращения: 25.02.2023).
2. 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: 25.02.2023).
3. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; под ред. А.П.Зайцева - 7 изд., исправ. — Москва: Горячая линия-Телеком, 2012. — 442с. — ISBN 978-5-9912-0233-6. — URL: https://znanium.com/catalog/product/390284 (дата обращения: 25.02.2023).
4. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Юрайт, 2022. — 342 с. — ISBN 978-5-534-10671-8. — URL: https://urait.ru/bcode/495524 (дата обращения: 25.02.2023).
5. 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: Юрайт, 2022. — 312 с. — ISBN 978-5-534-13221-2. — URL: https://urait.ru/bcode/497433 (дата обращения: 25.02.2023).

6. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры: учебник для среднего профессионального образования / А.В. Назаров, А.Н. Енгалычев, В.П. Мельников. — Москва: КУРС: ИНФРА-М, 2022. — 360 с. - ISBN 978-5-906923-06-6. - URL: https://znanium.com/catalog/product/1860128 — URL: https://znanium.com/catalog/product/1999922 (дата обращения: 25.02.2023).
7. Нестеров, С. А. Основы информационной безопасности: учебник / С. А. Нестеров. — Санкт-Петербург: Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — URL: https://e.lanbook.com/book/165837 (дата обращения: 25.022023).
8. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений: учебное пособие / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург: Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — URL: https://e.lanbook.com/book/288974 (дата обращения: 25.02.2023).
9. Никифоров, С. Н. Методы защиты информации. Защищенные сети: учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 96 с. — ISBN 978-5-8114-8123-1. — URL: https://e.lanbook.com/book/171868 (дата обращения: 25.02.2023).
10. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2022. — 325 с. — ISBN 978-5-534-03600-8. — URL: https://urait.ru/bcode/498844 (дата обращения: 25.02.2023).
11. Партыка, Т. Л. Вычислительная техника: учебное пособие для среднего профессионального образования / Т.Л. Партыка, И.И. Попов. — 3-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2022. — 445 с. — ISBN 978-5-00091-510-3. — URL: https://znanium.com/catalog/product/1703191 (дата обращения: 25.02.2023).
12. Партыка, Т. Л. Информационная безопасность: учебное пособие для среднего профессионального образования / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 432 с. — ISBN 978-5-00091-473-1. — URL: https://znanium.com/catalog/product/1189328 (дата обращения: 25.02.2023).
13. Петренко, В. И. Защита персональных данных в информационных системах. Практикум / В. И. Петренко, И. В. Мандрица. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 108 с. — ISBN 978-5-507-45301-6. — URL: https://e.lanbook.com/book/264242 (дата обращения: 25.02.2023).
14. Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург: Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — URL: https://e.lanbook.com/book/293009 (дата обращения: 25.02.2023).
15. Хорев, П. Б. Программно-аппаратная защита информации: учебное пособие для среднего профессионального образования/ П.Б. Хорев. — 3-е изд., испр. и доп. — Москва: ИНФРА-М, 2021. — 352 с. — ISBN 978-5-00091-557-8. - URL: https://znanium.com/catalog/product/1189341 (дата обращения: 25.02.2023).
16. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для среднего профессионального образования / В.Ф. Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2023. — 416 с. — ISBN 978-5-8199-0754-2. — URL: https://znanium.com/catalog/product/1910870 (дата обращения: 25.02.2023).
17. 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: 25.02.2023).

**Электронные ресурсы:**

1. SecurityLab. Защита информации и информационная безопасность: информационный портал/ООО "PositiveTechnologies". - URL: http://www.securitylab.ru (дата обращения: 25.02.2023).
2. Библиотека учебных курсов Microsoft: [сайт] - URL: http://msdn.microsoft.com/ru-ru/gg638594 (дата обращения: 25.02.2023).
3. Интернет-Университет информационных технологий. Библиотека учебных курсов: [сайт]. -

URL: https://www.intuit.ru/studies/courses (дата обращения: 25.02.2023).

**Дополнительные источники:**


1. Басыня, Е. А. Сетевая информационная безопасность: учебник / Е. А. Басыня. — Москва: НИЯУ МИФИ, 2023. — 224 с. — ISBN 978-5-7262-2949-2. — URL: https://e.lanbook.com/book/355511 (дата обращения: 25.02.2023).
2. Богульская, Н. А. Модели безопасности компьютерных систем: учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск: Сиб. федер. ун-т, 2019. - 206 с. - ISBN 978-5-7638-4008-7. - URL: https://znanium.com/catalog/product/1819309 (дата обращения: 25.02.2023).
3. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П.Н. Девянин. - 2-е изд., испр. и доп. - Москва: Горячая Линия–Телеком, 2017. - 338 с. - ISBN 978-5-9912-0328-9. - URL: https://ibooks.ru/bookshelf/344413 (дата обращения: 25.02.2023).
4. Капгер, И. В. Управление информационной безопасностью: учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь: ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — URL: https://e.lanbook.com/book/328889 (дата обращения: 25.02.2023).
5. Карпухин, Е. О. Технологии и методы защиты инфокоммуникационных систем и сетей: учебное пособие для вузов / Е.О. Карпухин. - Москва: Горячая Линия–Телеком, 2021. - 120 с. - ISBN 978-5-9912-0896-3. - URL: https://ibooks.ru/bookshelf/386554 (дата обращения: 25.02.2023).
6. Киренберг, Г.А. Информационная безопасность современных операционных систем: учебное пособие / А.Г.Киренберг. — Кемерово: КузГТУ имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — URL: https://e.lanbook.com/book/295736 (дата обращения: 25.02.2023).
7. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учебное пособие / А. Г. Киренберг. — Кемерово: КузГТУ имени Т.Ф. Горбачева, 2022. — 120 с. — ISBN 978-5-00137-292-9. — URL: https://e.lanbook.com/book/257564 (дата обращения: 25.02.2023).
8. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем: учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва: РТУ МИРЭА, 2020. — 136 с. — URL: https://e.lanbook.com/book/167606 (дата обращения: 25.02.2023).
9. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — URL: https://e.lanbook.com/book/237770 (дата обращения: 25.02.2023).
10. Овчинникова, Е. А. Основы информационного права Российской Федерации: учебное пособие / Е. А. Овчинникова, С. Н. Новиков. — Новосибирск: СибГУТИ, 2021. — 138 с. — URL: https://e.lanbook.com/book/257315 (дата обращения: 25.02.2023).
11. Потерпеев, Г. Ю. Безопасность операционных систем: учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва: РТУ МИРЭА, 2021. — 93 с. — URL: https://e.lanbook.com/book/182416 (дата обращения: 25.02.2023).
12. Радиоэлектронная защита объектов и информации: учебное пособие / В. В. Смирнов, Л. Б. Кочин, С. А. Певишев, А. С. Стукалова. — Санкт-Петербург: БГТУ "Военмех" им. Д.Ф. Устинова, 2020. — 38 с. — URL: https://e.lanbook.com/book/172236 (дата обращения: 25.02.2023).
13. Родичев, Ю.А. Нормативная база и стандарты в области информационной безопасности: учебное пособие / Ю.А. Родичев. - Санкт-Петербург: Питер, 2021. - 256 с. - ISBN 978-5-4461-0861-9. - URL: https://ibooks.ru/bookshelf/358147 (дата обращения: 25.02.2023).
14. Сычев, Ю. Н. Защита информации и информационная безопасность: учебное пособие для среднего профессионального образования / Ю.Н. Сычев. — Москва: ИНФРА-М, 2022. — 201 с. — ISBN 978-5-16-016583-7. - URL: https://znanium.com/catalog/product/1859978 (дата обращения: 25.02.2023).
15. Техническая защита информации: учебное пособие / А. С. Раков, О. Н. Маслов, О. Ю. Губарева [и др.]. — Самара: ПГУТИ, 2020. — 96 с. — URL: https://e.lanbook.com/book/255575 (дата обращения: 25.02.2023).

16. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — URL: https://e.lanbook.com/book/130184 (дата обращения: 25.02.2023).
17. Шейдаков, Н. Е. Физические основы защиты информации: учебное пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. — Москва: РИОР: ИНФРА-М, 2021. — 204 с. — ISBN 978-5-369-01603-9. - URL: https://znanium.com/catalog/product/1189956 (дата обращения: 25.02.2023).
18. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. - Москва: Горячая линия-Телеком, 2018. - 220 с. - ISBN 978-5-9912-0323-4. - URL: https://znanium.com/catalog/product/421968 (дата обращения: 25.02.2023).

**Отечественные журналы:**

1. Защита информации Inside. - Текст: непосредственный.
2. Information Security/ Информационная безопасность: [сайт]. - URL: https://lib.itsec.ru/imag/ (дата обращения: 25.02.2023).
3. Проблемы информационной безопасности. Компьютерные системы. - Текст: непосредственный.
4. Электросвязь. - Текст: непосредственный.

## 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**<br>Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности | классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно;<br>анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный;<br>возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно;<br>мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме;<br>недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выявлены в полном объеме,<br>тестирование систем с целью определения уровня защищенности выполнено,<br>уровень защищенности определен верно; | тестирование,<br>экзамен,<br>экспертное наблюдение выполнения лабораторных работ,<br>экспертное наблюдение выполнения практических работ,<br>оценка решения ситуационных задач,<br>оценка процесса и результатов выполнения видов работ на практике |
| **ПК 3.2**<br>Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. | для обеспечения информационной безопасности выбраны оптимальные способы;<br>выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях; | тестирование,<br>экзамен,<br>экспертное наблюдение выполнения лабораторных работ,<br>экспертное наблюдение выполнения практических работ,<br>оценка решения ситуационных задач,<br>оценка процесса и результатов выполнения видов работ на практике |

| | | |
|---|---|---|
| **ПК 3.3**<br>Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. | мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными;<br>политика безопасности сетевых элементов и логических сетей разработана в полном объеме;<br>расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми стандартами;<br>установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи выполнена в соответствии с отраслевыми стандартами;<br>конфигурирование автоматизированных систем и информационно-коммуникационных сетей осуществлено в соответствии с политикой информационной безопасности и отраслевыми стандартами;<br>базы данных максимально защищены при помощи специализированных программных продуктов;<br>ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами; | тестирование,<br>экзамен,<br>экспертное наблюдение выполнения лабораторных работ,<br>экспертное наблюдение выполнения практических работ,<br>оценка решения ситуационных задач,<br>оценка процесса и результатов выполнения видов работ на практике |
| **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 |
| **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 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. | - взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;<br>- обоснованность анализа работы членов команды (подчиненных) |
| **ОК 05** | Осуществлять устную и письменную коммуникацию на государственном языке РФ с учетом особенностей социального и культурного контекста. | -грамотность устной и письменной речи,<br>- ясность формулирования и изложения мыслей |
| **ОК 06** | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения | - соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, |
| **ОК 07** | Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях. | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;<br>- знание и использование ресурсосберегающих технологий в области телекоммуникаций |
| **ОК 08** | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; |
| **ОК 09** | Пользоваться профессиональной документацией на государственном и иностранных языках | понимание общего смысла четко произнесенных высказываний на известные темы (профессиональные и |

| | | |
|---|---|---|
| | | бытовые), текстов на базовые профессиональные темы, участие в диалогах на знакомые общие и профессиональные темы |
| ЛР1–ЛР4, ЛР9, ЛР10, ЛР13-ЛР15, ЛР20, ЛР23–ЛР28 | | |