АННОТАЦИЯ

производственной практики

Б2.В.03(П) «ПРЕДДИПЛОМНАЯ ПРАКТИКА»

Специальность – *10.05.03* «*Информационная безопасность автоматизированных систем*»

Квалификация (степень) выпускника – *специалист по защите информации*

Профиль/специализация/магистерская программа – *Безопасность автоматизированных систем на железнодорожном транспорте*

**1. Вид практики, способы и формы ее проведения**

Практика относится к части, формируемой участниками образовательных отношений, Блока 2 «*Практика*» и является обязательной.

Тип практики – преддипломная практика*.*

Способ проведения практики – стационарная.

Практика проводится дискретно по видам практик.

**2. Перечень планируемых результатов обучения при прохождении практики**

Проведение практики направлено на практическую подготовку обучающегося к будущей профессиональной деятельности. Практическая подготовка осуществляется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенции (части компетенций) по профилю образовательной программы.

Прохождение практики направлено на формирование следующих компетенций, сформированность которых оценивается с помощью индикаторов достижения компетенций:

|  |  |
| --- | --- |
| Компетенция | Индикатор компетенции |
| ПК-1. Тестирование систем защиты информации автоматизированных систем | ПК-1.1.1. Знает принципы построения и функционирования систем и сетей передачи информацииПК-1.1.2. Знает эталонную модель взаимодействия открытых системПК-1.1.3. Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системахПК-1.1.4. Знает основные меры по защите информации в автоматизированных системахПК-1.1.5. Знает технические средства контроля эффективности мер защиты информацииПК-1.2.1. Умеет анализировать основные характеристики и возможности телекоммуникационных систем по передаче информацииПК-1.2.2. Умеет анализировать основные узлы и устройства современных автоматизированных системПК-1.2.3. Умеет контролировать безотказное функционирование технических средств защиты информацииПК-1.2.4. Умеет восстанавливать (заменять) отказавшие технические средства защиты информацииПК-1.3.1. Имеет навыки проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных системПК-1.3.2. Имеет навыки выявления уязвимости информационно-технологических ресурсов автоматизированных системПК-1.3.3. Имеет навыки выявления основных угроз безопасности информации в автоматизированных системахПК-1.3.4. Имеет навыки составления методик тестирования систем защиты информации автоматизированных системПК-1.3.5. Имеет навыки подбора инструментальных средств тестирования систем защиты информации автоматизированных системПК-1.3.6. Имеет навыки составления протоколов тестирования систем защиты информации автоматизированных систем |
| ПК-2. Разработка проектных решений по защите информации в автоматизированных системах | ПК-2.1.1. Знает нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информацииПК-2.1.2. Знает принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентовПК-2.1.3. Знает критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных системПК-2.1.4. Знает принципы организации и структуру систем защиты информации программного обеспечения автоматизированных системПК-2.1.5. Знает принципы формирования политики информационной безопасности в автоматизированных системахПК-2.2.1. Умеет применять нормативные документы по противодействию технической разведкеПК-2.2.2. Умеет определять типы субъектов доступа и объектов доступа, являющихся объектами защитыПК-2.2.3. Умеет определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системеПК-2.2.4. Умеет определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системахПК-2.2.5. Умеет определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информацииПК-2.2.6. Умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных системПК-2.3.1. Имеет навыки разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системахПК-2.3.2. Имеет навыки разработки моделей автоматизированных систем и подсистем безопасности автоматизированных системПК-2.3.3. Имеет навыки разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах |
| ПК-3. Разработка эксплуатационной документации на системы защиты информации автоматизированных систем | ПК-3.1.1. Знает основные методы управления информационной безопасностьюПК-3.1.2. Знает информационные воздействия и критерии оценки защищенности автоматизированных системПК-3.1.3. Знает методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и систем защиты информации автоматизированных системахПК-3.1.4. Знает основные средства, способы и принципы построения систем защиты информации автоматизированных системПК-3.2.1. Умеет проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документовПК-3.2.2. Умеет разрабатывать модели автоматизированных систем и систем защиты информации автоматизированных системПК-3.2.3. Умеет исследовать модели автоматизированных систем и систем защиты безопасности автоматизированных системПК-3.2.4. Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных системПК-3.2.5. Умеет оценивать информационные риски в автоматизированных системах и определять информационную инфраструктуру и информационные ресурсы, подлежащие защитеПК-3.2.6. Умеет исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенностиПК-3.2.7.Умеет проводить комплексное тестирование и отладку аппаратных и программных систем защиты информацииПК-3.3.1. Имеет навыки анализа технической документации информационной инфраструктуры автоматизированной системыПК-3.3.2. Имеет навыки анализа защищенности информационной инфраструктуры автоматизированной системыПК-3.3.3. Имеет навыки формирования требований по защите информации, включая использование математического аппарата для решения прикладных задачПК-3.3.4. Имеет навыки документирования программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информацииПК-3.3.5. Имеет навыки обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем |
| ПК-4. Разработка программных и программно-аппаратных средств для систем защиты информации автоматизированных систем | ПК-4.1.1. Знает современные технологии программированияПК-4.1.2. Знает основные протоколы локальных и глобальных сетей ПК-4.1.3. Знает последовательность и содержание этапов построения и функционирования современных локальных и глобальных компьютерных сетейПК-4.1.4. Знает принципы организации документирования разработки и процесса сопровождения программного и аппаратного обеспеченияПК-4.1.5. Знает методы тестирования и отладки программного и аппаратного обеспеченияПК-4.2.1. Умеет разрабатывать технические задания на создание подсистем безопасности информации автоматизированных систем, проектировать такие подсистемы с учетом требований нормативных документов, ЕСКД и ЕСПДПК-4.3.1. Имеет навыки разработки технической документации в соответствии с требованиями Единой системы конструкторской документации (ЕСКД) и Единой системы программной документации (ЕСПД) на компоненты автоматизированных системПК-4.3.2. Имеет навыки синтеза структурных и функциональных схем защищенных автоматизированных системПК-4.3.3. Имеет навыки разработки программного обеспечения, технических средств, баз данных и компьютерных сетей с учетом требований по обеспечению защиты информации |

**3. Объем практики и ее продолжительность**

Практика проводится концентрировано.

Объем практики – 21 зачетная единица (756 часов, 14 недель)

Форма контроля знаний – зачет.