

**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  
02.03.02 Фундаментальная информатика и  
информационные технологии,  
утвержденной первым проректором РУТ (МИИТ)  
Тимониным В.С.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Безопасность компьютерных систем**

Направление подготовки: 02.03.02 Фундаментальная информатика и  
информационные технологии

Направленность (профиль): Квантовые вычислительные системы и сети

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: 25.10.2024

## 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.

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

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

**ОПК-4** - Способен участвовать в разработке технической документации программных продуктов и комплексов с использованием стандартов, норм и правил, а также в управлении проектами создания информационных систем на стадиях жизненного цикла;

**ПК-8** - Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты и принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации.

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

### **Знать:**

- виды угроз информационной безопасности;
- принципы работы информационно-коммуникационных технологий;
- политики информационной безопасности
- стандарты, нормы и правила по разработке технической документации программных продуктов и комплексов

### **Уметь:**

- использовать информационные технологии с учетом угроз информационной безопасности
- разрабатывать техническую документацию программных продуктов и комплексов с использованием стандартов
- применять комплексный подход к обеспечению информационной безопасности объекта защиты.

**Владеть:**

- навыками управления проектами создания информационных систем на стадиях жизненного цикла
- навыками применения информационно-коммуникационных технологий, программных средств системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.
- навыками по организации и сопровождению аттестации объекта информатизации по требованиям безопасности информации.

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	Семестр №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>Реверс-инжиниринг в информационной безопасности</p> <p>Рассматриваются вопросы:</p> <ul style="list-style-type: none"> <li>- построения процесса реверс-инжиниринга программного обеспечения на этапах дизассемблирования, декомпиляции, отладки для решения задач по обеспечению политики информационной безопасности;</li> <li>- аттестации объекта информатизации по требованиям безопасности информации.</li> </ul>
2	<p>Анализ сетевого трафика</p> <p>Рассматриваются вопросы анализа сетевого трафика с помощью технологии реверс-инжиниринга.</p>
3	<p>Эксплуатация уязвимостей веб-приложения</p> <p>Рассматриваются вопросы возникновения уязвимостей и их распространения. Приводятся типовые уязвимости.</p>
4	<p>Инструменты поиска уязвимостей</p> <p>Рассматриваются принципы работы средств поиска уязвимостей на примере Wapiti, Nikto, Vega, SQLmap.</p>
5	<p>Использование HTTP-прокси для работы с трафиком</p> <p>Рассматриваются вопросы использования HTTP-прокси для анализа трафика приложения и поиска особенностей в поведении приложения на низком уровне.</p>
6	<p>Уязвимости веб-приложений IDOR</p> <p>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>
7	<p>Бинарные уязвимости</p> <p>Рассматриваются вопросы возникновения бинарных уязвимостей, их вредоносное воздействие, примеры использования, методология и контрольный список для тестирования</p>
8	<p>Атаки на базы данных</p> <p>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	Реверс-инжиниринг В результате выполнения работы студент получит навыки по проведению реверс-инжиниринга и выбору необходимых инструментов.
2	Реверс-инжиниринг(продолжение) В результате выполнения работы студент получит навыки по проведению анализа сетевого трафика с помощью технологии реверс-инжиниринга.
3	Уязвимости веб-приложения В результате выполнения работы студент получит понимание о возникновении уязвимостей веб-приложений, механизмах их распространения.
4	Поиск уязвимостей веб-приложений В результате выполнения работы студент получит навыки по использованию различных инструментов поиска уязвимостей.
5	Поиск уязвимостей веб-приложений(продолжение) В результате выполнения работы студент получит навыки по использованию HTTP-прокси в работе с сайтами с использованием Burp Suite и OWASP ZAP.
6	Поиск уязвимостей веб-приложений(продолжение) В результате выполнения работы студент получит навыки по локализации уязвимости IDOR.
7	Поиск уязвимостей веб-приложений(продолжение) В результате выполнения работы студент получит навыки по выявлению бинарных уязвимостей с помощью полезных нагрузок.
8	Поиск уязвимостей веб-приложений(продолжение) В результате выполнения работы студент получит навыки по выявлению уязвимостей в базы данных и их локализации.

#### 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	Информационная безопасность : учебное пособие / составители И. Б. Тесленко [и др.] ; под редакцией И. Б. Тесленко. — Владимир : ВлГУ, 2023. — 212 с. — ISBN 978-5-9984-1783-2. — Текст : электронный // Лань : электронно-библиотечная система.	<a href="https://e.lanbook.com/book/434282">https://e.lanbook.com/book/434282</a>

2	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.	<a href="https://e.lanbook.com/book/118219">https://e.lanbook.com/book/118219</a>
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>
4	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>

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).

- Microsoft Windows
- Microsoft Office
- Интернет-браузер (Yandex и др.)

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

- Учебная аудитория (Компьютерный класс) для проведения учебных

занятий (занятий лекционного типа, практических занятий):

- компьютер преподавателя, мультимедийное оборудование, рабочие станции студентов, доска.

Аудитория подключена к сети «Интернет».

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