**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: 009b47d8b89b08d0f6
Владелец: Киричек Руслан Валентинович
Действителен с 13.02.2023 по 12.02.2028

УТВЕРЖДАЮ
Первый проректор – проректор по учебной работе
_____ А.В. Абилов
_____ 2023 г.

Регистрационный № 11.09.23/174

РАБОЧАЯ ПРОГРАММА

ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

(наименование вида практики)

по специальности

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

квалификация
техник по защите информации

Санкт-Петербург
2023

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена 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» 30 марта 2023 г., протокол № 3.

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

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

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 9 (Информационной безопасности телекоммуникационных систем)
1 февраля 2023 г., протокол № 6
Председатель предметной (цикловой) комиссии: _____ Н.В. Кривоносова
(подпись)

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля
8 февраля 2023 г., протокол № 3

Заместитель директора по учебной работе колледжа СПб ГУТ _____ Н.В. Калинина
(подпись)

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

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

Рабочая программа производственной практики (преддипломной) 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» 30 марта 2023 г., протокол №3.

СОГЛАСОВАНО

ЗГД по безопасности АО НПП "Сигнал"

_____ В.В. Ипатов

СОГЛАСОВАНО

Заместитель руководителя Управления Роскомнадзора по Северо-Западному федеральному округу

_____ И.Ю. Потехин

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

1.1. Область применения программы

Рабочая программа производственной практики (преддипломной) – является частью 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. Место производственной (преддипломной) практики в структуре программы подготовки специалистов среднего звена

Производственная практика (преддипломная) базируется на междисциплинарных курсах профессиональных модулей:

ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей

МДК.01.01. Приемо-передающие устройства, линейные сооружения связи и источники электропитания

МДК.01.02. Телекоммуникационные системы и сети

МДК.01.03. Электрорадиоизмерения и метрология

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе, криптографических средств защиты

МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

МДК.02.02. Криптографическая защита информации

ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

МДК.03.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей

ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (Оператор электронно-вычислительных и вычислительных машин)

МДК.04.01 Технология выполнения работ

1.3. Цели и задачи - требования к результатам освоения производственной практики (преддипломной)

Цель - углубление первоначального практического опыта обучающегося, развитие общих и профессиональных компетенций, проверка его готовности к самостоятельной трудовой деятельности, а также подготовка к выполнению выпускной квалификационной работы (дипломного проекта) в организациях различных организационно-правовых форм.

Задачи:

- овладение профессиональной деятельностью, развитие профессионального мышления;
- закрепление, углубление, расширение и систематизация знаний, закрепление практических навыков и умений, полученных при изучении дисциплин и профессиональных модулей, определяющих специфику специальности;
- обучение навыкам решения практических задач при подготовке выпускной квалификационной работы;
- проверка профессиональной готовности к самостоятельной трудовой деятельности выпускника;
- развитие и углубление навыков программирования;
- сбор материалов к государственной итоговой аттестации.

Для освоения программы производственной практики (преддипломной) студент должен иметь практический опыт, полученный в результате освоения междисциплинарных курсов профессиональных модулей по 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-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:

Основной вид деятельности	Умения и 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 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;

Основной вид деятельности	Умения и практический опыт в
	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.

1.4. Количество часов на освоение рабочей программы производственной практики (преддипломной)

В рамках освоения продолжительность производственной практики (преддипломной) 144 часа. Практика обучающихся имеет продолжительность 4 недели.

2 РЕЗЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Результатом освоения рабочей программы преддипломной практики является углубление первоначального практического опыта обучающихся, развитие общих и профессиональных компетенций, готовность к самостоятельной трудовой деятельности, а также к выполнению выпускной квалификационной работы в организациях различных организационно-правовых форм.

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

Код	Наименование компетенции
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
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
ПК 1.1.	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.
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 ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

3.1. Тематический план программы производственной практики (преддипломной)

Коды профессиональных компетенций	Наименования профессионального модуля и его разделов	Производственная практика (преддипломная) (часов)
ПМ.01.Эксплуатация информационно-телекоммуникационных систем и сетей		
ПК 1.1-ПК 1.4 ОК 01-11	МДК.01.01.Приемо-передающие устройства, линейные сооружения связи и источники электропитания	
	МДК.01.02.Телекоммуникационные системы и сети	
	МДК.01.03.Электрорадиоизмерения и метрология	
ПМ.02.Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты		
ПК 2.1, ОК 01-11	МДК.02.01.Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	
ПК 2.2, ПК 2.3, ОК 01-11	МДК.02.02.Криптографическая защита информации	**144**
ПМ.03.Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты		
ПК 3.1-ПК 3.4, ОК.01-11	МДК.03.01.Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	
ПК 3.1, ОК.01-11	МДК.03.02.Физическая защита линий связи информационно-телекоммуникационных систем и сетей	
ПМ.04.Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (Оператор электронно-вычислительных и вычислительных машин)		
ПК 4.1-ПК 4.4 ОК 01-11	МДК.04.01.Технология выполнения работ	
	Всего часов	**144**

3.2. Содержание производственной практики (преддипломной)

№ п/п	Разделы (этапы) практики	Содержание разделов (этапов) практики	Количество часов
1.	Организационные вопросы оформления на предприятии, установочная лекция, инструктаж по охране труда и технике безопасности, распределение по рабочим местам	1. Изучение инструкции по охране труда. 2. Изучение инструкции по технике безопасности и пожаробезопасности, схем аварийных проходов и выходов, пожарного инвентаря. 3. Изучение правил внутреннего распорядка. 4. Изучение правил и норм охраны труда, техники безопасности при работе с вычислительной техникой.	20
2.	Ознакомление со структурой и характером деятельности предприятия	1. Знакомство со штатным расписание 2. Знакомство с отделами организации 3. Знакомство с видами деятельности отделов организации	20
3.	Сбор материалов для составления технического задания по теме дипломного проекта	1. Подготовка списка источников 2. Изучение нормативных документов 3. Составление плана 4. Изучение технической документации	50
4.	Расчет показателей экономической эффективности программного продукта	1. Сбор показателей и коэффициентов для расчета единовременных затрат на проектирование системы и разработку программного обеспечения. 2. Расчет затрат на проектирование системы. 3. Расчет затрат на разработку программного обеспечения. 4. Расчет показателей эффективности внедрения информационной системы. 5. Оценка показателей экономической эффективности по методу дисконтирования	30
5.	Оформление отчета о прохождении производственной практики (преддипломной)	Оформление отчета в соответствии с требованиями ГОСТа	24

4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

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 объектов;

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

4.2. Информационное обеспечение реализации программы

Для реализация программы библиотечный фонд образовательной организации имеет электронные издания и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

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.

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.

Приложение 1

**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

АТТЕСТАЦИОННЫЙ ЛИСТ по производственной (преддипломной) ПРАКТИКЕ

_____

ФИО

Обучающийся(аяся) на _____ курсе по специальности СПО

_____ _____

код *наименование*

База практики:

_____

успешно прошел(ла) производственную практику (преддипломную) по профессиональному модулю

_____

_____

в объеме __ часа с __.202_ г. по _____ 202_ г.

Виды и качество выполнения работ

Работы, выполненные обучающ(имся/ейся) во время практики		***Оценка выполнения работ (положительная - 1, отрицательная – 0)***
Виды работ	***Объем работ (час.)***	
Интегральная оценка(медиана)		
Характеристика учебной и профессиональной деятельности обучающегося во время учебной / производственной практики (по профилю специальности) *(дополнительно используются произвольные критерии по выбору ОУ)* Аттестуемый(ая) *продемонстрировал(а) / не продемонстрировал(а)* владение общими компетенциями:		

Дата _____ 202__ г. **Подпись(и) руководителя(ей) практики от организации:**

От подразделения _____ _____ _____

должность ФИО *подпись*

От организации _____ _____ _____

должность ФИО *подпись*

М.П.

Приложение 2

**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**

Д Н Е В Н И К
ПРАКТИКИ
ОБУЧАЮЩЕГОСЯ

ФИО _____

Отделение:_____
Курс:_____
Группа:_____

Специальность:_____

База практики: *(полное наименование профильной организации/ подразделения СПбГУТ юридический адрес)*
_____
_____
_____

САНКТ-ПЕТЕРБУРГ
2022