

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**  
**(РУТ (МИИТ))**



Рабочая программа дисциплины (модуля),  
как компонент образовательной программы  
высшего образования - программы магистратуры  
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: 10.12.2024

## 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):

**ОПК-5** - Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

**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 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 №2
Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
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 116 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	<b>Общая система оценки уязвимостей</b> Рассматриваемые вопросы: понятие уязвимости, - база уязвимости CVE, - база уязвимости NVD, - база уязвимостей ФСТЭК России.
2	<b>Методика анализа защищенности компании GlobalTrust</b> Рассматриваемые вопросы: - методы исследования защищенности; - этапы работ по анализу защищенности; - тестирование системы защиты.
3	<b>Сканер уязвимостей OWASP ZAP</b> Рассматриваемые вопросы: - сканирование сайта; - информация об уязвимости; - просмотр сессий.
4	<b>Уязвимость SQL-внедрение. Способы внедрения. Защита от SQL-внедрения</b> Рассматриваемые вопросы: - получение несанкционированного доступа - изменение пароля администратора - методы защиты.
5	<b>Работа с уязвимым приложением Damn Vulnerable NodeJS Application</b> Рассматриваемые вопросы: - структура приложения; - запуск приложения; - демонстрация уязвимостей.
6	<b>SQL-внедрение в приложении DVNA и методы защиты</b> Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
7	<b>Недостатки аутентификации. Небезопасный сброс пароля</b> Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
8	<b>Разглашение конфиденциальных данных</b> Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
9	<b>Внешние сущности XML (XXE)</b> Рассматриваемые вопросы: - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.

№ п/п	Тематика лекционных занятий / краткое содержание
10	Недостатки контроля доступа Рассматриваемые вопросы: - описание уязвимости; - 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	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	<b>Разработка серверной части веб-приложения</b> В результате практического занятия студент получает навык разработки серверной части приложения на языке JavaScript в среде Node
5	<b>Сканер уязвимостей OWASP ZAP</b> В результате практического занятия студент получает навык работы со сканером уязвимостей, поиска основных уязвимостей с использованием сканера
6	<b>Уязвимое приложение DVNA</b> В результате практического занятия студент получает навык определения уязвимых мест в веб-приложении
7	<b>Эксплуатация и устранение уязвимости A1 приложения DVNA</b> В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
8	<b>Эксплуатация и устранение уязвимости A2 приложения DVNA</b> В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
9	<b>Эксплуатация и устранение уязвимости A3 приложения DVNA</b> В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
10	<b>Эксплуатация и устранение уязвимости A4 приложения DVNA</b> В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
11	<b>Эксплуатация и устранение уязвимости A5 приложения DVNA</b> В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
12	<b>Эксплуатация и устранение уязвимости A6 приложения DVNA</b> В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
13	<b>Эксплуатация и устранение уязвимости A7 приложения DVNA</b> В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
14	<b>Эксплуатация и устранение уязвимости A8 приложения DVNA</b> В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
15	<b>Эксплуатация и устранение уязвимости A9 приложения DVNA</b> В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
16	<b>Эксплуатация и устранение уязвимости A10 приложения DVNA</b> 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, DVNA
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	Подготовка к промежуточной аттестации.
7	Подготовка к текущему контролю.

#### 4.4. Примерный перечень тем курсовых проектов

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

1. А1-Внедрение
2. А2-Недостатки аутентификации
3. А3-Разглашение конфиденциальных данных
4. А4-Внешние сущности XML (XXE)
5. А5-Недостатки контроля доступа
6. А6-Некорректная настройка параметров безопасности
7. А7-Межсайтовое выполнение сценариев (XSS)
8. А8-Небезопасная десериализация
9. А9-Использование компонентов с известными уязвимостями
10. А10-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.	<a href="https://www.elibrary.ru/item.asp?id=45603698">https://www.elibrary.ru/item.asp?id=45603698</a> (дата обращения: 04.12.2024). - Текст: электронный.
2	Диогенес Ю. , Озкайя Э. Кибербезопасность. стратегия атак и обороны. - Издательство "ДМК Пресс", 2020. - 326 с. ISBN: 978-5-97060-709-1	<a href="https://reader.lanbook.com/book/131717#4">https://reader.lanbook.com/book/131717#4</a> (дата обращения: 04.12.2024). - Текст: электронный.

3	Дэвис Р. Искусство тестирования на проникновение в сеть. - Издательство "ДМК Пресс", 2021. - 310 с. ISBN: 978-5-97060-529-5	<a href="https://reader.lanbook.com/book/241076">https://reader.lanbook.com/book/241076</a> (дата обращения: 04.12.2024). - 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.miiit.ru>)
- Википедия (<https://ru.wikipedia.org>)
- Материалы по информационным технологиям ([www.citforum.ru](http://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 занятий лекционного типа, практических занятий, лабораторных работ.
- Аудиовизуальное оборудование для 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:



Курсовой проект 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, сети и  
информационная безопасность»

М.А. Давыдовский

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической  
комиссии

Н.А. Андриянова