МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
специализированного высшего образования
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Методы исследования защищенности объектов информатизации

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

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 РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 03.06.2026

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-4 - Способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.

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 6 з.е. (216 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 №2
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	16	16

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 168 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	Общая система оценки уязвимостей Рассматриваемые вопросы: понятие уязвимости, - база уязвимости CVE, - база уязвимости NVD, - база уязвимостей ФСТЭК России.
2	Методика анализа защищенности компании GlobalTrust Рассматриваемые вопросы: - методы исследования защищенности; - этапы работ по анализу защищенности; - тестирование системы защиты.
3	Сканер уязвимостей OWASP ZAP Рассматриваемые вопросы: - сканирование сайта; - информация об уязвимости; - просмотр сессий.
4	Уязвимость SQL-внедрение. Способы внедрения. Защита от SQL-внедрения Рассматриваемые вопросы: - получение несанкционированного доступа - изменение пароля администратора - методы защиты.
5	Работа с уязвимым приложением Damn Vulnerable NodeJS Application Рассматриваемые вопросы: - структура приложения; - запуск приложения; - демонстрация уязвимостей.
6	SQL-внедрение в приложении DVNA и методы защиты Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
7	Недостатки аутентификации. Небезопасный сброс пароля Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
8	Разглашение конфиденциальных данных Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
9	Внешние сущности XML (XXE) Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
10	Недостатки контроля доступа Рассматриваемые вопросы: - описание уязвимости;

№ п/п	Тематика лекционных занятий / краткое содержание
	- уязвимый код приложения; - модификация кода с целью устранения уязвимости.
11	Некорректная настройка параметров безопасности Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
12	Межсайтовое выполнение сценариев Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
13	Небезопасная десериализация Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
14	Использование компонентов с известными уязвимостями Рассматриваемые вопросы: - описание уязвимостей; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
15	Недостатки журналирования и мониторинга Рассматриваемые вопросы: - описание уязвимостей; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
16	Методологии анализа защищенности. Сетевые сканеры безопасности Рассматриваемые вопросы: - тестирование на проникновение; - российские и зарубежные методики тестирования; - этапы тестирования.

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	Сканер уязвимостей OWASP ZAP В результате практического занятия студент получает навык работы со сканером уязвимостей, поиска основных уязвимостей с использованием сканера
3	Эксплуатация и устранение уязвимости A1 и A2 приложения JUICE SHOP

№ п/п	Тематика практических занятий/краткое содержание
	В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения, и метод устранения уязвимостей
4	Эксплуатация и устранение уязвимости A3 и A4 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения, и метод устранения уязвимостей
5	Эксплуатация и устранение уязвимости A5 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения, и метод устранения уязвимостей
6	Эксплуатация и устранение уязвимости A6 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения, и метод устранения уязвимостей
7	Эксплуатация и устранение уязвимости A7 и A8 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения, и метод устранения уязвимостей
8	Эксплуатация и устранение уязвимости A9 и A10 приложения JUICE SHOP В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения, и метод устранения уязвимостей

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к практическим занятиям
2	Изучение учебной литературы из приведенных источников
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	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:

1. A1-Внедрение
2. A2-Недостатки аутентификации
3. A3-Разглашение конфиденциальных данных
4. A4-Внешние сущности XML (XXE)
5. A5-Недостатки контроля доступа

6. A6-Некорректная настрои?ка параметров безопасности

7. A7-Межсаи?товое выполнение сценариев (XSS)

8. A8-Небезопасная десериализация

9. A9-Использование компонентов с известными уязвимостями

10. A10-Недостатки журналирования и мониторинга

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: : 17.03.2025). - Текст: электронный.
2	Диогенес Ю. , Озкайя Э. Кибербезопасность. стратегия атак и обороны. - Издательство "ДМК Пресс", 2020. - 326 с. ISBN: 978-5-97060-709-1	https://reader.lanbook.com/book/131717#4 (дата обращения: : 17.03.2025). - Текст: электронный.
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: : 17.03.2025). - 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)
- Электронно-библиотечная система Лань (https://e.lanbook.com/)
- Материалы по информационным технологиям (www.citforum.ru)
- Сайт Node.js (https://nodejs.org/en/)
- Руководство по использованию DVNA с описанием имеющихся уязвимостей (https://appsecco.com/books/dvna-developers-security-guide/)

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)
- Damn Vulnerable NodeJS Application (https://github.com/appsecco/dvna)

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

Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий, лабораторных работ, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации):

- компьютер преподавателя, проектор, экран проекционный, рабочие станции студентов, маркерная доска.

Аудитория подключена к сети «Интернет»

9. Форма промежуточной аттестации:

Курсовая работа во 2 семестре.
Экзамен во 2 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