Приложение к рабочей программе дисциплины (практики)

Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН)

Факультет искусственного интеллекта

(наименование основного учебного подразделения)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

ТЕХНОЛОГИЧЕСКАЯ И ЭКСПЛУАТАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

(наименование дисциплины (практики))

Оценочные материалы рекомендованы МССН для направления подготовки/ специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/ специальности)

Освоение дисциплины (практики) ведется в рамках реализации основной профессиональной образовательной программы (ОП ВО, профиль/ специализация):

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(направленность (профиль) ОП ВО)

Москва, 2025

1. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ (ПРАКТИКЕ)

Фонд оценочных средств (ФОС) предназначен для оценки знаний, умений и компетенций студентов по дисциплине "Технологическая и эксплуатационная безопасность программного обеспечения". Он включает в себя следующие элементы:

1. Входной контроль

1.1. Тестирование

Для определения начального уровня знаний студентов проводится тестирование по основным понятиям и терминам, связанным с технологической и эксплуатационной безопасностью программного обеспечения. Примерные вопросы:

Определение уязвимости программного обеспечения.

Основные принципы безопасного программирования.

Методы анализа кода на наличие уязвимостей.

2. Текущая аттестация

2.1. Лабораторные работы

Студентам предлагается выполнять лабораторные работы, направленные на практическое освоение методов и технологий обеспечения безопасности программного обеспечения. Примеры лабораторных работ:

Анализ кода на наличие уязвимостей с использованием статических и динамических анализаторов.

Применение методов безопасного программирования при разработке простых приложений.

Проведение тестов на проникновение и оценка результатов.

2.2. Практические занятия

На практических занятиях студенты решают задачи, связанные с разработкой и тестированием безопасного программного обеспечения. Примеры задач:

Разработка простого приложения с использованием принципов безопасного программирования.

Проведение анализа кода стороннего приложения на предмет наличия уязвимостей.

Создание отчета по результатам анализа и предложения по устранению найденных

уязвимостей.

2.3. Рефераты и доклады

Студенты готовят рефераты и доклады на темы, связанные с технологической и эксплуатационной безопасностью программного обеспечения. Примеры тем:

Современные методы анализа кода на наличие уязвимостей.

Принципы безопасного программирования в различных языках программирования.

Обзор лучших практик по обеспечению безопасности программного обеспечения.

3. Промежуточная аттестация

3.1. Экзаменационные билеты

Промежуточная аттестация проводится в форме устного экзамена по билетам, содержащим вопросы по всему курсу. Примерные вопросы:

Основные этапы жизненного цикла безопасного программного обеспечения.

Методы тестирования программного обеспечения на соответствие требованиям безопасности.

Способы предотвращения распространенных типов уязвимостей.

3.2. Курсовая работа

Студенты выполняют курсовую работу, направленную на решение конкретной проблемы в области технологической и эксплуатационной безопасности программного обеспечения. Примерные темы курсовых работ:

Разработка методики анализа кода на наличие уязвимостей для конкретного типа программного обеспечения.

Проектирование и реализация системы контроля версий с учетом требований безопасности.

Исследование методов защиты программного обеспечения от обратного инжиниринга.