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

СМОЛЕНСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ (ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА».

КТ СМОЛЕНСК

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 1A30BAD460180FD2A79F95ADF83BFA73
Владелец: Иванешко Ирина Васильевна
Действителен: с 02.08.2024 до 26.10.2025

Утверждаю
Зам. директора по учебной работе
_____ И.В. Иванешко
«31» 08 2023г.

РАБОЧАЯ ПРОГРАММА

производственной практики (преддипломной)

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

г. Смоленск

2023

Рассмотрено на заседании
методической комиссии компьютерных
сетей и администрирование
Председатель _____ О.С. Скряго
Протокол № 1
«31» 08 2023

Составитель: Драницина М.Д.- заведующий практикой СКТ(ф) СПбГУТ

Рабочая программа разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерства образования и науки РФ от 09.12.2016г. №1551, а также на основании примерной основной образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, разработанной ФУМО в системе СПО по УГС 10.00.00 «Информационная безопасность».

Согласовано: Руководитель направления Управления безопасности Смоленского филиала ПАО «Ростелеком» _____ Петров В.А.

М.П.

2

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

1.1. Область применения программы

Программа практики– 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-коммуникационных систем и сетей;
- Защита информации в информационно-коммуникационных системах и сетях с использованием программных, программно-аппаратных, в том числе криптографических средств защиты;
- Защита информации в информационно-коммуникационных системах и сетях с использованием технических средств защиты.

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

1.1. Место производственной практики (преддипломной) 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

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

Цель - углубление первоначального практического опыта обучающегося, развитие общих и профессиональных компетенций, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку 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 к итоговой аттестации;
- проверка профессиональной готовности к самостоятельной трудовой деятельности выпускника.

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**
Эксплуатация информационно-телекоммуникационных систем и сетей	монтаж, настройка, проверка функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (далее –ИТКС);
	текущий контроль функционирования оборудования ИТКС;диагностика технического состояния приёмо-передающих устройств и линейных сооружений связи и источников питания;
	проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта оборудования ИТКС;
	текущий контроль функционирования оборудования ИТКС; мониторинг технического состояния и работоспособности приёмо-передающих устройств и линейных сооружений связи и источников питания ИТКС;
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программно-аппаратных, в том числе криптографических средств защиты	установка, настройка, испытаний и конфигурирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС;
	поддержание бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС
	защита 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;
	установка, монтаж, настройка и испытание технических средств защиты информации от утечки по техническим каналам
	установка, монтаж, настройка и испытание технических средств защиты информации от утечки по техническим каналам; проведение технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
	защита информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
	проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

Основной вид деятельности	Умения и практический опыт
	выявление технических каналов утечки информации.
Защита информации в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
	применять нормативные правовые акты и нормативные методические документы в области защиты информации;
	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
	проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;
	проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС;
	проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
	применять нормативные правовые акты и нормативные методические документы в области защиты информации;
	применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам;
	установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам; проведения технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
	защиты информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
	проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации

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

В рамках освоения продолжительность производственной практики (преддипломной) 144 часа.

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Результатом освоения рабочей программы производственной практики (преддипломной) является углубление практического опыта обучающихся, развитие общих и профессиональных компетенций, готовность к самостоятельной трудовой деятельности.

Код	Наименование компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
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
ПК1.1.	Производить монтаж, настройку и поверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей.
ПК 1.2.	Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно – телекоммуникационных систем и сетей.
ПК 1.3.	Проводить техническое обслуживание оборудования информационно – телекоммуникационных систем и сетей
ПК 1.4.	Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем

Код	Наименование компетенции
	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

3 СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

3.1. 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.	36
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	36
3.	Сбор материалов для составления технического задания по теме дипломного проекта и сдаче демонстрационного экзамена.	1. Подготовка списка источников 2. Изучение нормативных документов 3. Составление плана 4. Изучение технической документации	48
4.	Оформление отчета о прохождении производственной практики (преддипломной)	Оформление отчета в соответствии с требованиями	18
5.		Сдача технического отчета по производственной (преддипломной) практике	6
Всего часов			**144**

4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

4.1. Требования к минимальному материально-техническому обеспечению

Практическая подготовка в виде производственной практики (преддипломной) по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем проходит на базе предприятий, учреждений и организаций различных организационно-правовых форм и форм собственности на основе договоров, заключаемых между предприятием и колледжем, отвечающим следующим требованиям:

- наличие сфер деятельности, предусмотренных программой производственной практики;
- обеспечение квалифицированными кадрами для руководства производственной практикой.

Колледж имеет договоры о практической подготовке обучающихся специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем с предприятиями:

ПАО «Ростелеком»;
ОО «Ман-сеть»;
ООО Т2 Мобайл;
АО «НИИ СТТ» ;
ОГАУЗ «СОМИАЦ»;
ООО «Ситиком».

Для прохождения производственной практики на предприятиях организованы технически оснащенные рабочие места практиканта:
Локальная сеть с выходом в Интернет PROXY-SERVER.
Компьютер персональный.
Специализированное программное обеспечение систем приема; передачи и обработки сигналов.
Комплекс «Защита объекта от утечки информации по техническим каналам».
Сервер Dell PowerEdge .
R530 операционная система Windows Server 2012 R2;
Комплект нормативных документов.

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.

Нормативные документы:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

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».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
11. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
12. 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.
13. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
15. 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.
16. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
17. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
18. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
19. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
20. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
21. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
23. 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
24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
28. 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
29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
30. 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
31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
40. 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. Росстандарт, 2012.
41. 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). Росстандарт, 2013.
42. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
43. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
44. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
45. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
46. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
47. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

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. — М.: РИОР: ИНФРА-М, 2020.
2. Баранова, Е.К. Основы информационной безопасности: учебник для студ. учрежд. СПО / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019.
3. Берлин, А. Н. Высокоскоростные сети связи: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.
4. Берлин, А. Н. Оконечные устройства и линии абонентского участка информационной сети: учебное пособие / А. Н. Берлин. - 2-е изд. - Москва: ИНТУИТ, 2016.
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.
6. Заика, А.А. Локальные сети и Интернет/ А.А. Заика. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
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.
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.
9. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО /В.Я.Ищейнов, М.В.Мецатунян. - Москва: Форум: ИНФРА-М, 2018.
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.
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.
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.
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.
14. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов/В.Г.Олифер, Н.А.Олифер. – С.-Петербург: Питер, 2018.
15. 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.
16. Портнов, Э. Л. Оптические кабели связи, их монтаж и измерение: учебное пособие для вузов / Э.Л. Портнов. - Москва: Горячая линия-Телеком, 2012.
17. Программно-аппаратные средства обеспечения информационной безопасности / А.В.Душкин, О.М.Барсуков, Е.В.Кравцов, К.В.Славнов. – Москва: Горячая Линия–Телеком, 2016.
18. 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.
19. Родина, О.В. Волоконно-оптические линии связи: практическое руководство/О.В.Родина. - Москва: Горячая линия-Телеком, 2016.
20. 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.

21. Смычек, М.А. Технологические сети и системы связи: учебное пособие / М.А. Смычек. - 2-е изд. - Москва; Вологда: Инфра-Инженерия, 2019.
22. Соколов, С.А. Волоконно-оптические линии связи и их защита от внешних влияний: учебное пособие / С.А. Соколов. – М.: Инфра-Инженерия, 2019.
23. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие/П.Б.Хорев. - 2-е изд., испр. и доп. - Москва: Форум: ИНФРА-М, 2020.
24. Цуканов, В.Н. Волоконно-оптическая техника: практическое руководство/ В.Н. Цуканов, М.Я. Яковлев. – Москва: Инфра-Инженерия, 2019.
25. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА-М, 2020.
26. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учрежд. СПО. - М.: ФОРУМ: ИНФРА-М, 2020.

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.– Текст: электронный. - 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. Криптографическая защита информации: учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин.– Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006.– URL:https://tstu.ru/book/elib/pdf/2006/shamkin1.pdf/.
9. 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.
10. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - Москва: Национальный Открытый Университет ИНТУИТ. – URL:https://www.intuit.ru/studies/courses/4/102/info.
11. Пленкин, А.П. Построение, измерения и тестирование проводных линий связи телекоммуникационной сети. Часть 1: Методическая разработка /А.П.Пленкин, Ю.В. Зачиняев. URL: http://open-edu.rsu.ru/files/Методичка%20№4.pdf.
12. Пленкин, А.П. Построение, измерения и тестирование проводных линий связи телекоммуникационной сети. Оптическое волокно. Часть 2: Методическая разработка/А.П.Пленкин. –Таганрог, 2016. – URL: http://open-edu.rsu.ru/files/Методичка%20№5.pdf.

13. 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.
14. 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.
15. Энциклопедия инструментов: иллюстрированный справочник по инструментам и приборам. – URL: http://www.tools.ru/tools.htm.

3.2.3. Дополнительные источники:

1. Андреев, В.А. Направляющие системы электросвязи: учебник для вузов. В 2 т. Т.1. Теория передачи и влияния/ В.А.Андреев, Э.Л.Портнов, Л.Н.Кочановский. - Москва: Горячая линия-Телеком, 2011.
2. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: РИОР, 2013.
3. Берлин, А. Н. Абонентские сети доступа и технологии высокоскоростных сетей: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.
4. Берлин, А. Н. Телекоммуникационные сети и устройства: учебное пособие / А. Н. Берлин. - 2-е изд. - Москва: ИНТУИТ, 2016.
5. Ворона, В. А. Инженерно-техническая и пожарная защита объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая Линия–Телеком, 2012.
6. Ворона, В.А. Системы контроля и управления доступом/В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2013.
7. Ворона, В.А. Технические системы охранной и пожарной сигнализации /В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2012.
8. Голиков, А.М. Тестирование и диагностика в инфокоммуникационных системах и сетях: учебное пособие / А.М. Голиков. – М.: ТУСУР, 2016.
9. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - Москва: Форум: ИНФРА-М, 2019.
10. Груба, И.И. Системы охранной сигнализации. Технические средства обнаружения: справочное пособие / И.И.Груба. - М.: СОЛОН-Пресс, 2013.
11. Душкин, А.В. Аппаратные и программные средства защиты информации: учебное пособие / А.В.Душкин, А.Кольцов, А.Кравченко. - Воронеж: Научная книга, 2017.
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.
13. Запечников, С. В. Основы построения виртуальных частных сетей: учебное пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. - Москва: Гор. линия-Телеком, 2011.
14. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019.
15. Кенин, А.М. Практическое руководство системного администратора /А.М.Кенин. – С.-Петербург: БХВ-Петербург, 2013.
16. Кенин, А.М. Самоучитель системного администратора / А.М.Кенин, Д.Н.Колисниченко. - 4-е изд., перераб. и доп. – С.-Петербург: БХВ-Петербург, 2016.
17. Лапонина, О.Р. Межсетевое экранирование: учебное пособие / О.Р. Лапонина. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2017.

18. Метрология и электрорадиоизмерения в телекоммуникационных системах: учебное пособие / С.И. Боридько, Н.В. Дементьев и др.; под общ. ред. Б.Н. Тихонова - 2 изд., стер. - Москва: Горячая линия-Телеком, 2012.
19. Направляющие системы электросвязи. В 2-х т. Т. 2. Проектирование, строительство и техническая эксплуатация: учебник для ВУЗов/В.А.Андреев, А.В.Бурдин, Л.Н.Кочановский и др.; под ред. В.А.Андреева. - М.: Горячая линия-Телеком, 2010.
20. Портнов, Э. Л. Принципы построения первичных сетей и оптические кабельные линии связи: учебное пособие для вузов / Э.Л.Портнов. - Москва: Горячая линия-Телеком, 2013.
21. Портнов, Э.Л. Электрические кабели связи и их монтаж: учебное пособие/Э.Л.Портнов, А.Л.Зубилевич. - 2-е изд. - Москва: Горячая линия-Телеком, 2010.
22. Проскурин, В.Г. Защита в операционных системах: учебное пособие для вузов/В.Г.Проскурин. - М.: Горячая линия-Телеком, 2014.
23. Романьков, В.А. Введение в криптографию: курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. — Москва: Форум: ИНФРА-М, 2020.
24. Рябко, Б. Я. Криптографические методы защиты информации: учебное пособие/ Б.Я.Рябко, А.Н.Фионов. – Москва: Горячая линия–Телеком, 2017.
25. Рябко, Б. Я. Основы современной криптографии и стеганографии / Б.Я.Рябко, А.Н.Фионов. - 2-е изд. - Москва: Гор. линия-Телеком, 2016.
26. Субботин, Е. А. Методы и средства измерения параметров оптических телекоммуникационных систем: учебное пособие для вузов / Е.А. Субботин. - Москва: Горячая линия-Телеком, 2013.
27. Технологии защиты информации в компьютерных сетях / Н.А. Руденков [и др.]. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
28. 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.
29. Технологии защиты информации в компьютерных сетях / Н.А. Руденков [и др.]. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
30. Чащина, Е.Л. Обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники: учебник для студ. учрежд. СПО/Е.Л.Чащина. – Москва: Академия, 2016.
31. Чащина, Е.Л. Обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники: практикум: учебное пособие для студ. учрежд. СПО/Е.Л.Чащина. – Москва: Академия, 2016.
32. Чернышев, Е.И. Линейные сооружения связи: учебное пособие для студ. учрежд. СПО/Е.И.Чернышев. - Волгоград: Ин-Фолио, 2010.
33. 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.

Периодические издания:

1. Защита информации Inside.
2. InformationSecurity/Информационная безопасность.
3. Электросвязь.

4.3. Общие требования к организации практики

К прохождению производственной практики (преддипломной) допускаются студенты, не имеющие академической задолженности по междисциплинарным курсам, учебным практикам и производственным практикам в рамках освоения профессиональных модулей: ПМ.01, ПМ.02, ПМ. 03, ПМ.04 по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Организация производственной практики (преддипломной) осуществляется в сроки, установленные рабочим учебным планом, после изучения всех разделов междисциплинарных курсов и тем теоретического обучения.

Максимальный объем производственной практики (преддипломной) составляет 144 часа из расчета 36 академических часов в неделю.

База практики должна соответствовать профилю специальности студента.

На предприятии за студентом закрепляется руководитель, который проводит с ним инструктаж по технике безопасности, охране труда, знакомит обучающегося со структурой предприятия, помогает освоить программу производственной практики (преддипломной) и осуществляет контроль ее прохождения. В колледже подготовкой обучающегося к производственной практики (преддипломной), консультацией по вопросам прохождения практики занимаются специалисты Отдела практического обучения.

Во время прохождения практики студент ведет дневник практики, в котором руководитель от предприятия делает отметки и выставляет оценки. В конце практики студент оформляет отчет по производственной практике, согласно требованиям по составлению технического отчета. Руководитель практики от предприятия дает отзыв-характеристику о сформировавшихся у практиканта общих и профессиональных компетенциях, что учитывается в дальнейшем при получении итоговой оценки по практике.

Аттестация по итогам производственной практики (преддипломной) проводится с учетом результатов ее прохождения, подтверждаемых документами соответствующих организаций (баз практик). Студент должен представить в колледж для получения оценки по практике: технический отчет с выполненным заданием, заполненный дневник, аттестационный лист, который выдается студентам в колледже.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ) ПО СПЕЦИАЛЬНОСТИ 10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Одной из форм контроля результатов производственной практики (преддипломной) является дневник практики, который ведется обучающимся в процессе прохождения практики.

По результатам прохождения производственной практики (преддипломной) обучающийся составляет технический отчет, который утверждается организацией, на базе которой проходила практика. В качестве приложения к дневнику практики обучающийся оформляет материалы по индивидуальному заданию на практику, а так же графические, аудио-, фото-, видео-, материалы, подтверждающие практический опыт, полученный на практике.

Результаты (освоенные ПК)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей	- производить монтаж кабельных линий и оконечных кабельных устройств ИТКС; - проверять функционирование, производить регулировку и контроль основных параметров источников питания ИТКС; - измерять основные показатели и характеристики при выполнении работ по настройке, проверке функционирования и конфигурированияИТКС;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования ИТКС	- осуществлять техническую эксплуатацию линейных сооружений связи; - проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; - измерять основные параметры и характеристики при выполнении работ по диагностике технического состояния, поиска неисправностей и ремонте оборудования ИТКС;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 1.3**.** Проводить техническое обслуживание оборудования ИТКС	- осуществлять техническую эксплуатацию линейных сооружений ИТКС; - измерять основные параметры и характеристики при выполнении технического обслуживания оборудования ИТКС;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики,

	- производить контроль и регулировку основных параметров источников питания оборудования ИТКС;	Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 1.4. Осуществлять контроль функционирования ИТКС	- проводить мониторинг и контроль функционирования оборудования ИТКС; - измерять основные параметры и характеристики оборудования ИТКС; - вести эксплуатационно-техническую документацию на оборудование ИТКС;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
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.	- 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;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

	защиты информации; - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	
ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.	-проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 3.3. Осуществлять	- проводить измерение	- наблюдение за

защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные ОК)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-	- наблюдение за действиями на практике - оценка действий на практике

профессиональной деятельности.	ресурсы, периодические издания по специальности для решения профессиональных задач;	- оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- эффективность использования в профессиональной деятельности необходимой технической документации -грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов

общечеловеческих ценностей, применять стандарты антикоррупционного поведения.		дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ОК 09. Использовать информационные технологии в профессиональной деятельности	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

Итоговая аттестация по преддипломной практике проводится в форме дифференцированного зачета