

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

**ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ**  
по производственной практике (преддипломной)

обучающегося 4 курса \_\_\_\_\_ учебной группы

(фамилия, имя, отчество)

Специальность 10.02.05 «Обеспечение информационной безопасности  
автоматизированных систем»

Место прохождения практики Колледж информатики и программирования  
ФГОБУ ВО «Финансовый университет при Правительстве РФ»

Срок практики с «20» апреля 2023 г. по «17» мая 2023 г.

Наименование профессионального модуля	Содержание индивидуального задания и планируемые результаты (освоенные умения (практический опыт))
ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.	<p><u>Цель преддипломной практики:</u> сбор и изучение научно-практического материала по разделам дипломной работы, подбор фактического материала на базе организации, развитие практических навыков и компетенции в процессе выполнения определенных видов работ и заданий, связанных с будущей профессиональной деятельностью в соответствии с темой дипломной работы.</p> <p><u>Задачи преддипломной практики:</u></p> <ul style="list-style-type: none"><li>– проведение анализа и обобщения научно-технической информации по теме дипломной работы;</li><li>– подбор фактического материала по теме дипломной работы с учетом профессиональных модулей и его изучение;</li><li>– описание организационных (административных) мероприятий, включающее в себя: анализ действующей нормативной базы; разработанные нормативные документы, регламентирующие проведение организационных мероприятий;</li><li>– описание мероприятий инженерно-технической и программно-аппаратной защиты, включающее в себя: анализ существующих разработок (программных, аппаратных, физических средств защиты информации), используемых при практической реализации выбранных защитных мер; выбор конкретных разработок для реализации задачи дипломного проектирования; контрольный пример реализации;</li><li>– оформление и сдача отчета по преддипломной практике.</li></ul> <p><u>Вопросы, подлежащие изучению:</u></p> <ul style="list-style-type: none"><li>– литературные источники по разрабатываемой теме дипломной работы целью их использования при ее выполнении;</li><li>– методы исследования и проведения работ, анализа и обработки данных;</li></ul>
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	
ПМ.03 Защита информации техническими средствами	
ПМ.05 Противодействие отмыванию денег и финансированию терроризма (ПОД/ФТ)	

- информационные технологии и технические средства и программные продукты, относящиеся к профессиональной сфере;
- критерии выбора, сравнения и оценки эффективности решений по защите информации.
- требования к оформлению научно-технической документации;

Структура отчета по преддипломной практике:

Титульный лист

Содержание

Введение: описание актуальности выбора темы дипломной работы, объекта исследования (название предприятия, история развития предприятия, краткое описание организации, виды выпускаемой продукции (работ, услуг), положение, занимаемое предприятием в отрасли и т.д.), предмета исследования, цели и задачи дипломной работы.

Общая часть:

**1.1. Характеристика комплекса задач, задачи и обоснование необходимости совершенствования системы обеспечения информационной безопасности и защиты информации на предприятии.**

1.1.1. Выбор комплекса задач обеспечения информационной безопасности и защиты информации исходя из выполняемых предприятием задач и существующих рисков, характеристика существующих средств информационной безопасности.

1.1.2. Определение места проектируемого комплекса задач в комплексе задач предприятия, детализация задач информационной безопасности и защиты информации.

**1.2. Выбор защитных мер**

1.2.1. Выбор организационных мер

1.2.2. Выбор инженерно-технических мер

1.2.3. Выбор программных и программно- аппаратных средств

**2.1 Комплекс организационных мер обеспечения информационной безопасности и защиты информации**

2.1.1 Правовое обеспечение системы информационной безопасности и защиты информации.

2.1.2 Организационное обеспечение системы информационной безопасности и защиты информации. Политика информационной безопасности.

2.1.3 Стратегия обеспечения информационной безопасности и защиты информации.

**2.2 Техническое обеспечение информационной безопасности и защиты информации**

2.2.1 Анализ технических средств обеспечения информационной безопасности и защиты информации.

2.2.2. Обоснование выбора технических средств обеспечения информационной безопасности и защиты информации.

2.2.3 Технология установки или замены технических средств обеспечения информационной безопасности и защиты информации.

**2.3 Программное обеспечение информационной безопасности и защиты информации**

2.3.1 Анализ программных средств обеспечения информационной безопасности и защиты информации.

2.3.2 Обоснование выбора программных средств обеспечения информационной безопасности и защиты информации.

2.3.3 Технология установки или замены программных средств обеспечения информационной безопасности и защиты информации.

**2.4. Внедрение и оценка комплекса программно-аппаратных средств**

**обеспечения информационной безопасности.**

2.4.1 Программно-аппаратный комплекс информационной безопасности и защиты информации предприятия.

2.4.2 Внутренний аудит системы информационной безопасности и защиты информации.

2.4.3 Анализ результатов внутреннего аудита.

Заключение: ~~заключительные~~ выводы, ~~предложения~~ и ~~рекомендации~~,

Руководитель практики от колледжа:

\_\_\_\_\_

(подпись)

\_\_\_\_\_

(И.О. Фамилия)

Задание принял обучающийся:

\_\_\_\_\_

(подпись)

\_\_\_\_\_

(И.О. Фамилия)

СОГЛАСОВАНО

Руководитель практики от организации:

\_\_\_\_\_

(подпись)

\_\_\_\_\_

(И.О. Фамилия)