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
«_30_» _июня_____2022г.

РАБОЧАЯ ПРОГРАММА ПРЕДДИПЛОМНОЙ ПРАКТИКИ

по специальности среднего профессионального образования
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Москва 2022 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРСИТИКА РАБОЧЕЙ ПРОГРАММЫ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

1.1. Цель и планируемые результаты освоения программы практики преддипломной

- 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 выпускной квалификационной 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
ПМ. 01	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.
ПМ.02	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.
ПМ.03	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. Перечень личностных результатов

Код	Личностные результаты реализации программы воспитания
ЛР1	Осознающий себя гражданином и защитником великой страны
ЛР3	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
ЛР4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР7	Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
ЛР10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
ЛР13	Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности
ЛР14	Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности

ЛР15	Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем
ЛР16	Соответствующий ожиданиям работодателей: креативно мыслящий, эффективно сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, распределяющий время и другие ресурсы для выполнения поставленной задачи в установленный срок, ответственный, дисциплинированный, целеустремленный, стрессоустойчивый.
ЛР17	Демонстрирующий культуру речи, в том числе в деловой переписке/переговорах, способный презентовать себя и продукт профессиональной деятельности
ЛР18	Демонстрирующий способность использовать в цифровой среде различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве.

1.1.4. В результате прохождения преддипломной практики по видам профессиональной деятельности, обучающийся должен:

Вид деятельности: 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 исполнении информационной системы 1С: Предприятие;** *– 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*.*
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;** *– создавать, редактировать и обслуживать автоматизированную систему управления предприятием на базе «1С: Предприятие»;** *– проверять правильность передачи данных.**
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;** – *основные этапы разработки простого прикладного решения в системе «1С:Предприятие»**
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; – 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;* – 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; – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – 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; – 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 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, *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; – 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 преддипломной практики

Всего часов 144 часа - 4 недели.

2.СТРУКТУРА И СОДЕРЖАНИЕ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

2.2. Структура преддипломной практики

Коды профессиональных и общих компетенций, личностных результатов	Код и наименование профессиональных модулей	Виды работ	Наименование тем практики	Количество часов
1	2	3	4	5
ОК.01 - ОК.11 ПК 1.1- 1.4, ЛР1, ЛР4, ЛР7, ЛР10, ЛР13-ЛР18	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Выполнение определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой ВКР Проведение анализа и обобщения научно-технической информации по теме ВКР Подбор фактического материала по теме ВКР с учетом профессиональных модулей и его изучение Подготовка плана пояснительной записки к ВКР 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	– Установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем; – Администрирование автоматизированных систем в защищенном исполнении, *контроля стабильности характеристик системы защиты информации**; – Эксплуатация компонентов систем защиты информации автоматизированных систем; – Диагностика компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении, *контроля соответствия*	144

		задачи дипломного проектирования в соответствии с техническим заданием	*конфигурации системы защиты информации ее эксплуатационной документации*;* *– Администрирование информационной системы 1С: Предприятие;** *– Установка и настройка операционных систем семейств Windows и UNIX с учетом требований по обеспечению информационной безопасности*;* *– Обнаружение и устранение ошибок при передаче данных в компьютерных сетях*;* *– Работа с протоколами разных уровней*.*	
ОК.1 - ОК.11 ПК 2.1- 2.6, ЛР1, ЛР4, ЛР7, ЛР10, ЛР13-ЛР18	ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Выполнение определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой ВКР Проведение анализа и обобщения научно-технической информации по теме ВКР Подбор фактического материала по теме ВКР с учетом профессиональных модулей и его изучение Характеристика проектируемым для решения задач средствам обеспечения информационной	– Установка, настройка программных средств защиты информации в автоматизированной системе; – Обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – Тестирование функций, диагностика, устранения отказов и восстановления работоспособности	

		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 ВКР задачи. Разработка программно-аппаратного комплекса решения задачи.	программных и программно-аппаратных средств защиты информации; – Решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; – Применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; – Учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности, *информирование персонала об угрозах безопасности информации*;* – Работа с подсистемами регистрации событий; – Выявление событий и инцидентов безопасности в автоматизированной системе; – *Применение технологии фильтрации различных видов трафика; ** – *Осуществление фильтрации 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.**	
ОК.1 - ОК.11 ПК 3.1- 3.5, ЛР1, ЛР4, ЛР7, ЛР10, ЛР13-ЛР18	ПМ.03 Защита информации техническими средствами	Выполнение определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой ВКР Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР. 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.	– 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, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – 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; – *Техническое обслуживание, диагностика, устранение отказов и неисправностей технических средств защиты информации за счет побочных*	

			*электромагнитных излучений и наводок; ** – *Техническое обслуживание, диагностика, устранение отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам.**	

2.3.
2.2. Тематический план и содержание преддипломной практики

Профессиональные модули и междисциплинарные курсы, темы	Содержание практики	Объём часов
1	2	3
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Прохождение инструктажа по технике безопасности. Ознакомление с Политикой информационной безопасности. Ознакомление с организационной структурой. Ознакомление с должностными инструкциями. Изучение методов и средств обеспечения информационной безопасности и защиты информации. 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	144
МДК 01.01 Операционные системы		
Тема 1. Элементы теории операционных систем. Свойства операционных систем		
Тема 2. Безопасность операционных систем		
Тема 3. Особенности работы в современных операционных системах		
Тема 4. Защита в операционных системах		
МДК 01.02 Базы данных		
Тема 1. Основы теории баз данных		
Тема 2. Проектирование баз данных		
Тема 3. Организация баз данных		
Тема 4. Управление базой данных с помощью SQL		
Тема 5. Организация распределённых баз данных		

Тема 6 Администрирование и безопасность	Разработка базовой программной и технической архитектуры и формулирование предложений по их модернизации. Анализ деятельности предприятия/подразделения, определение методов и средств повышения эффективности обработки и защиты информации. Обобщение полученной информации, формулирование приобретенных и закрепленных навыков. Подготовка отчета.	
МДК 01.03 Сети и системы передачи информации		
Тема 1. Теория телекоммуникационных сетей		
Тема 2. Сети передачи данных		
Тема 3. Серверное оборудование и программное обеспечение		
МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		
Тема 1. Разработка защищенных автоматизированных (информационных) систем		
Тема 2. Разработка защищенной автоматизированной системы на примере 1С. Предприятие.*		
Тема 3. Эксплуатация защищенных (автоматизированных) систем		
МДК 01.05 Эксплуатация компьютерных сетей		
Тема 1. Основы передачи данных в компьютерных сетях		
Тема 2. Технологии коммутации и маршрутизации современных сетей Ethernet		
Тема 3. Межсетевые экраны		
ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Сбор и изучение научно-практического материала по разделам ВКР, 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 ВКР. Проведение анализа и обобщения научно-технической информации по теме ВКР. Подбор фактического материала по теме ВКР с учетом профессиональных модулей и его изучение. Подготовка плана пояснительной записки к ВКР.	
МДК 02.01 Программные и программно-аппаратные средства обеспечения информационной безопасности		
Тема 1. Основные принципы программной и программно-аппаратной защиты информации Защита автономных автоматизированных систем		
Тема 2. Защита автономных автоматизированных систем		
Тема 3. Защита информации в локальных сетях		

Тема 4. Защита информации в сетях общего доступа	Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР. Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием.	
Тема 5. Защита информации в базах данных		
Тема 6. Мониторинг систем защиты		
МДК 02.02 Криптографические средства и методы защиты информации		
Тема 1. Математические основы защиты информации		
Тема 2. Классическая криптография		
Тема 3. Современная криптография		
МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности		
Тема 1. Защита корпоративной информации с использованием автоматизированных систем контроля информационных потоков		
ПМ. 03 Защита информации техническими средствами	Сбор и изучение научно-практического материала по разделам ВКР, 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 ВКР. Проведение анализа и обобщения научно-технической информации по теме ВКР. Подбор фактического материала по теме ВКР с учетом профессиональных модулей и его изучение. Подготовка плана пояснительной записки к ВКР. Подбор программных, аппаратных и/или инженерно-технических средств для реализации практической части ВКР. Описание входных параметров задачи дипломного проектирования в соответствии с техническим заданием.	
МДК 03.01 Техническая защита информации		
Тема 1. Концепция инженерно-технической защиты информации		
Тема 2. Теоретические основы инженерно-технической защиты информации Физические основы технической защиты информации		
Тема 3. Физические основы технической защиты информации		
Тема 4. Системы защиты от утечки информации		
Тема 3. Применение и эксплуатация технических средств защиты информации		
МДК 03.02 Инженерно-технические средства физической защиты информации		
Тема 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 3. Применение и эксплуатация инженерно-технических средств физической защиты		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

3.1. Материально-техническое обеспечение

Преддипломная практика проходит в организациях, с которыми заключены договоры о проведении практики.

1. Федеральная служба государственной статистики по г. Москве (Мосгорстат), Договор № 01/2012 от 03.09.2012;
2. ФГУП «НПП «Пульсар», Договор № ДИР/4740 от 01.07.2014;
3. ФГБУ «Транспортный комбинат «Россия» Управления делами Президента, Договор № 01/2015 от 15.06.2015;
4. ЗАО «Научно-производственный центр информационных региональных систем», Договор № 3/2015 от 25.10.2015;
5. ООО Самсунг Электроникс, Договор №и 4/2015 от 28.10.2015;
6. ООО «ЦЛОТ «Здоровье», Договор №6/2015 от 01.11.2015;
7. ФБУ Российский федеральный центр судебной экспертизы при Министерстве юстиции РФ, Договор № 02/2015 от 08.09.2015;
8. Аппарат Совета депутатов муниципального округа «Аэропорт», Договор №76-СР/2016 от 30.12.2016;
9. ООО «Дело Системы», Договор № 01/КИП-18/67а-СР/2018 от 09.01.2018;
10. ООО «Такском», Договор №02/2013 от 09.04.2013;
11. По гарантийным письмам и договорам о проведении практики обучающимся от предприятий.
12. ЗАО «Научно-производственный центр информационных региональных систем»

Для прохождения преддипломной практики организациями предоставляются автоматизированные рабочие места с необходимым оборудованием и программным обеспечением.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения преддипломной практики осуществляются с использованием следующих форм и методов: наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист, характеристика учебной и профессиональной деятельности студента, дневник прохождения практики). В результате освоения преддипломной практики 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 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 исполнении информационной системы 1С: Предприятие;** *– 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*.* **Уметь:** - осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем;	Наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист, характеристика учебной и профессиональной деятельности студента, дневник прохождения практики)

– 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;** – *создавать, редактировать и обслуживать автоматизированную систему управления предприятием на базе «1С: Предприятие»;** – *проверять правильность передачи данных.**	
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; – 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;	Наблюдение за деятельностью студента, анализ документов, подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист, характеристика учебной и профессиональной деятельности студента, дневник прохождения практики)

– 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;* – 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.**	
Вид деятельности: Защита информации техническими средствами	
Иметь практический опыт: – установки, монтажа и настройки технических средств защиты информации;	Наблюдение за деятельностью студента, анализ документов,

– 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.** **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, *технических средств защиты акустической речевой информации от утечки по техническим каналам*;* – применять инженерно-технические средства физической защиты объектов информатизации,	подтверждающих выполнение им соответствующих работ (отчёт по практике, аттестационный лист, характеристика учебной и профессиональной деятельности студента, дневник прохождения практики)

– *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 .**	