МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по направлению подготовки
09.03.01 Информатика и вычислительная техника,
утвержденной директором ФГАОУ ВО РУТ
(МИИТ) Париновым Д.В.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Инженерия безопасности программного обеспечения

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Технологии разработки программного обеспечения

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная ФГАОУ ВО РУТ (МИИТ)
ID подписи: 937226
Подписал: директор центра Проневич Ольга Борисовна
Дата: 12.11.2026

1. 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.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ДПК-БП-1 - Способен обеспечивать безопасность бизнес-приложения на протяжении жизненного цикла;

ОПК-4 - Способен решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и технологий искусственного интеллекта, а также с учетом основных требований информационной безопасности;

ППК-У1 - Осуществляет оценку и управление рисками.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- принципы информационной и библиографической культуры, источники профессиональной информации;
- возможности и ограничения технологий искусственного интеллекта в профессиональной деятельности;
- основные требования информационной безопасности при работе с информацией (защита персональных данных, коммерческая тайна);
- критерии, методы, правила идентификации риска;
- возможности инструментов риск-менеджмента для идентификации рисков организации;
- законодательство Российской Федерации, базовые положения международных стандартов и отраслевые стандарты по управлению рисками;
- критерии, методы и инструменты воздействия на риски в разрезе отдельных их видов;
- план мероприятий по управлению рисками;
- виды, методы, формы и инструменты внутреннего контроля.

Уметь:

- находить, систематизировать и критически оценивать информацию из профессиональных источников;

- применять ИКТ и инструменты искусственного интеллекта для решения профессиональных задач;

- соблюдать требования информационной безопасности при обработке информации и использовании ИИ;

- выделять активы и границы доверия;

- формировать сценарии злоупотребления и проверяемые требования безопасности;

- выбирать меры безопасности и документировать остаточный риск;

- проектировать меры безопасности в архитектуре, программном коде, конвейере непрерывной интеграции и поставки, а также в инфраструктуре;

- автоматизировать статический анализ кода, анализ состава зависимостей, поиск секретов, проверку контейнеров и инфраструктуры как кода с контрольными условиями качества;

- формировать ведомость состава программного обеспечения (SBOM) и правила управления зависимостями, исключениями и происхождением артефактов;

- разрабатывать риск-ориентированный план проверки и воспроизводить уязвимости;

- приоритизировать находки, устранять первопричину и добавлять регрессионную проверку;

- документировать доказательства исправления и остаточный риск;

- выявлять контекст рисков, их идентификацию и формировать портфель рисков проекта;

- осуществлять мониторинг рисков проекта;

- проводить качественную и количественную статистическую оценку рисков на основе фактических событий базы рисковых событий;

- осуществлять оценку рисковых ситуаций в динамике, тестирование и верификацию методик идентификации рисков с учетом отраслевой специфики и контекста функционирования организации;

- разрабатывать мероприятия по управлению рисками, осуществлять мониторинг и оценку их эффективности совместно с ответственными за риск сотрудниками организации – владельцами риска;

- определять и отбирать эффективные методы воздействия на риск, разрабатывать и внедрять планы воздействия на риски (совместно с ответственными за риск сотрудниками – владельцами риска), оказывать помощь ответственным за риск сотрудникам в правильной оценке риска и разработке мероприятий по их управлению;

- осуществлять расчеты, прогнозировать, тестировать и верифицировать методики управления рисками с учетом отраслевой специфики;

- формировать формы отчетности, дорожные карты для целей реализации и мониторинга мероприятий по воздействию на риски.

Владеть:

- навыками безопасного и ответственного использования цифровых и ИИ-инструментов в профессиональной деятельности.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

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

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №7
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	32	32

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 60 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Безопасная разработка ПО как инженерная дисциплина Рассматриваемые вопросы: - место безопасности в жизненном цикле программного обеспечения по ГОСТ Р 56939-2024; - нормативный контур: 149-ФЗ, 152-ФЗ, 187-ФЗ, базовая модель угроз ФСТЭК России; - роль разработчика в обеспечении безопасности и ответственность за безопасность изменения; - профессиональные источники информации: Банк данных угроз ФСТЭК, рекомендации OWASP, документация инструментов.
2	Модель угроз и границы доверия Рассматриваемые вопросы: - модель злоумышленника и таксономия угроз бизнес-приложений; - инвентаризация активов и построение диаграмм потоков данных; - выявление границ доверия в распределённой архитектуре; - методология STRIDE: категории угроз и порядок анализа.
3	Требования безопасности и классификации уязвимостей Рассматриваемые вопросы: - формирование проверяемых требований безопасности по OWASP ASVS; - трассировка требований к сценариям угроз; - референсные классификации индустрии: OWASP Top 10, CWE/SANS Top 25; - актуальный ландшафт угроз: нарушение контроля доступа, сбои цепочки поставки, инъекции.
4	Безопасное проектирование и безопасное кодирование Рассматриваемые вопросы: - принципы безопасного проектирования: минимизация привилегий, глубокая защита, безопасные умолчания; - паттерны безопасного кодирования на Java: нейтрализация инъекций и защита сериализации; - контроль доступа и безопасная обработка ввода; - типовые ошибки реализации мер защиты и их последствия.
5	DevSecOps и безопасная цепочка разработки и поставки Рассматриваемые вопросы: - концепция DevSecOps: смещение безопасности «влево» и непрерывный контроль; - встраивание проверок в конвейер непрерывной интеграции: контрольные условия качества и пороги допуска; - Policy-as-Code: правила безопасности как версионируемый код; - защита цепочки поставки: происхождение артефактов и аттестация сборки.
6	Автоматизированный анализ защищённости Рассматриваемые вопросы: - статический анализ исходного кода (SAST): методика, настройка правил, ложные срабатывания; - анализ состава программного обеспечения (SCA): сканирование зависимостей и базы уязвимостей; - ведомость состава программного обеспечения (SBOM) в формате CycloneDX; - поиск секретов в коде и проверка контейнерных образов и инфраструктуры как кода.
7	Проверка защищённости и устранение уязвимостей Рассматриваемые вопросы: - риск-ориентированное планирование проверки защищённости; - шкала CVSS: расчёт базовой оценки и приоритизация находок; - воспроизведение уязвимости в изолированном стенде и анализ первопричины; - доказательное устранение: регрессионная проверка и документирование результата.
8	Безопасность систем с компонентами искусственного интеллекта и управление рисками Рассматриваемые вопросы: - угрозы систем с компонентами искусственного интеллекта: утечки данных через ИИ-инструменты, недостоверность рекомендаций, угрозы систем ИИ в БДУ ФСТЭК;

№ п/п	Тематика лекционных занятий / краткое содержание
	- архитектурные меры защиты контура применения ИИ: изоляция данных, разграничение доступа, контроль результатов модели; - нормативные и методические основы управления рисками информационной безопасности: законодательство РФ, международные и отраслевые стандарты; - методы идентификации и оценки уровня рисков, варианты воздействия на риск и инструменты внутреннего контроля.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Инвентаризация активов и построение диаграммы потоков данных сервиса перерасчёта Студент изучает описание учебного сервиса контролируемого перерасчёта на Java и Spring и выделяет защищаемые активы, участников и внешние взаимодействия. Он строит диаграмму потоков данных сервиса и наносит на неё внешние сущности, процессы и хранилища. Результатом занятия становится оформленная в Р7-Офис диаграмма потоков данных, которая используется как основа анализа угроз на следующем занятии.
2	Выявление границ доверия и построение сценариев злоупотребления Студент наносит на построенную диаграмму потоков данных границы доверия и обосновывает их размещение. По методологии STRIDE он формирует сценарии злоупотребления для каждого пересечения потока данных с границей доверия. Сценарии сверяются с записями Банка данных угроз ФСТЭК России. Итогом становится каталог сценариев угроз, привязанный к элементам диаграммы.
3	Приоритизация угроз и утверждение версии модели угроз Студент оценивает выявленные сценарии по вероятности и ущербу и ранжирует их по уровню риска. Он отбирает приоритетные сценарии, которые будут преобразованы в требования безопасности, и документирует отклонённые сценарии с обоснованием. Итоговая версия модели угроз утверждается как исходный документ для проектирования защиты.
4	Формирование проверяемых требований безопасности Студент преобразует приоритетные сценарии угроз в проверяемые требования безопасности, опираясь на разделы OWASP ASVS. Для каждого требования он формулирует критерий проверки и способ подтверждения выполнения. Требования трассируются к сценариям модели угроз в едином каталоге. Каталог требований становится основой для выбора мер защиты и настройки автоматизированных проверок.
5	Проектирование мер защиты в архитектуре и программном коде Студент выбирает меры защиты для каждого требования безопасности, применяя принципы минимизации привилегий, глубокой защиты и безопасных умолчаний. Он определяет, какие меры реализуются в архитектуре сервиса, какие – в программном коде на Java, а какие – в инфраструктуре. Решения фиксируются в таблице мер с обоснованием выбора. Таблица мер передаётся на проектирование защищённой цепочки разработки.
6	Проектирование схемы защищённой цепочки разработки и поставки Студент определяет обязательные автоматизированные проверки для кода, зависимостей, секретов, контейнерного образа и инфраструктурных описаний. Для каждой проверки он задаёт контрольное условие допуска к выпуску, включая порог по критичности находок. Он строит схему защищённого конвейера с точками контроля и оформляет её как техническое задание на автоматизацию. Схема конвейера реализуется на последующих занятиях.

№ п/п	Тематика практических занятий/краткое содержание
7	Встраивание статического анализа кода в конвейер Студент подключает инструмент статического анализа к учебному репозиторию сервиса и настраивает набор правил под технологический стек Java и Spring. Он задаёт контрольное условие качества, при котором наличие критичных находок блокирует сборку. Проверка запускается в конвейере, и студент фиксирует первый отчёт анализа. Отчёт становится входными данными для работы с находками и исключениями.
8	Анализ состава зависимостей и формирование ведомости SBOM Студент выполняет сканирование зависимостей сервиса инструментом анализа состава и сопоставляет компоненты с базами уязвимостей. Он формирует ведомость состава программного обеспечения в формате CycloneDX и проверяет происхождение артефактов. В ведомости отмечаются компоненты с известными уязвимостями и их оценки. Ведомость и результаты сканирования включаются в конвейер как обязательная проверка.
9	Поиск секретов и проверка контейнерного образа Студент настраивает поиск секретов в истории репозитория инструментом Gitleaks и разбирает обнаруженные совпадения. Затем он проверяет контейнерный образ сервиса сканером Trivy и анализирует находки по базовому образу и пакетам. Для обеих проверок задаются пороги допуска, и проверки встраиваются в конвейер. Журнал запусков пополняет портфель доказательств.
10	Политика управления зависимостями и исключениями Студент разбирает накопленные находки анализаторов, отделяет истинные угрозы от ложных срабатываний и оформляет исключения с обоснованием и сроком пересмотра. Он формулирует политику обновления зависимостей, правила принятия новых компонентов и сроки устранения по категориям критичности. Политика утверждается как правило конвейера. На этом фаза автоматизации контроля завершается исполняемым защищённым конвейером.
11	Разработка риск-ориентированного плана проверки защищённости Студент сводит находки конвейера и приоритетные сценарии модели угроз в единый перечень объектов проверки. Он рассчитывает оценки CVSS для выявленных слабостей и ранжирует проверки по уровню риска. План проверки определяет порядок, глубину и критерии завершения испытаний. По плану выбирается первая уязвимость для воспроизведения.
12	Воспроизведение уязвимости в изолированном стенде Студент воспроизводит выбранную уязвимость в учебном стенде при помощи OWASP ZAP и ручных проверок, строго в границах стенда. Он фиксирует шаги воспроизведения, наблюдаемый эффект и затронутый актив. По диагностическим журналам и исходному коду он выявляет первопричину дефекта. Протокол воспроизведения становится основанием для исправления.
13	Устранение первопричины и регрессионная проверка Студент исправляет уязвимость в коде сервиса, применяя безопасный паттерн кодирования, и устраняет первопричину, а не симптом. Он добавляет автоматизированную регрессионную проверку, которая подтверждает отсутствие повторного появления дефекта. Конвейер перезапускается, и студент документирует доказательство исправления. Исправленный инкремент включается в портфель.
14	Модель угроз контура локального помощника программиста Студент анализирует схему подключения локального ИИ-помощника к среде разработки, хранилищу кода и программному интерфейсу генерации. Он определяет активы, категории защищаемых данных и границы доверия контура. Для типовых угроз, включая раскрытие корпоративных материалов и недостоверные рекомендации, строятся сценарии злоупотребления. Версия модели угроз контура передаётся на проектирование защиты.
15	Проектирование защиты контура ИИ и контроль рекомендаций Студент проектирует защищённую конфигурацию контура с программным шлюзом, разграничением доступа и журналированием обращений к модели. Он проверяет предложенную конфигурацию и фрагменты кода шлюза на Java, устраняет раскрытие данных и обход проверки

№ п/п	Тематика практических занятий/краткое содержание
	доступа. Он вводит правила контроля рекомендаций модели и порядок аварийного отключения помощника. Журнал решений пополняет портфель.
16	Реестр рисков и заключение о допустимости выпуска Студент сводит все нерешённые находки в реестр рисков, назначает владельцев, пороги и сроки, выбирает меры воздействия и строит дорожную карту. Он документирует остаточный риск и формирует обоснованное заключение о допустимости выпуска защищённого инкремента. Заключение оформляется в Р7-Офис и защищается перед комиссией. Итогом становится собранный портфель «Защищённый конвейер разработки и поставки».

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение рекомендованной литературы.
2	Подготовка к практическим работам.
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. – Москва : Издательство Юрайт, 2024. – 312 с. – ISBN 978-5-9916-9043-0.	Юрайт: электронно-библиотечная система. — URL: https://urait.ru/bcode/538066 (дата обращения: 17.10.2026).
2	Щербак А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. – 2-е изд. – Москва : Издательство Юрайт, 2026. – 252 с. – ISBN 978-5-9916-4299-6.	Юрайт: электронно-библиотечная система. — URL: https://urait.ru/bcode/589902 (дата обращения: 17.10.2026).
3	рохорова О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. – 7-е изд., стер. – Санкт-Петербург : Лань, 2026. – 124 с.	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/525917 (дата обращения: 17.10.2026).
4	Гафаров А. Г., Шелухин А. А. Управление рисками информационной безопасности : учебник и практикум для вузов / А. Г. Гафаров, А. А. Шелухин. – Москва : Издательство Юрайт, 2023. – 232 с.	Юрайт : электронно-библиотечная система. — URL: https://urait.ru/bcode/583643 (дата обращения: 17.10.2026).

5	Башлы П. Н., Бабаш А. В., Баранова Е. К. Информационная безопасность : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – Москва : ЕАОИ, 2009. – 376 с. – ISBN 978-5-374-00301-7.	Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/126331 (дата обращения: 17.10.2026).

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

ЭБС «Лань» – https://e.lanbook.com;

ЭБС «Юрайт» – https://urait.ru;

Банк данных угроз безопасности информации ФСТЭК России – https://bdu.fstec.ru;

ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» – https://docs.cntd.ru/document/1310017763;

OWASP Top 10 – https://owasp.org/Top10;

OWASP Application Security Verification Standard (ASVS) – https://owasp.org/www-project-application-security-verification-standard;

OWASP CycloneDX (спецификация SBOM) – https://owasp.org/projects/cyclonedx;

OWASP ZAP – официальная документация – https://www.zaproxy.org/docs;

OWASP Dependency-Check – https://owasp.org/www-project-dependency-check;

Semgrep – официальная документация – https://semgrep.dev/docs;

Gitleaks – https://github.com/gitleaks/gitleaks;

Trivy – официальная документация – https://trivy.dev/docs;

PT Application Inspector – документация Positive Technologies – https://help.ptsecurity.com;

Solar appScreener – https://rt-solar.ru/products/solar_appscreener/docs.

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Операционные системы: Astra Linux Special Edition / ALT Linux / РЕД ОС.

Офисные пакеты: Р7-Офис / МойОфис (для подготовки модели угроз, каталогов требований, политик и заключения о выпуске по ГОСТ).

Платформы совместной разработки и CI/CD: GitVerse / GitFlic (командные репозитории, конвейеры сборки и проверки).

Статический анализ кода (SAST): PT Application Inspector (реестр российского ПО) / Semgrep OSS с набором правил OWASP ASVS / PVS-Studio (бесплатная лицензия для учебных целей).

Анализ состава и зависимостей (SCA): CodeScoring (реестр российского ПО) / OWASP Dependency-Check.

Динамический анализ (DAST): Solar appScreener (реестр российского ПО) / OWASP ZAP.

Поиск секретов: Gitleaks.

Проверка контейнеров и инфраструктуры как кода, генерация SBOM: Trivy (формат CycloneDX, поддержка VEX).

Контейнеризация учебных стендов: Docker / Podman.

Контур безопасного применения ИИ: Ollama / LM Studio с открытыми языковыми моделями; программный шлюз разрабатывается на Java (Spring).

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

Для практических занятий – наличие персональных компьютеров вычислительного класса.

9. Форма промежуточной аттестации:

Зачет в 7 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

старший преподаватель кафедры
«Цифровые технологии управления
транспортными процессами»
Института железнодорожного
транспорта И.С. Разживайкин

Согласовано:

Заведующий кафедрой ЦТУТП В.Е. Нутович

Директор ЦС IT - программ ВИШ О.Б. Проневич

Председатель учебно-методической
комиссии Н.А. Андриянова