

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

СОГЛАСОВАНО

УТВЕРЖДАЮ



АО «ОКБ САИП»

Генеральный директор

И.Г. Назаров

15 07 2024 г.

Заместитель директора
по учебно-практической работе и
стратегическому развитию

A handwritten signature in blue ink, likely belonging to O.M. Sumlina.

О.М. Сумлинова

«27» июня 2024 г.

**РАБОЧАЯ ПРОГРАММА
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)**

по специальности

10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

Москва 2024 г.

Рабочая программа производственной практики (преддипломной) разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г. № 1551 (зарегистрирован в Министерстве юстиции Российской Федерации 26 декабря 2016 г. № 44944).

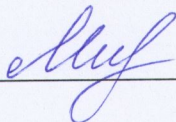
Организации – партнеры: ПАО «Ростелеком»; АО «Особое Конструкторское Бюро Систем автоматизированного Проектирования» (АО «ОКБ «САПР»), ООО «РусБИТех-Астра», АО «ИнфоВотч», АО «ИнфоТеКС», АО «Научно-производственное предприятие «САПФИР» (АО «НПП «САПФИР»), Управление Федеральной службы государственной статистики по г. Москве и Московской области, АО «НПП «Пульсар», Инспекция ФНС России по г. Москве, МРУ Росфинмониторинга по ЦФО, ПАО "Сбербанк России", Консорциум "Интегра-С".

Разработчики:

Демкина Н.И., к.э.н., директор Колледжа информатики и программирования, преподаватель ВКК; Сумлинова О.М., зам. директора по учебно-практической работе и стратегическому развитию Колледжа информатики и программирования; Маринич А.Л., преподаватель 1КК Колледжа информатики и программирования.

Рабочая программа производственной (преддипломной) практики рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии Обеспечение информационной безопасности автоматизированных систем
Протокол от «13» июня 2024 г. № 10

Председатель ПЦК _____



А.Л. Маринич

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

1.1. Цель и планируемые результаты освоения программы производственной практики (преддипломной)

Программа направлена на углубление первоначального практического опыта обучающегося, развитие общих и профессиональных компетенций, личностных результатов, проверку его готовности к самостоятельной трудовой деятельности, а также на подготовку к выполнению демонстрационного экзамена и дипломной работы.

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
<i>Вид деятельности</i>	<i>Эксплуатация информационно-телекоммуникационных систем и сетей</i>
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.
<i>Вид деятельности</i>	<i>Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты</i>
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 систем и сетей с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.
<i>ПК 2.4.*</i>	<i>Участие в формировании требований к системе безопасности значимых объектов значимых объектах критической информационной инфраструктуры*</i>
<i>ПК 2.5.*</i>	<i>Участие в планировании мероприятий по обеспечению безопасности значимых объектов значимых объектах критической информационной инфраструктуры*</i>
<i>ПК 2.6.*</i>	<i>Разработка организационно-распорядительных документов по обеспечению безопасности значимых объектов значимых объектах критической информационной инфраструктуры*</i>
<i>ПК 2.7*</i>	<i>Осуществление в установленном порядке реагирования на компьютерные инциденты в значимых объектах критической информационной инфраструктуры*</i>
<i>Вид деятельности</i>	<i>Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты</i>
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.
---------	--

1.1.3. В результате прохождения производственной практики (преддипломной) по видам профессиональной деятельности студент должен:

ВД: *Эксплуатация информационно-телекоммуникационных систем и сетей*

иметь практический опыт	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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;

	<ul style="list-style-type: none"> -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, используемые 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 проверок 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.
<p><i>ВД: Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты</i></p>	
иметь практический опыт	<ul style="list-style-type: none"> 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; <i>Анализ защищенности информационной инфраструктуры значимых объектов критической информационной инфраструктуры</i>

	<p>Участие в формировании требований к назначению, структуре и конфигурации создаваемой значимых объектов критической информационной инфраструктуры</p> <p>Участие в разработке модели угроз безопасности информации и модели нарушителя в значимых объектах критической информационной инфраструктуры</p> <p>Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации значимых объектов критической информационной инфраструктуры</p> <p>Участие в определении комплекса мер для защиты информации значимых объектов критической информационной инфраструктуры</p> <p>Участие в формировании разделов технических заданий на создание систем безопасности значимых объектов критической информационной инфраструктуры</p> <p>Участие в определении правил и процедур защиты информации при выводе значимых объектов критической информационной инфраструктуры объектов информатизации из эксплуатации</p> <p>Анализ технической документации информационной инфраструктуры значимых объектов критической информационной инфраструктуры</p> <p>Работа с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами</p> <p>Эксплуатация системы безопасности значимого объекта КИИ</p> <p>Участие в восстановлении после сбоев и отказов программного обеспечения значимых объектов критической информационной инфраструктуры</p> <p>Подготовка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации</p> <p>Подготовка документов, определяющих правила и процедуры управления конфигурацией системой безопасности значимых объектов критической информационной инфраструктуры</p> <p>Подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в автоматизированной системе</p> <p>Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ</p> <p>Установка обновлений программного обеспечения значимых объектов критической информационной инфраструктуры</p> <p>Управление полномочиями пользователей значимых объектов критической информационной инфраструктуры</p> <p>Обнаружение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры</p> <p>Устранение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры</p> <p>Устранение инцидентов, возникших в процессе эксплуатации значимых объектов критической информационной инфраструктуры</p> <p>Осуществление автономной наладки технических и программных средств системы защиты информации значимых объектов критической информационной инфраструктуры;</p>
--	--

	<p>Участие в разработке организационных и технических мероприятий по защите объектов КИИ;</p> <p>Установка, настройка и применение современных средств защиты информации, обрабатываемой объектами КИИ;</p> <p>Работа с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами</p> <p>Эксплуатация системы безопасности значимого объекта КИИ</p> <p>Участие в восстановлении после сбоев и отказов программного обеспечения значимых объектов критической информационной инфраструктуры</p>
уметь	<p>выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;</p> <p>определять рациональные методы и средства защиты на объектах и оценивать их эффективность;</p> <p>производить установку и настройку типовых программно-аппаратных средств защиты информации;</p> <p>пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;</p> <p>применять нормативные правовые акты, определяющие требования к обеспечению информационной безопасности объекта критической информационной инфраструктуры, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;*</p> <p>определять информационную инфраструктуру и информационные ресурсы значимых объектов критической информационной инфраструктуры, подлежащие защите;*</p> <p>классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте);*</p> <p>определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта КИИ;*</p> <p>определять требования к параметрам настройки программных и программно-аппаратных средств, наличия средств защиты информации, обеспечивающих реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации;</p> <p>оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;*</p> <p>участвовать в выборе мер защиты информации, подлежащие реализации в системе защиты информации значимых объектов критической информационной инфраструктуры;*</p> <p>принимать участие в выборе программно-аппаратных средств защиты информации для использования их в составе значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов;*</p>

	<p>участвовать в определении комплекса мер для обеспечения безопасности информационной безопасности в значимых объектах критической информационной инфраструктуры;*</p> <p>выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации;*</p> <p>применять нормативные документы по противодействию технической разведке;*</p> <p>планировать политику безопасности программных компонентов значимых объектах критической информационной инфраструктуры;*</p> <p>участвовать в разработке политики безопасности информации значимых объектов критической информационной инфраструктуры;*</p> <p>конфигурировать параметры средств защиты информации и системы безопасности значимых объектов критической информационной инфраструктуры;*</p> <p>определять параметры настройки программного обеспечения системы защиты информации значимых объектов критической информационной инфраструктуры;*</p> <p>использовать криптографические методы и средства защиты информации в значимых объектах критической информационной инфраструктуры;*</p> <p>регистрировать события, связанные с защитой информации в значимых объектах критической информационной инфраструктуры;*</p> <p>анализировать события, связанные с защитой информации в значимых объектах критической информационной инфраструктуры;*</p> <p>использовать программные средства для архивирования информации;*</p> <p>использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации;*</p> <p>применять типовые программные средства резервирования и восстановления информации в значимых объектах критической информационной инфраструктуры;*</p> <p>применять средства обеспечения отказоустойчивости значимых объектов критической информационной инфраструктуры;*</p> <p>определять источники и причины возникновения инцидентов;*</p> <p>оценивать последствия выявленных инцидентов;*</p> <p>обнаруживать нарушения правил разграничения доступа;*</p> <p>устранять нарушения правил разграничения доступа*</p>
знать	<p>типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;</p> <p>основные протоколы идентификации и аутентификации в телекоммуникационных системах;</p> <p>состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;</p> <p>особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах;</p> <p>основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;</p>

	<p>основные понятия криптографии и типовые криптографические методы защиты информации;</p> <p>Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры</p> <p>Нормативные правовые акты в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.</p> <p>Основные методические и руководящие документы по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры</p> <p>Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности)</p> <p>Модель угроз информационной безопасности, модель нарушителя информационной безопасности на объекте информатизации</p> <p>Эксплуатационная и проектная документация на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование объекта информатизации</p> <p>Основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;</p> <p>Основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ;</p> <p>Принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования;</p> <p>Процедура категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ;</p> <p>Процедура подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий</p> <p>Основные принципы выявления наличия критических процессов у субъектов КИИ</p> <p>Основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;</p> <p>Общие требования по обеспечению безопасности значимых объектов КИИ;</p> <p>Общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования;</p> <p>Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ</p> <p>Основные угрозы безопасности информации и модели нарушителя в значимых объектах критической информационной инфраструктуры</p> <p>Регламент информирования персонала значимых объектов критической информационной инфраструктуры</p> <p>Регламент учета выявленных инцидентов</p> <p>Регламент устранения инцидентов</p>
--	--

	<p>Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в значимых объектах критической информационно-инфраструктуры</p> <p>Процедуры по архивированию информации, обрабатываемой на значимых объектах критической информационно-инфраструктуры</p> <p>Регламент значимых объектов критической информационно-инфраструктуры по уничтожению информации и машинных носителей информации</p> <p>Содержание и порядок деятельности персонала по эксплуатации защищенных значимых объектов критической информационно-инфраструктуры и систем безопасности значимых объектов критической информационно-инфраструктуры</p> <p>Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ;</p> <p>Цели, задачи, основные принципы организации государственного контроля в области обеспечения безопасности значимых объектов КИИ;</p> <p>Порядок обработки результатов контроля (проверки) состояния безопасности значимых объектов КИИ</p> <p>Критерии оценки защищенности значимых объектов критической информационно-инфраструктуры</p> <p>Технические средства контроля эффективности мер защиты информации</p> <p>Содержание и порядок деятельности персонала по эксплуатации защищенных значимых объектов критической информационно-инфраструктуры и систем безопасности значимых объектов критической информационно-инфраструктуры</p> <p>Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в значимых объектах критической информационно-инфраструктуры</p>
<p><i>ВД: Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты</i></p>	
иметь практический опыт	<p>установка, монтаж и настройка технических средств защиты информации;</p> <p>техническое обслуживание технических средств защиты информации;</p> <p>применение основных типов технических средств защиты информации;</p> <p>выявление технических каналов утечки информации;</p> <p>участие в мониторинге эффективности технических средств защиты информации;</p> <p>диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации;</p> <p>проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации;</p> <p>проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;</p> <p>установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты.</p>
уметь	<p>применять технические средства для криптографической защиты информации конфиденциального характера;</p> <p>применять технические средства для уничтожения информации и носителей информации;</p>

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

1.2. Количество часов, отводимое на освоение производственной практики (преддипломной)

Всего часов 144 часа - 4 недели, из них

на освоение ПМ.01 - 48

на освоение ПМ.02 - 48

на освоение ПМ.03 - 48

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДИДИПЛОМНОЙ)

Профессиональные модули и междисциплинарные курсы, коды профессиональных, общих компетенций	Виды работ	Объем часов
ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей		
МДК 01.01 Прием-передающие устройства, линейные сооружения связи и источники электропитания		
МДК 01.02 Телекоммуникационные системы и сети		
МДК 01.03 Электроизмерения и метрология		
ПК 1.1- 1.4	<ul style="list-style-type: none"> ➤ Ознакомление с целями и задачами практики. Инструктаж по технике безопасности и пожарной безопасности. Составление плана и графика работы на период практики, опираясь на индивидуальное задание производственной практики и учитывая специфику и режим работы организации – места прохождения практики. ➤ Знакомство с правилами внутреннего распорядка, рабочим местом и руководителем практики от предприятия (организации), вводный инструктаж по технике безопасности и охране труда. ➤ Анализ вида, структуры, функций организации. ➤ 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. ➤ Выполнение обязанностей стажера на закрепленном рабочем месте. ➤ Выполнение индивидуального задания по практике: <ul style="list-style-type: none"> ✓ производить монтаж кабельных линий и оконечных кабельных устройств ИТКС; ✓ проверять функционирование, производить регулировку и контроль основных параметров источников питания ИТКС; ✓ измерять основные показатели и характеристики при выполнении работ по настройке, проверке функционирования и конфигурирования ИТКС; ✓ осуществлять техническую эксплуатацию линейных сооружений связи; ✓ проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; 	48

	<ul style="list-style-type: none"> ✓ измерять основные параметры и характеристики при выполнении работ по диагностике технического состояния, поиска неисправностей и ремонте оборудования ИТКС; ✓ осуществлять техническую эксплуатацию линейных сооружений ИТКС; ✓ измерять основные параметры и характеристики при выполнении технического обслуживания оборудования ИТКС; ✓ производить контроль и регулировку основных параметров источников питания оборудования ИТКС; ✓ проводить мониторинг и контроль функционирования оборудования ИТКС; ✓ измерять основные параметры и характеристики оборудования ИТКС; ✓ вести эксплуатацию-техническую документацию на оборудование ИТКС ✚ Выполнение определенных видов работ и заданий в соответствии с темой дипломной работы (далее – ДР). ✚ Проведение анализа и обобщения научно-технической информации по теме дипломной работы. ✚ Подбор фактического материала по теме ДР с учетом профессионального модуля и его изучение. ✚ Подготовка плана пояснительной записки к ДР. ✚ Описание технико-экономической характеристики предметной области и объекта исследования. ✚ Анализ видов и категорий обрабатываемой в информационной (автоматизированной) системе информации. ✚ Определение требований по информационной безопасности. ✚ Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием 	
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		
ПК 2.1- 2.3	<ul style="list-style-type: none"> ✓ 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. 	48

	<ul style="list-style-type: none"> ✓ Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. ✓ Администрирование систем безопасности беспроводной защищенной локальной сети. ✓ 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. <p>Выбор программных средств шифрования в соответствии с решаемой задачей</p> <ul style="list-style-type: none"> ✓ Подключение, установка драйверов, настройка программных средств абонентского шифрования ✓ Администрирование внедренных средств ✓ Настройка средств электронной подписи ✓ Администрирование средств электронной подписи ✓ Администрирование средств РКИ ✓ 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 контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; ✓ Проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; ✓ Проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации; ✓ Проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации ✚ Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием. ✚ Подбор фактического материала по теме ДР с учетом профессионального модуля и его изучение
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	

ПК 3.1- 3.4	<ul style="list-style-type: none"> ✓ 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 ✓ 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 оборудованием ИТКС; ✓ Проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; ✓ 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. <p>✚ Сбор и изучение научно-практического материала по разделам ДР, 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 ДР.</p> <p>✚ Разработка состава технических и инженерно-технических средств для решения поставленной в ТЗ задачи.</p> <p>✚ Расчет параметров утечки информации.</p> <p>✚ Разработка схемы соединений.</p> <p>✚ Оформление пояснительной записки к выпускной квалификационной работе.</p>	48
Промежуточная аттестация в форме дифференцированного зачета		
Итого		144

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

3.1. Материально-техническое обеспечение

Производственная практика (преддипломная) проводится в организациях, осуществляющих деятельность по профилю соответствующей образовательной программы (далее – профильная организация), имеющих базу для освоения профессиональных компетенций, в том числе в структурном подразделении профильной организации, предназначенном для проведения практики. Практика может быть организована в Финансовом университете, в том числе в колледже.

При организации производственной практики (преддипломной) профильные организации - индустриальные партнеры создают условия для реализации профильных компонентов образовательной программы в форме практической подготовки, предоставляют оборудование и технические средства обучения в объеме, позволяющем выполнять определенные виды работ, связанных с будущей профессиональной деятельностью студентов.

3.2. Техника безопасности

В течение всего периода практики на обучающихся распространяются требования по соблюдению правил противопожарной безопасности, правил охраны труда, техники безопасности и санитарно-эпидемиологических правил и гигиенических нормативов, правил внутреннего распорядка принимающей профильной организации.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Контроль и оценка результатов практики осуществляются с использованием следующих форм и методов: наблюдение за деятельностью студента на производственной практике (преддипломной), анализ документов, подтверждающих выполнение им соответствующих работ (отчёт о практике, отзыв о прохождении практики, индивидуальное задание, дневник практики). В результате прохождения производственной практики (преддипломной) в рамках профессиональных модулей студенты проходят промежуточную аттестацию в форме дифференцированного зачёта.

Результаты обучения (освоенные умения, практический опыт в рамках вида деятельности)	Формы и методы контроля и оценки
ВД: Эксплуатация информационно-телекоммуникационных систем и сетей	
<p>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</p> <p>освоенные умения:</p> <ul style="list-style-type: none"> - 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 приемопередающих 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; 	<p>Наблюдение за деятельностью студента, анализ документов (отчёт о практике, отзыв о прохождении практики, индивидуальное задание, дневник практики), подтверждающих выполнение им соответствующих работ, защита отчета по практике на дифференцированном зачете промежуточной аттестации</p>

<ul style="list-style-type: none"> - 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; 	
ВД: Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты	
<p>практический опыт:</p> <ul style="list-style-type: none"> - 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; <p>освоенные умения:</p> <ul style="list-style-type: none"> - 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 	<p>Наблюдение за деятельностью студента, анализ документов (отчёт о практике, отзыв о прохождении практики, индивидуальное задание, дневник практики), подтверждающих выполнение им соответствующих работ, защита отчета по практике на дифференцированном зачете промежуточной аттестации</p>
ВД: Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	
<p>практический опыт:</p> <ul style="list-style-type: none"> 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; 	<p>Наблюдение за деятельностью студента, анализ документов (отчёт о практике, отзыв о прохождении практики, индивидуальное задание, дневник практики), подтверждающих выполнение им соответствующих работ,</p>

<p>диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации;</p> <p>проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации;</p> <p>проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;</p> <p>установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты.</p> <p>освоенные умения:</p> <p>применять технические средства для криптографической защиты информации конфиденциального характера;</p> <p>применять технические средства для уничтожения информации и носителей информации;</p> <p>применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;</p> <p>применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;</p> <p>применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;</p> <p>применять инженерно-технические средства физической защиты объектов информатизации</p>	<p>защита отчета по практике на дифференцированном зачете промежуточной аттестации</p>
--	--

Формы и виды отчетных документов по практике устанавливаются Регламентом организации и проведения практической подготовки студентов, обучающихся по образовательным программам среднего профессионального образования – программам подготовки специалистов среднего звена в Финансовом университете, утвержденным приказом Финансового университета.

Требования к отчету по производственной практике (преддипломной) устанавливаются «Методическими рекомендациями по составлению и оформлению отчетной документации по видам практики», рассмотренными и одобренными Методическим советом Колледжа информатики и программирования.

Требования к оценке сформированности профессиональных компетенций по производственной практике (преддипломной) устанавливаются ФОСом (фондом оценочных средств), принятым предметной (цикловой) комиссией, используемом при проведении дифференцируемого зачета по преддипломной практике.