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

УТВЕРЖДАЮ
Первый проректор – проректор по учебной работе
_____ А.В. Абилов
01 апреля 2025 г.

Регистрационный № 11.09.25/206

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
2025

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» 28 марта 2025 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)
12 февраля 2025 г., протокол № 6

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

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля
19 февраля 2025 г., протокол № 4

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)

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

УТВЕРЖДАЮ
Первый проректор – проректор по учебной работе
_____ А.В. Абилов
_____ 2025 г.

Регистрационный № 11.09.25/206

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
2025

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» 28 марта 2025 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)
12 февраля 2025 г., протокол № 6

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

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля
19 февраля 2025 г., протокол № 4

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; – выявлении угроз и уязвимости в сетевой инфраструктуре; – разработке комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи; – осуществлении текущего администрирования для защиты инфокоммуникационных сетей и систем связи; – использовании специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.
уметь	– классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; – определять оптимальные способы обеспечения информационной безопасности; – осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; – выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов; – выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; – защищать базы данных при помощи специализированных программных продуктов.
знать	– принципы построения систем радиосвязи, мобильной связи и телерадиовещания; – международные стандарты информационной безопасности; – акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия; – технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия; – классификацию угроз сетевой безопасности; – методы и способы защиты информации, передаваемой по кабельным направляющим системам; – правила проведения возможных проверок согласно нормативным документам ФСТЭК; – 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		12

	несанкционированного доступа		
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.	10
	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.	
	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.	14
	33	**Занятие 75.** Шифрование данных ассимметричными алгоритмами.	
	34	**Занятие 76.** Криптоанализ (часть 1).	
	35	**Занятие 77.** Криптоанализ (часть 2).	
	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 печатные и электронные издания:

1. Новикова, Е. Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи: учебник для среднего профессионального образования / Е. А. Новикова. - 2-е изд., стер. - Москва: Академия, 2023. - 189 с. - ISBN 978-5-0054-1212-6.
2. 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: 25.01.2024).
3. 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: 25.01.2024).

Электронные ресурсы:

1. SecurityLab. Защита информации и информационная безопасность: информационный портал/ООО "PositiveTechnologies". - URL: http://www.securitylab.ru (дата обращения: 25.01.2024).
2. Библиотека учебных курсов Microsoft: [сайт] - URL: http://msdn.microsoft.com/ru-ru/gg638594 (дата обращения: 25.01.2024).
3. Интернет-Университет информационных технологий. Библиотека учебных курсов: [сайт]. - URL: https://www.intuit.ru/studies/courses (дата обращения: 25.01.2024).

Дополнительные источники:

1. 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: 25.01.2024).
2. 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: 25.01.2024).
3. 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: 25.01.2024).
4. 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: 25.01.2024).
5. 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: 25.01.2024).

Отечественные журналы:

1. Защита информации Inside //ИВИС: информационные услуги: официальный сайт. - URL: https://www.ivis.ru/ (дата обращения: 25.01.2024).
2. Information Security/ Информационная безопасность: [сайт]. - URL: https://lib.itsec.ru/imag/ (дата обращения: 25.01.2024).
3. Электросвязь: научно-технический журнал. – 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 Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	– проведение анализа сетевой инфраструктуры; – выявление угроз и уязвимости в сетевой инфраструктуре; – определение оптимальные способы обеспечения информационной безопасности	- ассесмеит-центр, - выполнение лабораторных и самостоятельных работ, - результаты тестирования, - 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; – 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; – работа с использованием специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи; – выполнение расчетов и установки специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; – -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; – анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; – выявлять и эффективно искать	

	информацию, необходимую для решения задачи и/или проблемы; – составлять план действия; – определять необходимые ресурсы; – владение актуальными методами работы в профессиональной и смежных сферах; – 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; – планирование процесса поиска; – структурирование получаемой информации; – оценивание практической значимости результатов поиска; – применение средств информационных технологий для решения профессиональных задач; – использование современного программного обеспечения; – 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; – применение современной научной профессиональной терминологии; – определение инвестиционной привлекательности коммерческих идей в рамках профессиональной деятельности;	
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	– организация работы коллектива и команды; – 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 ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	– -определение значимости своей специальности; – применение стандартов 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; – определение направления ресурсосбережения в рамках профессиональной деятельности по специальности, осуществление работы с соблюдением принципов бережливого производства; – 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		