

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

УТВЕРЖДАЮ

Первый проректор – проректор по
учебной работе

А.В. Абилов

2025 г.

Регистрационный № 11.09.25/129



РАБОЧАЯ ПРОГРАММА

ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

(наименование вида практики)

по специальности

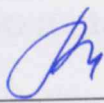
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код и наименование специальности)

квалификация
техник по защите информации

Санкт-Петербург
2025

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, утвержденным ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 28 марта 2025 г., протокол № 3.

Составитель:
Преподаватель



(подпись) Н.В. Кривоносова

СОГЛАСОВАНО
Главный специалист НТБ УИОР

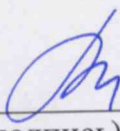


(подпись) Р.Х. Ахтреева

ОБСУЖДЕНО

на заседании предметной (цикловой) комиссии № 9 (Информационной безопасности телекоммуникационных систем)
12 февраля 2025 г., протокол № 6

Председатель предметной (цикловой) комиссии:

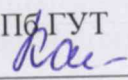


(подпись) Н.В. Кривоносова

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля
19 февраля 2025 г., протокол № 4

Заместитель директора по учебной работе колледжа СПб ГУТ



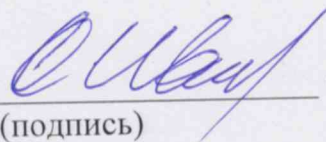
(подпись) Н.В. Калинина

СОГЛАСОВАНО
Директор колледжа СПб ГУТ



(подпись) Т.Н. Сиротская

СОГЛАСОВАНО
Директор департамента ОКОД



(подпись) С.И. Ивасишин

СОДЕРЖАНИЕ

1	ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)	4
2	РЕЗУЛЬТАТЫ ОСВОЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)	6
3	СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)	8
4	УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)	10
5	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)	22

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;
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; эффективно пользоваться запросами базы данных;

Основной вид деятельности	Умения и практический опыт в
	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 обслуживании 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 РЕЗУЛЬТАТЫ 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
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста

Код	Наименование компетенции
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 оборудовании 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		144
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	
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 расписанием 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, оснащенные 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 реализации 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/> (дата обращения: 22.02.2023).
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» //Гарант: информационно-правовой портал. – URL: <https://base.garant.ru/12148567/> (дата обращения: 22.02.2023).
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» //Гарант: информационно-правовой портал. – URL: <https://base.garant.ru/12129354/> (дата обращения: 22.02.2023).
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/> (дата обращения: 22.02.2023).
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/> (дата обращения: 22.02.2023).
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/> (дата обращения: 22.02.2023).
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/> (дата обращения: 22.02.2023).

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/> (дата обращения: 22.02.2023).
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/> (дата обращения: 22.02.2023) (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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-reglamenti/1362-prikaz-fstek-rossii-ot-17-iyulya-2017-g-n-134-2> (дата обращения: 22.02.2023).
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-reglamenti/478-prikaz-fstek-rossii-ot-12-iyulya-2012-g-n-84> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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/> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).
 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> (дата обращения: 22.02.2023).

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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023).
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> (дата обращения: 22.02.2023). 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->

4.2.2. Основные электронные издания:

1. Бабушкин, В. М. Разработка защищенных программных средств информатизации производственных процессов предприятия: учебное пособие / В. М. Бабушкин. — Казань: КНИТУ-КАИ, 2020. — 256 с. — ISBN 978-5-7579-2463-2. — URL: <https://e.lanbook.com/book/193486> (дата обращения: 26.02.2023).
2. Баранова, Е.К. Основы информационной безопасности: учебник для студ. учреждений СПО / Е.К. Баранова, А.В. Бабаш. — Москва: РИОР: ИНФРА-М, 2022. — 202 с. — ISBN 978-5-369-01806-4. URL: <https://znanium.com/catalog/product/1860126> (дата обращения: 26.02.2023).
3. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А.Бузов. — Москва: Горячая линия-Телеком, 2018. — 586 с. — ISBN 978-5-9912-0424-8. — URL: <https://ibooks.ru/products/354357> (дата обращения: 26.02.2023).
4. Бурлаков, М. Е. Акустические и виброакустические каналы утечки информации. Теоретические основы и базовый практикум: учебное пособие / М. Е. Бурлаков, М. Н. Осипов. — Самара: Самарский университет, 2021. — 96 с. — ISBN 978-5-7883-1659-8. — URL: <https://e.lanbook.com/book/257039> (дата обращения: 26.02.2023).
5. Васильков, А.В. Безопасность и управление доступом в информационных системах: учебное пособие для среднего профессионального образования /А.В.Васильков, И.А.Васильков. — Москва: ФОРУМ, 2020. — 368 с. — ISBN 978-5-91134-360-6. — URL: <https://znanium.com/catalog/product/1082470> (дата обращения: 26.02.2023).
6. Введение в криптографическую защиту информации объектов: учебник / С. Н. Ильиных, С. Г. Алюшина, Т. И. Калинкина [и др.]. — Москва: МТУСИ, 2021. — 276 с. — URL: <https://e.lanbook.com/book/215231>. — URL: <https://e.lanbook.com/book/215231> (дата обращения: 26.02.2023).
7. Гладких, А. А. Основы современных криптографических систем и перспективы их развития: учебное пособие / А. А. Гладких, В. Е. Дементьев, Н. Ю. Чилихин. — Ульяновск: УлГТУ, 2020. — 214 с. — ISBN 978-5-9795-2096-4. — URL: <https://e.lanbook.com/book/259745> (дата обращения: 26.02.2023).
8. Грекул В. И. Проектное управление в сфере информационных технологий / В.И. Грекул, Н.В. Коровкина, Ю.В. Куприянов. — Москва: Лаборатория знаний, 2020. — 339 с. — ISBN 978-5-00101-792-9. -- URL: <https://ibooks.ru/bookshelf/350334> (дата обращения: 26.02.2023).
9. Емельянова, Н. З. Защита информации в персональном компьютере: учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва: ФОРУМ: ИНФРА-М, 2021. — 368 с. — ISBN 978-5-00091-466-3. — URL: <https://znanium.com/catalog/product/1189325> (дата обращения: 26.02.2023).
10. Епишкина, А. В. Нормативное регулирование в области защиты информации: Конспект лекций: учебное пособие / А. В. Епишкина, С. В. Запечников. — Москва: НИЯУ МИФИ, 2021. — 116 с. — ISBN 978-5-7262-2807-5. — URL: <https://e.lanbook.com/book/284345> (дата обращения: 26.02.2023).
11. 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. — 442 с. — ISBN 978-5-9912-0233-6. — URL: <https://ibooks.ru/products/333981> (дата обращения: 26.02.2023).
12. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва: РИОР: ИНФРА-М, 2021. — 400 с. — ISBN 978-5-369-01759-3. — URL: <https://znanium.com/catalog/product/1210523> (дата обращения: 26.02.2023).
13. Зырянова, Т. Ю. Управление информационной безопасностью: учебное пособие / Т. Ю. Зырянова. — Екатеринбург: Уральский гос. ун-т путей сообщения, 2023. — URL: <https://e.lanbook.com/book/369482> (дата обращения: 26.02.2023).
14. Игнатьев, Е. Б. Основы криптографии: учебное пособие / Е. Б. Игнатьев. — Иваново: ИГЭУ, 2020. — 88 с. — URL: <https://e.lanbook.com/book/154559> (дата обращения: 26.02.2023).

15. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учреждений СПО / В.Я.Ищейнов, М.В.Мецатунян. – Москва: Форум: ИНФРА-М, 2021. — 208 с. — ISBN 978-5-00091-489-2. — URL: <https://znanium.com/catalog/document?id=365084> (дата обращения: 26.02.2023).
16. 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. — 342 с. — ISBN 978-5-534-10671-8. — URL: <https://urait.ru/bcode/456792> (дата обращения: 26.02.2023).
17. 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. — 342 с. — ISBN 978-5-534-10671-8. — URL: <https://urait.ru/bcode/456792> (дата обращения: 26.02.2023).
18. Калабухова, Г. В. Компьютерный практикум по информатике. Офисные технологии: учебное пособие / Г.В. Калабухова, В.М. Титов. – Москва: ФОРУМ: ИНФРА-М, 2022. — 336 с. — ISBN 978-5-8199-0916-4. — URL: <https://znanium.com/catalog/document?id=385006> (дата обращения: 26.02.2023).
19. Каширская, Е. Н. Криптографический анализ и методы защиты информации: учебное пособие / Е. Н. Каширская. — Москва: РТУ МИРЭА, 2020. — 91 с. — URL: <https://e.lanbook.com/book/163861> (дата обращения: 26.02.2023).
20. Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара: Самарский университет, 2020. — 183 с. — URL: <https://e.lanbook.com/book/189043> (дата обращения: 26.02.2023).
21. Комплексные системы защиты информации на: учебное пособие / составители Д. С. Алексеев, О. В. Щекочихин. — Кострома: КГУ, 2021. — 167 с. — ISBN 978-5-8285-1164-8. — URL: <https://e.lanbook.com/book/201884> (дата обращения: 26.02.2023).
22. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — URL: <https://e.lanbook.com/book/156401> (дата обращения: 26.02.2023).
23. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем: учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва: РТУ МИРЭА, 2020. — 136 с. — URL: <https://e.lanbook.com/book/167606> (дата обращения: 26.02.2023).
24. Лагоша, О. Н. Сертификация информационных систем: учебное пособие / О. Н. Лагоша. — Санкт-Петербург: Лань, 2020. — 112 с. — ISBN 978-5-8114-4668-1. — URL: <https://e.lanbook.com/book/139268> (дата обращения: 26.02.2023).
25. Леонтьев, А. С. Защита информации: учебное пособие / А. С. Леонтьев. — Москва: РТУ МИРЭА, 2021. — 79 с. — URL: <https://e.lanbook.com/book/182491> (дата обращения: 26.02.2023).
26. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — URL: <https://e.lanbook.com/book/237770> (дата обращения: 26.02.2023).
27. Мошак, Н. Н. Защищенные информационные системы: учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — URL: <https://e.lanbook.com/book/180099> (дата обращения: 26.02.2023).
28. Нестеров, С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. — Санкт-Петербург: Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — URL: <https://e.lanbook.com/book/165837> (дата обращения: 26.02.2023).
29. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург: Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — URL: <https://e.lanbook.com/book/288974> (дата обращения: 26.02.2023).
30. Никифоров, С. Н. Методы защиты информации. Защищенные сети: учебное пособие для вузов / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 96 с. — ISBN 978-5-8114-8123-1. — URL: <https://e.lanbook.com/book/171868> (дата обращения: 26.02.2023).

31. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург: Лань, 2023. — 124 с. — ISBN 978-5-507-47181-2. — URL: <https://e.lanbook.com/book/338018> (дата обращения: 26.02.2023).
32. Никифоров, С. Н. Методы защиты информации. Шифрование данных: учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 160 с. — ISBN 978-5-8114-4042-9. — URL: <https://e.lanbook.com/book/206285> (дата обращения: 26.02.2023).
33. Особенности функционирования, подключения и настройки средств обнаружения и контроля: практикум / сост. А. В. Паринов, О. В. Исаев, О. А. Андреева. — Иваново: ПресСто, 2022. — 112 с. — URL: <https://znanium.com/catalog/product/1998968> (дата обращения: 26.02.2023).
34. Петренко, В. И. Защита персональных данных в информационных системах: практикум / В. И. Петренко, И. В. Мандрица. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 108 с. — ISBN 978-5-507-45301-6. — URL: <https://e.lanbook.com/book/264242> (дата обращения: 26.02.2023).
35. Поляков, Е. А. Основы информационной безопасности: учебное пособие / Е. А. Поляков. — Нижний Новгород: ННГУ им. Н. И. Лобачевского, 2021. — 71 с. — URL: <https://e.lanbook.com/book/282890> (дата обращения: 26.02.2023).
36. Потерпеев, Г. Ю. Безопасность операционных систем: учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва: РТУ МИРЭА, 2021. — 93 с. — ISBN 978-5-7339-1393-3. — URL: <https://e.lanbook.com/book/182416> (дата обращения: 26.02.2023).
37. Программно-аппаратные средства обеспечения информационной безопасности / А.В.Душкин, О.М.Барсуков, Е.В.Кравцов, К.В.Славнов. — Москва: Горячая Линия–Телеком, 2016. — 248 с. — ISBN 978-5-9912-0470-5. — URL: <https://ibooks.ru/bookshelf/357887> (дата обращения: 26.02.2023).
38. Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург: Лань, 2021. — 124 с. — ISBN 978-5-8114-7970-2. — URL: <https://e.lanbook.com/book/169817> (дата обращения: 26.02.2023).
39. Свешников, И. В. Основы информационной безопасности телекоммуникационных систем: учебное пособие / И. В. Свешников, В. В. Савватеев. — Чита: ЗабГУ, 2022. — 230 с. — ISBN 978-5-9293-3034-6. — URL: <https://e.lanbook.com/book/363503> (дата обращения: 26.02.2023).
40. Сергеев, А. Н. Основы локальных компьютерных сетей: учебное пособие для вузов / А. Н. Сергеев. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 184 с. — ISBN 978-5-507-44766-4. — URL: <https://e.lanbook.com/book/242867> (дата обращения: 26.02.2023).
41. Степанова, И.В. Надежность систем управления: учебное пособие /И.В.Степанова. — Москва: МТУСИ, 2021. — 70 с. — URL: <https://e.lanbook.com/book/215315> (дата обращения: 26.02.2023).
42. Страшун, Ю. П. Технические средства автоматизации и управления на основе ПоТ/ЮТ: учебное пособие / Ю. П. Страшун. — Санкт-Петербург: Лань, 2020. — 76 с. — ISBN 978-5-8114-5018-3. — URL: <https://e.lanbook.com/book/143701> (дата обращения: 26.02.2023).
43. Сычев, Ю. Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. — Москва: ИНФРА-М, 2022. — 201 с. — ISBN 978-5-16-014976-9. — URL: <https://znanium.com/catalog/product/1844364> (дата обращения: 26.02.2023).
44. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов / Ю. Н. Сычев. — Москва: ИНФРА-М, 2021. — 223 с. — ISBN 978-5-16-016533-2. — URL: <https://znanium.com/catalog/product/1178148> (дата обращения: 26.02.2023).
45. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — URL: <https://e.lanbook.com/book/130184> (дата обращения: 26.02.2023).
46. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — URL: <https://e.lanbook.com/book/207095> (дата обращения: 26.02.2023).

47. Хорев, П. Б. Программно-аппаратная защита информации: учебное пособие для среднего профессионального образования/ П.Б. Хорев. — 2-е изд., испр. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 352 с. — ISBN 978-5-00091-557-8. — URL: <https://znanium.com/catalog/product/1189341> (дата обращения: 26.02.2023).
48. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2020. — 592 с. — ISBN 978-5-8199-0730-6. — URL: <https://znanium.com/catalog/product/1093695> (дата обращения: 26.02.2023).
49. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для среднего профессионального образования/В.Ф.Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2020. — 416 с. — ISBN 978-5-8199-0754-2. — URL: <https://znanium.com/catalog/document?id=358701> (дата обращения: 26.02.2023).
50. Шелухин, О. И. Учебно-методическое пособие по дисциплине «Интеллектуальные технологии информационной безопасности анонимизация и деанонимизация пользователей Интернет-порталов»: учебно-методическое пособие / О. И. Шелухин, А. В. Ванюшина; составители О. И. Шелухин, А. В. Ванюшина. — Москва: МТУСИ, 2021. — 49 с. — URL: <https://e.lanbook.com/book/215345> (дата обращения: 26.02.2023).

4.2.3. Дополнительные источники:

1. Бергер, Е. Г. Единая система программной документации: учебно-методическое пособие / Е. Г. Бергер. — Москва: РТУ МИРЭА, 2020. — 109 с. — URL: <https://e.lanbook.com/book/163817> (дата обращения: 26.02.2023).
2. Бергер, Е. Г. Нормоконтроль документации: методические рекомендации / Е. Г. Бергер. — Москва: РТУ МИРЭА, 2020. — 30 с. — URL: <https://e.lanbook.com/book/167623> (дата обращения: 26.02.2023).
3. Варфаловская, В. В. Экономическое обоснование проектных решений: учебно-методическое пособие / В. В. Варфаловская, Н. Н. Куликова. — Москва: РТУ МИРЭА, 2022. — 83 с. — URL: <https://e.lanbook.com/book/256796> (дата обращения: 26.02.2023).
4. Ехлаков, Ю. П. Управление программными проектами. Стандарты, модели: учебное пособие для вузов / Ю. П. Ехлаков. — 3-е изд., стер. — Санкт-Петербург: Лань, 2021. — 244 с. — ISBN 978-5-8114-8362-4. — URL: <https://e.lanbook.com/book/175498> (дата обращения: 26.02.2023).
5. Корниенко, А. А. Система требований к обеспечению безопасности автоматизированных систем и значимых объектов критической информационной инфраструктуры: учебное пособие / А.А.Корниенко, С.В.Корниенко, А.П.Глухов. — Санкт-Петербург: ПГУПС, 2022. — 63 с. — ISBN 978-5-7641-1837-6. — URL: <https://e.lanbook.com/book/329477> (дата обращения: 26.02.2023).
6. Петренко, С. А. Политики безопасности компании при работе в Интернет / С.А. Петренко, В.А. Курбатов. — Москва: ДМК Пресс, 2018. — 397 с. — ISBN 978-5-93700-057-6. — URL: <https://ibooks.ru/bookshelf/384751> (дата обращения: 26.02.2023).
7. Петровский, В. И. Принципы построения системы защиты информации на предприятиях различных форм собственности: учебное пособие / В. И. Петровский; под редакцией В. И. Петровского. — Казань: КНИТУ-КАИ, 2016. — 512 с. — ISBN 978-5-7579-2150-1. — URL: <https://e.lanbook.com/book/149575> (дата обращения: 26.02.2023).
8. Потерпеев, Г. Ю. Безопасность операционных систем: учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Кriuлин. — Москва: РТУ МИРЭА, 2021. — 93 с. — ISBN 978-5-7339-1393-3. — URL: <https://e.lanbook.com/book/182416> (дата обращения: 26.02.2023).

Электронные ресурсы:

1. Техэксперт. Электронный фонд правовой и нормативно-технической документации/АО «Кодекс»: Профессиональные справочные системы: официальный сайт. — URL: <http://docs.cntd.ru/> (дата обращения: 26.02.2023).
2. Единая система программной документации: [сайт]. — URL: <http://prog-cpp.ru/espd/>
3. Библиотека учебных курсов Microsoft. Документация: [сайт]. — URL: <http://msdn.microsoft.com/library/> (дата обращения: 26.02.2023).

4. ГОСТЭксперт: единая база ГОСТов РФ. Документация на разработку программного обеспечения и системная документация: [сайт]. – URL: <http://gostexpert.ru/oks/35/80> (дата обращения: 26.02.2023).
5. Общероссийский классификатор стандартов. ГОСТы, СНИПы, СанПиНы и др.: образовательный ресурс. Информационные технологии: [сайт]. – URL: <http://gostedu.ru/001/035/> (дата обращения: 26.02.2023).
6. Руководство по требованиям к документации ISO 9001: 2008//KlubOK.net: управление качеством: [сайт]. – URL: www.klubok.net/pageid506.html (дата обращения: 26.02.2023).

Периодические издания:

1. Information Security/Информационная безопасность: официальный сайт. – URL: <https://lib.itsec.ru/imag/> (дата обращения: 26.02.2023).
2. Защита информации Inside.
3. Информационные технологии и телекоммуникации: научный журнал // Санкт-Петербургский гос. университет телекоммуникаций им. М.А.Бонч-Бруевича: официальный сайт. – URL: <http://ijitt.ru/> (дата обращения: 26.02.2023).
4. Проблемы информационной безопасности. Компьютерные системы.
5. Электросвязь.

**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(ая) 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.

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