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 специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Методы исследования защищенности объектов информатизации

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (в сфере связи, информационных и коммуникационных технологий)

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения дисциплины (модуля) являются:

- изучение методов и программных средств для анализа защиты информации;
- изучение основных уязвимостей объектов информатизации и угроз безопасности;
- изучение методов анализа защищенности информационных систем;
- изучение методов тестирования системы защиты;
- изучение средств анализа защищенности объектов информатизации.

Задачами освоения дисциплины (модуля) являются:

- разработка методов защиты программных систем от уязвимостей;
- проектирование программного обеспечения, способного противостоять угрозам безопасности;
- проведение анализа защищенности программного комплекса.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-1 - Способность анализировать и оценивать защищенность программно-аппаратных средств защиты информации;

ПК-6 - Способность анализировать архитектуру, компоненты и характеристики телекоммуникационных и автоматизированных систем, выявлять потенциальные уязвимости и оценивать информационные риски.

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

Знать:

- основные термины и определения информационной безопасности;
- методы анализа защищенности информации от внешних и внутренних нарушителей, защищенности веб-приложений и баз данных.

Уметь:

- определять внешние и внутренние угрозы безопасности информации;
- оценивать степень защищенности объекта информатизации;
- определять актуальные угрозы и уязвимости;
- использовать сканеры безопасности для поиска уязвимостей объектов информатизации.

Владеть:

- методикой определения угроз безопасности информации;
- программными средствами анализа защищенности;
- достаточными знаниями в теории тестирования системы защиты информации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 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 №9
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	48	48
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 100 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	Основные понятия защиты информации Рассматриваемые вопросы: - понятие уязвимости, - объекты защиты, - свойства и доступ к информации, - виды защиты информации; - цель и средства защиты; - факторы, воздействующие на безопасность.
2	Угрозы информационной безопасности Рассматриваемые вопросы: - классификация и источники угроз, - этапы и способы доступа к ресурсам ИС, - виды угроз, основные угрозы ИС; - методы реализации угроз.
3	Разработка динамических сайтов Рассматриваемые вопросы: - среда разработки Node.js, - модули, - промежуточное программное обеспечение; - экспорт из модулей.
4	Разработка динамических сайтов Рассматриваемые вопросы: - шаблон документа и шаблонизаторы, - GET и POST запросы, - маршрутизация; - статические ресурсы.
5	Разработка динамических сайтов Рассматриваемые вопросы: - технологи AJAX, - отправка данных формы, - обработка данных на сервере; - обработка ответа клиентом.
6	Общая система оценки уязвимостей Рассматриваемые вопросы: понятие уязвимости, - база уязвимости CVE, - база уязвимости NVD, - база уязвимостей ФСТЭК России, - метрики оценки уязвимостей.
7	Методика анализа защищенности компании GlobalTrust Рассматриваемые вопросы: - методы исследования защищенности; - этапы работ по анализу защищенности; - тестирование системы защиты.
8	Основные уязвимости веб-приложений Рассматриваемые вопросы: - топ-10 угроз безопасности; - краткое описание угроз безопасности классов A1 - A10:2025.
9	Сканер уязвимостей OWASP ZAP Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- сканирование сайта; - информация об уязвимости; - просмотр сессий.
10	Уязвимость SQL-инъекция. Рассматриваемые вопросы: - получение несанкционированного доступа - изменение пароля администратора - методы защиты.
11	Работа с уязвимым приложением JUICE SHOP NodeJS Application Рассматриваемые вопросы: - структура приложения; - запуск приложения; - демонстрация уязвимостей.
12	IDOR-уязвимость Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
13	Обработка ошибок Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
14	Уязвимый компонент Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
15	Криптографические сбои Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
16	SQL-инъекция и методы защиты в JUICE SHOP Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
17	Хранимый XSS Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
18	Небезопасный дизайн Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
19	Сбои аутентификации Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
20	Нарушение целостности ПО и данных. Небезопасная десериализация Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
21	Сбои ведения журналов и оповещений Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
22	Некорректная обработка исключений Рассматриваемые вопросы: - описание уязвимостей; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
23	Некорректная обработка при загрузке файлов Рассматриваемые вопросы: - описание уязвимостей; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
24	Методологии анализа защищенности. Средства для проведения тестирования на проникновение Рассматриваемые вопросы: - тестирование на проникновение; - методы тестирования; - российские и зарубежные методики тестирования; - этапы тестирования; - поисковые системы; - сканер-ВС.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Оценка уязвимостей В результате практического занятия студент получает навык оценки уязвимостей по стандарту CVSS
2	Среда разработки веб-приложений Node.js В результате практического занятия студент получает навык разработки приложения в системе Node
3	Разработка клиентской части веб-приложения В результате практического занятия студент получает навык разработки клиентской части приложения на языке JavaScript и HTML

№ п/п	Тематика практических занятий/краткое содержание
4	Разработка серверной части веб-приложения В результате практического занятия студент получает навык разработки серверной части приложения на языке JavaScript в среде Node
5	Сканер уязвимостей OWASP ZAP В результате практического занятия студент получает навык работы со сканером уязвимостей, поиска основных уязвимостей с использованием сканера
6	Уязвимое приложение JUICE SHOP В результате практического занятия студент получает навык определения уязвимых мест в веб-приложении
7	Эксплуатация и устранение уязвимости A1 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
8	Эксплуатация и устранение уязвимости A2 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
9	Эксплуатация и устранение уязвимости A3 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
10	Эксплуатация и устранение уязвимости A4 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
11	Эксплуатация и устранение уязвимости A5 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
12	Эксплуатация и устранение уязвимости A6 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
13	Эксплуатация и устранение уязвимости A7 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
14	Эксплуатация и устранение уязвимости A8 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
15	Эксплуатация и устранение уязвимости A9 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
16	Эксплуатация и устранение уязвимости A10 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение документации по Node.js, OWASP ZAP, JUICE SHOP
2	Анализ и дополнительная проработка лекционного материала
3	Подготовка к практическим занятиям

№ п/п	Вид самостоятельной работы
4	Изучение учебной литературы из приведенных источников
5	Выполнение курсового проекта.
6	Выполнение курсовой работы.
7	Подготовка к промежуточной аттестации.
8	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

Реализовать уязвимое веб-приложение и решение по устранению уязвимостей. Приложение должно содержать набор уязвимостей из следующего списка согласно индивидуальному заданию:

A01 – Broken Access Control (Нарушение контроля доступа)

A02 – Security Misconfiguration (Ошибки конфигурации безопасности)

A03 – Software Supply Chain Failures (Сбои в цепочке поставок ПО)

A04 – Cryptographic Failures (Сбои в криптографической защите)

A05 – Injection (Инъекции)

A06 – Insecure Design (Небезопасный дизайн)

A07 – Authentication Failures (Сбои в аутентификации)

A08 – Software or Data Integrity Failures (Нарушения целостности ПО или данных)

A09 – Security Logging and Alerting Failures (Сбои ведения журналов и оповещений)

A10 - Mishandling of Exceptional Conditions (Некорректная обработка исключительных ситуаций)

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

№ п/п	Библиографическое описание	Место доступа
1	Давыдовский М.А. Разработка веб-сервисов: Учебное пособие. – М.: РУТ (МИИТ), 2020. – 111 с.	https://www.elibrary.ru/item.asp?id=45603698 (дата обращения: 06.06.2026). - Текст: электронный.
2	Диогенес Ю. , Озкайя Э. Кибербезопасность. стратегия атак и	https://reader.lanbook.com/book/131717#4 (дата обращения: 06.06.2026). - Текст: электронный.

	обороны. - Издательство "ДМК Пресс", 2020. - 326 с. ISBN: 978-5-97060-709-1	
3	Дэвис Р. Искусство тестирования на проникновение в сеть. - Издательство "ДМК Пресс", 2021. - 310 с. ISBN: 978-5-97060-529-5	https://reader.lanbook.com/book/241076 (дата обращения: 06.06.2026). - Текст: электронный.

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

- Научная электронная библиотека (http://elibrary.ru)
- Электронно-библиотечная система Научно-технической библиотеки МИИТ (http://library.miit.ru)
- Википедия (https://ru.wikipedia.org)
- Материалы по информационным технологиям (www.citforum.ru)
- Сайт Node.js (https://nodejs.org/en/)
- Руководство по использованию JUICE SHOP с описанием имеющихся уязвимостей (https://owasp.org/www-project-juice-shop/)

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

- Язык программирования JavaScript
- Программная платформа Node.js (лицензия X11, свободно-распространяемое ПО)
- Сканер уязвимостей OWASP ZAP (https://www.zaproxy.org/download)
- GitHub. Juice Shop (https://github.com/juice-shop/juice-shop)

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

- Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ.
- Аудиовизуальное оборудование аудитории.
- АРМ управляющий, для вывода изображения на экран для студентов.
- Акустическая система.
- Место для преподавателя, оснащенное компьютером.
- персональные компьютеры, мониторы, принтер, доска учебная.
- Аудитория подключена к интернету РУТ(МИИТ).

9. Форма промежуточной аттестации:

Зачет в 9 семестре.
Курсовая работа в 9 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, доцент, к.н. кафедры
«Вычислительные системы и
квантовые коммуникации» М.А. Давыдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова