

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ И.С.  
ТУРГЕНЕВА»  
ЛИВЕНСКИЙ ФИЛИАЛ ОГУ им. И.С. ТУРГЕНЕВА**



**ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА  
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ –  
ПРОГРАММА ПОДГОТОВКИ СПЕЦИАЛИСТОВ СРЕДНЕГО ЗВЕНА (ППССЗ)**

**10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ**  
специальность

Утверждена на заседании  
Ученого совета  
ОГУ имени И.С. Тургенева  
Протокол № 15 от 29.05.2025 г.

Образовательная программа среднего профессионального образования (СПО) по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем разработана в Ливенском филиале ОГУ им. И.С. Тургенева в соответствии с федеральным государственным образовательным стандартом по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденным приказом Министерства науки и высшего образования Российской Федерации от «09» декабря 2016 г. № 1551 (ред. №3 от 03.07.2024).

Образовательная программа разработана совместно с профильной организацией АО ИРК «Принт-ТВ»

Директор Г.И. Карзов

Образовательная программа среднего профессионального образования рассмотрена на заседании кафедры информационных технологий и экономики (протокол от «28» 03 2025 № 8).

И.о. зав. кафедрой О.В.Псарева

Образовательная программа среднего профессионального образования рассмотрена и одобрена на заседании Ученого совета технико-экономического факультета (протокол от «19» апреля 2025 № 9)

Декан факультета Ю.А. Бакурова

Образовательная программа среднего профессионального образования рассмотрена и одобрена на заседании Ученого совета Ливенского филиала ОГУ им. И.С. Тургенева (протокол от «28» мая 2025 № 11).

Директор Ливенского филиала  
ОГУ им. И.С. Тургенева Е.А. Колякина

## СОДЕРЖАНИЕ

1 Общая характеристика образовательной программы .....	4
1.1 Цель образовательной программы.....	4
1.2 Квалификация, присваиваемая выпускникам.....	5
1.3 Срок получения образования .....	5
1.4 Требования к уровню образования, необходимому для освоения образовательной программы .....	5
1.5 Язык реализации образовательной программы.....	5
2 Характеристика профессиональной деятельности выпускников образовательной программы.....	5
2.1 Область профессиональной деятельности выпускников .....	5
2.2 Основные виды деятельности выпускников .....	5
2.3 Соответствие профессиональных модулей присваиваемым квалификациям.....	6
3 Требования к результатам освоения образовательной программы .....	7
4 Структура и объем образовательной программы .....	47
5 Документы, регламентирующие содержание и организацию образовательного процесса при реализации образовательной программы ....	48
5.1 Учебный план.....	49
5.2 Календарный учебный график .....	49
5.3 Рабочие программы дисциплин (модулей) .....	49
5.4 Программы учебной и производственной практик.....	50
5.5 Программа государственной итоговой аттестации.....	51
5.6 Методические материалы .....	51
6 Документы, регламентирующие содержание и организацию воспитательной работы при реализации образовательной программы .....	52
7 Оценка качества освоения образовательной программы.....	52
8 Условия реализации образовательной программы.....	53
8.1 Кадровое обеспечение реализации образовательной программы .....	54
8.2 Материально-техническое обеспечение образовательной программы .	54
8.3 Учебно-методическое обеспечение образовательной программы .....	57
9 Характеристика социокультурной среды .....	59
10 Список разработчиков образовательной программы .....	61

## **1 Общая характеристика образовательной программы**

Образовательная программа среднего профессионального образования (программа подготовки специалистов среднего звена – далее образовательная программа, ППССЗ) по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, реализуемая в Ливенском филиале ОГУ им. И.С. Тургенева представляет собой комплекс документов, разработанных и утвержденных университетом на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по указанной специальности, утвержденного приказом Министерства образования и науки Российской Федерации от «09» декабря 2016 г. № 1551 (ред. №3 от 03.07.2024) и с учетом соответствующей примерной образовательной программы, включенной в реестр примерных образовательных программ (далее - ПОП), а также с учетом потребностей регионального рынка труда.

ППССЗ по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем направлена на удовлетворение потребностей регионального рынка, конкретизирует конечные результаты обучения в виде компетенций, умений и знаний, приобретаемого практического опыта.

Конкретные виды деятельности, к которым готовится обучающийся, соответствуют присваиваемой квалификации.

Содержание образовательной программы разработано совместно с профильной организацией АО ИРК «Принт-ТВ», соответствующей видам профессиональной деятельности.

### **1.1 Цель образовательной программы**

Образовательная программа имеет своей целью формирование общих и профессиональных компетенций в соответствии с требованиями ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, требованиями соответствующих профессиональных стандартов.

В области обучения целью программы является подготовка специалиста, обладающего общими и профессиональными компетенциями в соответствии с требованиями ФГОС, способного успешно работать в избранной сфере деятельности и быть устойчивым на рынке труда.

В области воспитания целью программы является формирование социально-личностных и профессионально важных качеств выпускников: целеустремленности, организованности, трудолюбия, коммуникабельности, умения работать в коллективе, гражданственности, толерантности; ответственности за конечный результат в профессиональной деятельности, адаптивности.

## **1.2 Квалификация, присваиваемая выпускникам**

По результатам освоения образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем базовой подготовки присваивается квалификация: техник по защите информации.

## **1.3 Срок получения образования**

Срок получения образования – 3 года 10 месяцев (очная форма обучения на базе основного общего образования).

## **1.4 Требования к уровню образования, необходимому для освоения образовательной программы**

К освоению образовательных программ среднего профессионального образования допускаются лица, имеющие образование не ниже основного общего образования.

## **1.5 Язык реализации образовательной программы**

Образовательная программа реализуется на государственном языке Российской Федерации.

# **2 Характеристика профессиональной деятельности выпускников образовательной программы**

## **2.1 Область профессиональной деятельности выпускников**

Область профессиональной деятельности, в которой выпускники, освоившие образовательную программу, могут осуществлять профессиональную деятельность: 06 Связь, информационные и коммуникационные технологии, 12 Обеспечение безопасности.

## **2.2 Основные виды деятельности выпускников**

Выпускник, освоивший образовательную программу, должен быть готов к выполнению основных видов деятельности согласно получаемой квалификации специалиста среднего звена:

- эксплуатация информационно-телекоммуникационных систем и сетей;
- защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты;
- защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты.
- выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

### **2.3 Соответствие профессиональных модулей присваиваемым квалификациям**

<b>Наименование основных видов деятельности</b>	<b>Наименование профессиональных модулей</b>	<b>Квалификация</b> Техник по защите информации
Эксплуатация информационно-телекоммуникационных систем и сетей	ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей	осваивается
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе криптографических средств защиты	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных(в том числе криптографических) средств защиты	осваивается
Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	осваивается
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	осваивается одна профессия рабочего 14601 Монтажник оборудования связи

### **3 Требования к результатам освоения образовательной программы**

В результате освоения образовательной программы у выпускника должны быть сформированы общие и профессиональные компетенции.

#### **ОБЩИЕ КОМПЕТЕНЦИИ**

<b>Код компетенции</b>	<b>Формулировка компетенции</b>	<b>Знания, умения</b>
OK 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	<p><b>Умения:</b> 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; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)</p> <p><b>Знания:</b> актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности</p>
OK 02	Использовать современные средства поиска, анализа и интерпритации информации и информационные технологии для выполнения задач профессиональной деятельности	<p><b>Умения:</b> определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение</p> <p><b>Знания:</b> номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности</p>

OK 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	<p><b>Умения:</b> определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования; выявлять достоинства и недостатки коммерческой идеи; презентовать идеи открытия собственного дела в профессиональной деятельности; оформлять бизнес-план; рассчитывать размеры выплат по процентным ставкам кредитования; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования</p> <p><b>Знания:</b> содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты</p>
OK 04	Эффективно взаимодействовать и работать в коллективе и команде	<p><b>Умения:</b> организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности</p> <p><b>Знания:</b> психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности</p>
OK 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	<p><b>Умения:</b> грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе</p> <p><b>Знания:</b> особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.</p>
OK 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	<p><b>Умения:</b> описывать значимость своей специальности для развития экономики и среды жизнедеятельности граждан российского государства; проявлять и отстаивать базовые общечеловеческие, культурные и национальные ценности российского государства в современном обществе</p> <p><b>Знания:</b> сущность гражданско-патриотической позиции, общечеловеческих ценностей в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, ; значимость профессиональной деятельности по специальности для развития экономики и среды жизнедеятельности граждан российского государства ; основы нравственности и морали демократического общества; основные компоненты активной гражданско-патриотической позиции, основы культурных, национальных традиций народов российского государства; стандарты антикоррупционного поведения</p>

	антикоррупционного поведения	
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережении, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	<p><b>Умения:</b> соблюдать нормы экологической безопасности; определять направления ресурсосбережения, применения знаний об изменении климата в рамках профессиональной деятельности по специальности при выполнении строительно-монтажных работ, в том числе отделочных работ, текущего ремонта и реконструкции строительных объектов, оценить чрезвычайную ситуацию, составить алгоритм действий и определять необходимые ресурсы для её устранения; использовать энергосберегающие и ресурсосберегающие технологии, принципы бережливого производства в профессиональной деятельности по специальности при выполнении строительно-монтажных работ, в том числе отделочных работ, текущего ремонта и реконструкции строительных объектов,</p> <p><b>Знания:</b> правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения и бережливого производства; основные виды чрезвычайных событий природного и техногенного происхождения, опасные явления, порождаемые их действием; технологии по повышению энергоэффективности зданий, сооружений и инженерных систем</p>
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	<p><b>Умения:</b> использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной для данной специальности при выполнении строительно-монтажных работ, в том числе отделочных работ, ремонтных работ и работ по реконструкции и эксплуатации строительных объектов</p> <p><b>Знания:</b> роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности при выполнении строительно-монтажных работ, в том числе отделочных работ, ремонтных работ и работ по реконструкции и эксплуатации строительных объектов; средства профилактики перенапряжения</p>
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	<p><b>Умения:</b> понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснять свои действия (текущие и</p>

		планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
		<b>Знания:</b> правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

## ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ

Основные виды деятельности	Код и наименование компетенции	Показатели освоения компетенции
Эксплуатация информационно – телекоммуникационных систем и сетей	ПК1.1. Производить монтаж, настройку и поверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей.	<p><b>Практический опыт:</b> монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей (далее –ИТКС);</p> <p><b>Умения:</b> осуществлять техническую эксплуатацию линейных сооружений связи; производить монтаж кабельных линий и оконечных кабельных устройств; настраивать, эксплуатировать и обслуживать оборудование ИТКС; осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС; производить испытания, проверку и приемку оборудования ИТКС; производить монтаж кабельных линий и оконечных кабельных устройств ИТКС; применять средства измерений характеристик функционирования электрических цепей и сигналов ИТКС;</p> <p><b>Знания:</b> принципов построения и основных характеристик ИТКС; принципов передачи информации в ИТКС; видов и характеристик сигналов в ИТКС; видов помех в каналах связи ИТКС и методов защиты от них; разновидностей линий передач, конструкций и характеристик электрических и оптических кабелей</p>

		<p>связи; технологий и оборудования удаленного доступа в ИТКС; принципов построения, основные характеристики активного сетевого и коммуникационного оборудования ИТКС; основных характеристик типовых измерительных приборов и правил работы с ними;</p>
	<p>ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно – телекоммуникационных систем и сетей.</p>	<p><b>Практический опыт:</b> текущего контроля функционирования оборудования ИТКС; диагностики технического состояния приёмо-передающих устройств и линейных сооружений связи и источников питания;</p> <p><b>Умения:</b> осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС; производить испытания, проверку и приемку оборудования ИТКС; осуществлять диагностику технического состояния ИТКС; применять средства измерений характеристик функционирования электрических цепей и сигналов ИТКС;</p> <p><b>Знания:</b> принципов построения и основных характеристик ИТКС; принципы передачи информации в ИТКС; разновидностей линий передач, конструкций и характеристик электрических и оптических кабелей связи; технологий и оборудования удаленного доступа в ИТКС; периодичности выполнения поверок контрольно-измерительной аппаратуры; требований метрологического обеспечения функционирования ИБТКС;</p>
	<p>ПК 1.3. Проводить техническое обслуживание оборудования информационно – телекоммуникационных систем и сетей</p>	<p><b>Практический опыт:</b> проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта оборудования ИТКС;</p> <p><b>Умения:</b> осуществлять техническую эксплуатацию линейных сооружений связи;</p>

	<p>проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; производить настройку программного обеспечения коммутационного оборудования защищенных телекоммуникационных систем; производить контроль параметров функционирования ИТКС;</p> <p><b>Знания:</b></p> <p>принципов построения и основных характеристик ИТКС; видов и характеристика сигналов в ИТКС; разновидностей линий передач, конструкции и характеристик электрических и оптических кабелей связи; принципов построения, основных характеристик активного сетевого и коммуникационного оборудования ИТКС; принципов организации технической эксплуатации ИТКС;</p>
ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей	<p><b>Практический опыт:</b></p> <p>текущего контроля функционирования оборудования ИТКС; мониторинга технического состояния и работоспособности приёмо-передающих устройств и линейных сооружений связи и источников питания ИТКС;</p> <p><b>Умения:</b></p> <p>осуществлять техническую эксплуатацию линейных сооружений связи; настраивать, эксплуатировать и обслуживать оборудование ИТКС; производить испытания, проверку и приемку оборудования ИТКС; проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС; осуществлять техническую эксплуатацию приемо-передающих устройств; оформлять эксплуатационно-техническую документацию;</p> <p><b>Знания:</b></p> <p>принципов построения и основных характеристик ИТКС; принципов передачи информации в ИТКС; видов и характеристик сигналов в ИТКС;</p>

		<p>видов помех в каналах связи ИТКС и методов защиты от них; принципов построения, основных характеристик активного сетевого и коммуникационного оборудования ИТКС.</p> <p>спецификацию изделий, комплектующих, запасного имущества и принадлежностей ИТКС;</p>
Защита информации в информационно – телекоммуникационных системах и сетях с использованием программно- аппаратных, в том числе криптографических средств защиты	<p>ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно- аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей</p>	<p><b>Практический опыт:</b> установки, настройки, испытаний и конфигурирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС;</p> <p><b>Умения:</b> выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;</p> <p><b>Знания:</b> способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; типовых программных и программно-аппаратных средств защиты информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;</p>
	<p>ПК 2.2. Поддерживать бесперебойную работу программных и программно- аппаратных, в том числе и криптографических средств защиты информации в оборудование информационно – телекоммуникационных системах и сетях</p>	<p><b>Практический опыт:</b> поддержания бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС;</p> <p><b>Умения:</b> выявлять и оценивать угрозы безопасности информации в ИТКС; проводить контроль показателей и процесса функционирования программных и программно-аппаратных</p>

	<p>(в том числе криптографических) средств защиты информации; проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;</p> <p><b>Знания:</b></p> <p>возможных угроз безопасности информации в ИТКС; способов защиты информации от НСД и специальных воздействий на нее; порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации; организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации; порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации;</p>
	<p><b>ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно- аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.</b></p> <p><b>Практический опыт:</b></p> <p>защиты информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты в соответствии с предъявляемыми требованиями;</p> <p><b>Умения:</b></p> <p>выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;</p> <p><b>Знания:</b></p> <p>возможных угроз безопасности информации в ИТКС;</p>

		<p>способов защиты информации НСД и специальных воздействий на нее; типовых программных и программно-аппаратных средств защиты информации в ИТКС; криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС; порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации.</p>
Защита информации в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты	<p>ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях.</p>	<p><b>Практический опыт:</b> установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам;</p> <p><b>Умения:</b> проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;</p> <p><b>Знания:</b> способов защиты информации от утечки по техническим каналам с использованием технических средств защиты; основных типов технических средств защиты информации от утечки по техническим каналам; законодательства в области информационной безопасности, структуру государственной системы защиты информации, нормативных актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;</p>
	<p>ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации,</p>	<p><b>Практический опыт:</b> установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам; проведения технического обслуживания и ремонта технических средств защиты информации от утечки по техническим</p>

	<p>используемых информационно телекоммуникационных системах и сетях</p>	<p>в –</p>	<p>каналам;</p> <p><b>Умения:</b> проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;</p> <p><b>Знания:</b> основных типов технических средств защиты информации от утечки по техническим каналам; организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам; порядка и правил ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;</p>
	<p>ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам</p> <p>в –</p> <p>информационно телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.</p>	<p>в –</p>	<p><b>Практический опыт:</b> защиты информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;</p> <p><b>Умения:</b> проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;</p> <p><b>Знания:</b> способов защиты информации от утечки по техническим каналам с использованием технических средств защиты; основных типов технических средств защиты информации от утечки по техническим каналам;</p>

		<p>методик измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;</p> <p>порядка и правил ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;</p>
	<p>ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно – телекоммуникационных систем и сетей</p>	<p><b>Практический опыт:</b> проводение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации.</p> <p><b>Умения:</b> применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.</p> <p><b>Знания:</b> номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.</p>
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	<p>ПК 4.1. Выполнять монтаж и настройку сетей проводного и беспроводного абонентского доступа в соответствии с действующими отраслевыми стандартами</p>	<p><b>Практический опыт:</b> по монтажу и кроссировке станционных кабелей; по прокладке и монтажу перемычек заземления на распределительной коробке, на защитные полосы кросса; проводить монтаж оптических станционных кроссов; установки абонентского телекоммуникационного оборудования; настройки абонентского оборудования; подключать PLC адаптера; монтажа коннекторов, розеток электрического кабеля «витая пара»</p> <p><b>Умения:</b> выявлять недостатки и причины в работе компьютера; проводить установку оконечного абонентского оборудования; проводить сверление и пробивку отверстий по готовой разметке; проводить установку электрической розетки;</p>

	<p>проводить крепление стыков металлоконструкций монтажными болтами, установку дюбелей; проводить тестирование сети абонентских подключений; проводить прокладку и крепление кабелей в коробах, резку кабеля по размерам; проводить чистку коннекторов на оптических шнурах; проводить тестирование кроссового и абонентского оборудования; проводить инфокоммуникационных устройств абонентского подключения; проводить инсталляцию, настройку и обслуживание IP телефонии; осуществлять клиентский сервис при проведении работ у абонента.</p>
	<p><b>Знания:</b></p> <p>основы электротехники; простые электрические и монтажные схемы; ассортимент и маркировку применяемых материалов; марки кабелей и проводов; устройство и назначение абонентского оборудования; способы и технологии выполнения монтажных работ; устройство и правила применения такелажных средств; назначение и устройство применяемых измерительных приборов, правила пользования ими; устройство электрифицированного инструмента и механизмов, телефонных аппаратов, ПК, ONT; алгоритм взаимодействия при абонентском сервисе; технику безопасности и охрану труда</p>

		<p>настройки абонентского оборудования; подключать PLC адаптера; монтажа коннекторов, розеток электрического кабеля «витая пара»</p>
		<p><b>Умения:</b></p> <p>выявлять недостатки и причины в работе компьютера; проводить сверление и пробивку отверстий по готовой разметке; проводить установку электрической розетки; проводить крепление стыков металлоконструкций монтажными болтами, установку дюбелей; проводить тестирование сети абонентских подключений; проводить прокладку и крепление кабелей в коробах, резку кабеля по размерам; проводить чистку коннекторов на оптических шнурах; проводить тестирование кроссового и абонентского оборудования; проводить инфокоммуникационных устройств абонентского подключения; проводить инсталляцию, настройку и обслуживание IP телефонии; осуществлять клиентский сервис при проведении работ у абонента.</p>
		<p><b>Знания:</b></p> <p>основы электротехники; простые электрические и монтажные схемы; ассортимент и маркировку применяемых материалов; марки кабелей и проводов; устройство и назначение абонентского оборудования; способы и технологии выполнения монтажных работ; устройство и правила применения такелажных средств; назначение и устройство применяемых измерительных приборов, правила пользования ими; устройство электрифицированного инструмента и механизмов, телефонных аппаратов, ПК, ONT; алгоритм взаимодействия при</p>

		<p>абонентском сервисе; технику безопасности и охрану труда</p>
	<p>ПК 4.3 Выполнять монтаж, демонтаж, первичную инсталляцию, мониторинг, диагностику инфокоммуникационных систем передачи в соответствии с действующими отраслевыми стандартами.</p>	<p><b>Практический опыт:</b> по монтажу и кроссировке станционных кабелей; по прокладке и монтажу перемычек заземления на распределительной коробке, на защитные полосы кросса; проводить монтаж оптических станционных кроссов; проводить работы по демонтажу простых деталей оборудования; установки абонентского телекоммуникационного оборудования; настройки абонентского оборудования; подключать PLC адаптера; монтажа коннекторов, розеток электрического кабеля «витая пара»</p> <p><b>Умения:</b> выявлять недостатки и причины в работе компьютера; проводить сверление и пробивку отверстий по готовой разметке; проводить установку электрической розетки; проводить крепление стыков металлоконструкций монтажными болтами, установку дюбелей; проводить тестирование сети абонентских подключений; проводить прокладку и крепление кабелей в коробах, резку кабеля по размерам; проводить чистку коннекторов на оптических шнурах; проводить тестирование кроссового и абонентского оборудования; проводить инфокоммуникационных устройств абонентского подключения; проводить инсталляцию, настройку и обслуживание IP телефонии; осуществлять клиентский сервис при проведении работ у абонента.</p> <p><b>Знания:</b> основы электротехники; простые электрические и монтажные схемы; ассортимент и маркировку применяемых материалов; марки кабелей и проводов; устройство и назначение абонентского оборудования;</p>

		способы и технологии выполнения монтажных работ; устройство и правила применения такелажных средств; назначение и устройство применяемых измерительных приборов, правила пользования ими; устройство электрифицированного инструмента и механизмов, телефонных аппаратов, ПК, ONT; алгоритм взаимодействия при абонентском сервисе; технику безопасности и охрану труда
--	--	--

**ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ,  
СООТВЕТСТВУЮЩИХ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ  
ВЫПУСКНИКОВ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ПО  
СПЕЦИАЛЬНОСТИ 10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ**

№ п/п	Код профессионального стандарта	Наименование профессионального стандarta	Уровень квалификации
1	06.030	Профессиональный <a href="#">стандарт</a> "Специалист по защите информации в телекоммуникационных системах и сетях", утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. N 536н (зарегистрирован Министерством юстиции Российской Федерации 18.10.2022 г., регистрационный N 70596)	5
2	06.032	Профессиональный <a href="#">стандарт</a> "Специалист по безопасности компьютерных систем и сетей", утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. N 533н (зарегистрирован Министерством юстиции Российской Федерации 14 октября 2022 г., регистрационный N 70515)	5
3	06.033	Профессиональный <a href="#">стандарт</a> "Специалист по защите информации в автоматизированных системах", утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. N 525н (зарегистрирован Министерством юстиции Российской Федерации 14 октября 2022 г., регистрационный N 70543)	5
4	06.034	Профессиональный <a href="#">стандарт</a> "Специалист по технической защите информации", утвержден приказом Министерства труда и социальной	5

		защиты Российской Федерации от 09 августа 2022 г. N 474н (зарегистрирован Министерством юстиции Российской Федерации 09 сентября 2022 г., регистрационный N 70015)	
--	--	--	--

## СОПОСТАВЛЕНИЕ ФГОС И ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ

<b>ФГОС СПО</b>	<b>Профессиональный стандарт</b>
ВД1: Эксплуатация информационно-телекоммуникационных систем и сетей	ОТФ А: Выполнение комплекса мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НД и компьютерных атак (ПС 06.030 Специалист по защите информации в телекоммуникационных системах и сетях) ОТФ А: Техническое обслуживание средств защиты информации в компьютерных системах и сетях (ПС 06.032 Специалист по безопасности компьютерных систем и сетей)
ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно-телекоммуникационных систем и сетей	ТФ А/01.5 Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД (ПС 06.030 Специалист по защите информации в телекоммуникационных системах и сетях) ТФ А/01.5 Установка и настройка средств защиты информации в автоматизированных системах (ПС 06.033 Специалист по защите информации в автоматизированных системах)
ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей	ТФ А/02.5 Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях (ПС 06.032 Специалист по безопасности компьютерных систем и сетей)
ПК 1.3. Проводить техническое обслуживание оборудования информационно-телекоммуникационных систем и сетей	ТФ А/03.5 Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НД, средств для поиска признаков компьютерных атак в сетях электросвязи (ПС 06.030 Специалист по защите информации в телекоммуникационных системах и сетях) ТФ А/03.5 Техническое обслуживание средств защиты информации прикладного и системного программного обеспечения (ПС 06.032 Специалист по безопасности компьютерных систем и сетей)
ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей	ТФ А/02.5 Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НД, средств для поиска признаков компьютерных атак в сетях электросвязи (ПС 06.030 Специалист по защите информации в телекоммуникационных системах и сетях)
<b>Практический опыт</b>	<b>Трудовые действия</b>
монтаже, настройке, проверке функционирования и конфигурировании оборудования ИТКС; текущем контроле функционирования оборудования ИТКС; проведении технического обслуживания, диагностике технического состояния, поиске неисправностей и	Монтаж оборудования СССЭ Первичная настройка и проверка функционирования СССЭ Монтаж программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД Установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НД

ремонте оборудования ИТКС.	Первичная настройка и проверка функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД
ВД2: Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	<p>ОТФ А: Выполнение комплекса мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НД и компьютерных атак (ПС 06.030 Специалист по защите информации в телекоммуникационных системах и сетях)</p> <p>ОТФ А: Техническое обслуживание средств защиты информации в компьютерных системах и сетях (ПС 06.032 Специалист по безопасности компьютерных систем и сетей)</p> <p>ОТФ А: Проведение работ по установке и техническому обслуживанию средств защиты информации (ПС 06.034 Специалист по технической защите информации)</p>
ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей	<p>ТФ А/01.5 Проведение технического обслуживания систем защиты информации автоматизированных систем (ПС 06.033 Специалист по защите информации в автоматизированных системах)</p> <p>ТФ А/03.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программных (программно-технических) средств защиты информации от несанкционированного доступа (ПС 06.034 Специалист по технической защите информации)</p>
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях	ТФ А/02.5 Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НД, средств для поиска признаков компьютерных атак в сетях электросвязи (ПС 06.030 Специалист по защите информации в телекоммуникационных системах и сетях)
ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями	ТФ А/03.5 Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НД, средств для поиска признаков компьютерных атак в сетях электросвязи (ПС 06.030 Специалист по защите информации в телекоммуникационных системах и сетях)
Практический опыт	Трудовые действия
установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей;	<p>Установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НД</p> <p>Первичная настройка и проверка функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД</p> <p>Ввод в эксплуатацию программно-аппаратных средств защиты информации в операционных системах</p>

<p>поддержании бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях;</p> <p>защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.</p>	<p>Установка программно-аппаратных средств защиты информации Настройка программно-аппаратных средств защиты информации, в том числе средств антивирусной защиты, в операционных системах по заданным шаблонам Установка средств антивирусной защиты в соответствии с действующими требованиями Инструктирование пользователей по порядку безопасной работы в операционных системах Проверка работоспособности системы защиты информации автоматизированной системы Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации Контроль стабильности характеристик системы защиты информации автоматизированной системы Установка и настройка программных (программно-технических) средств защиты информации от несанкционированного доступа Испытания программных (программно-технических) средств защиты информации от несанкционированного доступа Техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа Обнаружение и исправление ошибок в программных средствах защиты информации от несанкционированного доступа Устранение неисправностей и организация ремонта программно-технических средств защиты информации от несанкционированного доступа</p>
<p>ВДЗ: Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты</p>	<p>ОТФ А: Проведение работ по установке и техническому обслуживанию средств защиты информации (ПС 06.034 Специалист по технической защите информации)</p>
<p>ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях</p>	<p>ТФ А/02.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от утечки по техническим каналам (ПС 06.034 Специалист по технической защите информации)</p>
<p>ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях</p>	<p>ТФ А/03.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от ее утечки по техническим каналам (ПС 06.034 Специалист по технической защите информации)</p>
<p>ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в</p>	<p>ТФ А/03.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программных (программно-технических) средств защиты информации от несанкционированного доступа (ПС 06.034 Специалист по технической защите информации)</p>

соответствии с предъявляемыми требованиями	
ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей	ТФ А/03.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программных (программно-технических) средств защиты информации от несанкционированного доступа (ПС 06.034 Специалист по технической защите информации)
<b>Практический опыт</b>	<b>Трудовые действия</b>
установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам; защите информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями; проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.	Установка и монтаж технических средств защиты акустической речевой информации от утечки по техническим каналам Настройка и испытания технических средств защиты акустической речевой информации от утечки по техническим каналам Техническое обслуживание технических средств защиты акустической речевой информации от утечки по техническим каналам Устранение неисправностей и организация ремонта технических средств защиты акустической речевой информации от утечки по техническим каналам Установка и настройка программных (программно-технических) средств защиты информации от несанкционированного доступа Испытания программных (программно-технических) средств защиты информации от несанкционированного доступа Техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа Обнаружение и исправление ошибок в программных средствах защиты информации от несанкционированного доступа Устранение неисправностей и организация ремонта программно-технических средств защиты информации от несанкционированного доступа

## ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОП СПО С УЧЕТОМ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ

ФГОС СПО	Профессиональный стандарт 06.030	06.030
	Специалист по защите информации в телекоммуникационных системах и сетях	
	<b>ТФ А/01.5 Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД</b>	
<b>Уметь</b>	<b>Трудовые действия</b>	<b>Необходимые умения</b>
Осуществлять техническую эксплуатацию линейных сооружений связи Производить монтаж кабельных линий и оконечных кабельных устройств Настраивать, эксплуатировать и обслуживать оборудование ИТКС Осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС	Монтаж оборудования СССЭ Первичная настройка и проверка функционирования СССЭ Монтаж программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД Установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НД Первичная настройка и проверка функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД	Проводить проверку комплектности СССЭ, средств и систем защиты СССЭ от НД Проводить монтаж (для программных средств - установку) СССЭ, средств и систем защиты СССЭ от НД Проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НД
<b>Знать</b>	<b>Необходимые знания</b>	
Принципы построения и основных характеристик информационно-телекоммуникационных систем и сетей (далее - ИТКС) Принципы передачи информации в ИТКС Виды и характеристики сигналов в ИТКС Виды помех в каналах связи ИТКС и методы защиты от них Разновидности линий передач, конструкции и характеристики электрических и оптических кабелей связи Технологии и оборудование	Номенклатура, функциональное назначение и основные характеристики СССЭ Номенклатура, функциональное назначение и основные характеристики средств и систем защиты СССЭ от НД Нормативные требования к составу и содержанию эксплуатационной документации СССЭ, а также средств и систем защиты СССЭ от НД Нормативные правовые акты в области связи, информатизации и защиты информации	

удаленного доступа в ИТКС Принципы построения, основные характеристики активного сетевого и коммуникационного оборудования ИТКС		
	<b>ТФ А/02.5 Обеспечение бесперебойной работы СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</b>	
<b>Уметь</b>	<b>Трудовые действия</b>	<b>Необходимые умения</b>
Осуществлять техническую эксплуатацию линейных сооружений связи проводить работы по техническому Обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС	<p>Текущий, в том числе автоматизированный, контроль функционирования СССЭ с установленными показателями</p> <p>Текущий, в том числе автоматизированный, контроль функционирования с установленными показателями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</p> <p>Внесение изменений в настройки СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи без прерывания процесса их функционирования</p>	<p>Проводить текущий контроль показателей и процесса функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи, предусмотренный регламентом их эксплуатации</p> <p>Выполнять предусмотренные в технической документации работы по изменению настроек СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</p> <p>Проводить предусмотренные регламентом работы по восстановлению процесса и параметров функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</p>
<b>Знать</b>		<b>Необходимые знания</b>

<p>Принципы построения и основных характеристик информационно-телекоммуникационных систем и сетей (далее - ИТКС)</p> <p>Принципы передачи информации в ИТКС</p> <p>Виды и характеристики сигналов в ИТКС</p> <p>Виды помех в каналах связи ИТКС и методы защиты от них</p> <p>Разновидности линий передач, конструкции и характеристики электрических и оптических кабелей связи</p> <p>Технологии и оборудование удаленного доступа в ИТКС</p> <p>Принципы построения, основные характеристики активного сетевого и коммуникационного оборудования ИТКС</p>	<p>Восстановление процесса функционирования после сбоев и отказов СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</p> <p>Восстановление значений показателей функционирования СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</p>	<p>Типы, основные характеристики средств измерений и контроля процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</p> <p>Последовательность действий в целях изменения настроек СССЭ, а также средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи без прерывания процесса их функционирования</p> <p>Последовательность действий в целях восстановления процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</p> <p>Организационные меры по защите информации</p> <p>Нормативные правовые акты в области связи, информатизации и защиты информации, обеспечения безопасности критической информационной инфраструктуры</p>
<b>ТФ А/03.5 Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</b>	<b>Трудовые действия</b>	<b>Необходимые умения</b>
<p>Уметь</p> <p>Осуществлять техническую эксплуатацию линейных сооружений связи</p> <p>Производить монтаж кабельных линий и оконечных кабельных устройств</p> <p>Настраивать, эксплуатировать и обслуживать оборудование ИТКС</p> <p>Осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС</p> <p>Производить испытания, проверку и</p>	<p>Диагностика СССЭ штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами</p> <p>Диагностика программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами</p> <p>Выполнение предусмотренных регламентом операций по техническому обслуживанию</p>	<p>Обнаруживать неисправности СССЭ, а также средств и подсистем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи согласно технической документации</p> <p>Взаимодействовать с организациями, осуществляющими гарантийный и послегарантийный ремонт СССЭ, а также средств и подсистем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</p> <p>Проводить работы по техническому обслуживанию, в том числе по обновлению версий программного обеспечения, СССЭ, а также средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи</p>

приемку оборудования ИТКС Проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС	средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи Обновление в соответствии с регламентом эксплуатации программных компонентов СССЭ, программных, программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи	Устранять неисправности СССЭ, а также средств и подсистем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи, если это предусмотрено технической документацией
<b>Знать</b>		<b>Необходимые знания</b>
Принципы построения и основных характеристик информационно-телекоммуникационных систем и сетей (далее - ИТКС) Принципы передачи информации в ИТКС Виды и характеристики сигналов в ИТКС Виды помех в каналах связи ИТКС и методы защиты от них Разновидности линий передач, конструкции и характеристики электрических и оптических кабелей связи Технологии и оборудование удаленного доступа в ИТКС Принципы построения, основные характеристики активного сетевого и коммуникационного оборудования ИТКС		Организация и содержание диагностики и технического обслуживания СССЭ, а также средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи Правила ведения эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи Методики и приемы ремонта СССЭ, а также средств и систем защиты СССЭ от НД, средств для поиска признаков компьютерных атак в сетях электросвязи
ФГОС СПО	Профессиональный стандарт 06.032 <b>Специалист по безопасности компьютерных систем и сетей</b>	06.032
Уметь	Трудовые действия	Необходимые умения

<p>Осуществлять техническую эксплуатацию линейных сооружений связи</p> <p>Настраивать, эксплуатировать и обслуживать оборудование ИТКС</p> <p>Осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС</p> <p>Производить испытания, проверку и приемку оборудования ИТКС</p> <p>Проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС</p>	<p>Ввод в эксплуатацию программно-аппаратных средств защиты информации в компьютерных сетях</p> <p>Установка программно-аппаратных средств защиты информации в компьютерных сетях</p> <p>Установка средств межсетевого экранования в соответствии с действующими требованиями по защите информации</p> <p>Настройка программно-аппаратных средств защиты информации в компьютерных сетях по заданным шаблонам</p> <p>Устранение неисправностей программно-аппаратных средств защиты информации в компьютерных сетях согласно технической документации</p> <p>Инструктирование пользователей по порядку безопасной работы в компьютерных сетях</p> <p>Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в компьютерных сетях</p>	<p>Применять программно-аппаратные средства защиты информации в компьютерных сетях</p> <p>Устанавливать межсетевые экраны в компьютерных сетях</p> <p>Конфигурировать межсетевые экраны в соответствии с заданными правилами</p> <p>Контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами</p> <p>Работать в компьютерных сетях с соблюдением действующих требований по защите информации</p> <p>Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в компьютерных сетях</p> <p>Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации</p> <p>Формулировать предложения по применению программно-аппаратных средств защиты информации в компьютерных сетях</p>
<b>Знать</b>		<p><b>Необходимые знания</b></p> <p>Топология и протоколы сетевого взаимодействия, применяемые в эксплуатируемых компьютерных сетях</p> <p>Состав и основные характеристики оборудования, применяемого при построении компьютерных сетей</p> <p>Типовые методы и протоколы идентификации, аутентификации и авторизации в компьютерных сетях</p> <p>Типичные сетевые атаки и способы защиты от них</p> <p>Сущность и содержание понятия информационной безопасности, характеристики ее составляющих</p> <p>Основные источники угроз информационной безопасности и меры по их предотвращению</p> <p>Программно-аппаратные средства и методы защиты информации</p> <p>Основные методы организации и проведения технического обслуживания коммутационного оборудования компьютерных сетей</p> <p>Порядок оформления эксплуатационной документации</p> <p>Общие принципы функционирования средств криптографической защиты информации в компьютерных сетях</p>

ИТКС		Порядок обеспечения безопасности информации при эксплуатации компьютерных сетей Формы и методы инструктажа пользователей по порядку работы в компьютерных сетях Нормативные правовые акты в области защиты информации Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры Организационные меры по защите информации
ФГОС СПО	Профессиональный стандарт 06.033 <b>Специалист по защите информации в автоматизированных системах</b>	06.033
<b>ТФ А/01.5 Проведение технического обслуживания систем защиты информации автоматизированных систем</b>		
<b>Уметь</b>	<b>Трудовые действия</b>	<b>Необходимые умения</b>
осуществлять техническую эксплуатацию линейных сооружений связи; производить монтаж кабельных линий и оконечных кабельных устройств; настраивать, эксплуатировать и обслуживать оборудование ИТКС; осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС; производить испытания, проверку и приемку оборудования ИТКС; производить монтаж кабельных линий и оконечных кабельных устройств ИТКС; применять средства измерений характеристик функционирования электрических цепей и сигналов ИТКС;	Ввод в эксплуатацию программно-аппаратных средств защиты информации в операционных системах Установка программно-аппаратных средств защиты информации Настройка программно-аппаратных средств защиты информации, в том числе средств антивирусной защиты, в операционных системах по заданным шаблонам Установка средств антивирусной защиты в соответствии с действующими требованиями Инструктирование пользователей по порядку безопасной работы в операционных системах Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах Восстановление работоспособности программно-аппаратных средств защиты информации в операционных системах согласно технической документации	Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации Производить монтаж и диагностику компьютерных сетей Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи

<b>Знать</b>	Проверка корректности работы программно-аппаратных средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением	<b>Необходимые знания</b> Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях Базовая конфигурация системы защиты информации автоматизированной системы Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах Типовые средства, методы и протоколы идентификации, аутентификации и авторизации Нормативные правовые акты в области защиты информации Организационные меры по защите информации
ФГОС СПО	Профессиональный стандарт 06.032 <b>Специалист по безопасности компьютерных систем и сетей</b>	06.032
	ТФ А/01.5 Техническое обслуживание программно-аппаратных средств защиты информации в операционных системах	
<b>Уметь</b>	<b>Трудовые действия</b> Выявлять и оценивать угрозы безопасности информации в ИТКС Настраивать и применять средства защиты информации в операционных системах, в том числе средства	<b>Необходимые умения</b> Настраивать компоненты подсистем защиты информации операционных систем Управлять учетными записями пользователей, в том числе генерированием, сменой и восстановлением паролей Применять программно-аппаратные средства защиты

<p>антивирусной защиты</p> <p>Проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации</p> <p>Проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации</p> <p>Проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;</p>	<p>Настройка программно-аппаратных средств защиты информации, в том числе средств антивирусной защиты, в операционных системах по заданным шаблонам</p> <p>Установка средств антивирусной защиты в соответствии с действующими требованиями</p> <p>Инструктирование пользователей по порядку безопасной работы в операционных системах</p> <p>Оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах</p> <p>Восстановление работоспособности программно-аппаратных средств защиты информации в операционных системах согласно технической документации</p> <p>Проверка корректности работы программно-аппаратных средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением</p>	<p>информации в операционных системах</p> <p>Применять антивирусные средства защиты информации в операционных системах</p> <p>Работать в операционных системах с соблюдением действующих требований по защите информации</p> <p>Проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах</p> <p>Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации</p> <p>Выполнять резервное копирование и аварийное восстановление работоспособности средств защиты информации</p> <p>Контролировать целостность подсистем защиты информации операционных систем</p> <p>Устранять неисправности подсистем защиты информации операционных систем и программно-аппаратных средств защиты информации согласно технической документации</p> <p>Оформлять эксплуатационную документацию программно-аппаратных средств защиты информации</p>
<p><b>Знать</b></p> <p>Возможные угрозы безопасности информации в ИТКС</p> <p>Способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее</p> <p>Типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях</p> <p>Криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-</p>		<p><b>Необходимые знания</b></p> <p>Архитектура и пользовательские интерфейсы операционных систем</p> <p>Порядок обеспечения безопасности информации при эксплуатации операционных систем</p> <p>Источники угроз информационной безопасности и меры по их предотвращению</p> <p>Сущность и содержание понятия информационной безопасности, характеристики ее составляющих</p> <p>Типовые средства защиты информации в операционных системах</p> <p>Программно-аппаратные средства и методы защиты информации</p> <p>Порядок эксплуатации средств антивирусной защиты в операционных системах</p> <p>Формы и методы инструктирования пользователей по порядку работы в операционных системах</p>

телекоммуникационных системах и сетях Порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации		Общие принципы функционирования программно-аппаратных средств криптографической защиты информации Порядок оформления эксплуатационной документации Нормативные правовые акты в области защиты информации Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры Организационные меры по защите информации
ФГОС СПО	Профессиональный стандарт 06.034 <b>Специалист по технической защите информации</b>	06.034
<b>ТФ А/03.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программных (программно-технических) средств защиты информации от несанкционированного доступа</b>		
<b>Уметь</b>	<b>Трудовые действия</b>	<b>Необходимые умения</b>
Выявлять и оценивать угрозы безопасности информации в ИТКС Настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты Проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации Проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации Проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты	Установка и настройка программных (программно-технических) средств защиты информации от несанкционированного доступа Испытания программных (программно-технических) средств защиты информации от несанкционированного доступа Техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа Обнаружение и исправление ошибок в программных средствах защиты информации от несанкционированного доступа Устранение неисправностей и организация ремонта программно-технических средств защиты информации от несанкционированного доступа	Производить установку и настройку программных (программно-технических) средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами Проводить испытания программных (программно-технических) средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами Проводить обнаружение и исправление ошибок в программных средствах защиты информации от несанкционированного доступа Проводить техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами Проводить устранение выявленных неисправностей программно-технических средств защиты информации от несанкционированного доступа и при необходимости организовывать их ремонт

<p>информации Проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации Проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации</p>	
<p><b>Знать</b></p> <p>Возможные угрозы безопасности информации в ИТКС Способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее Типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях Порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации</p>	<p><b>Необходимые знания</b></p> <p>Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации от несанкционированного доступа и аттестации автоматизированных систем на соответствие требованиям по защите информации Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах Методы и средства защиты информации от несанкционированного доступа и специальных программных воздействий на нее Средства и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий Технические описания и инструкции по эксплуатации программных (программно-технических) средств защиты информации от несанкционированного доступа Порядок технического обслуживания программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий Порядок устранения неисправностей программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий, организации их ремонта</p>

	<b>ТФ А/02.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от ее утечки по техническим каналам</b>	
<b>Уметь</b>	<b>Трудовые действия</b>	<b>Необходимые умения</b>
<p>Проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам</p> <p>Проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам</p> <p>Использовать средства физической защиты линий связи ИТКС</p>	<p>Установка и монтаж технических средств защиты акустической речевой информации от утечки по техническим каналам</p> <p>Настройка и испытания технических средств защиты акустической речевой информации от утечки по техническим каналам</p> <p>Техническое обслуживание технических средств защиты акустической речевой информации от утечки по техническим каналам</p> <p>Устранение неисправностей и организация ремонта технических средств защиты акустической речевой информации от утечки по техническим каналам</p>	<p>Производить установку и монтаж технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами</p> <p>Проводить настройку и испытания технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с технической документацией, инструкциями по эксплуатации и эксплуатационно-техническими документами</p> <p>Проводить техническое обслуживание технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами</p> <p>Проводить устранение выявленных неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам и при необходимости организовывать их ремонт</p>
<b>Знать</b>	<b>Необходимые знания</b>	
<p>Способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;</p> <p>Основные типы технических средств защиты информации от утечки по техническим каналам</p> <p>Методики измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам</p>	<p>Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации</p> <p>Технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акустоэлектромагнитные)</p> <p>Возможности средств акустической речевой разведки</p> <p>Технические каналы утечки акустической речевой информации, создаваемые за счет возможно внедренных электронных устройств перехвата информации в технические средства и (или) помещения</p> <p>Основные характеристики электронных устройств перехвата информации</p> <p>Способы и средства защиты акустической речевой информации</p>	

<p>Организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам</p> <p>Порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам</p> <p>содержание и организацию работ по физической защите линий связи ИТКС</p> <p>Принципы действия и основные характеристики технических средств физической защиты</p> <p>Законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности</p> <p>Принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях</p>		<p>от утечки по техническим каналам Средства и методики контроля эффективности защиты акустической речевой информации от утечки по техническим каналам Технические описания и инструкции по эксплуатации технических средств защиты речевой информации от утечки по техническим каналам Проектная документация на систему защиты выделенного помещения (в части защиты акустической речевой информации от утечки по техническим каналам) Порядок технического обслуживания технических средств защиты речевой информации от утечки по техническим каналам Порядок устранения неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам и организация их ремонта</p>
	<b>ТФ А/01.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок</b>	
<b>Уметь</b>	<b>Трудовые действия</b>	<b>Необходимые умения</b>
Проводить установку, монтаж, настройку и испытание технических	Установка и монтаж технических средств защиты информации от утечки за счет	Проводить установку и монтаж технических средств защиты информации от утечки за счет побочных электромагнитных

<p>средств защиты информации от утечки по техническим каналам</p> <p>Проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам</p> <p>Проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам</p> <p>Использовать средства физической защиты линий связи ИТКС</p> <p>Применять нормативные правовые акты и нормативные методические документы в области защиты информации</p>	<p>побочных электромагнитных излучений и наводок</p> <p>Настройка и испытание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок</p> <p>Техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок</p> <p>Устранение неисправностей и организация ремонта технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок</p>	<p>излучений и наводок в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами</p> <p>Проводить настройку и испытание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов</p> <p>Проводить техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами</p> <p>Проводить устранение выявленных неисправностей технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок и при необходимости организовывать их ремонт</p>
<p><b>Знать</b></p> <p>Способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;</p> <p>основные типы технических средств защиты информации от утечки по техническим каналам</p> <p>Методики измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам</p> <p>Организацию и содержание</p>		<p><b>Необходимые знания</b></p> <p>Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации</p> <p>Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом высокочастотного облучения основных технических средств и систем и за счет возможно внедренных электронных устройств перехвата информации в основных технических средствах и системах</p> <p>Способы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок</p>

<p>технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам</p> <p>Порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам</p> <p>содержание и организацию работ по физической защите линий связи ИТКС</p> <p>Принципы действия и основные характеристики технических средств физической защиты</p> <p>законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности</p> <p>Принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях</p>		<p>Средства и методики контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок</p> <p>Технические описания и инструкции (руководства) по эксплуатации технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок</p> <p>Проектная документация на систему защиты объекта информатизации (в части защиты объекта от утечки информации за счет побочных электромагнитных излучений и наводок)</p> <p>Порядок технического обслуживания технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.</p> <p>Порядок устранения неисправностей и организации ремонта средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок</p>
ФГОС СПО	Профессиональный стандарт 06.033 Специалист по защите информации в автоматизированных системах	06.033
	<b>ТФ А/01.5 Проведение технического обслуживания систем защиты информации автоматизированных систем</b>	
<b>Уметь</b>	<b>Трудовые действия</b>	<b>Необходимые умения</b>
Выявлять и оценивать угрозы	Проверка работоспособности системы защиты	Конфигурировать параметры системы защиты информации

<p>безопасности информации в ИТКС</p> <p>Настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты</p> <p>Проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации</p> <p>Проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации</p> <p>Проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации</p> <p>Проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации</p> <p>Проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации</p>	<p>информации автоматизированной системы</p> <p>Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации</p> <p>Контроль стабильности характеристик системы защиты информации автоматизированной системы</p>	<p>автоматизированной системы в соответствии с ее эксплуатационной документацией</p> <p>Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации</p> <p>Производить монтаж и диагностику компьютерных сетей</p> <p>Использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи</p>
<b>Знать</b>		<b>Необходимые знания</b>
Возможные угрозы безопасности информации в ИТКС		Проведение технического обслуживания систем защиты информации автоматизированных систем
Способы защиты информации от		Типовые средства и методы защиты информации в локальных и

<p>несанкционированного доступа (далее - НСД) и специальных воздействий на нее</p> <p>Типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях</p> <p>Порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации</p>		<p>глобальных вычислительных сетях</p> <p>Базовая конфигурация системы защиты информации автоматизированной системы</p> <p>Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах</p> <p>Типовые средства, методы и протоколы идентификации, аутентификации и авторизации</p> <p>Нормативные правовые акты в области защиты информации</p> <p>Организационные меры по защите информации</p>
--	--	---

## Матрица соответствия компетенций и составных частей образовательной программы

Индекс	Наименование	Формируемые компетенции
ОП	ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПОДГОТОВКА	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 2.1.
ОУП	Общеобразовательный цикл	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 2.1.
ОУП.01	ОБЯЗАТЕЛЬНЫЕ УЧЕБНЫЕ ПРЕДМЕТЫ	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 2.1.
ОУП.01.01	Учебные предметы базового уровня	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.
ОУП.01.01.01	Русский язык	ОК 05.; ОК 09.
ОУП.01.01.02	Литература	ОК 05.; ОК 06.
ОУП.01.01.03	Иностранный язык	ОК 09.
ОУП.01.01.04	История	ОК 05.; ОК 06.
ОУП.01.01.05	Физическая культура	ОК 08.
ОУП.01.01.06	Основы безопасности и защиты Родины	ОК 06.; ОК 07.
ОУП.01.01.07	Обществознание	ОК 02.; ОК 03.; ОК 04.; ОК 06.
ОУП.01.01.08	География	ОК 01.; ОК 07.
ОУП.01.01.09	Химия	ОК 01.; ОК 02.
ОУП.01.01.10	Биология	ОК 01.; ОК 07.
ОУП.01.02	Учебные предметы углубленного уровня	ОК 01.; ОК 02.; ПК 1.1.; ПК 2.1.
ОУП.01.02.01	Математика (алгебра и начала математического анализа, геометрия, вероятность и статистика)	ОК 01.; ОК 02.
ОУП.01.02.02	Информатика	ОК 02.; ПК 2.1.
ОУП.01.02.03	Физика	ОК 01.; ОК 02.; ПК 1.1.
ОУП.02	ДОПОЛНИТЕЛЬНЫЕ УЧЕБНЫЕ ПРЕДМЕТЫ, КУРСЫ ПО ВЫБОРУ	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.
ОУП.02.01	Индивидуальный проект	ОК 01.; ОК 02.; ОК 04.
ОУП.02.ДВ.01	Учебные предметы, курсы по выбору 1 (ДВ.1)	
ОУП.02.ДВ.01.01	Второй иностранный язык	ОК 09.
ОУП.02.ДВ.01.02	Практикум по иностранному языку	ОК 09.
ОУП.02.ДВ.01.03	Практикум по информатике	ОК 02.
ОУП.02.ДВ.02	Учебные предметы, курсы по выбору 2 (ДВ.2)	

ОУП.02.ДВ.02.01	Родная литература	ОК 05.; ОК 06.
ОУП.02.ДВ.02.02	Практикум решения задач повышенной сложности по математике	ОК 01.; ОК 02.
ОУП.02.ДВ.02.03	История родного края	ОК 05.; ОК 06.
ОУП.02.ДВ.03	Учебные предметы, курсы по выбору 3 (ДВ.3)	
ОУП.02.ДВ.03.01	Родной язык	ОК 05.
ОУП.02.ДВ.03.02	Практикум решения задач по физике	ОК 01.; ОК 02.
ОУП.02.ДВ.03.03	Эффективное поведение на рынке труда	ОК 01.; ОК 03.
ПП	ПРОФЕССИОНАЛЬНАЯ ПОДГОТОВКА	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.; ПК 2.1.; ПК 2.2.; ПК 2.3.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 4.1.; ПК 4.2.; ПК 4.3
ОГСЭ	Общий гуманитарный и социально-экономический цикл	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 08.; ОК 09.
ОГСЭ.01	Основы философии	ОК 01.; ОК 03.; ОК 05.
ОГСЭ.02	История	ОК 05.; ОК 06.
ОГСЭ.03	Иностранный язык в профессиональной деятельности	ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 09.
ОГСЭ.04	Физическая культура	ОК 08.
ОГСЭ.ДВ.01	Дисциплины по выбору 1 (ДВ.1)	
ОГСЭ.ДВ.01.01	Основы социологии и политологии	ОК 02.; ОК 04.; ОК 06.; ОК 09.
ОГСЭ.ДВ.01.02	Основы социализации для лиц с ограниченными возможностями здоровья (адаптационная дисциплина)	ОК 02.; ОК 06.
ОГСЭ.ДВ.01.03	Русский язык и культура речи	ОК 05.; ОК 09.
ЕН	Математический и общий естественнонаучный цикл	ОК 01.; ОК 02.; ОК 03.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.
ЕН.01	Математика	ОК 01.; ОК 02.; ОК 03.
ЕН.02	Информатика	ОК 01.; ОК 02.; ОК 03.; ОК 09.
ЕН.03	Элементы математической логики	ОК 01.; ОК 02.; ОК 03.; ПК 1.1.; ПК 1.2.; ПК 1.3.
ОПЦ	Общепрофессиональный цикл	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.; ПК 2.1.; ПК 2.3.; ПК 3.1.; ПК 3.2.
ОПЦ.01	Электроника и схемотехника	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ПК 1.2.; ПК 1.3.; ПК 3.1.; ПК 3.2.
ОПЦ.02	Основы информационной безопасности	ОК 03.; ОК 06.; ОК 09.
ОПЦ.03	Организационное и правовое обеспечение информационной безопасности	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 06.; ПК 1.4.; ПК 2.1.; ПК 3.2.

ОПЦ.04	Основы алгоритмизации и программирования	ОК 01.; ОК 02.; ОК 03.; ПК 1.1.; ПК 1.4.
ОПЦ.05	Экономика и управление	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 09.; ПК 1.4.
ОПЦ.06	Безопасность жизнедеятельности	ОК 01.; ОК 04.; ОК 06.; ОК 07.; ОК 08.
ОПЦ.07	Технические средства информатизации	ОК 01.; ПК 1.1.; ПК 1.4.; ПК 3.1.
ОПЦ.08	Основы цифровых компетенций	ОК 01.; ОК 02.; ОК 05.; ПК 2.3.
ОПЦ.09	Основы предпринимательской деятельности и финансовой грамотности	ОК 01.; ОК 03.
ОПЦ.10	Инженерная и компьютерная графика	ОК 01.; ОК 02.; ОК 03.
ОПЦ.11	Электротехника	ОК 01.; ОК 02.; ОК 03.; ОК 04.
ОПЦ.12	Вычислительная техника	ОК 01.; ОК 02.; ОК 09.; ПК 1.1.
ОПЦ.13	Операционные системы	ОК 01.; ОК 02.; ОК 09.; ПК 2.1.
ПЦ	Профессиональный цикл	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.; ПК 2.1.; ПК 2.2.; ПК 2.3.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 4.1.; ПК 4.2.; ПК 4.3
ПМ.01	Эксплуатация информационно-телекоммуникационных систем и сетей	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.
МДК.01.01	Приемо-передающие устройства, линейные сооружения связи и источники электропитания	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.
МДК.01.02	Телекоммуникационные системы и сети	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.
МДК.01.03	Электрорадиоизмерения и метрология	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.
УП.01.01	Учебная практика	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.
ПП.01.01	Производственная практика	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.
ПМ.01.01(К)	Экзамен по модулю	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.
ПМ.02	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.; ПК 2.1.; ПК 2.2.; ПК 2.3.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 4.1.; ПК 4.2.; ПК 4.3
МДК.02.01	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 2.1.; ПК 2.2.; ПК 2.3.
МДК.02.02	Криптографические средства защиты информации	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 2.1.; ПК 2.2.; ПК 2.3.
МДК.02.03	Технология разработки и защиты баз данных	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 2.1.; ПК 2.2.; ПК 2.3.
УП.02.01	Учебная практика	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 2.1.; ПК 2.2.; ПК 2.3.
ПП.02.01	Производственная практика	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 2.1.; ПК 2.2.; ПК 2.3.

ПП.02.02	Производственная практика (преддипломная практика)	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.; ПК 2.1.; ПК 2.2.; ПК 2.3.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 4.1.; ПК 4.2.; ПК 4.3
ПМ.02.01(К)	Экзамен по модулю	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 09.; ПК 2.1.; ПК 2.2.; ПК 2.3.
ПМ.03	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.
МДК.03.01	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.
МДК.03.02	Физическая защита линий связи информационно-телекоммуникационных систем и сетей	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.
УП.03.01	Учебная практика	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.
ПП.03.01	Производственная практика	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.
ПМ.03.01(К)	Экзамен по модулю	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.
ПМ.04	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ПК 1.1.; ПК 4.1; ПК 4.2; ПК 4.3
МДК.04.01	Выполнение работ по профессии рабочих Монтажник оборудования связи	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ПК 1.1.; ПК 4.1; ПК 4.2; ПК 4.3
УП.04.01	Учебная практика	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ПК 4.1; ПК 4.2; ПК 4.3
ПП.04.01	Производственная практика	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ПК 4.1; ПК 4.2; ПК 4.3
ПМ.04.01(К)	Квалификационный экзамен	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ПК 1.1.; ПК 4.1; ПК 4.2; ПК 4.3
ГИА	Государственная итоговая аттестация	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.; ПК 2.1.; ПК 2.2.; ПК 2.3.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 4.1; ПК 4.2; ПК 4.3
ГИА.01(Г)	Демонстрационный экзамен	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.; ПК 2.1.; ПК 2.2.; ПК 2.3.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 4.1; ПК 4.2; ПК 4.3
ГИА.02(Д)	Защита дипломного проекта (работы)	ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 07.; ОК 08.; ОК 09.; ПК 1.1.; ПК 1.2.; ПК 1.3.; ПК 1.4.; ПК 2.1.; ПК 2.2.; ПК 2.3.; ПК 3.1.; ПК 3.2.; ПК 3.3.; ПК 3.4.; ПК 4.1; ПК 4.2; ПК 4.3

## **4 Структура и объем образовательной программы**

Образовательная программа реализуется на базе основного общего образования на основе требований федерального государственного образовательного стандарта среднего общего образования и ФГОС СПО с учетом получаемой специальности.

В соответствии с требованиями ФГОС образовательная программа имеет следующую структуру:

- общеобразовательный цикл;
- общий гуманитарный и социально-экономический цикл;
- математический и общий естественнонаучный цикл;
- общепрофессиональный цикл;
- профессиональный цикл;
- государственная итоговая аттестация.

Структура образовательной программы включает обязательную часть и часть, формируемую участниками образовательных отношений (вариативную часть). Объем обязательной части ППССЗ по учебным циклам соответствует требованиям ФГОС (69,5%). Вариативная часть образовательной программы дает возможность расширения основных видов деятельности, к которым должен быть готов выпускник, освоивший образовательную программу, согласно получаемой квалификации, углубления подготовки обучающегося, а также получения дополнительных компетенций, необходимых для обеспечения конкурентоспособности выпускника в соответствии с запросами регионального рынка труда и составляет 30,5%.

Обязательная часть общего гуманитарного и социально-экономического цикла базовой подготовки предусматривает изучение следующих обязательных дисциплин: «Основы философии», «История», «Иностранный язык в профессиональной деятельности», «Физическая культура». Общий объем дисциплины «Физическая культура» соответствует требованиям ФГОС.

В общепрофессиональном цикле предусмотрено изучение дисциплины «Безопасность жизнедеятельности» в объеме 68 часов, из них на освоение основ военной службы (для юношей) - 70 процентов от общего объема времени, отведенного на указанную дисциплину (для подгрупп девушек может использоваться на освоение основ медицинских знаний).

Профессиональный цикл образовательной программы включает профессиональные модули, которые формируются в соответствии с основными видами деятельности, предусмотренными ФГОС по специальности и практики.

В профессиональный цикл образовательной программы входят следующие виды практик: учебная практика и производственная (в рамках профессиональных модулей и преддипломная) практика. Учебная и производственная практики в рамках профессиональных модулей проводятся при освоении обучающимися профессиональных компетенций и реализуются

в несколько периодов. Часть образовательной программы, выделяемой на проведение всех видов практик, определена в объеме 38,95% от профессионального цикла.

Объем учебной нагрузки обучающегося составляет 36 академических часов в неделю, включая все виды работы: во взаимодействии с преподавателем и самостоятельную работу.

Структура ППССЗ, соотношение объемов обязательной и вариативной части в соответствии требованиями ФГОС СПО, а также с учетом примерной основной образовательной программы представлена в таблице:

**Структура и объем ППССЗ**

Наименование учебных циклов	Объем образовательной программы в академических часах		
	всего	обязательная часть	вариативная часть
<b>Общеобразовательный цикл</b>	<b>1476</b>	<b>1209</b>	267
<b>Общий гуманитарный и социально-экономический цикл</b>	<b>563</b>	<b>468</b>	<b>95</b>
<b>Математический и общий естественнонаучный цикл</b>	<b>300</b>	<b>144</b>	<b>156</b>
<b>Общепрофессиональный цикл</b>	<b>1135</b>	<b>577</b>	<b>558</b>
<b>Профессиональный цикл:</b>	<b>2250</b>	<b>1763</b>	<b>487</b>
Профессиональные модули	1386	1015	371
Учебная практика	252	216	36
Производственная практика	612	532	80
<b>Государственная итоговая аттестация</b>	<b>216</b>	<b>216</b>	-
Общий объем образовательной программы на базе основного общего образования, включая получение среднего общего образования на основе требований федерального государственного образовательного стандарта среднего общего образования	<b>5940</b>	<b>4377</b>	<b>1563</b>

## **5 Документы, регламентирующие содержание и организацию образовательного процесса при реализации образовательной программы**

Содержание и организация образовательного процесса при реализации образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем регламентируется учебным планом, календарным учебным графиком, рабочими программами дисциплин (модулей), программами учебных и производственных практик, а также методическими материалами,

обеспечивающими качество подготовки и воспитания обучающихся, и реализацию соответствующих образовательных технологий.

### **5.1 Учебный план**

Учебный план определяет перечень, трудоемкость, последовательность и распределение по периодам обучения учебных предметов, курсов дисциплин (модулей), практики, иных видов учебной деятельности обучающихся и формы промежуточной аттестации.

Учебный план представлен в приложении.

### **5.2 Календарный учебный график**

В календарном учебном графике определены сроки изучения учебных дисциплин, междисциплинарных курсов, прохождения учебной и производственной практики обучающихся, промежуточной аттестации, каникул, итоговой государственной аттестации.

Календарный учебный график представлен в приложении.

### **5.3 Рабочие программы дисциплин (модулей)**

Рабочие программы дисциплин (модулей) разработаны в соответствии с Положением «О порядке разработки рабочей программы учебной дисциплины (профессионального модуля) среднего профессионального образования».

В образовательной программе представлены следующие рабочие программы дисциплин (модулей): Русский язык, Литература, Иностранный язык, История, Физическая культура, Основы безопасности и защиты Родины, Обществознание, География, Химия, Биология, Учебные предметы углубленного уровня: Математика (алгебра и начала математического анализа, геометрия, вероятность и статистика), Информатика, Физика; ДОПОЛНИТЕЛЬНЫЕ УЧЕБНЫЕ ПРЕДМЕТЫ, КУРСЫ ПО ВЫБОРУ: Индивидуальный проект; Учебные предметы, курсы по выбору 1: Второй иностранный язык, Практикум по иностранному языку, Практикум по информатике; Учебные предметы, курсы по выбору 2: Родная литература, Практикум решения задач повышенной сложности по математике, История родного края; Учебные предметы, курсы по выбору 3: Родной язык, Практикум решения задач по физике, Эффективное поведение на рынке труда;

**ПРОФЕССИОНАЛЬНАЯ ПОДГОТОВКА:** Основы философии, История, Иностранный язык в профессиональной деятельности, Физическая культура, Основы социологии и политологии, Основы социализации для лиц с ограниченными возможностями здоровья (адаптационная дисциплина), Русский язык и культура речи, Математика, Информатика, Элементы математической логики, Инженерная и компьютерная графика, Электротехника, Электроника и схемотехника, Основы информационной безопасности, Основы алгоритмизации и программирования, Экономика и управление, Безопасность жизнедеятельности, Организационно-правовое

обеспечение информационной безопасности, Технические средства информатизации, Вычислительная техника, Операционные системы, Основы предпринимательской деятельности и финансовой грамотности, Основы цифровых компетенций, Эксплуатация информационно-телекоммуникационных систем и сетей, Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты, Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.

В рабочих программах учебных дисциплин (профессиональных модулей) отражены все виды учебных занятий, промежуточной аттестации, предусмотренные учебным планом, предусмотрено использование активных и интерактивных форм проведения занятий (компьютерных симуляций, деловых и ролевых игр, разбора конкретных ситуаций, психологических и иных тренингов, групповых дискуссий и др.).

Рабочие программы учебных дисциплин и профессиональных модулей представлены в приложении.

#### **5.4 Программы учебной и производственной практик**

Программы практик разработаны в соответствии с Положением «О практике обучающихся среднего профессионального образования».

Практика имеет целью комплексное освоение студентами всех видов профессиональной деятельности по специальности (профессии) СПО, формирование общих и профессиональных компетенций, а также приобретение студентами необходимых умений и опыта практической работы по специальности (профессии).

Видами практики студентов, осваивающих образовательные программы СПО, являются: учебная практика и производственная (в рамках профессиональных модулей и преддипломная) практика.

Учебная практика направлена на формирование у студентов умений, приобретение первоначального практического опыта и реализуется в рамках профессиональных модулей образовательной программы для последующего освоения обучающего общих и профессиональных компетенций по избранной специальности.

Производственная практика включает в себя следующие этапы: производственная практика (в рамках профессиональных модулей) и производственная практика (преддипломная).

Производственная практика (в рамках профессиональных модулей) направлена на формирование у студентов общих и профессиональных компетенций, приобретение практического опыта и реализуется в рамках профессиональных модулей образовательной программы СПО по каждому из видов профессиональной деятельности, предусмотренных ФГОС СПО по специальности.

Производственная практика (преддипломная) является завершающим этапом обучения, она направлена на углубление студентами первоначального практического опыта, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению выпускной квалификационной работы в организациях различных организационно-правовых форм.

Учебная практика организуется в лабораториях и компьютерных классах филиала.

Основными базами производственной практики студентов являются профильные организации ООО ИПФ «Беталир-Информ», АО ИРК «Принт-ТВ». Имеющиеся базы практики обеспечивают возможность прохождения практики всеми студентами в соответствии с учебным планом.

Рабочие программы учебных и производственных практик представлены в приложении.

## **5.5 Программа государственной итоговой аттестации**

Государственная итоговая аттестация выпускника является обязательной и осуществляется после освоения ППССЗ в полном объеме.

Программа государственной итоговой аттестации отражает цели и задачи, формы проведения, учебно-методическое и информационное обеспечение государственной итоговой аттестации, перечень примерных тем ВКР.

Программа государственной итоговой аттестации включает требования к дипломным проектам (работам) и порядку их выполнения, критерии оценки результатов защиты дипломных проектов (работ) и проводится в соответствии с Положением «О порядке проведения государственной итоговой аттестации выпускников среднего профессионального образования».

Программа государственной итоговой аттестации по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем представлена в приложении.

## **5.6 Методические материалы**

Для формирования требуемых ФГОС СПО результатов обучения - профессиональных и общих компетенций, основанных на практическом опыте, умениях, знаниях необходимо выполнение лабораторных, практических работ, курсовых работ (проектов), предусмотренных учебным планом.

Методические материалы включают в себя указания к практическим и лабораторным занятиям, методические указания по выполнению курсовой работы (курсового проекта), указания по организации самостоятельной работы обучающихся.

Методические материалы разработаны на основании следующих локальных актов:

- Положение «Об организации выполнения и защиты курсовой работы (проекта) обучающимися среднего профессионального образования»;
- Положение «Об организации самостоятельной работы обучающихся среднего профессионального образования»;
- Положение «О планировании, организации и проведении лабораторных и практических занятий обучающихся среднего профессионального образования»

## **6 Документы, регламентирующие содержание и организацию воспитательной работы при реализации образовательной программы**

### **6.1 Рабочая программа воспитания**

Рабочая программа воспитания является частью образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем и определяет комплекс ключевых характеристик системы воспитательной работы филиала принципы, методологические подходы, цель, задачи, направления, формы, средства и методы воспитания, планируемые результаты и др.

Рабочая программа воспитания представлена в приложении.

### **6.2 Календарный план воспитательной работы**

Календарный план воспитательной работы, конкретизирует перечень событий и мероприятий воспитательной направленности, которые организуются и проводятся в филиале и в которых обучающиеся как субъекты воспитательного процесса принимают участие.

Календарный план воспитательной работы представлен в приложении.

## **7 Оценка качества освоения образовательной программы**

Контроль качества освоения образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем включает в себя текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию обучающихся.

Для проведения текущего контроля успеваемости и промежуточной аттестации студентов на соответствие их достижений планируемым результатам освоения образовательной программы - компетенциям, созданы фонды оценочных средств по всем учебным дисциплинам (модулям) учебного плана.

Фонд оценочных средств для проведения текущего контроля успеваемости содержит: контрольные вопросы, типовые задания для практических занятий, лабораторных и контрольных работ, коллоквиумов, тесты и компьютерные тестирующие программы, примерную тематику

рефератов, ролевые и деловые игры, а также другие формы контроля, позволяющие оценивать степень сформированности компетенций.

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю) или практике включает в себя:

- перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;
- описание показателей и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Для каждого результата обучения по дисциплине (модулю) или практике определены показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

Фонды оценочных средств для промежуточной аттестации по профессиональным модулям и для государственной итоговой аттестации - разработаны и утверждены после положительного заключения представителей работодателей. Для экспертизы фондов оценочных средств по дисциплинам привлечены внешние эксперты, а также преподаватели смежных дисциплин (курсов).

Порядок проведения текущего контроля успеваемости и промежуточной аттестации студентов, государственной итоговой аттестации определяется в локальных нормативных актах университета :

- Положение «Об организации текущего контроля успеваемости и промежуточной аттестации студентов среднего профессионального образования»;
- Положение «Об организации выполнения и защиты курсовой работы (проекта) обучающимися среднего профессионального образования»;
- Положение «О порядке организации и проведении экзамена (квалификационного) для обучающихся среднего профессионального образования».
- Положение «О порядке проведения государственной итоговой аттестации выпускников среднего профессионального образования».

## **8 Условия реализации образовательной программы**

Фактическое ресурсное обеспечение образовательной программы формируется на основе требований к условиям реализации ОП СПО, определяемых ФГОС СПО по специальности.

Фактическое ресурсное обеспечение образовательной программы включает в себя описание кадрового, материально-технического, учебно-методического обеспечения реализации ОП СПО.

## **8.1 Кадровое обеспечение реализации образовательной программы**

Реализация образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, 12 Обеспечение безопасности и имеющих стаж работы в данной профессиональной области не менее 3 лет.

Квалификация педагогических работников образовательной организации отвечает квалификационным требованиям, указанным в Едином квалификационном справочнике должностей руководителей, специалистов и служащих (далее – ЕКС).

Все преподаватели, участвующие в реализации ППССЗ по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, 12 Обеспечение безопасности, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее 3 лет в организациях, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, 12 Обеспечение безопасности, в общем числе педагогических работников, реализующих образовательную программу, соответствует ФГОС СПО.

## **8.2 Материально-техническое обеспечение образовательной программы**

Ливенский филиал ОГУ им. И.С. Тургенева располагает достаточной материально - технической базой, обеспечивающей проведение всех видов лабораторных работ и практических занятий, дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работы студентов, предусмотренных учебным планом специальности и соответствующей действующим санитарным и противопожарным нормам.

Специальные помещения представляют собой учебные аудитории для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для

самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

В учебных аудиториях социально-экономических дисциплин; иностранного языка; математики; нормативного правового обеспечения информационной безопасности имеются комплекты учебно-наглядных пособий, иллюстративного материала.

Учебная аудитория информатики содержит: оборудованные компьютерные места для студентов; локальную сеть с доступом в сеть Интернет, комплект учебно-наглядных пособий, мультимедийное оборудование; программное обеспечение: Операционная система Linux, свободно распространяемое ПО, ежегодно обновляемое ПО; Пакет офисных приложений Libre Office 6.4.4, свободно распространяемое ПО, ежегодно обновляемое ПО; Пакет офисных приложений Apache OpenOffice 4.1.7, свободно распространяемое ПО, ежегодно обновляемое ПО; Веб-браузер Mozilla Firefox 76.0.1, свободно распространяемое ПО, ежегодно обновляемое ПО; Файловый архиватор 7 Zip 20.00, свободно распространяемое ПО, ежегодно обновляемое ПО; Просмотрщик файлов в формате PDF Adobe Reader DC 2019.008.20071, свободно распространяемое ПО, ежегодно обновляемое ПО.

Учебная аудитория безопасности жизнедеятельности имеет набор демонстрационного оборудования и учебно-наглядных пособий, измеритель шума и вибрации ВШВ -003- М2, психрометр аспирационный М-34, анемометр АП-1, люксметр Ю-116, дозиметр ДП-5А, дозиметр «ФОН» ДБГБ-01У, барометр М110.

Уровень оснащения лабораторий достаточен для ведения учебного процесса и соответствует требованиям ФГОС к материально-техническому обеспечению учебного процесса.

Лаборатория электроники и схемотехники содержит: лабораторный комплекс «Электротехника, электрические цепи и основы электроники» (устройство лабораторное по электротехнике К4822-2, столы лабораторные 4.135.042, блоки питания БП4822-2 2.087.051, платы 1 6.120.227, платы 2 6.120.228, платы 3 6.120.229, платы 4 6.120.230, катушки индуктивности L1 5.764.007, сердечник магнитный СМ 7.773.000, модель трансформатора), Стенд «Основы электрических машин и электропривода», Стенд «Основы электропривода», Стенды «Электрические цепи и основы электроники», Стенды «Элементы систем автоматики и вычислительной техники», Комплект «Основы автоматизации и схемотехника» (на базе Arduino). Приборы измерительные: Мультиметры, амперметр постоянного тока 1 А 5.174.001, амперметр переменного тока 1 А 5.174.001-06, миллиамперметр постоянного тока 10 mA 5.174.001-20, миллиамперметр переменного тока

300 mA 5.174.001-26, микроамперметр постоянного тока 50  $\mu$ A 5.174.001-18, ваттметр 0,6 kW 5.172.009, вольтметр постоянного тока 3 V 5.174.001-07, вольтметр постоянного тока 50 V 5.174.001-11, вольтметр переменного тока 50 V 5.174.001-15.

Лаборатория информационных технологий, сетей и систем передачи информации, программирования и баз данных содержит: рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет; программное обеспечение сетевого оборудования; обучающее программное обеспечение; эмуляторы активного сетевого оборудования; программное обеспечение межсетевого экранирования и мониторинга технического состояния активного сетевого оборудования Cisco Packet Tracer, GNS3, Cisco Cloud Service Router 1000V, Kaspersky Endpoint Security 10.

Лаборатория программных и программно-аппаратных средств защиты информации содержит: оборудованные компьютерные места для студентов; локальная сеть с доступом в сеть Интернет, комплект учебно-наглядных пособий; программное обеспечение: операционная система Microsoft Windows XP Home (OEM), пакет офисных приложений Libre Office 6.0.3.2, пакет офисных приложений Apache OpenOffice 4.1.6, Антивирусные программные комплексы - Kaspersky Endpoint Security 10 ; Программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности - Secret Net Studio; Программные и программно-аппаратные средства обнаружения вторжений - Kaspersky Endpoint Security 10, Программно-аппаратный комплекс (ПАК) ViPNet IDS; Средства уничтожения остаточной информации в запоминающих устройствах - Secret Net Studio; Программные средства выявления уязвимостей в АС и СВТ - Windows Vulnerability Scanner, Nikto, Nmap; Программные средства криптографической защиты информации - Secret Net Studio, OpenSSL; Программные средства защиты среды виртуализации – vGate, среда виртуального моделирования электрических цепей, схем и электронного оборудования Fritzing 0.9.3b, веб-браузер Mozilla Firefox 76.0.1, просмотрщик файлов в формате DJV и DjVu Djview 2.1, файловый архиватор 7 Zip 20.00, файловый менеджер Far 3.0 Build 5300; просмотрщик файлов в формате PDF Adobe Reader 2019.008.20071; комплекс автоматизированного проектирования T-FLEX CAD 2D, T-FLEX CAM, T-FLEX Техно-ПРО, T-FLEX ЧПУ, сетевая версия; система автоматизированных расчетов деталей машин APM WinMachine сетевая версия; система трехмерного моделирования Компас-3D сетевая версия; программное обеспечение для контроля и проверки знаний SunRav TestOfficePro..

Лаборатория технических средств защиты информации содержит: комплект учебно-наглядных пособий; аппаратные средства аутентификации пользователя; средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок; средства измерения параметров физических полей (в том числе электромагнитных излучений и наводок, акустических

(виброакустических) колебаний); стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов. Оборудованные компьютерные места для студентов; локальная сеть с доступом в сеть Интернет.

Лаборатория информационных технологий в профессиональной деятельности содержит: оборудованные компьютерные места для студентов; локальная сеть с доступом в сеть Интернет, комплект учебно-наглядных пособий; программное обеспечение: Операционная система Linux, свободно распространяемое ПО, ежегодно обновляемое ПО; Пакет офисных приложений Libre Office 6.4.4, свободно распространяемое ПО, ежегодно обновляемое ПО; Пакет офисных приложений Apache OpenOffice 4.1.7, свободно распространяемое ПО, ежегодно обновляемое ПО; Веб-браузер Mozilla Firefox 76.0.1, свободно распространяемое ПО, ежегодно обновляемое ПО; Файловый архиватор 7 Zip 20.00, свободно распространяемое ПО, ежегодно обновляемое ПО; Просмотрщик файлов в формате PDF Adobe Reader DC 2019.008.20071, свободно распространяемое ПО, ежегодно обновляемое ПО.

В филиале имеется физкультурно – оздоровительный комплекс: спортивный зал с соответствующим спортивным инвентарем; открытый стадион широкого профиля с элементами полосы препятствий; стрелковый тир.

Имеется библиотека, читальный зал с выходом в сеть Интернет, актовый зал.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду организации.

### **8.3 Учебно-методическое обеспечение образовательной программы**

Образовательная программа обеспечена доступом для каждого обучающегося к базам данных и библиотечным фондам, формируемым по всем учебным дисциплинам (модулям). Во время самостоятельной подготовки обучающиеся обеспечены доступом к сети Интернет.

Каждый обучающийся в течение всего периода обучения обеспечен учебными, учебно-методическими печатными и (или) электронными изданиями по всем учебным дисциплинам (модулям) в соответствии с требованиями ФГОС.

Каждому обучающемуся обеспечен доступ к комплектам библиотечного фонда, включая официальные справочно-библиографические и периодические издания, в соответствии с требованиями ФГОС.

Для обучающихся предоставлена возможность доступа к современным профессиональным базам данных и информационным ресурсам сети Интернет.

Обучающиеся имеют доступ к следующим базам данных.

*Электронная библиотека образовательных ресурсов (ЭБОР)*  
<http://elib.oreluniver.ru/>

Доступ осуществляется из любой точки интернета по логину и паролю после регистрации на сайте.

Содержит учебную, учебно-методическую литературу, монографии, выпущенные на полиграфической базе университета, статьи из периодических и продолжающихся изданий, сборников трудов конференций. Документы размещены в БД на основе лицензионных договоров с правообладателями.

*Научная электронная библиотека E-LIBRARY* <https://elibrary.ru/>

Доступ к полнотекстовым электронным периодическим изданиям возможен только с компьютеров филиала в локальной сети по логину и паролю после регистрации каждого пользователя.

Научная электронная библиотека eLibrary - это проект Российского фонда фундаментальных исследований (РФФИ) (г. Москва), который осуществляется в рамках «Программы поддержки российских научных библиотек», начатой РФФИ в 1997 году. Предоставляет доступ к электронным версиям журналов, базам данных по всем направлениям фундаментальной науки.

*ЭБС «Издательство Лань»* <http://e.lanbook.com/>

Доступ осуществляется из любой точки интернета по логину и паролю после регистрации с IP-адреса филиала.

Ресурс, включающий в себя электронные версии книг издательства «Лань» и других ведущих издательств учебной литературы, электронные версии периодических изданий.

Доступны пакеты: Инженерно-технические науки; Социально-гуманитарные науки; Экономика и менеджмент; Информатика.

*Образовательный ресурс «IPRsmart»* <https://www.iprbookshop.ru/>

Доступ осуществляется из любой точки интернета по логину и паролю после регистрации с IP-адреса филиала.

*Образовательная платформа «Юрайт»* <https://urait.ru/>

Доступ осуществляется из любой точки интернета по логину и паролю после регистрации с IP-адреса филиала. Доступны учебники для среднего профессионального образования

*Универсальная база данных электронных периодических изданий ИВИС*  
<https://dlib.eastview.com/browse/udb/12#/>

Доступ осуществляется из локальной сети филиала без предварительной регистрации. Доступ вне стен филиала возможен по логину и паролю.

*Национальный цифровой ресурс РУКОНТ* <http://rucont.ru/>

Для доступа необходимо получить логин и пароль в Зале электронных ресурсов библиотеки филиала

Образовательная программа обеспечена необходимым комплектом лицензионного программного обеспечения, состав которого ежегодно обновляется.

## **9 Характеристика социокультурной среды**

В филиале сформирована благоприятная социокультурная среда, которая обеспечивает возможность формирования общекультурных компетенций выпускника, всестороннего развития личности и способствует освоению основной образовательной программы соответствующего направления подготовки. Социально-воспитательная работа со студентами ориентирована как на формирование социально-значимых качеств, установок и ценностных ориентаций личности, так и на создание благоприятных условий для всестороннего гармоничного нравственного, интеллектуального и физического развития, самосовершенствования и творческой самореализации личности будущего специалиста.

Воспитание в каждом обучающемся человечности, доброты, гражданственности, творческого отношения к деятельности, бережного, внимательного отношения к окружающему миру, владение культурой своего народа – вот ведущие ценности, на которые опирается воспитательная система филиала.

Социокультурная среда формируется с помощью комплекса мероприятий, предполагающих:

- создание оптимальных социокультурных и образовательных условий для социального и профессионального становления личности социально активного, жизнеспособного, гуманистически ориентированного, высококвалифицированного специалиста;
- формирование гражданской позиции, патриотических чувств, ответственности, приумножение нравственных, культурных и научных ценностей в условиях современной жизни, правил хорошего тона,
- сохранение и преумножение традиций филиала;
- создание условий для удовлетворения потребностей личности в интеллектуальном, культурном, нравственном и физическом развитии;
- привитие умений и навыков управления коллективом в различных формах студенческого самоуправления.

Социальная работа с обучающимися в филиале предполагает комплекс мер, направленных на предоставление социальных выплат, льгот нуждающимся, сопровождение обучающихся из числа детей-сирот и детей, оставшихся без попечения родителей, медицинское обслуживание обучающихся, оказание консультативной помощи. Социальная работа с обучающимися осуществляется на основании действующего законодательства РФ, а также локальных нормативных актов.

Воспитательная работа включает в себя следующие направления:

- гражданско-правовое воспитание;
- патриотическое;
- духовно-нравственное воспитание;
- профессионально-трудовое воспитание и содействие занятости молодежи;
- валеологическое воспитание;
- художественно-эстетическое воспитание;

- социально-психологическая поддержка студентов.

В целях воспитания любви и уважения к Родине, формирования гражданственности, толерантности, повышения уровня правовой культуры создан и функционирует Центр духовно-патриотического воспитания студентов. В его структуру входят студенческие клубы, созданные на кафедрах филиала:

Краеведческий клуб «Родник» создан в целях изучения исторических, социально-экономических, культурных аспектов и жизни города и района; проведения анализа научно-исследовательского, литературного материала, умелого использование газетно-журнальной информации, посещения краеведческих экскурсий, обсуждения книг, новинок.

Деятельность клуба молодых избирателей «Демократ» направлена на воспитание активной гражданской позиции, получение правовых знаний о выборах, правовое просвещение, повышение электоральной активности молодых избирателей. Проводятся встречи с депутатами городского совета народных депутатов. Члены клуба активно участвуют в различных конкурсах, организуемых областной и территориальной избирательными комиссиями.

Главной целью работы клуба «Данко» является участие студенческой молодежи в добровольческой (волонтерской) деятельности, направленной на формирование общечеловеческих ценностей в молодежной среде, улучшение благосостояния общества; распространение идей и принципов социального служения среди населения. Студенты принимают активное участие в благоустройстве города и уборке территории в рамках Дней экологической культуры, в акциях «Милосердие», «Больше доноров – больше жизни!», во Всероссийской неделе добра, посещают Дом ветеранов, социально-реабилитационный центр для несовершеннолетних с культурной программой.

В филиале функционирует Центр студенческого творчества, в состав которого входят творческая мастерская «Студенческая волна», разработаны, утверждены и реализуются дополнительные общеразвивающие общеобразовательные программы «Основы вокальной работы в эстрадном коллективе» и «Классическая и современная хореография», которые формируют у обучающихся художественный вкус, приобщают к истокам и сохранению культурных традиций, стимулируют художественное самодеятельное творчество обучающихся.

В филиале реализуются социально значимые проекты «Мы – верные сыны твои, Россия!», «Толерантность – основа мира и культуры», «От сердца к сердцу», «Премия студенческих симпатий «Признание», «Победа ради жизни», «Здоровый студент - здоровая нация», способствующие повышению уровня правовой культуры обучающихся, воспитанию понятий чести, человеческого достоинства, чувства самоуважения, формированию активной жизненной позиции.

В коллективе создана профессиональная и социокультурная толерантная среда, необходимая для формирования гражданской, правовой и

профессиональной позиции соучастия, готовности всех членов коллектива к общению и сотрудничеству, к способности толерантно воспринимать социальные, личностные и культурные различия.

## **10 Список разработчиков образовательной программы**

Декан технико-экономического факультета, канд. техн. наук Ю.А. Бакурова;

и.о. заведующего кафедрой информационных технологий и экономики, канд. экон. наук О.В. Псарева;

представитель профильной организации директор АО ИРК «Принт-ТВ» Г.И. Карзов.