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 специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором ФГАОУ ВО
РУТ (МИИТ) Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Основы построения защищенных компьютерных сетей

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе 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: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.09.2026

1. Общие сведения о дисциплине (модуле).

Целью изучения дисциплины «Основы построение защищенных компьютерных сетей» является теоретическая и практическая подготовка обучающихся к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.

Задачи дисциплины:

- изучение типовых угроз безопасности в компьютерных сетях;
- изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;
- овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-3 - Способен на основании совокупности математических методов, физических законов и моделей разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

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

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

Знать:

- Современные тенденции развития криптографических методов и средств, применяемых для защиты информации в компьютерных сетях.
- Методики мониторинга работоспособности и критерии оценки эффективности средств защиты информации в компьютерных сетях.
- Основные этапы исторического развития России и роль информационной безопасности в обеспечении национальных интересов.

- Нормативно-правовую документацию в области информационной безопасности, регламентирующую порядок аттестации объектов информатизации.

- Основные принципы управления информационной безопасностью компьютерных систем и методы оценки эффективности политик безопасности.

- Типовые неисправности и уязвимости программных, программно-аппаратных средств и подсистем защиты информации в сетях.

- Методы и средства реализации частных политик информационной безопасности, а также методики анализа эффективности систем защиты информации в компьютерных системах.

Уметь:

- Использовать средства криптографической защиты информации (VPN, IPSec, SSL/TLS) при решении задач обеспечения безопасности компьютерных сетей.

- Проводить мониторинг событий безопасности и анализировать эффективность функционирования средств защиты в компьютерных сетях.

- Анализировать исторические процессы и их влияние на формирование современных требований к защите информации.

- Проводить анализ информационной безопасности объектов и систем для подготовки к процедуре аттестации.

- Разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы.

- Выполнять работы по восстановлению работоспособности средств защиты информации (межсетевых экранов, СОВ, VPN-шлюзов) после сбоев.

- Реализовывать частные политики информационной безопасности и проводить мониторинг эффективности действующих систем защиты в компьютерных системах.

Владеть:

- Навыками применения криптографических протоколов для организации защищенного сетевого взаимодействия.

- Инструментальными средствами мониторинга эффективности штатных и дополнительных средств защиты компьютерных сетей.

- Навыками формирования гражданской позиции при решении задач обеспечения безопасности в профессиональной среде.

- Методами анализа информационной безопасности объектов информатизации на предмет соответствия требованиям защиты информации.

- Методами оценки эффективности действующих политик безопасности и управления информационной безопасностью компьютерной системы.

- Навыками тестирования и проверки работоспособности программно-аппаратных средств защиты информации в сетях.

- Методами и средствами мониторинга и анализа эффективности реализации систем защиты информации в компьютерных системах.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 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 №8
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	48	48

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 64 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	КС и их организация / Сетевые атаки. Рассматриваемые вопросы: - Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI.
2	Механизмы реализации атак в сетях TCP/IP. Рассматриваемые вопросы: - Методы сканирования портов. - Методы обнаружения пакетных снифферов. - Методы обхода МЭ.
3	Методы перехвата сетевых соединений в сетях TCP/IP. Рассматриваемые вопросы: - Технические меры защиты от сетевых атак. - Атаки направленные на сетевую инфраструктуру
4	Примеры сетевых атак в сетях TCP/IP. Рассматриваемые вопросы: - Технические меры защиты от сетевых атак - Принуждение к ускоренной передаче. - Атаки, направленные на отказ в обслуживании. - Изменение конфигурации и состояния хостов. - Программно-технические меры защиты от сетевых атак
5	Криптографические методы защиты информации в компьютерных сетях. Рассматриваемые вопросы: - Криптографические протоколы обеспечения безопасности. - Протоколы аутентификации на прикладном уровне. - Протокол Kepberos. - Протоколы аутентификации на транспортном уровне: протокол SSI/TLS
6	Защита виртуальных частных сетей (VPN). Рассматриваемые вопросы: - Назначение, основные возможности и варианты реализации VPN. - Достоинства и недостатки применения VPN - Протокол IPSEC/ Протоколы AH и ESP. - Использование протокола L2TP для организации виртуальных частных сетей.
7	Разработка защищенных сетевых приложений. Рассматриваемые вопросы: - Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. - Программный интерфейс Open SSI.
8	Программно-аппаратные средства обеспечения безопасности в компьютерных сетях. Рассматриваемые вопросы: - Средства защиты локальных сетей при подключении к Интернет. - Место и роль МЭ в обеспечении сетевой безопасности. - Основные возможности и схемы развертывания МЭ
9	Методы сетевой трансляции адресов (NAT). Рассматриваемые вопросы: - Построение правил фильтрации. - Реализация сетевой политики безопасности с использованием МЭ. - Методы обхода межсетевых экранов

№ п/п	Тематика лекционных занятий / краткое содержание
10	Защита серверов и рабочих станций. Рассматриваемые вопросы: - Системы обнаружения вторжений (СОВ). - Место и роль СОВ в общей системе обеспечения сетевой безопасности. - Классификация СОВ.
11	Средства и методы предотвращения в обнаружении вторжений. Рассматриваемые вопросы: - Выявление атак на основе сигнатур атак и выявление аномалий. - Аудит прикладных служб. - Средства обнаружения уязвимостей сетевых служб. - Системы виртуальных ловушек (Honey Pot и Paded Geet).

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Средства проведения атак В результате выполнения лабораторной работы студент рассматривает основные инструментальные средства проведения атак.
2	Сети TSP/IP В результате выполнения лабораторной работы студент изучает методы и средства перехвата в сетях TSP/IP.
3	Меры защиты от сетевых атак В результате выполнения лабораторной работы студент рассматривает технические меры защиты от сетевых атак.
4	VPN с использованием IPSEC В результате выполнения лабораторной работы студент рассматривает особенности развертывания VPN с использованием IPSEC.
5	Программный интерфейс SSPI В результате выполнения лабораторной работы студент рассматривает особенности обеспечения целостного с использованием программного интерфейса SSPI
6	VPN базовыми средствами ОС Linux В результате выполнения лабораторной работы студент получает навык развертывания VPN базовыми средствами ОС Linux с использованием L2TP.
7	Пакетный фильтр ОС Linux iptables. В результате выполнения лабораторной работы студент отрабатывает умение по настройке и использование встроенного пакетного фильтра ОС Linux iptables.
8	Прокси-сервер SQUID В результате выполнения лабораторной работы студент учится настроивать и использовать прокси-сервера SQUID.
9	Средства обнаружения вторжений Snort В результате выполнения лабораторной работы студент отрабатывает умение по использованию и настройке средств обнаружения вторжений Snort.
10	Анализ сетевого трафика средствами tcpdump и Wireshark В результате работы студент умеет захватывать и фильтровать сетевой трафик, анализировать заголовки TCP/IP, выявлять признаки подозрительной активности и оформлять результаты анализа.

№ п/п	Наименование лабораторных работ / краткое содержание
11	Сканирование сети и поиск уязвимостей средствами Nmap и OpenVAS В результате работы студент умеет проводить инвентаризацию сетевых узлов, сканировать порты и службы, интерпретировать результаты сканирования уязвимостей и формировать рекомендации по их устранению.
12	Развертывание VPN на основе OpenVPN В результате работы студент умеет настраивать сервер и клиент OpenVPN, создавать и использовать сертификаты и ключи, проверять установление защищенного туннеля и диагностировать параметры подключения.
13	Анализ защищенности веб-приложений В результате работы студент умеет выявлять основные уязвимости веб-приложений (такие как SQL-инъекции и XSS), использовать инструменты вроде Burp Suite и OWASP ZAP, а также разрабатывать меры по их устранению.
14	Аудит стойкости паролей и хэшей В результате работы студент умеет извлекать хэши паролей из различных систем, применять словари и правила мутации с использованием утилит Hashcat и John the Ripper, а также оценивать надежность корпоративных парольных политик.
15	Защита и аудит беспроводных сетей Wi-Fi В результате работы студент умеет перехватывать рукопожатия (handshakes) в сетях стандартов WPA2/WPA3, проводить аудит их криптостойкости с помощью Aircrack-ng и настраивать безопасные методы аутентификации (например, WPA-Enterprise).
16	Анализ безопасности Active Directory В результате работы студент умеет проводить разведку в доменной сети, выявлять ошибки конфигураций прав доступа, использовать инструменты вроде BloodHound для поиска путей повышения привилегий и предлагать меры защиты контроллеров домена.
17	Развертывание и анализ систем класса SIEM В результате работы студент умеет настраивать централизованный сбор и корреляцию логов безопасности, создавать собственные правила алертинга для выявления инцидентов и расследовать кибератаки на основе агрегированных данных.
18	Компьютерная форензика и анализ артефактов ОС В результате работы студент умеет создавать и анализировать образы жестких дисков и дампы оперативной памяти, извлекать скрытые артефакты (реестр, журналы событий) для реконструкции хронологии инцидента информационной безопасности.
19	Анализ вредоносного ПО в изолированной среде В результате работы студент умеет разворачивать безопасные песочницы (sandbox), проводить статический и динамический анализ подозрительных файлов, выявлять сетевые индикаторы компрометации (IOC) и поведенческие паттерны вредоносов.
20	Развертывание и использование сетевых ловушек (Honeypots) В результате работы студент умеет устанавливать и настраивать интерактивные и неинтерактивные ловушки (например, Cowrie или Dionaea), анализировать тактики, техники и процедуры (TTP) злоумышленников на основе собранных логов.
21	Безопасность сред контейнеризации В результате работы студент умеет проводить аудит безопасности образов Docker, выявлять уязвимости конфигураций оркестраторов, настраивать жесткую изоляцию контейнеров и предотвращать попытки побега (container escape) из изолированной среды.
22	Моделирование фишинговых атак и защита электронной почты В результате работы студент умеет разворачивать инфраструктуру для тестового фишинга (например, с помощью GoPhish), анализировать восприимчивость пользователей к социальной инженерии и настраивать почтовые фильтры аутентификации (SPF, DKIM, DMARC).

№ п/п	Наименование лабораторных работ / краткое содержание
23	Стеганография и методы скрытия данных В результате работы студент умеет применять методы сокрытия информации в аудио-, видео- и графических файлах, а также использовать инструменты стеганоанализа для обнаружения фактов нелегитимной передачи данных по открытым каналам.
24	Аудит безопасности облачных инфраструктур В результате работы студент умеет анализировать конфигурации IAM (Identity and Access Management), выявлять публично доступные хранилища данных, оценивать настройки групп безопасности и применять best practices для защиты облачных сред.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к лабораторным работам.
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1) Технология SIEM и ее функциональные возможности. Преимущества и недостатки по сравнению с другими решениями.

2) Сетевые пакетные фильтры и их разновидности.

3) Посредники и особенности их применения для сетевой защиты.

4) Технология NAT и варианты ее развития

5) Сеансовый посредник SoC и специфика его применения

6) Инспекторы состояния как инструмент фильтрации для обеспечения требуемого уровня ИБ.

7) Обеспечение межсетевой защиты ресурсов посредством UTM-устройств и NG firmware

8) Виртуальные частные сети и наиболее часто используемые протоколы VPN

9) Характеристика и архитектура протокола IPsec.

10) Системы обнаружения вторжений структуры и принципы построения

11) Сравнительный анализ систем обнаружения вторжений и для сетевой безопасности

12) DLP-системы и их возможности. Анализ часто применяемых DLP-систем.

13) Сетевые сканеры уязвимостей, как средства анализа защищенности сетей

14) Ловушки, как средство сбора информации о злоумышленнике.

15) Защита локальных вычислительных сетей от атак канального уровня

16) Защита информации от ПЭМИН

17) Обеспечение аутентификации пользователей и разграничение доступа к информационным ресурсам

18) Обеспечение защиты информационных ресурсов компании от сетевых атак

19) Построение систем безопасности сетевого уровня на базе протокола IPSec

20) Построение отказоустойчивой ЛВС на базе протокола STP

21) Защита рабочих станций сети от вредоносного ПО и несанкционированных действий сотрудников

22) Защита информации и конфиденциальных данных, передаваемых по e-mail

23) Система обнаружения вторжений RealSecure

24) Управление ключами в вычислительных системах

25) Инструментальные средства предотвращения сетевых атак

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

№ п/п	Библиографическое описание	Место доступа
1	Компьютерные сети Ракитин Р. Ю., Москаленко Е. В. Учебное пособие Алтайский государственный педагогический университет, - 340 с. - ISBN 978-5-.88210-942-3 , 2019	https://reader.lanbook.com/book/139182
2	Сетевые технологии Васин Н.Н. Учебник Самара, ПГУПИ, - 265 с. , 2019	https://reader.lanbook.com/book/223364#2

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

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

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

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

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

Microsoft Internet Explorer (или другой браузер).

Microsoft Office.

Распространяемая система виртуализации Virtual Box.

Операционная система Linux.

Свободно распространяемый пакетный фильтр iptables.

Свободно распространяемый прокси-сервер SQUID.

Свободно распространяемые ПО для организации виртуальных сетей OPEN VPN.

Свободно распространяемая система обнаружения вторжений Snort.

Свободно распространяемый сервер удаленного доступа OPENSSH.

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

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Курсовая работа в 8 семестре.

Экзамен в 8 семестре.

10. Оценочные материалы.

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

Авторы:

профессор, профессор, д.н. кафедры «Интеллектуальное управление и информационная безопасность в высокоавтоматизированных транспортных системах» Института железнодорожного транспорта М.Я. Клепцов

Согласовано:

Заведующий кафедрой ИУиИБ Л.А. Баранов

Председатель учебно-методической комиссии Н.А. Андриянова