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 РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Безопасность сетей

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем

Форма обучения: Очная

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:

- методы и алгоритмы проектирования распределенных информационных систем, их компоненты и протоколы взаимодействия;
- методы и алгоритмы проектирования распределенных информационных систем, их компоненты и протоколы взаимодействия.

Уметь:

- выбирать средства для проектирования систем, компоненты проектирования протоколы их связей;

-выбирать средства для проектирования систем, компоненты проектирования протоколы их связей.

Владеть:

- навыками выбора инструментальных средств разработки и обеспечения безопасности компьютерных сетей;
- навыками определения набора средств обеспечения безопасности;
- навыками выбора средств создания и ведения репозитория, учета инцидентов информационной безопасности, сборки и непрерывной интеграции, базы знаний;
- навыками организации процесса использования инфраструктуры;
- навыками мониторинга функционирования инфраструктуры;
- навыками принятия управленческих решений.

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 №6
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	Стандарты по опытной эксплуатации средств и систем защиты СССЭ от НСД и типы сетевых атак. Рассматриваемые вопросы: - безопасность информационных технологий; - методы и средства обеспечения безопасности, критерии оценки безопасности информационных технологий. - архитектура эшелонированой защиты сети; - классификация уязвимостей в сетях; - классификация атак в сетях; - механизмы и методы проведения сетевых атак с стеке протоколов TCP/IP.
2	Обеспечение безопасности на канальном уроне модели OSI и уровне интернет. Рассматриваемые вопросы: - сетевые анализаторы, «снифферы» и их обнаружение; - аутентификация на основе MAC-адресов; - уязвимости сетевого оборудования канального уровня. - фильтрация пакетов; - ограничение маршрутной информации; - фильтрация трафика ICMP; - фрагментация; - ARP Spoofing.
3	Обеспечение безопасности транспортного уровня Рассматриваемые вопросы: - сеансы протоколов TCP и UDP; - сканирование портов; - атаки UDP flood; - атаки SYN flood; - атаки TCP reset; - подмена участника TCP-соединения.
4	Обеспечение безопасности служб прикладного уровня.Протокол DHCP и DNS Рассматриваемые вопросы: - уязвимость протокола DHCP; - ложный DHCP-сервер; - защита от атак DHCP. - угрозы DNS-атак; - подмена DNS-ответа; - атаки типа DNS- flood; - защита от атак на DNS

№ п/п	Тематика лекционных занятий / краткое содержание
5	Безопасность трафика на прикладном уровне Рассматриваемые вопросы: - протоколы SSL/TLS, SSH; - атака типа «человек посередине».
6	Маршрутизация в виртуальных частных сетях с архитектурой клиент-сервер Рассматриваемые вопросы: - remote-access VPN. - Cisco Any Connect. - создание туннельного интерфейса. - использование Cisco ASA в качестве VPN-сервера.
7	Обеспечение безопасности сети с помощью АПКШ «Континент» Рассматриваемые вопросы: - задачи комплекса; - используемые средства защиты; - принципы работы. - размещение элементов АПКШ в сети; - состав аппаратной платформы АПКШ; - сравнение версий; - работа с ПАК «Соболь».
8	Обеспечение безопасности сети с помощью АПКШ «Континент».Конфигурирование АПКШ. Инициализация компонентов системы. Обеспечение безопасности сети с помощью АПКШ «Континент».Конфигурирование АПКШ. Инициализация компонентов системы. Рассматриваемые вопросы: - инициализация ЦУС и СД; - установка программы управления комплексом; - конфигурация базы данных и настройка агента ЦУС и СД; - инициализация КШ. - установка подсистемы управления; - настройка контроля целостности; - запуск подсистемы управления и подключение к ЦУС. Управление компонентами Рассматриваемые вопросы: - генерация главных ключей всех сетевых устройств; - генерация ключей для организации криптографической связи КШ. - смена ключей;

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Анализ сетевого трафика В результате выполнения работы студент получит практические навыки по анализу, передаваемой по сети, информации.

№ п/п	Тематика практических занятий/краткое содержание
	В результате выполнения работы студент получит практические навыки по анализу, передаваемой по сети, информации.
2	MAC-спуфинг. ARP-спуфинг В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостью «MAC-спуфинг» и «ARP-спуфинг»..
3	DHCP-спуфинг TCP-reset. В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостью «DHCP-спуфинг» и «TCP-reset»..
4	CiscoAnyConnect (Remote-accessVPN). В результате выполнения работы студент получит практические навыки по настройке Remote-accessVPN
5	Инициализация ЦУС и СД АПКШ «Континент» . Установка подсистемы управления комплексом АПКШ. Конфигурирование журналов баз данных. Настройка агента ЦУС и СД комплексом АПКШ. Конфигурирование журналов баз данных. Настройка агента ЦУС и СД В результате выполнения работы студент получит практические навыки по инициализации центра управления сетями и управления доступом и по установке подсистемы управления комплексом, конфигурированию журналов баз данных и настройке агента ЦУС и СД..
6	Инициализация КШ. Смена ключей КШ. Управление учетными записями администраторов В результате выполнения работы студент получит практические навыки по инициализации, по смене ключей и управлению учетными записями администраторов.КШ.
7	Правила фильтрации между компьютерами из защищаемой сети и сети общего доступа В результате выполнения работы студент получит практические навыки по конфигурированию правил фильтрации между компьютерами из защищаемой сети и сети общего доступа
8	Правила фильтрации между компьютерами из внутренних сетей, защищаемых разными криптошлюзами В результате выполнения работы студент получит практические навыки по конфигурированию правил фильтрации между компьютерами из внутренних сетей, защищаемых разными криптошлюзами

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 978-5-7782-3233-4. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/118219 (дата обращения: 30.04.2025)
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 6 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