МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по направлению подготовки
10.03.01 Информационная безопасность,
утвержденной первым проректором ФГАОУ ВО
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 ФГАОУ ВО РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 01.09.2026

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-6 - Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;

ОПК-7 - Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

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	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	Конфигурирование и настройка Microsoft Windows Server Рассматриваемые вопросы: - конфигурирование и настройка сервера - настройка сетевых параметров, параметров безопасности и производительности - модель логической организации сети «рабочая группа» - модель логической организации сети «домен», сравнительные характеристики
2	Логическая и физическая структура Active Directory Рассматриваемые вопросы: - структурные элементы Active Directory: объекты и их классы, домены, организационные подразделения, деревья, леса - физическая структура Active Directory: контроллер доменов, сайты - создание сетевого домена - оснастки консоли администрирования для работы с доменами
3	Управление объектами в Active Directory. Рассматриваемые вопросы: - учетные записи и политика именования - управление доменными учетными записями - управление организационными подразделениями - делегирование административных полномочий управления в подразделении
4	Администрирование сетевых служб DHCP, WINS и DNS Рассматриваемые вопросы: - служба DHCP автоматического конфигурирования TCP/IP - служба WINS разрешения символических имен узлов; конфигурирование и обслуживание службы - служба DNS разрешения доменных имен узлов; - схемы разрешения запросов на разрешение имен, конфигурирование службы
5	Механизмы безопасности MS Windows Server Рассматриваемые вопросы: - общая модель безопасности Windows Server, права, привилегии и разрешения доступа, встроенные и специальные группы - защита ресурсов с помощью прав доступа по сети, администрирование доступа к общим ресурсам - защита ресурсов разрешениями файловой системы NTFS, администрирование доступа с помощью разрешений NTFS - совместное применение прав сетевого доступа и разрешений файловой системы
6	Доменные структуры сети Рассматриваемые вопросы: - многодоменная модель организации сети, доверительные отношения между доменами - транзитивная аутентификация в многодоменной сети, реализация прав доступа в многодоменной сети - доменные модели: модель одиночного домена, модель с одним главным доменом, модель с

№ п/п	Тематика лекционных занятий / краткое содержание
	несколькими главными доменами, модель с полным доверием - иерархическая система доменов: деревья и леса
7	Отказоустойчивые и производительные дисковые конфигурации Рассматриваемые вопросы: - базовые конфигурации дисковых структур - технологии дисковых массивов (RAID) - характеристики RAID-технологии, уровни спецификаций - набор томов JBOD - чередующийся набор RAID0 - зеркальный набор RAID1 - чередующийся набор с четностью RAID5
8	Мониторинг событий безопасности сети Рассматриваемые вопросы: - политики аудита и управление аудитом, - настройки аудита для объектов файловой системы; анализ журнала безопасности - мониторинг производительности и процессов, - мониторинг сетевого трафика, сетевой монитор и его использование

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Создание виртуальных машин В результате выполнения работы студент получает практические навыки использования средств виртуализации, установки серверных ОС, создания виртуальной одноранговой сети, настройки сетевой идентификации и проверки сетевого взаимодействия
2	Конфигурирование сервера В результате выполнения работы студент получает практические навыки установки и конфигурирования параметров сервера, логической конфигурации сетевого домена, установка и настройки основных служб сетевой доменной инфраструктуры
3	Управление объектами Active Directory. В результате выполнения работы студент получает практические навыки создания и настройки доменных учетных записей пользователей и групп, настройки в домене парольной политики, перемещаемых профилей и сценариев входа пользователей в домен
4	Защита ресурсов сети с помощью разрешений общего доступа по сети. Защита ресурсов сети с помощью разрешений NTFS. В результате выполнения работы студент получает практические навыки настройки избирательного доступа пользователей домена к общему сетевому ресурсу, проверки эффективных разрешений в

№ п/п	Тематика практических занятий/краткое содержание
	комбинации личных и групповых сетевых разрешений, использования разрешений файловой системы для защиты доступа к файлам и каталогам
5	Многодоменные структуры сети В результате выполнения работы студент получает опыт создания многодоменной сети виртуальных узлов, настройки доверительных отношений между доменами, проверки действия доверительных отношений и закрепляет знания о механизмах действия разрешений общего доступа и разрешений файловой сиситемы в многодоменной сети
6	Дисковые массивы Raid5 и Raid0 В результате выполнения работы студент получает навыки конфигурации сервера с несколькими дисковыми накопителями, создания программного RAID-массива типа Raid5 и Raid0, проверки характеристик отказоустойчивости, создания программных массивов дисков типа Raid1 и Jbod и проверки их характеристики отказоустойчивости
7	Мониторинг событий сети В результате выполнения работы студент получает опыт использования средств аудита для наблюдения событий безопасности в сети, приобретает умения и навыки анализа сетевого трафика, использования штатных средств мониторинга производительности сети

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	Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/460715 (дата обращения: 18.03.2026)
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	https://e.lanbook.com/book/118219 (дата обращения: 30.04.2025)

	978-5-7782-3233-4. — Текст : электронный // Лань : электронно-библиотечная система.	
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.	https://e.lanbook.com/book/160059 (дата обращения: 30.04.2025)
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.	https://e.lanbook.com/book/193486 (дата обращения: 30.04.2025)
5	Раченко, Т. А. Информационная безопасность : учебно-методическое пособие / Т. А. Раченко. — Тольятти : ТГУ, 2024. — 135 с. — ISBN 978-5-8259-1612-5. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/427130 (дата обращения: 19.03.2026)
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	https://e.lanbook.com/book/216533 (дата обращения: 10.03.2026)

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).

- ОС Windows
- Microsoft Office

- Интернет-браузер (Yandex и др.)

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

-Учебная аудитория для проведения учебных занятий (занятий лекционного типа, практических занятий):

- компьютер преподавателя, рабочие станции студентов, мультимедийное оборудование, 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
и квантовые коммуникации» Б.В. Желенков

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова