Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Колледж информатики и программирования

УТВЕРЖДАЮ

Заместитель директора по УПР и СР

_____ О.М. Сумлинова
«_23_» _ноября_2023г.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

по специальности среднего профессионального образования
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Москва 2023 г.

Рабочая программа производственной практики разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г. №1553

Рабочая программа производственной практики рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии Обеспечение информационной безопасности автоматизированных систем
Протокол от «09» ноября 2023 г.№ 4
Председатель ПЦК Маринич А.Л. Маринич

Рабочая программа производственной практики рассмотрена и одобрена Методическим советом Колледжа информатики и программирования Финансового университета при Правительстве Российской Федерации

Протокол от «16» ноября 2023 г.№ 5

1. ОБЩАЯ ХАРАКТЕРСИТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей

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

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

1.1. Цель и планируемые результаты освоения программы производственной практики

- формирование у обучающихся практических умений и приобретение первичного практического опыта в рамках освоения профессиональных модулей образовательной программы СПО по основным видам деятельности в соответствии с ФГОС СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.1.1 Перечень общих компетенций

Код	Общие 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

1.1.2 Перечень профессиональных компетенций

Код	Профессиональные компетенции
ПМ. 01	Эксплуатация информационно-телекоммуникационных систем и сетей
ПК 1.1.	Производить монтаж, настройку, проверку 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
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.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях
ПК 2.3.	Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации
ПМ.03	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала 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

1.1.3.В результате прохождения производственной практики по видам профессиональной деятельности, обучающийся должен:

Вид деятельности: Эксплуатация информационно-телекоммуникационных систем и сетей	
иметь практический опыт	– монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (ИТКС); – текущего контроля функционирования оборудования ИТКС; – проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта оборудования ИТКС.
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 телекоммуникационных систем; – проводить работы по техническому обслуживанию, диагностики технического состояния и ремонту оборудования ИТКС; – измерять основные качественные показатели и характеристики при выполнении профилактических и ремонтных работ приемо-передающих устройств (ППУ); – читать принципиальные схемы блоков ППУ; – выполнять расчеты, связанные с определением значений параметров режима и элементов ППУ; – контролировать работу и осуществлять техническую эксплуатацию ППУ; – настраивать, эксплуатировать и обслуживать локальные вычислительные сети; – сопрягать между собой различные телекоммуникационные устройства;

	– производить настройку программного обеспечения коммутационного оборудования телекоммуникационных систем; – осуществлять настройку модемов, используемых в защищенных телекоммуникационных системах; – проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; – проводить типовые измерения; – пользоваться стандартными средствами электрорадиоизмерений; – оценивать точность проводимых измерений; – оформлять эксплуатационную и ремонтную документацию.
знать	– принципы построения информационно-телекоммуникационных систем и сетей; – базовые технологии построения и состав оборудования мультисервисных сетей связи; – состав и основные характеристики типового оборудования ИТКС; – принципы передачи информации в ИТКС; – принцип модуляции сигналов ИТКС; – принципы помехоустойчивого кодирования сигналов ИТКС; – виды и характеристики сигналов в ИТКС; – принципы аналого-цифрового преобразования, работы компандера, кодера и декодера; – особенности распространения электромагнитных волн различных диапазонов частот; – виды помех в каналах связи, методы защиты от них; – разновидности проводных линий передачи; – конструкцию и характеристики электрических и оптических кабелей связи; – способы коммутации в сетях связи; – принципы построения многоканальных систем передачи; – принципы построения радиолиний и систем радиосвязи; – основы маршрутизации в информационно-телекоммуникационных сетях; – принципы построения, основные характеристики и оборудование систем подвижной радиосвязи; – технологии и оборудование удаленного доступа в информационно-телекоммуникационных сетях; – типовые услуги, предоставляемые с использованием информационно-телекоммуникационных сетей, виды информационного обслуживания, предоставляемые пользователям; – принципы построения и технические средства локальных

	сетей; – принципы функционирования маршрутизаторов; – модемы, использующиеся в ИТКС, принципы подключения и функционирования; – спецификацию изделий, комплектующих, запасного имущества и ремонтных материалов, порядок их учета и хранения; – принципы организации эксплуатации ИТКС; – содержание технического обслуживания и восстановления работоспособности оборудования ИТКС; – принципы организации и технологию ремонта оборудования ИТКС; – периодичность поверок контрольно-измерительной аппаратуры; – принцип действия выпрямителей переменного тока; – принципы работы стабилизаторов напряжения и тока, импульсных источников питания. – принципы защиты электронных устройств от недопустимых режимов работы; – принципы построения, основные характеристики типовых измерительных приборов и правила работы с ними; – основные понятия и определения метрологии, стандартизации и сертификации.
Вид деятельности: Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	
иметь практический опыт	– определения необходимых средств криптографической защиты информации; – использования программно-аппаратных криптографических средств защиты информации; – установки, настройки специализированного оборудования криптографической защиты информации; – применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; – шифрования информации.
уметь	– выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; – определять рациональные методы и средства защиты на объектах и оценивать их эффективность; – производить установку и настройку типовых программно-аппаратных средств защиты информации; – пользоваться терминологией современной

	криптографии, использовать типовые криптографические средства защиты информации.
знать	– типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; – основные протоколы идентификации и аутентификации в телекоммуникационных системах; – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; – особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; – основные способы противодействия – несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы; – основные понятия криптографии и типовые криптографические методы защиты информации;
Вид деятельности: Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты	
иметь практический опыт	– установка, монтаж и настройка технических средств защиты информации; – техническое обслуживание технических средств защиты информации; – применение основных типов технических средств защиты информации; – выявление технических каналов утечки информации; – участие в мониторинге эффективности технических средств защиты информации; – диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; – проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации; – проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты.
уметь	– применять технические средства для криптографической защиты информации конфиденциального характера;

	– применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять инженерно-технические средства физической защиты объектов информатизации.
знать	– порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – структуру и условия формирования технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты информации; – номенклатуру применяемых средств физической защиты объектов информатизации.

1.2. Количество часов на освоение рабочей программы производственной практики:

Всего 468 часов, в том числе:

в рамках освоения ПМ.01 (ПП 01.01) – 5 нед., 180 ч.;

в рамках освоения ПМ.02 (ПП 02.01) – 4 нед., 144 ч.;

в рамках освоения ПМ.03 (ПП.03.01) – 4 нед., 144 ч.;

1. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

1.1. Структура производственной практики

Коды профессиональных и общих компетенций, личностные результаты	Код и наименование профессиональных модулей	Суммарный объём нагрузки, час.	Виды работ	Наименование тем производственной практики	Количество часов по темам
ПК 1.1.-1.4. ОК.01-ОК.11	ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей	**5 нед./180 ч**	Ознакомление со структурой предприятия, вводный инструктаж по технике безопасности и охране труда. Ознакомление с кабельными цехами и участками. Работа с технической документацией. Изучение оборудования и устройств, повышающих работоспособность и надежность кабельных линий. Ознакомление с оборудованием ИТКС. Изучение и работа с контрольно-измерительным оборудованием. Самостоятельная работа на закрепленном рабочем месте. Выполнение индивидуального задания по практике. Участите в аварийных и профилактических работах, проводимых на кабельном участке. Обобщение материала, оформление отчета, сдача зачета.	Тема 1. Ознакомление со структурой предприятия, вводный инструктаж по технике безопасности и охране труда; Тема 2. Ознакомление с кабельными цехами и участкам; Тема 3 Работа с технической документацией.; Тема 4. Изучение оборудования и устройств, повышающих работоспособность и надежность кабельных линий; Тема 5. Ознакомление с оборудованием ИТКС Тема 6. Изучение и работа с контрольно-измерительным оборудованием; Тема 7. Самостоятельная работа на закрепленном рабочем месте;	18 18 18 18 18 18 18

				Тема 8. Выполнение индивидуального задания по практике; Тема 9. Участите в аварийных и профилактических работах, проводимых на кабельном участке; Тема 10. Обобщение материала, оформление отчета, сдача зачета.	18 18
ПК 2.1-2.6. ОК.01-ОК.11	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	**4 нед./144 ч**	Участие в организации работ по защите персональных компьютеров на предприятии Участие в организации работ по защите локальных сетей на предприятии Участие в организации работ по защите работ в глобальной сети интернет на предприятии Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. Администрирование систем безопасности проводной защищенной локальной сети. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. Администрирование систем безопасности беспроводной защищенной локальной сети.	Тема 1. Проведение инструктажа по технике безопасности. Ознакомление с предприятием; Тема 2. Участие в организации работ по защите локальных сетей на предприятии; Тема 3. Участие в организации работ по защите работ в глобальной сети интернет на предприятии; Тема 4. Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети; Тема 5. Администрирование систем безопасности проводной защищенной локальной сети; Тема 6. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети;	6 10 10 10 10 10

			Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей Подключение, установка драйверов, настройка программных средств абонентского шифрования Администрирование внедренных средств Настройка средств электронной подписи Администрирование средств электронной подписи Администрирование средств PKI	Тема 7. Администрирование систем безопасности беспроводной защищенной локальной сети; Тема 8. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей: Тема 9. Участие в организации работ по защите персональных компьютеров на предприятии; Тема 10. Выбор программных средств шифрования в соответствии с решаемой задачей; Тема 11. Подключение, установка драйверов, настройка программных средств абонентского шифрования; Тема 12. Администрирование внедренных средств; Тема 13. Настройка средств электронной подписи Администрирование средств электронной подписи; Тема 14. Администрирование средств PKI.	10 10 10 10 10 16 10

ПК 3.1-3.5. ОК.01-ОК.11	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	**4 нед./144ч**	Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	Тема 1. Установка, монтаж и настройка технических средств защиты информации; Тема 2. Техническое обслуживание технических средств защиты информации; Тема 3. Применение основных типов технических средств защиты информации; Тема 4. Выявление технических каналов утечки информации; Тема 5. Участие в мониторинге эффективности технических средств защиты информации; Тема 6. Диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; Тема 7. Проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	16 16 16 16 16 16 16

				Тема 8. Проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; Тема 9. Установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты.	16
	Всего часов	**468**			

1.2. Тематический план и содержание производственной практики

Профессиональные модули и междисциплинарные курсы, темы	Содержание практики	Объём часов
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		180
Тема 1. Ознакомление со структурой предприятия, вводный инструктаж по технике безопасности и охране труда; Тема 2. Ознакомление с кабельными цехами и участкам; Тема 3 Работа с технической документацией.; Тема 4. Изучение оборудования и устройств, повышающих работоспособность и надежность кабельных линий; Тема 5. Ознакомление с оборудованием ИТКС	Прохождение инструктажа по технике безопасности. Ознакомление с Политикой информационной безопасности. Ознакомление с организационной структурой. Ознакомление с должностными инструкциями. Изучение оборудования и устройств, повышающих работоспособность и надежность кабельных линий. Оценка информационных активов, уязвимостей, угроз и рисков информационной безопасности.	

Тема 6. Изучение и работа с контрольно-измерительным оборудованием; Тема 7. Самостоятельная работа на закрепленном рабочем месте; Тема 8. Выполнение индивидуального задания по практике; Тема 9. Участите в аварийных и профилактических работах, проводимых на кабельном участке; Тема 10. Обобщение материала, оформление отчета, сдача зачета.	Изучение и работа с контрольно-измерительным оборудованием. Сбор и изучение научно-практического материала по разделам дипломной работы, подбор фактического материала на базе организации, развитие практических навыков и компетенции в процессе выполнения определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой дипломной работы. Проведение анализа и обобщения научно-технической информации по теме дипломной работы. Подбор фактического материала по теме дипломной работы с учетом профессиональных модулей и его изучение. Подготовка плана пояснительной записки к дипломной работы. Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием. Подготовка отчета.	
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		144
Тема 1. Проведение инструктажа по технике безопасности. Ознакомление с предприятием; Тема 2. Участие в организации работ по защите локальных сетей на предприятии; Тема 3. Участие в организации работ по защите работ в глобальной сети интернет на предприятии; Тема 4. Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети; Тема 5. Администрирование систем безопасности проводной защищенной локальной сети;	Прохождение инструктажа по технике безопасности. Ознакомление с Политикой информационной безопасности. Ознакомление с организационной структурой. Ознакомление с должностными инструкциями. Разработка базовой сетевой архитектуры предприятия и формулирование предложений по их модернизации. Анализ деятельности предприятия/подразделения, определение методов и средств повышения эффективности обработки и защиты информации.	

Тема 6. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети; Тема 7. Администрирование систем безопасности беспроводной защищенной локальной сети; Тема 8. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей: Тема 9. Участие в организации работ по защите персональных компьютеров на предприятии; Тема 10. Выбор программных средств шифрования в соответствии с решаемой задачей; Тема 11. Подключение, установка драйверов, настройка программных средств абонентского шифрования; Тема 12. Администрирование внедренных средств; Тема 13. Настройка средств электронной подписи Администрирование средств электронной подписи; Тема 14. Администрирование средств PKI.	Сбор и изучение научно-практического материала по разделам дипломной работы, подбор фактического материала на базе организации, развитие практических навыков и компетенции в процессе выполнения определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой дипломной работы. Проведение анализа и обобщения научно-технической информации по теме дипломной работы. Подбор фактического материала по теме дипломной работы с учетом профессиональных модулей и его изучение. Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части дипломной работы. Подготовка отчета.	
ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты МДК.03.01Защита информации в ИТКС с использованием технических средств защиты МДК.03.02Физическая защита линий связи ИТКС		144
Тема 1. Установка, монтаж и настройка технических средств защиты информации; Тема 2. Техническое обслуживание технических средств защиты информации; Тема 3. Применение основных типов технических средств защиты информации; Тема 4. Выявление технических каналов утечки информации; Тема 5. Участие в мониторинге эффективности технических средств защиты информации;	Прохождение инструктажа по технике безопасности. Ознакомление с Политикой информационной безопасности. Ознакомление с организационной структурой. Ознакомление с должностными инструкциями. Разработка базовой сетевой архитектуры предприятия и формулирование предложений по их модернизации. Выявление каналов утечки информации. Анализ деятельности предприятия/подразделения, определение методов и средств повышения эффективности обработки и защиты информации.	

Тема 6. Диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; Тема 7. Проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; Тема 8. Проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; Тема 9. Установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты.	Сбор и изучение научно-практического материала по разделам дипломной работы, подбор фактического материала на базе организации, развитие практических навыков и компетенции в процессе выполнения определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой дипломной работы. Проведение анализа и обобщения научно-технической информации по теме дипломной работы. Подбор фактического материала по теме дипломной работы с учетом профессиональных модулей и его изучение. Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части дипломной работы. Подготовка отчета.	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение

Производственная практика проходит в организациях, с которыми заключены договоры о проведении практики.
Договор № 44-СР/2023 от 27.10.2023 по организации проведения практики.
Срок действия договора: 5 лет.

Для прохождения производственной практики организациями предоставляются автоматизированные рабочие места с программным обеспечением, соответствующим профилю профессионального модуля производственной практики.

Руководство практикой осуществляется преподавателями профессионального цикла.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Контроль и оценка результатов освоения производственной практики осуществляются с использованием следующих форм и методов: наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист). В результате освоения производственной практики в рамках профессионального модуля студенты проходят промежуточную аттестацию в форме дифференцированного зачёта.

Результаты обучения (освоенные умения, практический опыт в рамах вида деятельности)	**Формы и методы контроля и оценки результатов обучения**
Вид деятельности: Эксплуатация информационно-телекоммуникационных систем и сетей	
Иметь практический опыт: – монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (ИТКС); – текущего контроля функционирования оборудования ИТКС;	Наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им

– проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта оборудования ИТКС. **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 телекоммуникационных систем; – проводить работы по техническому обслуживанию, диагностики технического состояния и ремонту оборудования ИТКС; – измерять основные качественные показатели и характеристики при выполнении профилактических и ремонтных работ приемо-передающих устройств (ППУ); – читать принципиальные схемы блоков ППУ; – выполнять расчеты, связанные с определением значений параметров режима и элементов ППУ; – контролировать работу и осуществлять техническую эксплуатацию ППУ; – настраивать, эксплуатировать и обслуживать локальные вычислительные сети; – сопрягать между собой различные телекоммуникационные устройства; – производить настройку программного обеспечения коммутационного оборудования телекоммуникационных систем; – осуществлять настройку модемов, используемых в защищенных телекоммуникационных системах; – проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; – проводить типовые измерения; – пользоваться стандартными средствами электрорадиоизмерений; – оценивать точность проводимых измерений; – оформлять эксплуатационную и ремонтную документацию.	соответствующих работ (отчёт по практике, аттестационный лист)
Вид деятельности: Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	
Иметь практический опыт: – определения необходимых средств криптографической защиты информации; – использования программно-аппаратных криптографических средств защиты информации;	Наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им

– установки, настройки специализированного оборудования криптографической защиты информации; – применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; – шифрования информации. **Уметь:** – выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; – определять рациональные методы и средства защиты на объектах и оценивать их эффективность; – производить установку и настройку типовых программно-аппаратных средств защиты информации; – пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации.	соответствующих работ (отчёт по практике, аттестационный лист)
Вид деятельности: Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты	
Иметь практический опыт: – установка, монтаж и настройка технических средств защиты информации; – техническое обслуживание технических средств защиты информации; – применение основных типов технических средств защиты информации; – выявление технических каналов утечки информации; – участие в мониторинге эффективности технических средств защиты информации; – диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; – проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации; – проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты. **Уметь:** – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;	Наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист)

– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять инженерно-технические средства физической защиты объектов информатизации.	