

**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



«УТВЕРЖДАЮ»

Проректор по учебной
деятельности

Е.Н.Алексеева

2022г.

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

**СПЕЦИАЛЬНОСТЬ 10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ**

Утверждена на заседании
Ученого совета ОГУ
имени И.С. Тургенева
Протокол № 12 от 29.04.2022 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.

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 «12» апреля 2022 № 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 «22» апреля 2022 № 4)

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 «26» апреля 2022 № 4).

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.....	4
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	6
4	Структура и объем образовательной программы	48
5	Документы, регламентирующие содержание и организацию образовательного процесса при реализации образовательной программы ...	49
5.1	Учебный план.....	50
5.2	Календарный учебный график	50
5.3	Рабочие программы дисциплин (модулей)	50
5.4	Программы учебной и производственной практик.....	51
5.5	Программа государственной итоговой аттестации.....	52
5.6	Методические материалы	52
6	Документы, регламентирующие содержание и организацию воспитательной работы при реализации образовательной программы	53
7	Оценка качества освоения образовательной программы.....	53
8	Условия реализации образовательной программы.....	54
8.1	Кадровое обеспечение реализации образовательной программы	54
8.2	Материально-техническое обеспечение образовательной программы .	55
8.3	Учебно-методическое обеспечение образовательной программы	58
9	Характеристика социокультурной среды	59
10	Список разработчиков образовательной программы	62

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 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

Наименование основных видов деятельности	Наименование профессиональных модулей	Квалификация 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

Код компетенции	Формулировка компетенции	Знания, умения
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	<p>Умения: 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>Знания: 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>
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	<p>Умения: определять задачи 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.</p> <p>Знания номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации</p>
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие	<p>Умения: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития</p> <p>Знания: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования</p>
ОК 04	Работать в коллективе и команде, эффективно	<p>Умения: организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами</p>

	взаимодействовать с коллегами, руководством, клиентами	Знания: психология коллектива; психология личности; основы проектной деятельности
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Умения: излагать свои мысли на государственном языке; оформлять документы. Знания: особенности социального и культурного контекста; правила оформления документов.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	Умения: описывать значимость своей профессии, применять стандарты антикоррупционного поведения Презентовать структуру профессиональной деятельности по специальности. Знания: сущность гражданско-патриотической позиции. Общечеловеческие ценности. Правила поведения в ходе выполнения профессиональной деятельности.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Умения: соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности. Знания: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Умения: 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 специальности Знания: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения.
ОК 09	Использовать информационные технологии в	Умения: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение

	профессиональной деятельности	Знания: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках	Умения: 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 объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
		Знания: 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
ОК-11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	Умения: 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; Знание: основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты

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.	Практический опыт: монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (далее –ИТКС);
		Умения: осуществлять техническую эксплуатацию линейных сооружений связи; производить монтаж кабельных линий и оконечных кабельных устройств;

		<p>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>ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно – телекоммуникационных систем и сетей.</p>	<p>Знания: 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, конструкции и характеристик электрических и оптических кабелей 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>Практический опыт: текущего контроля функционирования оборудования ИТКС; диагностики технического состояния приёмо-передающих устройств и линейных сооружений связи и источников питания;</p> <p>Умения: осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС; производить испытания, проверку и приемку оборудования ИТКС;</p>

		<p>осуществлять диагностику технического состояния ИТКС; применять средства измерений характеристик функционирования электрических цепей и сигналов ИТКС;</p>
		<p>Знания: 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 проверок контрольно-измерительной аппаратуры; требований метрологического обеспечения функционирования ИБТКС;</p>
	<p>ПК 1.3. Проводить техническое обслуживание оборудования информационно – телекоммуникационных систем и сетей</p>	<p>Практический опыт: проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта оборудования ИТКС;</p> <p>Умения: осуществлять техническую эксплуатацию линейных сооружений связи; 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>Знания: принципов построения и основных характеристик ИТКС; видов и характеристик сигналов в ИТКС; разновидностей линий передач, конструкции и характеристик</p>

		<p>электрических и оптических кабелей связи;</p> <p>принципов построения, основных характеристик активного сетевого и коммуникационного оборудования ИТКС;</p> <p>принципов организации технической эксплуатации ИТКС;</p>
	<p>ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей</p>	<p>Практический опыт:</p> <p>текущего контроля функционирования оборудования ИТКС;</p> <p>мониторинг технического состояния и работоспособности приёмо-передающих устройств и линейных сооружений связи и источников питания ИТКС;</p>
		<p>Умения:</p> <p>осуществлять техническую эксплуатацию линейных сооружений связи;</p> <p>настраивать, эксплуатировать и обслуживать оборудование 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>осуществлять техническую эксплуатацию приёмо-передающих устройств;</p> <p>оформлять эксплуатационно-техническую документацию;</p>
		<p>Знания:</p> <p>принципов построения и основных характеристик ИТКС;</p> <p>принципов передачи информации в ИТКС;</p> <p>видов и характеристик сигналов в ИТКС;</p> <p>видов помех в каналах связи ИТКС и методов защиты от них;</p> <p>принципов построения, основных характеристик активного сетевого и коммуникационного оборудования ИТКС. спецификацию изделий, комплектующих, запасного имущества и принадлежностей ИТКС;</p>
<p>Защита информации в информационно – телекоммуникационных системах и сетях с</p>	<p>ПК 2.1. Производить установку, настройку, испытания и конфигурирование</p>	<p>Практический опыт:</p> <p>установки, настройки, испытаний и конфигурирования программных и программно-аппаратных (в том числе</p>

использованием программно-аппаратных, в том числе криптографических средств защиты	программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно – телекоммуникационных систем и сетей	криптографических) средств защиты информации в оборудовании ИТКС;
		<p>Умения:</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 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>Знания:</p> <p>способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее; типовых программных и программно-аппаратных средств защиты информации в ИТКС;</p> <p>криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;</p>
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях		<p>Практический опыт:</p> <p>поддержания бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС;</p>
		<p>Умения:</p> <p>выявлять и оценивать угрозы безопасности информации в ИТКС; 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</p>

		<p>защиты информации; проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;</p>
		<p>Знания: 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>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.</p>		<p>Практический опыт: 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>Умения: 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>Знания: возможных угроз безопасности информации в ИТКС;</p>

		<p>способов защиты информации НСД и специальных воздействий на нее;</p> <p>типовых программных и программно-аппаратных средств защиты информации в ИТКС;</p> <p>криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;</p> <p>порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации.</p>
<p>Защита информации в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты</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>Практический опыт:</p> <p>установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам;</p>
		<p>Умения:</p> <p>проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;</p> <p>применять нормативные правовые акты и нормативные методические документы в области защиты информации;</p>
		<p>Знания:</p> <p>способов защиты информации от утечки по техническим каналам с использованием технических средств защиты;</p> <p>основных типов технических средств защиты информации от утечки по техническим каналам;</p> <p>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,</p>	<p>Практический опыт:</p> <p>установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим</p>

	устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях	каналам; проведения технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
		Умения: 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;
		Знания: 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;
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	Практический опыт: защиты информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;	
	Умения: 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	

		<p>нормативные методические документы в области защиты информации;</p>
		<p>Знания: способов защиты информации от утечки по техническим каналам с использованием технических средств защиты; основных типов технических средств защиты информации от утечки по техническим каналам; 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; 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>Практический опыт: проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации.</p> <p>Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.</p> <p>Знания: номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.</p>

**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 стандарта	Уровень квалификации
1	06.030	Профессиональный стандарт "Специалист по защите информации в телекоммуникационных системах и сетях", утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. N 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44449)	5
2	06.032	Профессиональный стандарт "Специалист по безопасности компьютерных систем и сетей", утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный N 44464)	5
3	06.033	Профессиональный стандарт "Специалист по защите информации в автоматизированных системах", утвержден приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. N 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный N 43857)	5
4	06.034	Профессиональный стандарт "Специалист по технической защите информации", утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. N 599н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный N 44443)	5

СОПОСТАВЛЕНИЕ ФГОС И ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ

ФГОС СПО	Профессиональный стандарт
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 НСД (ПС Специалист по защите информации в телекоммуникационных системах и сетях) ОТФ А: Обслуживание средств защиты информации в компьютерных системах и сетях (ПС 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 НСД (ПС Специалист по защите информации в телекоммуникационных системах и сетях) ТФ С/01.6 Установка и настройка средств защиты информации в автоматизированных системах (ПС 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 В/01.6 Диагностика систем защиты информации автоматизированных систем (ПС Специалист по защите информации в автоматизированных системах)
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 НСД (ПС Специалист по защите информации в телекоммуникационных системах и сетях) ТФ А/03.5 Обслуживание средств защиты информации прикладного и системного программного обеспечения (ПС Специалист по безопасности компьютерных систем и сетей)
ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей	ТФ В/02.6 Управление функционированием СССЭ, защищенностью от НСД сооружений и СССЭ (ПС Специалист по защите информации в телекоммуникационных системах и сетях)
Практический опыт	Трудовые действия
монтаже, настройке, проверке функционирования и конфигурировании оборудования ИТКС; текущем контроле функционирования оборудования ИТКС; проведении технического обслуживания, диагностике технического состояния, поиске неисправностей и ремонте оборудования 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 НСД Установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НСД Первичная настройка и проверка функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД
ВД2: Защита информации в информационно-телекоммуникационных системах и сетях с	ОТФ В: Обеспечение защиты от НСД сооружений и СССЭ (за исключением сетей связи специального назначения) в процессе их эксплуатации (ПС Специалист по защите

использованием программных и программно-аппаратных, в том числе криптографических средств защиты	информации в телекоммуникационных системах и сетях) ОТФ D: Разработка средств защиты СССЭ (за исключением сетей связи специального назначения) от НСД (ПС Специалист по защите информации в телекоммуникационных системах и сетях) ОТФ С: Оценивание уровня безопасности компьютерных систем и сетей (ПС Специалист по безопасности компьютерных систем и сетей) ОТФ А: Проведение работ по установке и техническому обслуживанию средств защиты информации (ПС Специалист по технической защите информации)
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 оборудовании информационно-телекоммуникационных систем и сетей	ТФ С/01.6 Установка и настройка средств защиты информации в автоматизированных системах (ПС Специалист по защите информации в автоматизированных системах) ТФ А/03.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программно-технических средств защиты информации от несанкционированного доступа (ПС Специалист по технической защите информации)
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях	ТФ В/01.6 Мониторинг функционирования СССЭ, защищенности от НСД сооружений и СССЭ (ПС Специалист по защите информации в 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 НСД (ПС 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 НСД (ПС 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; поддержании бесперебойной работы программных и программно-аппаратных, в том числе	Диагностика СССЭ штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами Диагностика программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами Выполнение предусмотренных регламентом операций по техническому обслуживанию средств и систем защиты СССЭ от НСД Обновление в соответствии с регламентом эксплуатации программных компонентов СССЭ,

<p>криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях; 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>программных, программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НСД Устранение неисправностей СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД своими силами, если это допускается технической документацией Направление в ремонт и прием из ремонта сторонними организациями СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Ведение эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Установка программного обеспечения Настройка программного обеспечения с соблюдением требований по защите информации Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением Настройка встроенных средств защиты информации программного обеспечения по заданным шаблонам Проверка функционирования встроенных средств защиты информации программного обеспечения Своевременное обнаружение признаков наличия вредоносного программного обеспечения</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 Специалист по технической защите информации) ОТФ С: Производство, сервисное обслуживание и ремонт средств защиты информации (ПС 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 Специалист по технической защите информации) ТФ С/02.6 Производство, сервисное обслуживание и ремонт технических средств защиты акустической речевой информации от утечки по техническим каналам (ПС 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-</p>	<p>ТФ С/04.6 Производство, сервисное обслуживание и ремонт защищенных технических средств обработки информации (ПС Специалист по технической защите информации)</p>

телекоммуникационных системах и сетях	
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями	ТФ С/02.6 Производство, сервисное обслуживание и ремонт технических средств защиты акустической речевой информации от утечки по техническим каналам (ПС Специалист по технической защите информации)
ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей	ТФ С/05.6 Производство, сервисное обслуживание и ремонт технических средств контроля эффективности мер защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПС Специалист по технической защите информации)
Практический опыт	Трудовые действия
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

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОП СПО С УЧЕТОМ ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ

ФГОС СПО	Профессиональный стандарт	
	Специалист по защите информации в телекоммуникационных системах и сетях	
	ТФ А/01.5 Установка программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД	
Уметь	Трудовые действия	Необходимые умения
<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>Монтаж оборудования СССЭ</p> <p>Первичная настройка и проверка функционирования СССЭ</p> <p>Монтаж программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД</p> <p>Установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НСД</p> <p>Первичная настройка и проверка функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД</p>	<p>Проводить проверку комплектности СССЭ, средств и систем защиты СССЭ от НСД</p> <p>Проводить монтаж (для программных средств - установку) СССЭ, средств и систем защиты СССЭ от НСД</p> <p>Проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НСД</p>
Знать		Необходимые умения
<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</p>		<p>Номенклатура, функциональное назначение и основные характеристики СССЭ</p> <p>Номенклатура, функциональное назначение и основные характеристики средств и систем защиты СССЭ от НСД</p> <p>Нормативные требования к составу и содержанию эксплуатационной документации СССЭ, а также средств и систем защиты СССЭ от НСД</p> <p>Нормативные правовые акты в области связи, информатизации и защиты информации</p>

удаленного доступа в ИТКС Принципы построения, основные характеристики активного сетевого и коммуникационного оборудования ИТКС		
ТФ А/03.5 Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД		
Уметь	Трудовые действия	Необходимые умения
Осуществлять техническую эксплуатацию линейных сооружений связи проводить работы по техническому Обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС	Диагностика СССЭ штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами Диагностика программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами Выполнение предусмотренных регламентом операций по техническому обслуживанию средств и систем защиты СССЭ от НСД	Обнаруживать неисправности СССЭ, а также средств и подсистем защиты СССЭ от НСД согласно технической документации Взаимодействовать с организациями, осуществляющими гарантийный и послегарантийный ремонт СССЭ, а также средств и подсистем защиты СССЭ от НСД Проводить работы по техническому обслуживанию, в том числе по обновлению версий программного обеспечения, СССЭ, а также средств и систем защиты СССЭ от НСД Устранять неисправности СССЭ, а также средств и подсистем защиты СССЭ от НСД, если это предусмотрено технической документацией
Знать	Обновление в соответствии с регламентом эксплуатации программных компонентов СССЭ, программных, программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НСД	Необходимые знания
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	Устранение неисправностей СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД своими силами, если это допускается технической документацией Направление в ремонт и прием из ремонта сторонними организациями СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД	Организация и содержание диагностики и технического обслуживания СССЭ, а также средств и систем защиты СССЭ от НСД Правила ведения эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Методики и приемы ремонта СССЭ, а также средств и систем защиты СССЭ от НСД

<p>удаленного доступа в ИТКС Принципы построения, основные характеристики активного сетевого и коммуникационного оборудования ИТКС</p>	<p>Ведение эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД</p>	
<p>ТФ В/02.6 Управление функционированием СССЭ, защищенностью от НСД сооружений и СССЭ</p>		
<p>Уметь</p>	<p>Трудовые действия</p>	<p>Необходимые умения</p>
<p>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 Проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС</p>	<p>Определение необходимого состава, особенностей размещения и функциональных возможностей СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Организация и проведение монтажа и настройки СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Контроль соответствия параметров подсистем защиты СССЭ от НСД установленным требованиям, обеспечение своевременной корректировки настроек СССЭ, средств и систем их защиты от НСД в целях реагирования на выявленные нарушения</p>	<p>Осуществлять организацию и проведение монтажа и настройки СССЭ, а также средств и систем защиты СССЭ от НСД Осуществлять организацию бесперебойного функционирования СССЭ, а также средств и систем защиты СССЭ от НСД Использовать встроенные механизмы защиты от НСД в составе СССЭ Устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании Разрабатывать предложения по совершенствованию и повышению эффективности принимаемых технических мер и проводимых организационных мероприятий по защите СССЭ от НСД Организовывать работы по выполнению требований режима защиты информации ограниченного доступа в сети электросвязи Разрабатывать методические материалы и организационно-распорядительные документы по обеспечению защиты сооружений и СССЭ от НСД</p>
<p>Знать</p>	<p>Установка и настройка программного обеспечения, необходимого для управления СССЭ и средствами их защиты от НСД Разработка и организация выполнения мероприятий в соответствии с положениями политики информационной безопасности в сети электросвязи</p>	<p>Необходимые знания</p>
<p>Принципы построения и основных характеристик информационно-телекоммуникационных систем и сетей (далее - ИТКС) Принципы передачи информации в</p>		<p>Возможные угрозы НСД к сооружениям и СССЭ Сетевые протоколы и их параметры настройки Средства и способы обеспечения защиты от НСД к сооружениям и СССЭ, принципы построения средств и систем защиты сооружений и СССЭ от НСД</p>

<p>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</p>	<p>Проведение отдельных мероприятий в рамках аттестации на предмет соответствия требованиям по защите сооружений и СССЭ от НСД</p>	<p>Особенности применения программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Методы комплексного обеспечения защиты сетей электросвязи Показатели эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Нормативные правовые акты в области защиты информации ограниченного доступа Национальные, межгосударственные и международные стандарты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации</p>
ТФ В/01.6 Мониторинг функционирования СССЭ, защищенности от НСД сооружений и СССЭ		
Уметь	Трудовые действия	Необходимые умения
<p>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</p>	<p>Использование средств анализа функциональности СССЭ, защищенности от НСД сооружений и СССЭ Контроль целостности сооружений и СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Составление отчетов по результатам проверок, в том числе выявление инцидентов, которые могут привести к сбоям или нарушению функционирования или возникновению угроз безопасности информации, циркулирующей в СССЭ</p>	<p>Использовать средства мониторинга работоспособности и эффективности применяемых программных, программно-аппаратных (в том числе криптографических) и технических средств защиты СССЭ от НСД Проводить контроль функционирования СССЭ, их защищенности от НСД Определять технические характеристики СССЭ, их защищенности от НСД Оценивать помехоустойчивость и эффективность сетей электросвязи при передаче трафика, оптимизировать их параметры Осуществлять проверки СССЭ, программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД на соответствие заданным требованиям Проводить документационное обеспечение функционирования СССЭ, их защищенности от НСД</p>

информации		
<p>Знать</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-телекоммуникационных системах и сетях</p> <p>Порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации</p> <p>Порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации</p>		<p>Необходимые знания</p> <p>Методы контроля функционирования СССЭ, их защищенности от НСД</p> <p>Принципы построения современных сетей электросвязи, математические модели каналов связи, виды модуляции сигналов</p> <p>Функциональное назначение и основные характеристики средств контроля функционирования СССЭ, их защищенности от НСД</p> <p>Организация и содержание мониторинга функционирования СССЭ, их защищенности от НСД</p> <p>Возможные источники и технические каналы утечки информации</p> <p>Нормативные правовые акты в области связи и защиты информации</p>
	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 НСД	
Уметь	Трудовые действия	Необходимые умения

<p>Выявлять и оценивать угрозы безопасности информации в ИТКС</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>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 НСД</p> <p>Внесение изменений в настройки СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД без прерывания процесса их функционирования</p> <p>Восстановление процесса функционирования после сбоя и отказов СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД</p> <p>Восстановление значений показателей функционирования СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД</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 НСД, 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 НСД</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 НСД</p>
<p>Знать</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</p>		<p>Необходимые знания</p> <p>Типы, основные характеристики средств измерений и контроля процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НСД</p> <p>Последовательность действий в целях изменения настроек СССЭ, а также средств и систем защиты СССЭ от НСД 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 НСД</p> <p>Организационные меры по защите информации</p> <p>Нормативные правовые акты в области связи, информатизации и</p>

<p>сетях Криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях Порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации Организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации Порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации</p>		защиты информации
ФГОС СПО	Профессиональный стандарт Специалист по безопасности компьютерных систем и сетей	
	ТФ А/03.5 Обслуживание средств защиты информации прикладного и системного программного обеспечения	
Уметь	Трудовые действия	Необходимые умения
<p>Осуществлять техническую эксплуатацию линейных сооружений связи Настраивать, эксплуатировать и обслуживать оборудование ИТКС Осуществлять подключение, настройку мобильных устройств и</p>	<p>Установка программного обеспечения Настройка программного обеспечения с соблюдением требований по защите информации Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам</p>	<p>Устанавливать программное обеспечение в соответствии с технической документацией Выполнять настройку параметров работы программного обеспечения, включая системы управления базами данных и средства электронного документооборота Работать с программным обеспечением с соблюдением действующих требований по защите информации</p>

<p>распределенных сервисов ИТКС Производить испытания, проверку и приемку оборудования ИТКС Проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС</p>	<p>Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением Настройка встроенных средств защиты информации программного обеспечения по заданным шаблонам Проверка функционирования встроенных средств защиты информации программного обеспечения</p>	<p>Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации</p>
<p>Знать</p> <p>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</p>	<p>Своевременное обнаружение признаков наличия вредоносного программного обеспечения</p>	<p>Необходимые знания</p> <p>Порядок настройки программного обеспечения, систем управления базами данных и средств электронного документооборота Общие принципы функционирования вредоносного программного обеспечения Принципы функционирования средств антивирусной защиты Сущность и содержание понятия информационной безопасности, характеристики ее составляющих Источники угроз информационной безопасности и меры по их предотвращению Особенности источников угроз информационной безопасности, связанных с эксплуатацией программного обеспечения Признаки наличия вредоносного программного обеспечения Типовые уязвимости программного обеспечения и методы их эксплуатации Общие принципы функционирования средств защиты информации программного обеспечения, в том числе, средств криптографической защиты информации Порядок эксплуатации средств антивирусной защиты Порядок обеспечения безопасности информации при эксплуатации программного обеспечения Нормативные правовые акты в области защиты информации Основные руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации</p>
<p>ФГОС СПО</p>	<p>Профессиональный стандарт Специалист по защите информации в автоматизированных системах</p>	

ТФ В/01.6 Диагностика систем защиты информации автоматизированных систем		
Уметь	Трудовые действия	Необходимые умения
<p>Настраивать, эксплуатировать и обслуживать оборудование 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>Обнаружение инцидентов в процессе эксплуатации автоматизированной системы</p> <p>Идентификация инцидентов в процессе эксплуатации автоматизированной системы</p> <p>Оценка защищенности автоматизированных систем с помощью типовых программных средств</p> <p>Устранение инцидентов, возникших в процессе эксплуатации автоматизированной системы</p>	<p>Определять источники и причины возникновения инцидентов</p> <p>Оценивать последствия выявленных инцидентов</p> <p>Обнаруживать нарушения правил разграничения доступа</p> <p>Устранять нарушения правил разграничения доступа</p> <p>Осуществлять контроль обеспечения уровня защищенности в автоматизированных системах</p> <p>Использовать криптографические методы и средства защиты информации в автоматизированных системах</p>
Знать	Трудовые действия	Необходимые знания
<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>Расчет показателей эффективности защиты информации, обрабатываемой в автоматизированных системах</p> <p>Инструментальный контроль показателей эффективности защиты информации, обрабатываемой в автоматизированных системах</p>	<p>Нормативные правовые акты в области защиты информации</p> <p>Национальные, межгосударственные и международные стандарты в области защиты информации</p> <p>Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации</p> <p>Организационные меры по защите информации</p> <p>Принципы построения средств защиты информации от "утечки" по техническим каналам</p> <p>Критерии оценки защищенности автоматизированной системы</p> <p>Технические средства контроля эффективности мер защиты информации</p> <p>Регламент информирования персонала автоматизированной системы о выявленных инцидентах</p> <p>Регламент учета выявленных инцидентов</p> <p>Регламент устранения инцидентов</p> <p>Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в автоматизированных системах</p>
ТФ С/01.6 Установка и настройка средств защиты информации в автоматизированных системах		
Уметь	Трудовые действия	Необходимые умения
<p>Выявлять и оценивать угрозы</p>	<p>Входной контроль качества комплектующих</p>	<p>Администрировать программные средства системы защиты</p>

<p>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 информации</p>	<p>изделий системы защиты информации автоматизированной системы Осуществление автономной наладки технических и программных средств системы защиты информации автоматизированной системы Проведение приемочных испытаний системы защиты информации автоматизированной системы Внесение в эксплуатационную документацию изменений, направленных на устранение недостатков, выявленных в процессе испытаний</p>	<p>информации автоматизированных систем Устранять известные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации Применять нормативные документы по противодействию технической разведке Применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации Проводить анализ структурных и функциональных схем защищенной автоматизированной системы Определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы</p>
<p>Знать 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 Криптографические средства защиты информации конфиденциального</p>		<p>Необходимые знания Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Содержание эксплуатационной документации автоматизированной системы Типовые средства, методы и протоколы идентификации, аутентификации и авторизации Основные меры по защите информации в автоматизированных системах Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации</p>

<p>характера, которые применяются 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>ФГОС СПО</p>	<p>Профессиональный стандарт</p>	
	<p>Специалист по технической защите информации</p>	
	<p>ТФ А/03.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию программно-технических средств защиты информации от несанкционированного доступа</p>	
<p>Уметь</p>	<p>Трудовые действия</p>	<p>Необходимые умения</p>
<p>Выявлять и оценивать угрозы 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</p>	<p>Установка и настройка программно-технических средств защиты информации от несанкционированного доступа</p> <p>Испытания программно-технических средств защиты информации от несанкционированного доступа</p> <p>Техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа</p> <p>Устранение неисправностей и организация ремонта программно-технических средств защиты информации от несанкционированного доступа</p>	<p>Производить установку и настройку программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами</p> <p>Проводить испытания программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами</p> <p>Проводить техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами</p> <p>Проводить устранение выявленных неисправностей программно-технических средств защиты информации от несанкционированного доступа и при необходимости организовывать их ремонт с привлечением производителей этих средств</p>

<p>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>Знать</p>		<p>Необходимые знания</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>Порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации</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</p> <p>Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах</p> <p>Методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее</p> <p>Методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий</p> <p>Средства контроля защищенности информации от несанкционированного доступа</p> <p>Методики контроля защищенности информации от несанкционированного доступа</p> <p>Технические описания и инструкции по эксплуатации программно-технических средств защиты информации от несанкционированного доступа</p> <p>Техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа и</p>

		специальных воздействий Порядок устранения неисправностей программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий, организации их ремонта
	ТФ А/02.5 Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от утечки по техническим каналам	
Уметь	Трудовые действия	Необходимые умения
<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 с привлечением производителей технических средств защиты информации</p>
Знать		Необходимые знания
<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 -</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</p>

<p>ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам</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>устройств перехвата информации в технические средства и (или) помещения</p> <p>Основные характеристики электронных устройств перехвата информации</p> <p>Способы защиты акустической речевой информации от утечки по техническим каналам</p> <p>Технические средства защиты акустической речевой информации от утечки по техническим каналам</p> <p>Методы и методики контроля эффективности защиты акустической речевой информации от утечки техническим каналам</p> <p>Средства контроля эффективности защиты акустической речевой информации от утечки техническим каналам</p> <p>Технические описания и инструкции по эксплуатации технических средств защиты речевой информации от утечки по техническим каналам</p> <p>Проектная документация на систему защиты выделенного помещения (в части защиты акустической речевой информации от утечки по техническим каналам)</p> <p>Порядок технического обслуживания технических средств защиты речевой информации от утечки по техническим каналам</p> <p>Порядок устранения неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам и организация их ремонта</p>
ТФ С/02.6 Производство, сервисное обслуживание и ремонт технических средств защиты акустической		

речевой информации от утечки по техническим каналам		
Уметь	Трудовые действия	Необходимые умения
<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>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>Прием от разработчика комплектов конструкторской и технологической документации на техническое средство защиты акустической речевой информации от утечки по техническим каналам</p> <p>Корректировка конструкторской документации на изготовление технического средства защиты акустической речевой информации от утечки по техническим каналам для поставки, контроля и испытаний</p> <p>Отработка конструкции технического средства защиты информации на технологичность с учетом стандартов ЕСТД</p> <p>Заключение договоров (контрактов) с поставщиками комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности</p> <p>Изготовление опытного образца технического средства защиты акустической речевой информации от утечки по техническим каналам</p> <p>Разработка программы и методик испытаний опытного образца технического средства защиты акустической речевой информации от утечки по техническим каналам на соответствие техническим условиям</p> <p>Испытания опытного образца технического средства защиты акустической речевой информации от утечки по техническим каналам на соответствие техническим условиям</p> <p>Разработка программы и методик</p>	<p>Разрабатывать конструкторскую и технологическую документацию на техническое средство защиты акустической речевой информации от утечки по техническим каналам</p> <p>Отрабатывать конструкцию технического средства защиты информации на технологичность с учетом стандартов ЕСТД</p> <p>Изготавливать технические средства защиты акустической речевой информации от утечки по техническим каналам</p> <p>Разрабатывать программы и методики испытаний технических средств защиты акустической речевой информации от утечки по техническим каналам на соответствие требованиям безопасности информации и техническим условиям</p> <p>Проводить испытания технических средств защиты речевой информации от утечки по техническим каналам на соответствие требованиям безопасности информации и техническим условиям</p>
Знать		Необходимые знания
<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,</p>		<p>Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации</p> <p>Стандарты ЕСКД, ЕСТД и ЕСПД</p> <p>Технические каналы утечки акустической речевой информации</p> <p>Способы защиты акустической речевой информации от утечки по техническим каналам</p> <p>Принципы построения и основные характеристики технических</p>

<p>создаваемых техническими средствами защиты информации от утечки по техническим каналам</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>сертификационных испытаний технического средства защиты акустической речевой информации от утечки по техническим каналам на соответствие требованиям безопасности информации</p> <p>Сертификационные испытания технического средства защиты акустической речевой информации от утечки по техническим каналам на соответствие требованиям безопасности информации</p> <p>Изготовление сертифицированных технических средств защиты акустической речевой информации от утечки по техническим каналам</p> <p>Сервисное обслуживание и ремонт технических средств защиты акустической речевой информации от утечки по техническим каналам</p>	<p>средств защиты акустической речевой информации от утечки по техническим каналам</p> <p>Методы контроля эффективности защиты акустической речевой информации от утечки по техническим каналам</p> <p>Средства контроля эффективности защиты акустической речевой информации от утечки по техническим каналам</p> <p>Методы и методики проведения измерений, оценки и обработки их результатов</p> <p>Средства проектирования электронных схем</p> <p>Языки и современные технологии программирования</p> <p>Технологии производства электронной аппаратуры</p>
	<p>ТФ С/04.6 Производство, сервисное обслуживание и ремонт защищенных технических средств обработки информации</p>	
<p>Уметь</p>	<p>Трудовые действия</p>	<p>Необходимые умения</p>

<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>Проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС</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>Прием от разработчика комплектов конструкторской и технологической документации на защищенное техническое средство обработки информации</p> <p>Корректировка конструкторской документации на изготовление защищенного технического средства обработки информации для поставки, контроля и испытаний</p> <p>Отработка конструкции защищенного технического средства обработки информации на технологичность с учетом стандартов ЕСТД</p> <p>Заключение договоров (контрактов) с поставщиками комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности</p> <p>Изготовление опытного образца защищенного технического средства обработки информации</p> <p>Разработка программы и методики испытаний опытного образца защищенного технического средства обработки информации на соответствие техническим условиям</p> <p>Испытания опытного образца защищенного технического средства обработки информации на соответствие техническим условиям</p>	<p>Разрабатывать конструкторскую и технологическую документацию на защищенное техническое средство обработки информации</p> <p>Отрабатывать конструкцию защищенного технического средства обработки информации на технологичность с учетом стандартов ЕСТД</p> <p>Изготавливать защищенное техническое средство или систему обработки информации</p> <p>Разрабатывать программы и методики испытаний защищенных технических средств обработки информации на соответствие требованиям безопасности информации и техническим условиям</p> <p>Проводить испытания защищенных технических средств обработки информации на соответствие требованиям безопасности информации и техническим условиям</p>
<p>Знать</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>Организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по</p>	<p>на соответствие техническим условиям</p> <p>Разработка программы и методик сертификационных испытаний защищенного технического средства обработки информации на соответствие требованиям безопасности информации</p> <p>Сертификационные испытания защищенного технического средства обработки информации на соответствие требованиям безопасности информации</p> <p>Изготовление сертифицированных</p>	<p>Необходимые знания</p> <p>Нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации</p> <p>Стандарты ЕСКД, ЕСТД и ЕСПД</p> <p>Технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов</p>

<p>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>защищенных технических средств обработки информации</p> <p>Сервисное обслуживание и ремонт защищенных технических средств обработки информации</p>	<p>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 защиты технических средств обработки информации от утечки по техническим каналам</p> <p>Принципы построения и основные характеристики технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок</p> <p>Методы и средства контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок</p> <p>Методы и методики проведения измерений, оценки и обработки их результатов</p> <p>Современные информационные технологии (операционные системы, базы данных, вычислительные сети)</p> <p>Способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах</p> <p>Основные классы и виды уязвимостей программного обеспечения</p> <p>Методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее</p> <p>Программные (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее</p> <p>Методы и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий</p> <p>Средства контроля защищенности информации от несанкционированного доступа</p> <p>Средства проектирования электронных схем; Языки и</p>
---	---	---

Матрица соответствия компетенций и составных частей образовательной программы

Индекс дисциплины (модуля)	Наименование дисциплины (модуля)	Общие компетенции (ОК)											Профессиональные компетенции (ПК)										
		ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 08	ОК 09	ОК 10	ОК 11	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
ОУД.01	Общие	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+	+	+
ОУД.01.01	Учебные предметы базового уровня	+	+	+	+	+	+	+	+	+		+	+	+	+		+					+	+
ОУД.01.01.01	Русский язык	+		+	+	+	+			+		+										+	
ОУД.01.01.02	Литература	+		+	+	+	+			+		+		+									
ОУД.01.01.03	Иностранный язык	+		+	+	+	+			+								+					+
ОУД.01.01.04	История	+	+	+	+	+	+			+													
ОУД.01.01.05	Физическая культура			+	+			+															
ОУД.01.01.06	Основы безопасности жизнедеятельности	+		+	+			+						+								+	
ОУД.01.01.07	Астрономия	+	+	+	+		+		+	+		+					+	+					
ОУД.01.02	Учебные предметы углубленного уровня	+	+	+	+	+					+	+				+	+						
ОУД.01.02.01	Математика	+	+	+	+	+					+	+				+	+						
ОУД.02	ПО ВЫБОРУ ИЗ ОБЯЗАТЕЛЬНЫХ ПРЕДМЕТНЫХ ОБЛАСТЕЙ	+	+	+	+	+			+	+		+			+	+	+				+		
ОУД.02.01	Учебные предметы базового уровня	+		+	+	+	+			+		+											
ОУД.02.01.01	Родная литература	+		+	+	+	+			+		+											
ОУД.02.02	Учебные предметы углубленного уровня	+	+	+	+	+			+	+		+			+	+	+				+		
ОУД.02.02.01	Информатика	+	+	+	+	+			+	+		+				+					+		
ОУД.02.02.02	Физика	+	+	+	+	+			+	+		+			+		+						

Индекс дисциплины (модуля)	Наименование дисциплины (модуля)	Общие компетенции (ОК)											Профессиональные компетенции (ПК)										
		ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 08	ОК 09	ОК 10	ОК 11	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
ОУД.03	ДОПОЛНИТЕЛЬНЫЕ УЧЕБНЫЕ ПРЕДМЕТЫ, КУРСЫ ПО ВЫБОРУ	+	+	+	+	+	+	+		+	+	+		+								+	
ОУД.03.01	Обществознание (включая экономику и право)	+	+	+	+	+	+					+										+	
ОУД.03.02	Общая химия	+	+	+	+	+		+						+									
ОУД.03.03	Индивидуальный проект			+		+	+	+		+	+	+											
ОУД.03.ДВ.01	Курсы по выбору 1 (ДВ.1)		+	+	+			+														+	
ОУД.03.ДВ.01.01	Биология с основами экологии		+	+	+			+														+	
ОУД.03.ДВ.01.02	История родного края		+	+	+			+														+	
ОУД.03.ДВ.01.03	Практикум по физике		+	+	+			+														+	
ОУД.03.ДВ.02	Курсы по выбору 2 (ДВ.2)	+	+	+	+		+					+											
ОУД.03.ДВ.02.01	География с основами демографии	+	+	+	+		+					+											
ОУД.03.ДВ.02.02	Эффективное поведение на рынке труда	+	+	+	+		+					+											
ОУД.03.ДВ.02.03	Практикум решения задач повышенной сложности по математике	+	+	+	+		+					+											
ОГСЭ	Общий гуманитарный и социально-экономический цикл	+	+	+	+	+	+		+	+	+												
ОГСЭ.01	Основы философии	+		+		+				+													
ОГСЭ.02	История	+	+			+																	
ОГСЭ.03	Иностранный язык в профессиональной деятельности	+	+	+	+	+	+	+	+	+	+	+											
ОГСЭ.04	Физическая культура								+														
ОГСЭ.05	Основы социологии и политологии // Основы социализации		+/+		+		+/+			+													

Индекс дисциплины (модуля)	Наименование дисциплины (модуля)	Общие компетенции (ОК)											Профессиональные компетенции (ПК)											
		ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 08	ОК 09	ОК 10	ОК 11	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	
	для лиц с ограниченными возможностями здоровья (адаптационная дисциплина)																							
ЕН	Математический и общий естественнонаучный цикл	+	+	+						+				+	+	+								
ЕН.01	Математика	+	+	+						+														
ЕН.02	Информатика	+	+	+						+														
ЕН.03	Элементы математической логики	+	+	+						+				+	+	+								
ОПЦ	Общепрофессиональный цикл	+	+	+	+	+	+	+	+	+	+					+	+	+				+		
ОПЦ.01	Инженерная и компьютерная графика	+	+	+						+														
ОПЦ.02	Электротехника	+	+	+	+					+														
ОПЦ.03	Электроника и схемотехника			+						+	+			+		+								
ОПЦ.04	Основы информационной безопасности			+						+	+													
ОПЦ.05	Основы алгоритмизации и программирования													+		+								
ОПЦ.06	Экономика и управление	+	+	+	+	+	+					+	+											
ОПЦ.07	Безопасность жизнедеятельности	+			+		+	+																

Индекс дисциплины (модуля)	Наименование дисциплины (модуля)	Общие компетенции (ОК)											Профессиональные компетенции (ПК)											
		ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 08	ОК 09	ОК 10	ОК 11	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	
ОПЦ.08	Организационное и правовое обеспечение информационной безопасности	+	+	+	+		+			+						+	+					+		
ОПЦ.09	Технические средства информатизации	+								+			+			+					+			
ОПЦ.10	Вычислительная техника	+	+							+	+		+											
ОПЦ.11	Операционные системы	+	+							+	+						+							
ОПЦ.12	Основы предпринимательской деятельности и финансовой грамотности											+												
ПЦ	Профессиональный цикл	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+	+	+		
ПМ.01	Эксплуатация информационно-телекоммуникационных систем и сетей	+	+	+	+					+	+	+	+	+	+	+								
МДК.01.01	Приемо-передающие устройства, линейные сооружения связи и источники электропитания	+	+	+	+					+	+	+	+	+	+	+								
МДК.01.02	Телекоммуникационные системы и сети	+	+	+	+					+	+	+	+	+	+	+								
МДК.01.03	Электрорадиоизмерения и метрология	+	+	+	+					+	+	+	+	+	+	+								
УП.01.01	Учебная практика	+	+	+	+					+	+	+	+	+	+	+								
ПП.01.01	Производственная практика	+	+	+	+					+	+	+	+	+	+	+								

Индекс дисциплины (модуля)	Наименование дисциплины (модуля)	Общие компетенции (ОК)											Профессиональные компетенции (ПК)											
		ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 08	ОК 09	ОК 10	ОК 11	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	
ПМ.02	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных(в том числе криптографических) средств защиты	+	+	+	+					+	+	+					+	+						
МДК.02.01	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	+	+	+	+					+	+	+					+	+						
МДК.02.02	Криптографические средства защиты информации	+	+	+	+					+	+	+					+	+						
МДК.02.03	Технология разработки и защиты баз данных																							
УП.02.01	Учебная практика	+	+	+	+					+	+	+					+	+						
ПП.02.01	Производственная практика	+	+	+	+					+	+	+					+	+						
ПМ.03	Защита информации в информационно-телекоммуникационных системах и сетях с	+	+	+	+	+	+	+		+										+	+	+		

Индекс дисциплины (модуля)	Наименование дисциплины (модуля)	Общие компетенции (ОК)											Профессиональные компетенции (ПК)											
		ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 08	ОК 09	ОК 10	ОК 11	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	
	использованием технических средств защиты																							
МДК.03.01	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	+	+	+	+	+	+	+		+										+	+	+		
МДК.03.02	Физическая защита линий связи информационно-телекоммуникационных систем и сетей	+	+	+	+	+	+	+		+										+	+	+		
УП.03.01	Учебная практика	+	+	+	+	+	+	+		+										+	+	+		
ПП.03.01	Производственная практика	+	+	+	+	+	+	+		+										+	+	+		
ПМ.04	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих	+	+	+	+					+				+										
МДК.04.01	Выполнение работ по профессии рабочих 14601 Монтажник оборудования связи	+	+	+	+					+				+										
УП.04.01	Учебная практика	+	+	+	+					+				+										
ПП.04.01	Производственная практика	+	+	+	+					+				+										
ПДП	ПРОИЗВОДСТВЕННАЯ ПРАКТИКА	+	+	+	+					+	+			+	+	+	+	+		+	+	+		

Индекс дисциплины (модуля)	Наименование дисциплины (модуля)	Общие компетенции (ОК)											Профессиональные компетенции (ПК)											
		ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 08	ОК 09	ОК 10	ОК 11	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	
	(ПРЕДДИПЛОМНАЯ)																							
ГИА	Государственная итоговая аттестация	ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 08	ОК 09	ОК 10	ОК 11	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		

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 ППСЗ по учебным циклам соответствует требованиям ФГОС (70,5%). 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 29,5%.

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 объёме 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 38,84% 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
Общеобразовательный цикл	1476	1476	-
Общий гуманитарный и социально-экономический цикл	572	463	109
Математический и общий естественнонаучный цикл	300	260	40
Общепрофессиональный цикл	1124	673	451
Профессиональный цикл:	2252	1600	652
Профессиональные модули	1532	1067	465
Учебная практика	252	208	44
Производственная практика	468	325	143
Государственная итоговая аттестация	216	216	-
Общий объем образовательной программы на базе основного общего образования, включая получение среднего общего образования в соответствии с требованиями федерального государственного образовательного стандарта среднего общего образования	5940	4688	1252

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, Родная литература, Иностранный язык, История, Физическая культура, Основы безопасности жизнедеятельности, Астрономия, Общая химия, Математика, Информатика, Физика, Биология с основами экологии, История родного края, Практикум по физике, География с основами демографии. Эффективное поведение на рынке труда, Практикум решения задач повышенной сложности по математике, Обществознание (включая экономику и право), Индивидуальный проект, Основы философии, История, Иностранный язык в профессиональной деятельности, Физическая культура, Основы социологии и политологии, Основы социализации для лиц с ограниченными возможностями здоровья (адаптационная дисциплина), 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, 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 выпускным квалификационным работам и порядку их выполнения, критерии оценки результатов защиты выпускных квалификационных 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 работ 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 планируемыми 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 критериев 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 отвечает квалификационным требованиям, указанным в профессиональном стандарте «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования», утвержденном приказом Министерства труда и социальной защиты Российской Федерации от 8 сентября 2015 г. № 608н.

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 μ А 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 межсетевое 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 СБТ - 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-ППО, T-FLEX ЧПУ, сетевая версия; система автоматизированных расчетов деталей машин АРМ 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, оснащенные 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:

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

Доступ осуществляется из любой точки сети Интернет 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.

2. ЭБС «Лань» <http://e.lanbook.com/>

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

Пакеты: Инженерно-технические науки, Экономика и менеджмент, Право. Юридические науки, Социально-гуманитарные науки, Информатика.

3. ЭБС «IPRbooks» <http://www.iprbookshop.ru>

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

4. БД «Elibrary» <http://elibrary.ru/>

Доступ осуществляется из любой точки сети Интернет через личный кабинет после регистрации с IP-адреса филиала. 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.

5. СПС «Консультант ПЛЮС».

Доступ осуществляется в зале электронных ресурсов библиотеки.

6. Электронная библиотека «Издательский центр «Академия»
<http://www.academia-moscow.ru>.

Доступ осуществляется из любой точки сети Интернет по логину и паролю после регистрации и активации кода доступа. В электронной библиотеке центра доступны учебники для среднего профессионального образования.

7. ЭБС «ЮРАЙТ» <http://www.urait.ru>

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

8 Универсальная база данных (УБД) электронных периодических изданий ИВИС: <https://dlib.eastview.com/browse/udb/12>

Каждый студент имеет неограниченный доступ к электронным версиям учебников, учебных и методических пособий, сборникам научных и студенческих конференций, периодическим изданиям, выпускаемым университетом в Электронной библиотеке образовательных ресурсов (ЭБОР).

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 использования газетно-журнальной информации, посещения краеведческих экскурсий, обсуждения книг, новинок.

Студенческий клуб «Дела семейные» занимается проблемами семейного воспитания. Взгляды молодых людей на характер половых отношений, девальвация моральных ценностей, связанных с отношениями между людьми, обособленность членов семьи друг от друга, распределение ролей в семье – это тот круг вопросов, которые студенты с удовольствием обсуждают на заседаниях, встречаются с интересными людьми, семейными психологами.

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.

Центр здорового образа жизни способствует популяризации здорового образа жизни, формированию позитивного отношения к спорту, осуществляет эффективную пропаганду физической культуры и занятий спортом как составляющей здорового образа жизни.

В филиале функционирует Центр студенческого творчества, в состав которого входят творческая мастерская «Студенческая волна», танцевальный коллектив «MixDance», вокальная студия «Мелодия», 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.