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

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

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

СПбГУТ))) **Документ подписан простой электронной подписью**

Сертификат: 00fd759708ffd39703
Владелец: Бачевский Сергей Викторович
Действителен с 15.03.2021 по 14.03.2026

УТВЕРЖДАЮ
Первый проректор – проректор по учебной работе
_____ Т.М. Машков
_____ 2021 г.
Регистрационный № 11.05.19/533

РАБОЧАЯ ПРОГРАММА

ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

(наименование вида практики)

программа подготовки специалистов среднего звена

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код и наименование специальности)

квалификация
техник по защите информации

Санкт-Петербург
2021

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 27 мая 2021 г., протокол № 5.

Составитель:
Преподаватель _____ Н.В. Кривоносова
(подпись)

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

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 5 (информатики и программирования в компьютерных системах)
07 апреля 2021 г., протокол № 8
Председатель предметной (цикловой) комиссии:
_____ Н.В. Кривоносова
(подпись)

ОДОБРЕНО
Методическим советом Санкт-Петербургского колледжа телекоммуникаций
21 апреля 2021 г., протокол № 6
Зам. директора по УР колледжа СПб ГУТ
_____ О.В. Колбанёва
(подпись)

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

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

СОГЛАСОВАНО
ЭТД по безопасности АО ПП «Сигнал»
В.В. Петров

СОГЛАСОВАНО
Заместитель руководителя Управления Роскомнадзора по Северо-Западному федеральному округу
_____ И.Ю. Потехин

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

1.1. Область применения программы

Рабочая программа производственной практики – является частью основной образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (квалификация – техник по защите информации) в части освоения основных видов деятельности:

- 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: по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин».

Область профессиональной деятельности выпускников: Область профессиональной деятельности выпускников: 06 Связь, информационные и коммуникационные технологии. 12 Обеспечение безопасности.

1.2. Цели и задачи - требования к результатам освоения производственной практики (по профилю специальности)

Производственная практика (по профилю специальности) направлена на формирование у обучающихся общих и профессиональных компетенций, освоение современных производственных процессов, адаптация обучающихся к конкретным условиям деятельности организаций различных организационно-правовых форм, приобретение практического опыта в рамках профессиональных модулей ППССЗ СПО по каждому из основных видов профессиональной деятельности предусмотренных ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (квалификация – техник по защите информации).

В результате прохождения производственной практики (по профилю специальности), реализуемой в рамках модулей ППССЗ СПО по каждому из основных видов деятельности (ОВД), предусмотренных ФГОС СПО, обучающийся должен приобрести практический опыт работы:

Основной вид деятельности	Умения и практический опыт в
Эксплуатация информационно-телекоммуникационных систем и сетей	**Уметь:**
	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, диагностики технического состояния и ремонту оборудования ИТКС;
	Иметь практический опыт в:
	монтаже, настройке, проверке функционирования и конфигурировании оборудования ИТКС;
	текущем контроле функционирования оборудования ИТКС;
	проведении технического обслуживания, диагностике технического

Основной вид деятельности	Умения и практический опыт в
	состояния, поиска неисправностей и ремонта оборудования ИТКС.
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	**Уметь:**
	выявлять и оценивать угрозы безопасности информации в ИТКС;
	настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;
	проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
	проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;
	проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
	проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;
	проводить техническое обслуживание и ремонт программных и программно-аппаратных, в том числе криптографических средств защиты информации;
	Иметь практический опыт в:
	установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС;
	поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС;
	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.
Защита информации в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты	**Уметь:**
	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;
	проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
	проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
	использовать средства физической защиты линий связи ИТКС;
	применять нормативные правовые акты и нормативные методические документы в области защиты информации;
	Иметь практический опыт в:
	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.

Основной вид деятельности	Умения и практический опыт в
Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих: по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»	**Уметь:**
	выполнять требования техники безопасности при работе с вычислительной техникой;
	производить подключение блоков персонального компьютера и периферийных устройств;
	производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники;
	диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники;
	выполнять инсталляцию системного и прикладного программного обеспечения;
	создавать и управлять содержимым документов с помощью текстовых процессоров;
	создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц;
	создавать и управлять содержимым презентаций с помощью редакторов презентаций;
	использовать мультимедиа проектор для демонстрации презентаций; вводить, редактировать и удалять записи в базе данных;
	эффективно пользоваться запросами базы данных;
	создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики;
	производить сканирование документов и их распознавание;
	производить распечатку, копирование и тиражирование документов на принтере и других устройствах;
	управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете;
	осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера;
	осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов;
	осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;
	осуществлять резервное копирование и восстановление данных;
	Иметь практический опыт в:
	выполнение требований техники безопасности при работе с вычислительной техникой;
	организации рабочего места оператора электронно-вычислительных и вычислительных машин;
	подготовке оборудования компьютерной системы к работе;
	инсталляции, настройке и обслуживание программного обеспечения компьютерной системы;
	управлении файлами;
	применение офисного программного обеспечения в соответствии с прикладной задачей;
	использование ресурсов локальной вычислительной сети;
	использование ресурсов, технологий и сервисов Интернет;
	применение средств защиты информации в компьютерной системе.

1.3. Количество часов на освоение рабочей программы производственной практики (по профилю специальности)

Всего – 612 часов (17 нед.), в том числе:
В рамках освоения ПМ.01 –180 часов
В рамках освоения ПМ.02 - 180 часов
В рамках освоения ПМ.03 –180 часов
В рамках освоения ПМ.04 –72 часа

2 РЕЗЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Результатом освоения программы производственной практики (по профилю специальности) является сформированность у обучающихся практических профессиональных умений, приобретение первоначального практического опыта, необходимых для последующего освоения ими общих (ОК) и профессиональных (ПК) компетенций по 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Код	Наименование компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК1.1.	Производить монтаж, настройку и поверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей.
ПК 1.2.	Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно – телекоммуникационных систем и сетей.
ПК 1.3.	Проводить техническое обслуживание оборудования информационно – телекоммуникационных систем и сетей
ПК 1.4.	Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях

Код	Наименование компетенции
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.
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях.
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – 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.
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно – телекоммуникационных систем и сетей
ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4.	Обеспечивать применение средств защиты информации в компьютерной системе

3 СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

3.1. Структура программы производственной практики (по профилю специальности)

Коды профессиональных компетенций	Наименования профессиональных модулей и МДК	Объем часов
ПК 1.1 – ПК 1.4	**ПМ.01.Эксплуатация информационно-телекоммуникационных систем и сетей**	180
ПК 2.1 – ПК 2.3	**ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе, криптографических средств защиты**	180
ПК 3.1 – ПК 3.4	**ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты**	180
ПК 4.1 – ПК 4.4	**ПМ.04.Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (Оператор электронно-вычислительных и вычислительных машин)**	72
Всего часов		**612**

3.2. Содержание производственной практики (по профилю специальности)

Код и наименование профессиональных модулей, МДК и тем производственной практики (по профилю специальности)	Виды работ		Объем часов
ПМ.01.Эксплуатация информационно-телекоммуникационных систем и сетей	**Содержание производственной практики (по профилю специальности)**		
	1	Ознакомление со структурой предприятия, вводный инструктаж по технике безопасности и охране труда.	**180**
	2	Ознакомление с кабельными цехами и участками.	
	3	Работа с технической документацией.	
	4	Изучение оборудования и устройств, повышающих работоспособность и надежность кабельных линий.	
	5	Ознакомление с оборудованием ИТКС.	
	6	Изучение и работа с контрольно-измерительным оборудованием.	
	7	Самостоятельная работа на закрепленном рабочем месте.	
	8	Выполнение индивидуального задания по практике.	
	9	Участите в аварийных и профилактических работах, проводимых на кабельном участке.	
	10	Обобщение материала, оформление отчета, сдача зачета.	
ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	**Содержание производственной практики (по профилю специальности)**		
	1	Инструктаж по технике безопасности	**180**
	2	Ознакомление с рабочим местом	
	3	Ознакомление с организационной структурой предприятия	
	4	Резервное копирование информации	
	5	Восстановление данных	
	6	Проверка копий на предприятии, изучение технологии резервного копирования	
	7	Защита информации от несанкционированного доступа	
	8	Регистрация и учёт входа/выхода субъектов системы в/из системы (узла сети)	
	9	Учёт носителей информации	
	10	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	
	11	Работа с антивирусами	
	12	Обновление антивирусных программ	
	13	Защита почтовых ящиков	

Код и наименование профессиональных модулей, МДК и тем производственной практики (по профилю специальности)	Виды работ		Объем часов
	14	Шифрование конфиденциальной информаци	
	15	Работа в программе cryptoapi	
	16	Работа в программе Windows Defender	
	17	Изучение дискреционного принципа контроля доступа к информации	
	18	Создание системы защиты персональных данных	
	19	Создание комплекса мероприятий по защите персональных данных с использованием резервного копирования, шифрования информации, антивирусных программ	
	20	Участие в организации работ по защите персональных компьютеров на предприятии	
	21	Участие в организации работ по защите локальных сетей на предприятии	
	22	Участие в организации работ по защите работ в глобальной сети интернет на предприятии	
	23	Работа с криптографическими средствами защиты информации	
	24	Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети.	
	25	Администрирование систем безопасности беспроводной защищенной локальной сети.	
	26	Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей.	
	27	Выбор программных средств шифрования в соответствии с решаемой задачей	
	28	Подключение, установка драйверов, настройка программных средств абонентского шифрования	
	29	Администрирование внедренных средств	
	30	Настройка средств электронной подписи	
	31	Администрирование средств электронной подписи	
	32	Администрирование средств PKI	
	33	Сдача рабочего места	
	34	Подготовка дневника и аттестационного листа по практике	
	35	Подготовка и сдача отчета по практике	
ПМ.03. Защита информации в	**Содержание производственной практики (по профилю специальности)**		
	1	Проведение инструктажа по технике безопасности. Ознакомление с предприятием.	**180**

Код и наименование профессиональных модулей, МДК и тем производственной практики (по профилю специальности)	Виды работ		Объем часов
информационно-телекоммуникационных системах и сетях с использованием технических средств защиты		Получение заданий по тематике	
	2	Определение исходных данных по защищаемому объекту и плана работ по созданию системы защиты речевой информации (СЗРИ)	
	3	Выявление технических каналов утечки (ТКУ) речевой информации с использованием современных средств контроля и контрольно-измерительной аппаратуры	
	4	Подготовка предложений в проект технического задания на создание СЗРИ, в том числе специального защищенного (экранированного) помещения (СЗП)	
	5	Разработка рекомендаций по совершенствованию мер защиты речевой информации и предложения по корректировке СЗРИ и СЗП	
	6	Монтаж средств защиты информации и их настройка, инструментальная оценка эффективности защиты речевой информации и электромагнитного экранирования СЗП	
	7	Опытная эксплуатация СЗРИ и СЗП в целях проверки их работоспособности	
	8	Участие в монтаже средств охраны и безопасности, инженерной защиты	
	9	Анализ уязвимости системы	
	10	Выявление ПЭМИН в информационной системе и защита от них	
	11	Восстановление информации при перехвате ПЭМИН	
	12	Предотвращение утечки информации через ПЭМИН ПК	
	13	Организационные мероприятия по технической защите информации от утечки по каналам ПЭМИН	
	14	Организационные мероприятия по технической защите информации в средствах вычислительной техники, автоматизированных системах и сетях от утечки по каналам ПЭМИН	
	15	Применение активных методов защиты информации от утечки по каналам ПЭМИН	
	16	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами	
	17	Оценка защищенности основных технических средств в составе автоматизированной системы от утечки информации по каналу побочных электромагнитных излучений	
	18	Оценка защищенности информации, обрабатываемой основными техническими средствами в составе автоматизированной системы от её утечки за счет наводок информативного	

Код и наименование профессиональных модулей, МДК и тем производственной практики (по профилю специальности)	Виды работ		Объем часов
		сигнала	
	19	Участие в обслуживании технических средств защиты информации	
	20	Выполнение подбора, настройки и применения технических средств защиты информации	
	21	Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения	
	22	Использование средств охраны и безопасности объекта	
	23	Организация и реализация технической охраны объектов	
	24	Парольная аутентификация в системах ИБ и PIN-код в СКУД	
	25	Участие в организации работ по технической защите конфиденциальной информации	
	26	Контроль доступа к неструктурированным данным	
	27	Внутренний контроль обработки ПДн	
	28	Контроль за соответствием обработки ПДн	
	29	Участие в перехвате побочных электромагнитных излучений	
	30	Поиск и измерение ПЭМИ монитора на ЭЛТ (монитора на ЖК) в автоматическом и режиме управляющей программы	
	31	Составление протокол исследования с помощью расчетной программы	
	32	Съем наводок ПЭМИ ТСОИ с соединительных линий ВТСС и посторонних проводников	
	33	Защита информации в АСУ	
	34	Защита информации при передаче данных	
	35	Защита информации ограниченного доступа	
	36	Защита информации на жестком диске	
	37	Защита информации при использовании электронной почты	
	38	Комплексная защита информации в корпоративных системах	
	39	Защита информации в компьютерных сетях	
	40	Защита информации в локальных вычислительных сетях	
	41	Защита информации в VPN-сетях	
	42	Защита информации от несанкционированного доступа в сетях	
	43	Контроль доступа к информации	
	44	Управление доступом к информации	

Код и наименование профессиональных модулей, МДК и тем производственной практики (по профилю специальности)	Виды работ		Объем часов
	45	Техническая защита информации на предприятии	
	46	Инженерно-техническая защита информации на предприятии	
	47	Защита информации, составляющей коммерческую тайну	
	48	Разработка модели КСЗИ	
	49	Технологическое и организационное построение КСЗИ	
	50	Кадровое обеспечение функционирования КСЗИ	
	51	Участие в эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения	
	52	Участие в эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам	
	53	Установка и настройка средств защиты информации	
	54	Участие в монтаже технических средств защиты информации	
	55	Участие в монтаже средств охраны и безопасности, технической охраны объектов	
	56	Участие в монтаже средств защиты информации от несанкционированного съёма и утечки по техническим каналам	
	57	Настройка системы защиты информации от съема и утечки по техническим каналам	
	58	Выявление технических каналов	
	59	Поиск ЗУ и других технических каналов	
	60	Выявление путей утечки информации в ИС	
	61	Оценка уязвимости системы	
	62	Участие в монтаже средств охраны и безопасности и систем видеонаблюдения	
	63	Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам	
	64	Определение требований к системе защиты информации	
	65	Проектирование системы защиты информации	
	66	Разработка эксплуатационной документации на систему защиты информации	
	67	Установка и настройка средств защиты информации	
	68	Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты	

Код и наименование профессиональных модулей, МДК и тем производственной практики (по профилю специальности)	Виды работ		Объем часов
		информации в ходе эксплуатации объекта	
	69	Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению	
	70	Испытания и опытная эксплуатации системы защиты информации	
	71	Подтверждение соответствия системы защиты информации	
	72	Выполнение мероприятий по предотвращению несанкционированного доступа к информации	
	73	Оценка эффективности использованных мер и средств защиты информации	
	74	Контроль эффективности защиты информации	
	75	Защита информации обрабатываемой ТСПИ от утечки по техническим каналам	
	76	Защита от утечки информации по телефонному каналу	
	77	Защита от утечки информации по электросетевому каналу	
	78	Защита от утечки информации по вибрационному каналу	
	79	Защита от утечки информации по проводному каналу	
	80	Формирование требований к системе защиты информации	
	81	Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности обрабатываемой информации	
	82	Изучение порядка применения нормативных правовых актов	
	83	Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами	
	84	Выявление технических каналов утечки информации	
	85	Применение существующих способов выявления опасности целостности информации	
	86	Анализ объектов информатизации предприятий, учреждений, организаций	
	87	Анализ ресурсов обеспечения инженерно-технической защиты информации	
	88	Изучение основных этапов проектирования системы защиты информации техническими средствами	
	89	Проектирование рабочих проектов по системе пожарно-охранной сигнализации, видеонаблюдения, СКУД	
	90	Оформление отчета	

Код и наименование профессиональных модулей, МДК и тем производственной практики (по профилю специальности)	Виды работ		Объем часов
ПМ.04.Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (Оператор электронно-вычислительных и вычислительных машин)	**Содержание производственной практики (по профилю специальности)**		
	1	Ознакомление со структурой предприятия	**72**
	2	Прохождение инструктажа по технике безопасности охране труда	
	3	Приемка рабочего места	
	4	Подготовка рабочего места	
	5	Инсталляция системного программного обеспечения	
	6	Инсталляция системного программного обеспечения	
	7	Инсталляция системного программного обеспечения	
	8	Инсталляция и настройка прикладного программного обеспечения	
	9	Инсталляция и настройка прикладного программного обеспечения	
	10	Инсталляция и настройка прикладного программного обеспечения	
	11	Инсталляция и настройка прикладного программного обеспечения	
	12	Инсталляция и настройка прикладного программного обеспечения	
	13	Инсталляция и настройка прикладного программного обеспечения	
	14	Инсталляция и настройка прикладного программного обеспечения	
	15	Инсталляция и настройка прикладного программного обеспечения	
	16	Обслуживание прикладного программного обеспечения отраслевой направленности	
	17	Обслуживание прикладного программного обеспечения отраслевой направленности	
	18	Обслуживание прикладного программного обеспечения отраслевой направленности	
	19	Обслуживание прикладного программного обеспечения отраслевой направленности	
	20	Обслуживание прикладного программного обеспечения отраслевой направленности	
	21	Обслуживание прикладного программного обеспечения отраслевой направленности	
	22	Применение офисного программного обеспечения в соответствии с прикладной задачей	
	23	Применение офисного программного обеспечения в соответствии с прикладной задачей	
	24	Применение офисного программного обеспечения в соответствии с прикладной задачей	
	25	Применение офисного программного обеспечения в соответствии с прикладной задачей	
	26	Применение офисного программного обеспечения в соответствии с прикладной задачей	
	27	Применение офисного программного обеспечения в соответствии с прикладной задачей	
	28	Работа с программным обеспечением и ресурсами ЛВС	

Код и наименование профессиональных модулей, МДК и тем производственной практики (по профилю специальности)	Виды работ		Объем часов
	29	Работа с программным обеспечением и ресурсами ЛВС	
	30	Работа с программным обеспечением и ресурсами ЛВС	
	31	Применение программно-аппаратных комплексов для защиты информационных активов от несанкционированного доступа	
	32	Применение программно-аппаратных комплексов для защиты информационных активов от несанкционированного доступа	
	33	Применение программно-аппаратных комплексов для защиты информационных активов от несанкционированного доступа	
	34	Применение программно-аппаратных комплексов для защиты информационных активов от несанкционированного доступа	
	35	Сдача рабочего места	
	36	Оформление документации по практике	
Всего			**612**

4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

4.1. Требования к минимальному материально-техническому обеспечению

Персональные компьютеры с подключением их к системе телекоммуникаций (электронная почта, Интернет); Аппаратное и программное обеспечение для проведения опытно-экспериментальной и научно-исследовательской работы обучающихся в рамках производственной практики (по профилю специальности).

Все вышеперечисленные объекты должны соответствовать действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении производственных работ.

4.2. Информационное обеспечение реализации программы

4.2.1. Нормативные документы:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» //Гарант: информационно-правовой портал. - URL: https://base.garant.ru/12148555/
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» //Гарант: информационно-правовой портал. - URL: https://base.garant.ru/12148567/
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» //Гарант: информационно-правовой портал. - URL: https://base.garant.ru/12129354/
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» //Гарант: информационно-правовой портал. - URL: https://base.garant.ru/12185475/
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» //Гарант: информационно-правовой портал. - URL: https://base.garant.ru/12125267/
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» //Гарант: информационно-правовой портал. - URL: https://base.garant.ru/12136635/
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» //Гарант: информационно-правовой портал. - URL: https://base.garant.ru/10200083/
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» //Гарант: информационно-правовой портал. - URL: https://base.garant.ru/192944/
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 //Гарант: информационно-правовой портал. - URL: https://base.garant.ru/102670/
10. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г. //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/en/component/attachments/download/288
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21 //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL:

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 17 июля 2017 г. N 134// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/administrativnye-reglamenty/1362-prikaz-fstek-rossii-ot-17-iyulya-2017-g-n-134-2
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/administrativnye-reglamenty/478-prikaz-fstek-rossii-ot-12-iyulya-2012-g-n-84
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282 // РОСТРАНСНАДЗОР: Федеральная служба по надзору в сфере транспорта: официальный сайт. - URL: https://security.rostransnadzor.gov.ru/storage/documents/prikazy-i-rasporyazheniya-rostransnadzora/%D0%9F%D1%80%D0%B8%D0%BA%D0%B0%D0%B7-282-%D0%BE%D1%82-30.08.2002.doc
16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702
17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/370
18. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» //Гарант: информационно-правовой портал. - URL: https://base.garant.ru/187947/
19. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200048398
20. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200051499
21. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200051500
22. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200048416

23. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200044724
24. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200071694
25. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200069465
26. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200069464
27. ГОСТ Р 34.10-2001."Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200026578
28. ГОСТ Р 34-11-94. Информационная технология. Криптографическая защита информации. Функция хэширования // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200004857
29. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения// Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200058320
30. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200102287
31. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения// Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200108858
32. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения// Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200057516
33. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества// Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200044725
34. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения// Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200113006
35. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования// Электронный фонд правовых и нормативно-

технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200113336
36. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель// Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200101777
37. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008) // Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200105710
38. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г. //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god
39. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения// Электронный фонд правовых и нормативно-технических документов: информационно-правовой портал. - URL: https://docs.cntd.ru/document/1200057516
40. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17 //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. - URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702.
41. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument.

4.2.2. Электронные издания:

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие/ Е.К.Баранова, А.В.Бабаш. — 3-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2020. - URL: https://znanium.com/catalog/product/1114032
2. Баранова, Е.К. Основы информационной безопасности: учебник для студ. учрежд. СПО / Е.К. Баранова, А.В. Бабаш. - Москва: РИОР: ИНФРА-М, 2019. - URL: https://znanium.com/catalog/product/1014830
3. Берлин, А. Н. Высокоскоростные сети связи: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016. — URL: https://e.lanbook.com/book/100724
4. Берлин, А. Н. Оконечные устройства и линии абонентского участка информационной сети: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016. — URL: https://e.lanbook.com/book/100276
5. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А.Бузов. - Москва: Горячая линия-Телеком, 2018. - URL: https://ibooks.ru/products/354357
6. Заика, А.А. Локальные сети и Интернет/ А.А. Заика. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — URL: https://e.lanbook.com/book/100727
7. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А.П.Зайцев, Р.В.Мещеряков, А.А.Шелупанов. – 7-е изд., испр. – Москва: Горячая Линия–Телеком, 2018. - URL: https://ibooks.ru/products/333981

8. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019. - URL: https://znanium.com/catalog/product/1018901
9. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО /В.Я.Ищейнов, М.В.Мецатунян. - Москва: Форум: ИНФРА-М, 2021. - URL: https://znanium.com/catalog/document?id=365084
10. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. - Москва: Юрайт, 2020. — URL: https://urait.ru/bcode/456792
11. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2020. — URL: https://urait.ru/bcode/456792
12. Криптографическая защита информации: учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — Москва: РИОР: ИНФРА-М, 2020. - URL: https://znanium.com/catalog/product/1086444
13. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации): учебное пособие / В.К. Новиков. - Москва: Горячая Линия–Телеком, 2017. — URL: https://ibooks.ru/products/354366
14. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под ред. Т. А. Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2020. — URL: https://urait.ru/bcode/450371
15. Портнов, Э. Л. Оптические кабели связи, их монтаж и измерение: учебное пособие для вузов / Э.Л. Портнов. - Москва: Горячая линия-Телеком, 2012. - URL: https://ibooks.ru/products/334022
16. Программно-аппаратные средства обеспечения информационной безопасности / А.В.Душкин, О.М.Барсуков, Е.В.Кравцов, К.В.Славнов. – Москва: Горячая Линия–Телеком, 2016. - URL: https://ibooks.ru/bookshelf/357887
17. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей: учебное пособие для вузов/Е.Б.Алексеев, В.Н.Гордиенко, В.В.Крухмалев и др.; под ред. В.Н.Гордиенко, М.С.Тверецкого. - Москва: Горячая линия-Телеком, 2017. - URL: https://ibooks.ru/bookshelf/333349
18. Родина, О.В. Волоконно-оптические линии связи: практическое руководство/О.В.Родина. - Москва: Горячая линия-Телеком, 2016. - URL: https://ibooks.ru/products/334026
19. Сети и телекоммуникации: учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. - Москва: Юрайт, 2020. - URL: https://urait.ru/book/seti-i-telekommunikacii-456638
20. Смычек, М.А. Технологические сети и системы связи: учебное пособие / М.А. Смычек. - 2-е изд. - Москва; Вологда: Инфра-Инженерия, 2019. - URL: https://znanium.com/catalog/product/1053400
21. Соколов, С.А. Волоконно-оптические линии связи и их защита от внешних влияний: учебное пособие / С.А. Соколов. – Москва: Инфра-Инженерия, 2019. - URL: https://znanium.com/catalog/product/1053404
22. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие/П.Б.Хорев. - 2-е изд., испр. и доп. - Москва: Форум: ИНФРА-М, 2020. - URL: https://znanium.com/catalog/product/1035570
23. Цуканов, В.Н. Волоконно-оптическая техника: практическое руководство/ В.Н. Цуканов, М.Я. Яковлев. – Москва: Инфра-Инженерия, 2022. - URL: https://znanium.com/catalog/document?id=417223

24. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА-М, 2020. - URL: https://znanium.com/catalog/product/1093695
25. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учрежд. СПО. - Москва: ФОРУМ: ИНФРА-М, 2020. - URL: https://znanium.com/catalog/product/1093657.

Электронные ресурсы:

1. SecurityLab. Защита информации и информационная безопасность: информационный портал/ООО "PositiveTechnologies". – URL: http://www.securitylab.ru
2. Андрончик, А. Н. Сетевая защита на базе технологий фирмы CiscoSystems. Практический курс: учебное пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков; под общ. ред. Н. И. Синадского. – URL: http://elar.urfu.ru/handle/10995/28990
3. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова. – Екатеринбург: Изд-во Урал. ун-та, 2019. – URL: http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
4. Жданов, О. Криптографические методы защиты информации/О.Жданов, Ю.Ушаков. - Москва: ИНТУИТ, 2016. – URL: https://www.intuit.ru/studies/courses/13837/1234/info.
5. Жигулин, Г.П. Организационное и правовое обеспечение информационной безопасности/Г.П.Жигулин; НИУ ИТМО. – С.-Петербург: НИУ ИТМО, 2014. – URL: https://books.ifmo.ru/file/pdf/1484.pdf
6. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие/ Н.С.Кармановский, О.В.Михайличенко, Н.Н.Прохожев. – С.-Петербург: НИУ ИТМО, 2016. – URL: https://books.ifmo.ru/file/pdf/1093.pdf
7. Каторин, Ю.Ф. Защита информации техническими средствами: учебное пособие / Ю.Ф.Каторин, А.В.Разумовский, А.И.Спивак; под редакцией Ю.Ф. Каторина. – С.-Петербург: НИУ ИТМО, 2012. – URL: https://books.ifmo.ru/file/pdf/975.pdf
8. Маркина, Т.А. Средства защиты вычислительных систем и сетей: учебное пособие/Т.А.Маркина; НИУ ИТМО. – С.-Петербург: Университет ИТМО, 2016. - URL: https://books.ifmo.ru/file/pdf/2121.pdf
9. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - Москва: Национальный Открытый Университет ИНТУИТ. – URL: https://www.intuit.ru/studies/courses/4/102/info
10. Теория информационной безопасности и методология защиты информации /Ю.А.Гатчин, В.В.Сухостат, А.С.Куракин, Ю.В.Донецкая. – 2-е изд., испр. и доп. – С.-Петербург: Университет ИТМО, 2018. – URL: https://books.ifmo.ru/file/pdf/2372.pdf
11. Техническая эксплуатация линейных сооружений: учебное пособие/ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»; Колледж связи. – Самара, 2017. – URL: http://ks.psuti.ru/downloads/students/distance_learning/3МТС-74,75/МДК.В.01.05%20Техническая%20эксплуатация%20линейных%20сооружений/МДК.01.05%20Учебное%20пособие.pdf
12. Энциклопедия инструментов: иллюстрированный справочник по инструментам и приборам. – URL: http://www.tools.ru/tools.htm

4.2.3. Дополнительные источники:

1. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: РИОР, 2013. - URL: https://znanium.com/catalog/product/405000
2. Берлин, А. Н. Абонентские сети доступа и технологии высокоскоростных сетей: учебное пособие / А. Н. Берлин. - 2-е изд. - Москва: ИНТУИТ, 2016. - URL: https://e.lanbook.com/book/100553

3. Берлин, А. Н. Телекоммуникационные сети и устройства: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016. — URL: https://e.lanbook.com/book/100525
4. Ворона, В. А. Инженерно-техническая и пожарная защита объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая Линия–Телеком, 2012. – URL: https://ibooks.ru/products/333380
5. Ворона, В.А. Системы контроля и управления доступом/В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2013. - URL: https://ibooks.ru/products/333378
6. Ворона, В.А. Технические системы охранной и пожарной сигнализации /В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2012. - URL: https://ibooks.ru/products/333381
7. Ворона, В.А. Технические средства наблюдения в охране объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая линия-Телеком, 2011. - URL: https://ibooks.ru/products/333379
8. Голиков, А.М. Тестирование и диагностика в инфокоммуникационных системах и сетях: учебное пособие / А.М. Голиков. – Москва: ТУСУР, 2016. — URL: https://e.lanbook.com/book/110274
9. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - Москва: Форум: ИНФРА-М, 2019. - URL: https://znanium.com/catalog/product/1001363
10. Груба, И.И. Системы охранной сигнализации. Технические средства обнаружения: справочное пособие / И.И.Груба. - Москва: СОЛОН-Пресс, 2020. - URL: https://znanium.com/catalog/document?id=392274
11. Душкин, А.В. Аппаратные и программные средства защиты информации: учебное пособие / А.В.Душкин, А.Кольцов, А.Кравченко. - Воронеж: Научная книга, 2017. - URL: https://znanium.com/catalog/product/977192
12. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие / Н.Б. Ельчанинова; Южный федеральный университет. - Ростов-на-Дону - Таганрог: Издательство Южного федерального университета, 2017. - URL: https://znanium.com/catalog/product/1021578
13. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019. - URL: https://znanium.com/catalog/product/1018901
14. Кенин, А.М. Практическое руководство системного администратора /А.М.Кенин. – С.-Петербург: БХВ-Петербург, 2013. - URL: https://ibooks.ru/products/335234
15. Кенин, А.М. Самоучитель системного администратора / А.М.Кенин, Д.Н.Колисниченко. - 4-е изд., перераб. и доп. – С.-Петербург: БХВ-Петербург, 2021. - URL: https://ibooks.ru/products/380054
16. Лапонина, О.Р. Межсетевое экранирование: учебное пособие / О.Р. Лапонина. – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2017. — URL: https://e.lanbook.com/book/100648
17. Портнов, Э. Л. Принципы построения первичных сетей и оптические кабельные линии связи: учебное пособие для вузов / Э.Л.Портнов. - Москва: Горячая линия-Телеком, 2013. - URL: https://ibooks.ru/products/354348
18. Проскурин, В.Г. Защита в операционных системах: учебное пособие для вузов/В.Г.Проскурин. - Москва: Горячая линия-Телеком, 2014. - URL: https://ibooks.ru/products/344419
19. Романьков, В.А. Введение в криптографию: курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. — Москва: Форум: ИНФРА-М, 2020. - URL: https://znanium.com/catalog/product/1046925
20. Рябко, Б. Я. Основы современной криптографии и стеганографии / Б.Я.Рябко, А.Н.Фионов. - 2-е изд. - Москва: Горячая линия-Телеком, 2016. - URL: https://ibooks.ru/products/344422

21. Рябко, Б. Я. Криптографические методы защиты информации: учебное пособие/ Б.Я.Рябко, А.Н.Фионов. – Москва: Горячая линия–Телеком, 2017. - URL: https://ibooks.ru/products/334031
22. Субботин, Е. А. Методы и средства измерения параметров оптических телекоммуникационных систем: учебное пособие для вузов / Е.А. Субботин. - Москва: Горячая линия-Телеком, 2013. - URL: https://ibooks.ru/products/334042
23. Техническая диагностика современных цифровых сетей связи. Основные принципы и технические средства измерений параметров передачи для сетей PDH, SDH, IP, Ethernet и ATM/И.И. Власов, Э.В.Новиков, М.М.Птичников, Д.В.Сладких; под ред. М.М.Птичникова. - Москва: Горячая линия-Телеком, 2017. - URL: https://ibooks.ru/products/333376
24. Технологии защиты информации в компьютерных сетях / Н.А. Руденков [и др.]. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — URL: https://e.lanbook.com/book/100522
25. Электрорадиоизмерения: учебник для студ. учрежд. СПО /В.И.Нефедов, А.С.Сигов, В.К.Битюков, Е.В.Самохина; под ред. А.С.Сигова. - Москва: Форум: Инфра-М, 2020. — URL: https://znanium.com/catalog/document?id=350665.

Периодические издания:

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

4.3. Общие требования к организации производственной практики (по профилю специальности)

Производственная практика (по профилю специальности) проводится при освоении обучающимися профессиональных компетенций в рамках профессиональных модулей и реализуется как в несколько периодов, так и рассредоточено, чередуясь с теоретическими занятиями в рамках профессиональных модулей.

Производственная практика (по профилю специальности) проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся, на основе договоров, заключаемых между колледжем и этими организациями.

Обязательным условием допуска к производственной практике (по профилю специальности) в рамках профессиональных модулей является наличие всех положительных оценок промежуточных аттестаций, профессиональным модулям, выполнение рабочей программы.

4.4. Кадровое обеспечение образовательного процесса

Руководство производственной практикой (по профилю специальности) осуществляют руководители практики от образовательной организации и от организации, закрепленные за обучающимися.

5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей	- производить монтаж кабельных линий и оконечных кабельных устройств ИТКС; - проверять функционирование, производить регулировку и контроль основных параметров источников питания ИТКС; - измерять основные показатели и характеристики при выполнении работ по настройке, проверке функционирования и конфигурирования ИТКС;	Экспертное наблюдение
ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования ИТКС	- осуществлять техническую эксплуатацию линейных сооружений связи; - проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; - измерять основные параметры и характеристики при выполнении работ по диагностике технического состояния, поиска неисправностей и ремонте оборудования ИТКС;	Экспертное наблюдение
ПК 1.3. Проводить техническое обслуживание оборудования ИТКС	- осуществлять техническую эксплуатацию линейных сооружений ИТКС; - измерять основные параметры и характеристики при выполнении технического обслуживания оборудования ИТКС; - производить контроль и регулировку основных параметров источников питания оборудования ИТКС;	Экспертное наблюдение
ПК 1.4. Осуществлять контроль функционирования ИТКС	- проводить мониторинг и контроль функционирования оборудования ИТКС; - измерять основные параметры и характеристики оборудования ИТКС; - вести эксплуатационно-техническую документацию на оборудование ИТКС;	Экспертное наблюдение
ПК 2.1. Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить конфигурирование программных и программно-аппаратных (в	Экспертное наблюдение

	том числе криптографических) средств защиты информации;	
ПК 2.2. Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС и их диагностику, обнаружение отказов, формировать предложения по их устранению	- 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; - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение
ПК 2.3. Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС	- 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;	Экспертное наблюдение
ПК 2.4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества, приборов и принадлежностей	- 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;	Экспертное наблюдение
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в ИТКС	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание,	Экспертное наблюдение

неисправностей и ремонт технических средств защиты информации, используемых в ИТКС	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;	
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС	- 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;	Экспертное наблюдение
ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	- требования техники безопасности при работе с вычислительной техникой; - основные принципы устройства и работы компьютерных систем и периферийных устройств; - выполнять требования техники безопасности при работе с вычислительной техникой;	Экспертное наблюдение Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю.
ПК 4.2. Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	- производить подключение блоков персонального компьютера и периферийных устройств; - производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; - диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники; - выполнение требований техники безопасности при работе с вычислительной техникой; организация рабочего места оператора электронно-вычислительных и вычислительных машин - подготовка оборудования компьютерной системы к работе;	Экспертное наблюдение Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю.

	- инсталляция, настройка и обслуживание программного обеспечения компьютерной системы; - управление файлами.	
ПК 4.3. Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	- назначение и функции офисных приложений; создавать и управлять содержимым документов с помощью текстовых процессоров; - создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц; - создавать и управлять содержимым презентаций с помощью редакторов презентаций; - использовать мультимедиа проектор для демонстрации презентаций; вводить, редактировать и удалять записи в базе данных; - эффективно пользоваться запросами базы данных; - создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; производить сканирование документов и их распознавание; - производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода; - применение офисного программного обеспечения в соответствии с прикладной задачей; - управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; - осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; - осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; - создавать и обмениваться письмами электронной почты; - использование ресурсов локальной вычислительной сети; - использование ресурсов, технологий и сервисов Интернет, основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы;	Экспертное наблюдение Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю.
ПК 4.4. Обеспечивать применение средств защиты информации в	- осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ;	Экспертное наблюдение Оценка выполнения и

компьютерной системе	- осуществлять резервное копирование и восстановление данных; - выполнять архивирование информации;	защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю.
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Демонстрировать грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	Экспертное наблюдение
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	Экспертное наблюдение

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективное выполнение правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности	Экспертное наблюдение
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение