

**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 бакалавриата  
по направлению подготовки  
10.03.01 Информационная безопасность,  
утвержденной первым проректором РУТ (МИИТ)  
Тимониным В.С.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Безопасность компьютерных систем**

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

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: 13.03.2024

## 1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Безопасность компьютерных систем» являются формирование компетенций по основным разделам теоретических и практических основ безопасности компьютерных систем, получение опыта противодействия киберугрозам, практических навыков в различных областях информационной безопасности, таких как: анализ защищенности, расследование инцидента и устранение уязвимостей.

Основными задачами дисциплины являются:

- Изучение методов реверс-инжиниринга.
- Ознакомление со способами анализа действий злоумышленников.
- Ознакомление с методами устранения уязвимостей.
- Изучение методов защиты серверов с запущенными веб-приложениями от множественных атак.
- Изучение принципов выявления уязвимых мест путем атак.

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

Эксплуатационная деятельность:

- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;

Проектно-технологическая деятельность:

- сбор и анализ исходных данных для проектирования аппаратных средств защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;

Экспериментально-исследовательская деятельность:

- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств.

Организационно-управленческая деятельность:

- участие в совершенствовании системы управления информационной

безопасностью сетей и систем передачи информации;

- контроль эффективности реализации политики информационной безопасности сетей и систем передачи информации.

## 2. Планируемые результаты обучения по дисциплине (модулю).

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

**УК-1** - Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

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

### **Знать:**

- виды угроз информационной безопасности в современном обществе;
- принципы работы информационно-коммуникационных технологий,;
- программных средств системного и прикладного назначения

### **Уметь:**

-использовать информационные технологии с учетом угроз информационной безопасности для обеспечения объективных потребностей личности, общества и государства.

### **Владеть:**

-навыками оценки роли информации, информационных технологий и информационной безопасности в современном обществе;

- навыками применения информационно-коммуникационных технологий, программных средств системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.

## 3. Объем дисциплины (модуля).

### 3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 2 з.е. (72 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. №5
Контактная работа при проведении учебных занятий (всего):	32	32
В том числе:		
Занятия лекционного типа	16	16
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 40 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	<p>Тема 1. Реверс-инжиниринг в информационной безопасности. Рассматриваются вопросы построения процесса реверс-инжиниринга программного обеспечения на этапах дизассемблирования, декомпиляции, отладки.</p> <p>Тема 2 Анализ сетевого трафика. Рассматриваются вопросы анализа сетевого трафика с помощью технологии реверс-инжиниринга.</p> <p>Тема 3 Эксплуатация уязвимостей веб-приложения.</p>

№ п/п	Тематика лекционных занятий / краткое содержание
	<p>Рассматриваются вопросы возникновения уязвимостей и их распространения. Приводятся типовые уязвимости.</p> <p>Тема 4 Инструменты поиска уязвимостей. Рассматриваются принципы работы средств поиска уязвимостей на примере Wapiti, Nikto, Vega, SQLmap</p> <p>Тема 5 Использование HTTP-прокси для работы с трафиком. Рассматриваются вопросы использования HTTP-прокси для анализа трафика приложения и поиска особенностей в поведении приложения на низком уровне.</p> <p>Тема 6 Уязвимости веб-приложений IDOR. Рассматриваются вопросы локализации уязвимости Insecure Direct Object Reference (небезопасные прямые ссылки на объекты) при успешном получении доступа к странице, данным или файлу, доступа к которым у него быть не должно.</p> <p>Тема 7 Бинарные уязвимости. Рассматриваются вопросы возникновения бинарных уязвимостей, их вредоносное воздействие, примеры использования, методология и контрольный список для тестирования.</p> <p>Тема 8. Атаки на базы данных. Рассматриваются вопросы реализации атак на базы данных с помощью внедрения SQL-кода.</p>

#### 4.2. Занятия семинарского типа.

##### Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	<p>Практическое занятие 1. Реверс-инжиниринг. В результате выполнения работы студент получит навыки по проведению реверс-инжиниринга и выбору необходимых инструментов.</p> <p>Практическое занятие 2. В результате выполнения работы студент получит навыки по проведению анализа сетевого трафика с помощью технологии реверс-инжиниринга.</p> <p>Практическое занятие 3. Уязвимости веб-приложения. В результате выполнения работы студент получит понимание о возникновении уязвимостей веб-приложений, механизмах их распространения.</p> <p>Практическое занятие 4. Поиск уязвимостей веб-приложений.</p>

№ п/п	Тематика практических занятий/краткое содержание
	<p>В результате выполнения работы студент получит навыки по использованию различных инструментов поиска уязвимостей.</p> <p>Практическое занятие 5. В результате выполнения работы студент получит навыки по использованию HTTP-прокси в работе с сайтами с использованием Burp Suite и OWASP ZAP.</p> <p>Практическое занятие 6. В результате выполнения работы студент получит навыки по локализации уязвимости IDOR.</p> <p>Практическое занятие 7. В результате выполнения работы студент получит навыки по выявлению бинарных уязвимостей с помощью полезных нагрузок.</p> <p>Практическое задание 8. В результате выполнения работы студент получит навыки по выявлению уязвимостей в базы данных и их локализации.</p>

#### 4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим занятиям
3	Подготовка к промежуточной аттестации.

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

№ п/п	Библиографическое описание	Место доступа
1	<p>Информационная безопасность. Практические аспекты : учебник / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург : Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст : электронный // Лань : электронно-библиотечная система.</p>	<p><a href="https://e.lanbook.com/book/161340">https://e.lanbook.com/book/161340</a> (дата обращения: 10.03.2024).</p>
2	<p>Введение в информационную безопасность и защиту информации : учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск : НГТУ, 2017. — 132 с. — ISBN 978-5-7782-3233-4. — Текст : электронный // Лань : электронно-библиотечная система.</p>	<p><a href="https://e.lanbook.com/book/118219">https://e.lanbook.com/book/118219</a> (дата обращения: 29.02.2024)</p>

3	Чикунова, Н. Ф. Проектирование баз данных и организация их защиты в СУБД ACCESS : учебное пособие / Н. Ф. Чикунова. — Калининград : БГАРФ, 2019 — Часть 1 — 2019. — 106 с. — Текст : электронный // Лань : электронно-библиотечная система.	<a href="https://e.lanbook.com/book/160059">https://e.lanbook.com/book/160059</a> (дата обращения: 10.03.2024)
4	Введение в информационную безопасность: Учебное пособие для вузов / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатов. - Москва : Гор. линия-Телеком, 2011. - 288 с.: ил.; . - (Специальность). ISBN 978-5-9912-0160-5, 1000 экз. - Текст : электронный.	<a href="https://znanium.com/catalog/product/265558">https://znanium.com/catalog/product/265558</a> (дата обращения: 29.02.2024)
5	Бабушкин, В. М. Разработка защищенных программных средств информатизации производственных процессов предприятия : учебное пособие / В. М. Бабушкин. — Казань : КНИТУ-КАИ, 2020. — 256 с. — ISBN 978-5-7579-2463-2. — Текст : электронный // Лань : электронно-библиотечная система.	<a href="https://e.lanbook.com/book/193486">https://e.lanbook.com/book/193486</a> (дата обращения: 10.03.2024)
6	Аграновский, А. В. Тестирование веб-приложений : учебное пособие / А. В. Аграновский. — Санкт-Петербург : ГУАП, 2020. — 155 с. — ISBN 978-5-8088-1515-5. — Текст : электронный // Лань : электронно-библиотечная система	<a href="https://e.lanbook.com/book/216533">https://e.lanbook.com/book/216533</a> (дата обращения: 10.03.2024)

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

Научно-техническая библиотека РУТ(МИИТ) <http://library.miit.ru/>

Форум специалистов по информационным технологиям <http://citforum.ru/>

Интернет-университет информационных технологий <http://www.intuit.ru/>

Тематический форум по информационным технологиям <http://habrahabr.ru/>

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

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Компьютер должен быть

обеспечен лицензионными программными продуктами:

Microsoft Windows

Microsoft Office

Для проведения лабораторных работ необходимы персональные компьютеры с рабочими местами. Компьютер должен быть обеспечен лицензионными программными продуктами:

Microsoft Windows

Microsoft Office

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

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.

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

Рабочие станции для студентов, рабочая станция преподавателя, проектор, экран.

9. Форма промежуточной аттестации:

Зачет в 5 семестре.

10. Оценочные материалы.

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



Авторы:

заведующий кафедрой, доцент, к.н.  
кафедры «Вычислительные системы,  
сети и информационная  
безопасность»

Б.В. Желенков

Согласовано:

Заведующий кафедрой ВССиИБ  
Председатель учебно-методической  
комиссии

Б.В. Желенков

Н.А. Андриянова