Негосударственное аккредитованное некоммерческое
частное образовательное учреждение высшего образования
«АКАДЕМИЯ МАРКЕТИНГА И СОЦИАЛЬНО-ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ – ИМСИТ»
(г. Краснодар)

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ИННОВАЦИЙ

Кафедра математики и вычислительной техники

Рассмотрено и одобрено на заседании кафедры математики и вычислительной техники Академии ИМСИТ, протокол №3 от 13.10 2023 г
Зав. кафедрой доцент Исикова Н.П

УТВЕРЖДАЮ
Проректор по учебной работе, доцент
_____ Н.И. Севрюгина
2023г.

Б2.О.05(П)

Производственная практика: Преддипломная практика

АННОТАЦИЯ
для обучающихся направления
10.03.01 Информационная безопасность

Направленность «Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)»

квалификация (степень) выпускника

«Бакалавр»

Краснодар
2023

Цель и задачи изучения дисциплины:	Практика обеспечивает соответствие уровня теоретической подготовки практической направленности в системе обучения и будущей деятельности выпускника. Цель практики: – закрепление, расширение, углубление и систематизация знаний, полученных при изучении обязательных дисциплин базовой части учебного плана; – освоение современных технологий и технических средств, применяемых в области информационной безопасности; – совершенствование навыков подготовки, представления и защиты информационных, проектных, аналитических, руководящих и отчетных документов по результатам профессиональной деятельности и практики; – обеспечение возможности применения студентами теоретических знаний для решения практических задач; – развитие организаторских способностей и развитие исполнительских и лидерских навыков обучающихся; – формирование и развитие практических навыков в профессиональной сфере использования технологий и технических средств, применяемых в области информационной безопасности; – развитие у обучающихся компетенций, а также формирования опыта самостоятельной исследовательской и аналитической деятельности в изучении практического материала; – формирование общего представления студентов о будущей профессиональной деятельности и развитие интереса к профессии.
Место дисциплины в структуре ОПОП	Производственная практика: преддипломная относится к обязательной части Блока 2 образовательной программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность
Краткая характеристика учебной дисциплины (основные блоки, темы)	**Содержание практики:** **Подготовительный этап** Установочная конференция: цели и задачи учебной практики; инструктаж по технике безопасности; получение задания на практику (в том числе – индивидуальные варианты); требования к оформлению документов (отчет, дневник и пр.) **Содержательный этап** Выполнение практических работ Выполнение индивидуального задания **Отчетный этап** Подготовка и оформление отчета по практике
Компетенции,	УК-1: Способен осуществлять поиск, критический анализ

формируемые в результате освоения учебной дисциплины:	и синтез информации, применять системный подход для решения поставленных задач; ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности; ОПК-3: Способен использовать необходимые математические методы для решения задач профессиональной деятельности; ОПК-4: Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности; ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности; ОПК-6: Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; ОПК-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности; ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности; ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты; ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; ОПК-4.1: Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах; ОПК-4.2: Способен администрировать операционные системы, системы управления базами данных, вычислительные сети; ОПК-4.3: Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе

	криптографических) и технических средств защиты информации автоматизированных систем; ОПК-4.4: Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем; ПК-1: Способен эксплуатировать средства обеспечения информационной безопасности автоматизированных систем; ПК-2: Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности; ПК-3: Способен обеспечивать безопасную обработку данных в автоматизированных системах; ПК-4: Способен выполнять работы по проектированию автоматизированных систем в защищенном исполнении; ПК-5: Способен выполнять работы по обеспечению информационной безопасности автоматизированных систем на всех этапах их жизненного цикла; ПК-6: Способен документально оформлять работы по обеспечению информационной безопасности; ПК-7: Способен определять уровень защищённости автоматизированных систем; ПК-8: Способен выполнять задачи по выявлению уязвимых узлов автоматизированной системы; ПК-9: Способен организовывать работы по обеспечению информационной безопасности в автоматизированных системах; ПК-10: Способен собирать, анализировать и систематизировать информацию по зафиксированным инцидентам информационной безопасности.
Знания, умения и навыки, получаемые в процессе изучения дисциплины:	УК-1.1: Анализирует задачу, выделяя ее базовые составляющие УК-1.2: Определяет и ранжирует информацию, требуемую для решения поставленной задачи УК-1.3: Осуществляет поиск информации для решения поставленной задачи по различным типам запросов ОПК-2.1: Ищет информацию в глобальной информационной сети Интернет ОПК-2.2: Подготавливает документы в среде типовых офисных пакетов ОПК-2.3: Определяет состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств ОПК-2.4: Применяет технические и программные средств тестирования с целью определения исправности компьютера и оценки его производительности ОПК-3.1: Использует методы аналитической геометрии и векторной алгебры при решении прикладных задач ОПК-3.2: Использует типовые модели и методы математического анализа при решении стандартных прикладных задач ОПК-3.3: Выполняет типовые расчеты с использованием

	основных формул дифференциального и интегрального исчисления ОПК-3.4: Использует расчетные формулы и таблицы при решении стандартных вероятностно-статистических задач ОПК-3.5: Решает задачи профессиональной области с применением дискретных моделей ОПК-4.1: Решает базовые прикладные физические задачи ОПК-4.2: Анализирует электрические цепи в переходных и установившихся режимах в частотной и временной областях ОПК-4.3: Анализирует процессы, протекающие в линейных и нелинейных электрических цепях ОПК-5.1: Разрабатывает проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации ОПК-5.2: Формулирует основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации ОПК-5.3: Формулирует основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации ОПК-6.1: Разрабатывает модели угроз и модели нарушителя объекта информатизации ОПК-6.2: Определяет политику контроля доступа работников к информации ограниченного доступа ОПК-6.3: Формулирует требования, предъявляемые к физической защите объекта и пропускному режиму в организации ОПК-6.4: Разрабатывает проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ОПК-8.1: Составляет рефераты по результатам обзора научно-технической литературы, нормативных и методических документов ОПК-8.2: Систематизирует научную информацию в области информационной безопасности ОПК-8.3: Использует информационно-справочные системы при поиске информации в области профессиональной деятельности ОПК-9.1: Использует средства криптографической защиты информации в автоматизированных системах ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов

	ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации ОПК-9.5: Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации ОПК-10.1: Реализует требования политик безопасности на объектах информатизации ОПК-10.2: Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности ОПК-10.3: Применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях ОПК-12.1: Определяет информационную инфраструктуру и информационные ресурсы организации, подлежащие защите ОПК-12.2: Анализирует показатели качества и критерии оценки систем и отдельных методов и средств защиты информации ОПК-12.3: Оценивает информационные риски в автоматизированных системах ОПК-12.4: Разрабатывает основные показатели технико-экономического обоснования соответствующих проектных решений ОПК-4.1.1: Определяет подлежащие защите информационные ресурсы автоматизированных систем ОПК-4.1.2: Составляет комплексы правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе ОПК-4.1.3: Организует работу персонала автоматизированной системы с учетом требований по защите информации ОПК-4.1.4: Организует работу персонала автоматизированной системы с учетом требований по защите информации ОПК-4.2.1: Настраивает операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации ОПК-4.2.2: Применяет программные средства обеспечения безопасности данных ОПК-4.2.3: Управляет полномочиями пользователей автоматизированной системы ОПК-4.3.1: Осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы ОПК-4.3.2: Применяет программные средства обеспечения безопасности данных ОПК-4.3.3: Управляет полномочиями пользователей

	автоматизированной системы ОПК-4.4.1: Применяет инструментальные средства контроля защищенности информации в автоматизированных системах ОПК-4.4.2: Документирует действия по устранению неисправностей в работе системы защиты информации автоматизированной системы ОПК-4.4.3: Регистрирует события, связанные с защитой информации в автоматизированных системах ПК-1.1: Производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности ПК-1.2: Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности ПК-1.3: Выполняет регламентные работы по эксплуатации средств защиты информации ПК-1.4: Устраняет неисправности при эксплуатации средств защиты информации ПК-2.1: Формулирует критерии безопасности обработки информации в автоматизированных системах ПК-2.2: Выполняет мероприятия для реализации политики информационной безопасности ПК-2.3: Определяет состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД ПК-2.4: Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД ПК-2.5: Устанавливает программное обеспечение в соответствии с требованиями по защите информации ПК-3.1: Фиксирует возникновение инцидентов информационной безопасности ПК-3.2: Использует методы и средства резервного копирования информации ПК-3.3: Устраняет уязвимости в автоматизированной системе ПК-3.4: Соотносит изменения в конфигурации автоматизированной системы с её защищенностью ПК-4.1: Разрабатывает проектные документы на средства защиты информации создаваемых автоматизированных систем ПК-4.2: Готовит техническую и проектную документацию по вопросам создания и эксплуатации автоматизированных систем ПК-4.3: Проверяет программы и алгоритмы на предмет соответствия требованиям защиты информации ПК-4.4: Проводит сравнительный анализ вариантов конфигураций и состава автоматизированных систем ПК-5.1: Проверяет соответствие внедряемых решений и средств для обеспечения информационной безопасности

	требованиям реализуемой политики безопасности ПК-5.2: Восстанавливает работоспособность автоматизированных систем после инцидентов информационной безопасности ПК-5.3: Проводит операции вывода защищённых автоматизированных систем из эксплуатации ПК-6.1: Анализирует полноту и нормативным требованиям руководящих документов, описывающих работы по обеспечению информационной безопасности ПК-6.2: Формирует отчётные и руководящие документы для обеспечения защиты информации в информационной системе в ходе ее эксплуатации ПК-6.3: Формулирует в соответствии с требованиям руководящих документов состав и содержание процедур контроля обеспеченности уровня защищенности информации ПК-6.4: Готовит документы для проведения работ по аттестации объектов информатизации и автоматизированных систем ПК-7.1: Формулирует целевые показатели функционирования защищенных автоматизированных систем ПК-7.2: Анализирует уязвимости автоматизированных систем в соответствии с нормативными документами ПК-7.3: Формулирует угрозы информационной безопасности исходя из выявленных характеристик автоматизированной системы ПК-8.1: Разрабатывает методическую, техническую, рекомендательную и отчётную документацию по анализу защищённости автоматизированной системы ПК-8.2: Осуществляет подбор программных средств тестирования защищённости автоматизированной системы в зависимости от предъявляемым к ней требованиям ПК-8.3: Использует средств инструментального анализа защищённости программных и аппаратных платформ узлов автоматизированной системы ПК-8.4: Проводит контроль защищённости и функционирования программно-аппаратных и технических средств автоматизированной системы ПК-9.1: Формулирование правил работы персонала со средствами защиты информации ПК-9.2: Распределяет обязанности и полномочия персонала, обслуживающего защищённую автоматизированную систему ПК-9.3: Сопоставляет результат работы персонала, обслуживающего защищённую автоматизированную систему, с целевыми показателями функционирования службы защиты информации ПК-10.1: Соотносит инциденты информационной безопасности с характеристиками систем и средств защиты информации

	ПК-10.2: Обосновывает необходимость модернизации системы защиты информации автоматизированной системы ПК-10.3: Формулирует правила применения мер защиты информации, направленные на устранение причин возникновения инцидентов информационной безопасности ПК-10.4: Формулирует правила протоколирования результатов мониторинга безопасности автоматизированных систем
Формы проведения занятий, образовательные технологии:	Способы проведения практики – стационарная, выездная. Формы проведения практики – дискретно: путем чередования в календарном учебном графике периодов учебного времени для проведения практик с периодами учебного времени для проведения теоретических занятий. Технологии: метод «коллективной мыслительной деятельности», методы анализа проблемных ситуаций, логико-методологическое проектирование, решение задач.
Используемые инструментальные и программные средства:	Средства проекции (презентации), программированного контроля (тестирования), средства защиты информации
Формы промежуточного контроля:	Текущие оценки знаний, тестирование, доклады, самостоятельные работы
Общая трудоемкость изучения дисциплины:	108 ч./ 3 з.е.
Форма итогового контроля знаний:	Зачет с оценкой