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

СОГЛАСОВАНО

АО «ОКБ САПР»
Генеральный директор

_____ И.Г. Назаров
«_15_» _____07_____2024 г.

УТВЕРЖДАЮ

Заместитель директора
по учебно-практической работе и
стратегическому развитию

_____О.М. Сумлинова
«_17_» _____июня_____ 2024 г.

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Москва 2024 г.

Рабочая программа производственной практики (преддипломной) разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 г. № 1553 (зарегистрирован в Министерстве юстиции Российской федерации 26 декабря 2016 г. № 44938).

Организации – партнеры: 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»), ПАО «Ростелеком»; 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", ООО «НКО ЮМани», Минфин России. Научно-исследовательский финансовый институт

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 ХАРАКТЕРСИТИКА 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
Вид деятельности	*Эксплуатация автоматизированных (информационных) систем в защищенном исполнении*
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.
Вид деятельности	*Защита информации в автоматизированных системах программными и программно-аппаратными средствами*
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
Вид деятельности	*Защита информации техническими средствами:*
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

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

ВД: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

иметь практический опыт	– установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; – администрирования автоматизированных систем в защищенном исполнении, *контроля стабильности характеристик системы защиты информации**; – эксплуатации компонентов систем защиты информации автоматизированных систем; - диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении, *контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации*;* – *администрирования автоматизированных систем в защищенном на значимых объектах критической информационной инфраструктуры;** – *установки и настройки операционных систем семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности*;* – *обнаружения и устранения ошибок при передаче данных в компьютерных сетях*;* – *работы с протоколами разных уровней*.* – *разработка организационно-распорядительных документов по безопасности значимых объектов КИИ** – *установка обновлений программного обеспечения значимых объектов критической информационной инфраструктуры** – *управление полномочиями пользователей значимых объектов критической информационной инфраструктуры**
уметь	– осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем*;* – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности – *обеспечивать проверку функционирования встроенных средств защиты информации и своевременное обнаружение признаков наличия вредоносного программного обеспечения**; *– устанавливать, конфигурировать и контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами**; – *формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;** – *проверять правильность передачи данных.**

	*– создавать, удалять и изменять учетные записи пользователей значимых объектов критической информационной инфраструктуры** *– конфигурировать параметры средств защиты информации и системы безопасности значимых объектов критической информационной инфраструктуры**
знать	– состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных, *порядок настройки систем управления базами данных и средств электронного документооборота**; – принципы построения, физические основы работы периферийных устройств; – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях, *порядок обеспечения безопасности информации при эксплуатации компьютерных сетей*;* – принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; *– типовые уязвимости программного обеспечения, методы их эксплуатации и порядок обеспечения безопасности информации при эксплуатации программного обеспечения*;* *– особенности источников угроз, связанных с эксплуатацией программного обеспечения*;* *– эксплуатационную и проектную документацию, регламенты по уничтожению информации и машинных носителей информации автоматизированной системы*;* *– принципы построения и функционирования, примеры реализаций современных операционных систем;** *– программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах;** *– адресацию в сетях, организацию межсетового взаимодействия;**
Вид деятельности: Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
иметь практический опыт	– установки, настройки программных средств защиты информации в автоматизированной системе; – обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – - использование программных и программно-аппаратных средств для защиты информационной сети; – тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; – решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

	– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; – учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности, *информирование персонала об угрозах безопасности информации*;* – работы с подсистемами регистрации событий; – выявления событий и инцидентов безопасности в автоматизированной системе; – *применения технологии фильтрации различных видов трафика*; * – *осуществлять фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.**
уметь	– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации, *проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;* – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; – применять программные и программно-аппаратные средства для защиты информации в базах данных; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись; – применять средства гарантированного уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; *- оформлять эксплуатационную документацию программно-аппаратных средств защиты информации;** *- определять цели и задачи в изучении проекта;** *-разрабатывать политику информационной безопасности на основе самостоятельной классификации объектов защиты;*

	– *осуществлять установку, развёртывание, настройку и использованием DLP-систем.**
знать	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе в операционных системах, компьютерных сетях, базах данных; – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе в операционных системах, компьютерных сетях, базах данных; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации, *общие принципы функционирования средств защиты информации, в том числе и криптографической защиты информации**; – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа. – *теоретические основы корпоративной защиты информации от внутренних ИТ-угроз;** – *методику проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его; современные стандарты и средства корпоративной защиты.* *
Вид деятельности: Защита информации техническими средствами	
иметь практический опыт	– установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения 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;

	– проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – выявления технических каналов утечки информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты; – *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок;* * – *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам.**
уметь	– применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – 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 средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом, *технических средств защиты акустической речевой информации от утечки по техническим каналам**; – применять инженерно-технические средства физической защиты объектов информатизации, – *производить установку и монтаж, настройку и испытание, техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов .**
знать	– порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и 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;

	– структуру и условия формирования технических каналов утечки информации; – основные принципы действия и характеристики технических средств физической защиты; – номенклатуру применяемых средств физической защиты объектов информатизации; – основные способы физической защиты объектов информатизации; – *порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации** ; – *нормативно правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации **; – *номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.** .

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 (ПРЕДДИПЛОМНОЙ)

Профессиональные модули и междисциплинарные курсы, коды профессиональных, общих компетенций	Виды работ	Объем часов
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		
МДК 01.01 Операционные системы МДК 01.02 Базы данных МДК 01.03 Сети и системы передачи информации МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении МДК 01.05 Эксплуатация компьютерных сетей		
ПК 1.1- 1.4	– 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). – Анализ вида, структуры, функций организации. – Выполнение обязанностей стажера в соответствии с профилем специальности (изучение методов и средств обеспечения информационной безопасности и защиты информации предприятия; проведение анализа основных информационных угроз; ознакомление с нормативно-правовым обеспечением информационной безопасности, в том числе с политикой информационной безопасности, положением, регламентами, стандартами, которые используются в организации, рассматриваемой в ходе прохождения практики; составление таблиц с описанием активов, угроз и рисков информационной безопасности, комментарии к таблицам; разработка базовой программной и технической архитектуры и формулирование предложений по их модернизации; анализ деятельности предприятия, определение методов и средств повышения эффективности обработки и защиты информации; обобщение полученной информации, формулирование приобретенных и закрепленных навыков). – - Выполнение определенных видов работ и заданий в соответствии с темой дипломной работы (далее – ДР).	48

	– - 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 автоматизированных системах программными и программно-аппаратными средствами		
МДК 02.01 Программные и программно-аппаратные средства защиты информации **МДК 02.02** Криптографические средства защиты информации **МДК 02.03** Корпоративная защита от внутренних угроз информационной безопасности		
ПК 2.1- 2.6	– Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ДР. – Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием. – Подбор фактического материала по теме ДР с учетом профессионального модуля и его изучение – Характеристика проектируемым для решения задач средствам обеспечения информационной безопасности и защиты информации. – Анализ наиболее значимых угроз и типовые методы противодействия им. – Защита от внутренних угроз (разработка внутренней политики безопасности, разграничение доступа к информации и тд.) – Анализ существующих программных и программно-аппаратных средств для решения поставленной в ДР задачи. – Разработка программно-аппаратного комплекса решения задачи.	48
ПМ.03 Защита информации техническими средствами		
МДК 03.01 Техническая защита информации **МДК 03.02** Инженерно-технические средства физической защиты объектов информатизации		
ПК 3.1- 3.5	– Сбор и изучение научно-практического материала по разделам ДР, подбор фактического материала на базе организации, развитие практических навыков и компетенции в процессе	40

	выполнения определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой ДР. – Разработка состава технических и инженерно-технических средств для решения поставленной в ТЗ задачи. – Расчет параметров утечки информации. – Разработка схемы соединений. – Оформление пояснительной записки к выпускной квалификационной работе.	
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 рамах вида деятельности)	**Формы и методы контроля и оценки**
Вид деятельности: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	
практический опыт: – установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; – администрирования автоматизированных систем в защищенном исполнении, *контроля стабильности характеристик системы защиты информации**; – эксплуатации компонентов систем защиты информации автоматизированных систем; – диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении, *контроля соответствия конфигурации системы защиты информации ее эксплуатационной документации**; – *администрирования автоматизированных систем в защищенном на значимых объектах критической информационной инфраструктуры;** – *установки и настройки операционных систем семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности**; – *обнаружения и устранения ошибок при передаче данных в компьютерных сетях**; – *работы с протоколами разных уровней**. – *разработка организационно-распорядительных документов по безопасности значимых объектов КИИ** – *установка обновлений программного обеспечения значимых объектов критической информационной инфраструктуры** *управление полномочиями пользователей значимых объектов критической ин-формационной инфраструктуры** **освоенные умения:**	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

- осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности *– обеспечивать проверку функционирования встроенных средств защиты информации и своевременное обнаружение признаков наличия вредоносного программного обеспечения**; *– устанавливать, конфигурировать и контролировать корректность настройки межсетевых экранов в соответствии с заданными правилами**; *– формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;** *– – проверять правильность передачи данных.** *– создавать, удалять и изменять учетные записи пользователей значимых объектов критической информационной инфраструктуры** *– конфигурировать параметры средств защиты информации и системы безопасности значимых объектов критической информационной инфраструктуры**	
Вид деятельности: Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
практический опыт: – установки, настройки программных средств защиты информации в автоматизированной системе; – обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; – решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;	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

– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; – учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности, *информирование персонала об угрозах безопасности информации*;* – работы с подсистемами регистрации событий; – выявления событий и инцидентов безопасности в автоматизированной системе; – *применения технологии фильтрации различных видов трафика*; * – *осуществлять фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.** **освоенные умения:** – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации, *проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах;* – применять программные и программно-аппаратные средства для защиты информации в базах данных; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись; – применять средства гарантированного уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных	зачете промежуточной аттестации

средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; *- оформлять эксплуатационную документацию программно аппаратных средств защиты информации;** *- определять цели и задачи в изучении проекта;** *-разрабатывать политику информационной безопасности на основе самостоятельной классификации объектов защиты;* *- осуществлять установку, развёртывание, настройку и использованием DLP-систем.**	
Вид деятельности: Защита информации техническими средствами	
практический опыт: – установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения 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; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты; – *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок;* * – *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам.** **освоенные умения:** – применять технические средства для криптографической защиты информации конфиденциального характера;	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

– 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, *технических средств защиты акустической речевой информации от утечки по техническим каналам*;* – применять инженерно-технические средства физической защиты объектов информатизации, – *производить установку и монтаж, настройку и испытание, техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов .**	

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.