

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: 16.03.2023

1. Общие сведения о дисциплине (модуле).

Целью преподавания дисциплины «Методы исследования защищенности объектов информатизации» является изучение методов и программных средств для анализа защиты информации. Студенты должны изучить основные уязвимости объектов информатизации, угрозы безопасности, методы анализа защищенности информационных систем, методы тестирования системы защиты, средства анализа защищенности объектов информатизации.

Основной целью изучения учебной дисциплины «Методы исследования защищенности объектов информатизации» является формирование компетенций в области анализа защищенности информационных систем, для следующих видов деятельности:

- научно-исследовательская;
- проектная.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

научно-исследовательская деятельность:

разработка планов проведения научных исследований и технических разработок;

подготовка по результатам научных исследований отчетов;

проектная:

разработка систем, комплексов, средств и технологий обеспечения информационной безопасности.

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	Сем. №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	Основные понятия защиты информации Рассматриваемые вопросы: - объекты защиты; - свойства информации; - виды защиты информации; - угрозы безопасности.
2	Создание динамических сайтов. Рассматриваемые вопросы: - разработка динамических страниц в среде Node; - передача данных по технологии Ajax.
3	Общая система оценки уязвимостей Рассматриваемые вопросы: понятие уязвимости; - база уязвимости CVE; - база уязвимости NVD; - база уязвимостей ФСТЭК России.
4	Методика анализа защищенности компании GlobalTrust Рассматриваемые вопросы: - методы исследования защищенности; - этапы работ по анализу защищенности; - тестирование системы защиты.
5	Сканер уязвимостей OWASP ZAP Рассматриваемые вопросы: - сканирование сайта; - информация об уязвимости; - просмотр сессий.
6	Уязвимость SQL-внедрение. Способы внедрения. Защита от SQL-внедрения Рассматриваемые вопросы: - получение несанкционированного доступа - изменение пароля администратора - методы защиты.

№ п/п	Тематика лекционных занятий / краткое содержание
7	<p>Работа с уязвимым приложением Damn Vulnerable NodeJS Application</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - структура приложения; - запуск приложения; - демонстрация уязвимостей.
8	<p>SQL-внедрение в приложении DVNA и методы защиты</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
9	<p>Недостатки аутентификации. Небезопасный сброс пароля</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
10	<p>Разглашение конфиденциальных данных</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
11	<p>Внешние сущности XML (XXE)</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
12	<p>Недостатки контроля доступа</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
13	<p>Некорректная настройка параметров безопасности</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
14	<p>Межсайтовое выполнение сценариев</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
15	<p>Небезопасная десериализация</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - описание уязвимости; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
16	<p>Использование компонентов с известными уязвимостями</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - описание уязвимостей; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.

№ п/п	Тематика лекционных занятий / краткое содержание
17	Недостатки журналирования и мониторинга Рассматриваемые вопросы: - описание уязвимостей; - уязвимый код приложения; - модификация кода с целью устранения уязвимости.
18	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
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 DVNA В результате практического занятия студент получает навык определения уязвимых мест в веб-приложении
7	Эксплуатация уязвимостей приложения DVNA В результате практического занятия студент получает навык выполнения запросов, эксплуатирующих имеющиеся уязвимости веб-приложения
8	Устранение уязвимостей приложения DVNA В результате практического занятия студент получает навык разработки веб-приложения, в котором отсутствуют уязвимости

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	Петькина Е.Д., Марченко Л.С. Возможные уязвимости хранения информации. Научный альманах. 2016. 11-2(25). с.210-212	https://elibrary.ru/item.asp?id=27703629 (дата обращения: 03.10.2022)

2	Михнев И.П., Петросян М.К., Новикова А.А. Основы информационной безопасности хозяйственной деятельности: угрозы безопасности и средства защиты систем обработки информации. Современные проблемы управления и регулирования. Наука и просвещение. 2018. с. 228-237	https://elibrary.ru/item.asp?id=35436319 (дата обращения: 03.10.2022)
3	Коноваленко С.А., Королев И.Д., Симонов А.В. Оценка существующих средств анализа защищенности информационных систем. Наука вчера, сегодня, завтра. 2016. 10(32). с. 6-15	http://elibrary.ru/item.asp?id=27174103 (дата обращения: 03.10.2022)
4	Богораз А.Г., Пескова О.Ю. Методика тестирования и оценки межсетевых экранов. Известия ЮФУ. Технические науки. 2013. 12(149). с. 148-156	https://elibrary.ru/item.asp?id=21032472 (дата обращения: 03.10.2022)
5	Плешков А.С., Рудер Д.Д. Тестирование на проникновение как анализ защищенности компьютерных систем. Известия алтайского государственного университета. 2015. 1-1(85). с. 174-181	https://elibrary.ru/item.asp?id=23024662 (дата обращения: 03.10.2022)
6	Сельвесюк Н.И., Островский А.С., Сливинский В.Д. Методология анализа защищенности автоматизированных систем обработки информации. Информатика и системы управления. 2016. 2(48). с. 17-24	http://elibrary.ru/item.asp?id=26181354 (дата обращения: 03.10.2022)
7	Богданов Н.В., Кротова Е.Л., Шабуров А.С. Методика противодействия атакам типа SQL INJECTION. Наука и бизнес: пути развития. 2015. № 6	http://elibrary.ru/item.asp?id=24066266 (дата обращения: 04.10.2022)
8	Давыдовский М.А. Разработка веб-сервисов: Учебное пособие. – М.: РУТ (МИИТ), 2020. – 111 с.	https://www.elibrary.ru/item.asp?id=45603698 (дата обращения: 04.10.2022)

б. 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 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, групповых и индивидуальных консультаций .

Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером. Аудитория подключена к интернету РУТ(МИИТ).

- Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ .

Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран, персональные компьютеры , монитеры, 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. Клычева