МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Инженерия безопасности программного обеспечения

Направление подготовки:	09.03.01 – Информатика и вычислительная техника
Направленность (профиль):	Технологии разработки программного обеспечения
Форма обучения:	Очная

Общие сведения о дисциплине (модуле).

Дисциплина посвящена обеспечению безопасности программного продукта на протяжении всего жизненного цикла и отвечает на острый дефицит специалистов по информационной безопасности, который оценивается для российской экономики примерно в сто тысяч человек. Обучающийся осваивает полный цикл работы инженера по безопасности разработки – от актуализации модели угроз и формулирования проверяемых требований до автоматизации контроля кода, зависимостей, секретов и контейнеров, формирования ведомости состава программного обеспечения, воспроизведения и устранения уязвимостей и документирования остаточного риска. Обучение строится на материалах индустриального партнёра – учебном сервисе контролируемого перерасчёта на Java и Spring со специально внесёнными уязвимостями и контуре безопасного внедрения локального помощника программиста. На практике студент собирает защищённый конвейер разработки и поставки в соответствии с ГОСТ Р 56939-2024 на отечественных и свободно распространяемых инструментах и по итогам

семестра формирует обоснованное заключение о допустимости выпуска. Освоенные результаты востребованы работодателями транспортной и ИТ-отрасли, реализующими курс на импортозамещение.

Целью освоения дисциплины является формирование способности обеспечивать безопасность программного продукта на протяжении жизненного цикла – уточнять модель угроз, проектировать меры защиты в архитектуре и коде, автоматизировать проверки цепочки разработки и поставки, формировать состав программных компонентов, воспроизводить и устранять уязвимости и документировать остаточный риск.

Для достижения поставленной цели в рамках дисциплины решается комплекс задач, направленных на формирование у обучающихся способности: актуализировать модель угроз и преобразовывать приоритетные сценарии в проверяемые требования безопасности. Проектировать меры защиты в архитектуре, программном коде, инфраструктуре и цепочке поставки. Автоматизировать анализ исходного кода, зависимостей, секретов, контейнеров и инфраструктурных описаний с установленными порогами допуска. Формировать состав программных компонентов и управлять происхождением зависимостей, исключениями и сроками устранения. Разрабатывать риск-ориентированный план проверки, воспроизводить уязвимость в безопасном стенде и устранять её первопричину. Добавлять регрессионную проверку, подтверждать исправление и документировать остаточный риск. Идентифицировать риски проекта, выбирать меры воздействия и контролировать их эффективность совместно с владельцем риска.

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 академических часа(ов).