**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
_____ Г.М. Машков
_____ 2021 г.
Регистрационный № 11.05.19/532

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ПРАКТИКИ

(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)

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

1.1. Область применения программы

Рабочая программа учебной 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 (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 учебной практики

Практика имеет целью комплексное освоение обучающимися всех основных видов деятельности по специальности среднего профессионального образования, формирование общих и профессиональных компетенций, а также приобретение необходимых умений и опыта практической работы по специальности.

Учебная практика по специальности направлена на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках профессиональных модулей по основным видам деятельности для последующего освоения ими общих и профессиональных компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (квалификация – техник по защите информации).

В результате освоения программы учебной практики обучающийся должен уметь и иметь первоначальный практический опыт по основным видам деятельности

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 состояния, поиска неисправностей и ремонта оборудования ИТКС.
Защита информации в информационно	**Уметь:**
	выявлять и оценивать угрозы безопасности информации в ИТКС;
	настраивать и применять средства защиты информации в операционных

Основной вид деятельности	Умения и практический опыт в
-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	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.
Выполнение работ по одной или нескольким профессиям	**Уметь:**
	выполнять требования техники безопасности при работе с вычислительной техникой;
	производить подключение блоков персонального компьютера и

Основной вид деятельности	Умения и практический опыт в
рабочих, должностям служащих: по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»	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 учебной практики

Всего – 396 часов (11 нед.), в том числе:
В рамках освоения ПМ.01 – 108 часов
В рамках освоения ПМ.02 - 108 часов
В рамках освоения ПМ.03 –108 часов
В рамках освоения ПМ.04 –72 часа

2 РЕЗЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

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

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.
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.

Код	Наименование компетенции
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 СОДЕРАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1. Структура учебной практики

Коды профессиональных компетенций	Наименования профессиональных модулей и МДК	Объем часов
ПК 1.1 – ПК 1.4	**ПМ.01.Эксплуатация информационно-телекоммуникационных систем и сетей**	**108**
	МДК.01.01.Приемо-передающие устройства, линейные сооружения связи и источники электропитания	36
	МДК.01.02.Телекоммуникационные системы и сети	72
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**	**108**
	МДК.02.01.Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	72
	МДК.02.02.Криптографическая защита информации	36
ПК 3.1 – ПК 3.4	**ПМ.03.Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты**	**108**
	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	
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		**396**

3.2. Содержание учебной практики

Код и наименование профессиональных модулей	Виды работ		Объем часов
ПМ.01. Эксплуатация информационно-телекоммуникационных систем и сетей			**108**
МДК.01.01. Приемо-передающие устройства, линейные сооружения связи и источники электропитания	**1**	Монтаж кабелей НЧ и ВЧ различными технологиями	36
	2	Монтаж оконечных устройств, применяемых на местных телефонных сетях, магистральных и зоновых линиях связи для электрических и оптических кабелей	
	3	Контроль качества монтажа с применением измерительных приборов постоянного тока	
	4	Определение вида и места повреждения кабельной линии связи с помощью приборов переменного тока (рефлектометров)	
	5	Монтаж оптических кабелей/ Проверка качества монтажа оптических волокон с помощью рефлектометров и измерителей оптической мощности	
	6	Разделка кабелей с «витой парой» для включения в коннекторы соответствующей емкости	
МДК.01.02. Телекоммуникационные системы и сети	**1**	Настройка оборудования транспортной сети мультиплексоров вода/вывода.	72
	2	Настройка оборудования транспортной сети терминальных мультиплексоров.	
	3	Настройка оборудования транспортной сети регенераторов.	
	4	Настройка оборудования транспортной сети кросконнекторов.	
	5	Настройка оборудования синхронизации транспортной сети.	
	6	Настройка оборудования абонентского доступа станционной части.	
	7	Настройка оборудования абонентского доступа ADSL2+.	
	8	Настройка оборудования абонентского доступа DSLAM.	
	9	Диагностика работы оборудования абонентского доступа станционной части.	
	10	Диагностика работы оборудования абонентского доступа ADSL2+.	
	11	Диагностика работы оборудования абонентского доступа DSLAM.	
	12	Настройка аппаратных IP-телефонов.	
	13	Настройка программных IP-телефонов.	
	14	Диагностика работы аппаратных IP-телефонов.	
	15	Диагностика работы программных IP-телефонов.	
	16	Подсоединение абонентского устройства к мультисервисной сети.	
	17	Диагностика работы абонентского устройства в мультисервисной сети.	
	18	Настройка и диагностика работы беспроводной сети.	
ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе, криптографических средств защиты			**108**

Код и наименование профессиональных модулей	Виды работ		Объем часов
МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	**1**	Работа с учетными записями пользователей	72
	2	Настройка параметров безопасности ОС	
	3	Управление хранением данных.	
	4	Архивация данных	
	5	Восстановление данных	
	6	Аудит ресурсов ОС	
	7	Аудит событий ОС	
	8	Управление доступом в Linux	
	9	Управление доступом в Windows	
	10	Средства аутентификации операционных систем	
	11	Управление средствами аутентификации в Linux	
	12	Управление средствами аутентификации в Windows	
	13	Документирование политики безопасности	
	14	Выбор, подключение, настройка межсетевого экрана	
	15	Выбор, подключение, настройка межсетевого экрана	
	16	Администрирование межсетевого экрана	
	17	Ознакомление, подключение, настройка системы резервного копирования	
	18	Ознакомление, подключение, настройка системы резервного копирования	
	19	Администрирование системы резервного копирования	
	20	Администрирование системы резервного копирования	
	21	Ознакомление, подключение, настройка системы антивирусной защиты	
	22	Администрирование системы антивирусной защиты.	
	23	Изучение методов комплексного исследования объекта информатизации	
	24	Изучение информации циркулирующей в корпоративной информационной системе	
	25	Изучение построения системы защиты информации на основе нормативных актов и методических указаний	
	26	Изучение построения системы защиты информации на основе нормативных актов и методических указаний	
	27	Построение модели угроз ИСПДн	
	28	Определение вероятности реализации угроз безопасности в информационной системе персональных данных	
	29	Изучение действующей нормативной документации объекта информатизации	

Код и наименование профессиональных модулей	Виды работ		Объем часов
	30	Составление плана мероприятий по улучшению защищённости объекта информатизации	
	31	Составление плана мероприятий по улучшению защищённости объекта информатизации	
	32	Составление плана мероприятий по улучшению защищённости объекта информатизации	
	33	Разработка КСЗИ информационной системы: сбор данных	
	34	Разработка КСЗИ информационной системы: выбор технологий	
	35	Разработка КСЗИ информационной системы: разработка модели	
	36	Разработка КСЗИ информационной системы: оформление решения	
МДК.02.02. Криптографическая защита информации	**1**	Настройка и администрирование токена	36
	2	Настройка сервисов Рутокен-PinPad	
	3	Настройка сервисов Рутокен-ЭЦП	
	4	Настройка сервисов Рутокен–Bluetooth	
	5	Настройка сервисов Рутокен–S	
	6	Разработка алгоритма PGP	
	7	Изучение протоколов SSL, TLS, IPSec	
	8	Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2	
	9	Составление алгоритма хеш-функции	
	10	Составление алгоритма шифра	
	11	Подключение, установка драйверов, настройка программных средств шифрования Криптон.	
	12	Администрирование программных средств шифрования Криптон	
	13	Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон.	
	14	Администрирование аппаратных средств шифрования Криптон.	
	15	Инфраструктуры открытых ключей и стандарт X.509	
	16	Защита электронного документооборота с использованием электронной цифровой подписи	
	17	Программная реализация ГОСТ Р 34.12- 2015	
	18	Стандарты информационной безопасности в Интернете (IETF, RFC).	
ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием	**1**	Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике.	
	2	Монтаж различных типов датчиков.	**108**
	3	Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.	
	4	Применение промышленных осциллографов, частотомеров и генераторов и другого	

Код и наименование профессиональных модулей	Виды работ		Объем часов
технических средств защиты		оборудования для защиты информации	
	5	Рассмотрение системы контроля и управления доступом	
	6	Рассмотрение принципов работы системы видеонаблюдения и ее проектирование	
	7	Рассмотрение датчиков периметра, их принципов работы	
	8	Выполнение звукоизоляции помещений системы зашумления	
	9	Реализация защиты от утечки по цепям электропитания и заземления	
	10	Рассмотрение принципов работы ЛВП-10 Электромагнитный вибропреобразователь к ЛГШ-404 (для окон, стен, труб)	
	11	Рассмотрение многозонной системы обнаружения и блокирования мобильных средств связи для образовательных учреждений	
	12	Монтаж различных типов датчиков	
	13	Рассмотрение устройств обнаружения скрытых видеокамер «Алмаз»	
	14	Применение промышленных осциллографов, частотомеров и генераторов акустического шума, двухканального генератора, системы постановки виброакустических помех и другого оборудования для защиты информации.	
	15	Рассмотрение системы контроля и управления доступом	
	16	Рассмотрение принципов работы программно-аппаратного комплекса защиты объектов информационных технологий от разведки ПЭМИ, 0,009 - 1000 МГц	
	17	Рассмотрение датчиков периметра, их принципов работы	
	18	Изучение средств перехвата информации	
	19	Микрофоны	
	20	Акустические антенны	
	21	Выбор типа микрофона и места его установки	
	22	Изучение устройств подавления микрофонов	
	23	Изучение устройств для перехвата речевой информации в проводных каналах	
	24	Изучение оптико-акустической аппаратуры перехвата речевой информации	
	25	Оптико-механические приборы	
	26	Приборы ночного видения	
	27	Средства скрытой фотосъемки	
	28	Зоны подключения в линиях связи	
	29	Перехват телефонных переговоров в зонах «А», «Б», «В», «Г», «Д», «Е»	
	30	Изучение перехвата сообщений в каналах сотовой связи	

Код и наименование профессиональных модулей	Виды работ		Объем часов
	31	Методы поиска закладных устройств как физических объектов и электронных средств	
	32	Панорамные приемники	
	33	Аппаратура контроля и защиты линии связи	
	34	Средства создания акустических и электромагнитных маскирующих помех	
	35	Измерение токов, напряжений и сопротивлений	
	36	Исследование двухполюсников с помощью мультиметра	
	37	Прямые и косвенные однократные измерения	
	38	Обработка и представление однократных измерений при наличии систематической погрешности	
	39	Стандартная обработка результатов прямых измерений с многократным наблюдением	
	40	Обработка результатов прямых измерений с многократным наблюдением при наличии грубых погрешностей	
	41	Определение погрешности цифрового вольтметра сличения и прямых измерений	
	42	Измерение мощности и силы постоянного электромагнитного тока	
	43	Измерение постоянного напряжения методом компенсации	
	44	Измерение переменного электрического напряжения	
	45	Измерение частоты и периода электрических сигналов	
	46	Терморезисторные измерительные преобразователи. Измерители температуры	
	47	Емкостные измерительные преобразователи. Измерение размера	
	48	Индуктивные измерительные преобразователи. Измерение перемещения	
	49	Термоэлектрические измерительные преобразователи. Измерение температуры	
	50	Пьезоэлектрические измерительные преобразователи. Измерение переменных ускорений	
	51	Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами	
	52	Применение существующих способов выявления опасности целостности информации	
	53	Выявление технических каналов утечки информации	
	54	Оформление отчета по учебной практике	
ПМ.04. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (Оператор электронно-вычислительных и	**1**	Безопасная организация рабочего места оператора ЭВМ.	**108**
	2	Выполнение разборки системного блока и ТО компонентов.	
	3	Изучение компонентов ПК и сборка системного блока.	
	4	Подключение и запуск ПК. Первичные настройки ПК	
	5	Изучение аппаратных характеристик ПК и характеристик ОС ПК.	
	6	Установка и замена расходных материалов для оргтехники.	

Код и наименование профессиональных модулей	Виды работ		Объем часов
вычислительных машин)	**7**	Управление файлами данных ПК	
	8	Создание виртуального жесткого диска	
	9	Обслуживание жестких дисков в ОС	
	10	Создание комплексных документов в текстовом процессоре	
	11	Создание формул и уравнений в документах в текстовом процессоре.	
	12	Создание диаграмм в документах в текстовом процессоре.	
	13	Организация расчетов в редакторе электронных таблиц	
	14	Создание электронной книги. Относительная и абсолютная адресации в редакторе электронных таблиц.	
	15	Связанные таблицы. Расчет промежуточных итогов в редакторе электронных таблиц	
	16	Подбор параметра. Организация обратного расчета в редакторе электронных таблиц	
	17	Задачи оптимизации (поиск решения) в редакторе электронных таблиц	
	18	Связи между файлами и консолидация данных в редакторе электронных таблиц	
	19	Экономические расчеты в редакторе электронных таблиц	
	20	Обработка объектов слайдов презентации	
	21	Настройка анимации объектов в программе подготовки и просмотра презентаций	
	22	Редактирование и модификация таблиц базы данных в СУБД.	
	23	Создание пользовательских форм для ввода данных в СУБД.	
	24	Работа с данными с использованием запросов в СУБД.	
	25	Создание отчетов в СУБД.	
	26	Работа с эффектами в графическом редакторе	
	27	Вставка и редактирование готового изображения в графическом редакторе.	
	28	Настройка пользователей и групп в ОС	
	29	Настройка Резервного копирования ОС	
	30	Автоматизация процесса управления и обслуживания ОС	
	31	Безопасный режим ОС	
	32	Создание архивов из имеющихся файлов.	
	33	Локальные политики безопасности	
	34	Выполнение схемы классификации компьютерных сетей с использованием прикладных ПС	
	35	Настройка показа и демонстрация результатов работы средствами мультимедиа	
	36	Оформление отчетной документации в соответствии с перечнем работ	
		ИТОГО	**396**

4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Лаборатория «Защиты информации от утечки по техническим каналам». Лаборатория оснащена средствами защиты информации от утечки по акустическому (виброакустическому) каналу; средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок; средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок;

шумогенераторы;
комплексный поисковый прибор;
прожигатели телефонных линий;
устройство обнаружения скрытых видеокамер;
виброакустические генераторы;
подавители диктофонов;
подавители устройств сотовой связи;
устройство защиты аналоговых сигналов;
устройство защиты цифровых сигналов;

стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения, охранно-пожарной сигнализации и охраны объек-тов;

комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

4.2. Информационное обеспечение реализации программы

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.

4.2.1. Электронные издания:

1. 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
2. Берлин, А. Н. Высокоскоростные сети связи: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016. — URL: https://e.lanbook.com/book/100724
3. 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

4. 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
5. 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
6. 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
7. 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
8. 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
9. 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
10. 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
11. 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
12. 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
13. Родина, О.В. Волоконно-оптические линии связи: практическое руководство/О.В.Родина. - Москва: Горячая линия-Телеком, 2016. - URL: https://ibooks.ru/products/334026
14. 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
15. 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
16. 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
17. 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
18. 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

Электронные ресурсы:

1. RusCable.Ru. Энергетика. Электротехника. Связь: отраслевое электронное СМИ. – URL: http://www.ruscable.ru/.
2. Волхонский, В.В. Устройства охранной сигнализации/В.В.Волхонский; НИУ ИТМО. – Санкт-Петербург: Университет ИТМО, 2015. – URL: https://books.ifmo.ru/book/1633/ustroystva_ohrannoy_signalizacii.htm

3. 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
4. Марусина, М.Я. Метрологическое обеспечение средств измерений: учебное пособие М.Я.Марусина, В.Л.Ткалич, Р.Я.Лабковская. – Санкт-Петербург: Университет ИТМО, 2019. – URL: https://books.ifmo.ru/file/pdf/2422.pdf
5. Руководство по применению адресно-аналоговых систем пожарной сигнализации/ С.М. Щипицын, А. Н. Членов, И. В. Павлов, А. Е. Атаманов. – Москва: Систем Сенсор Фаир Детекторс, 2012// СИГМА: группа компаний: официальный сайт. – URL: http://www.sigma-is.ru/files/education/Rukovodstvo_AASPS_2012.pdf
6. Рыжова, В.А. Проектирование и исследование комплексных систем безопасности/В.А.Рыжова; НИУ ИТМО. –С.-Петербург: НИУ ИТМО, 2013. – URL: https://books.ifmo.ru/file/pdf/1018.pdf
7. 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
8. 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
9. 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. Пескин, А.Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации / А.Е. Пескин. - Москва: Горячая линия-Телеком, 2013. - URL: https://ibooks.ru/products/334018.
15. 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
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/products/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/products/333349
18. 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
19. Скрипник, Д.А. Общие вопросы технической защиты информации/ Д.А.Скрипник. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — URL: https://e.lanbook.com/book/100275
20. 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
21. 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.

Периодические издания:

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

5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

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 том числе криптографических) средств	Экспертное наблюдение

	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 неисправностей и	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт	Экспертное наблюдение

ремонт технических средств защиты информации, используемых в ИТКС	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; - инсталляция, настройка и обслуживание	Экспертное наблюдение Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю.

	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 компьютерной системе	- осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; - осуществлять резервное копирование и	Экспертное наблюдение Оценка выполнения и защиты практических

	восстановление данных; - выполнять архивирование информации;	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	- эффективное выполнение правил ТБ во	Экспертное

сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	время учебных занятий, при прохождении учебной и производственной практик; - демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности	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