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
11.03.02 Инфокоммуникационные технологии и системы связи,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Технологии киберзащиты в современных сетях

Направление подготовки: 11.03.02 Инфокоммуникационные технологии и системы связи

Направленность (профиль): Системы мобильной связи и сетевые технологии на транспорте

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: 167783
Подписал: руководитель образовательной программы Киселёва Анастасия Сергеевна
Дата: 25.06.2026

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Технологии киберзащиты в современных сетях» является формирование у обучающихся компетенций в соответствии с требованиями образовательного стандарта базового высшего образования по направлению подготовки «Инфокоммуникационные технологии и системы связи».

Задачами дисциплины являются:

- ознакомление обучающихся с архитектурой, принципами построения и эволюцией систем защиты информации в современных телекоммуникационных и инфокоммуникационных сетях;
- изучение современных методов и средств криптографической защиты данных, аутентификации, управления доступом и обеспечения конфиденциальности в гетерогенных сетевых средах;
- освоение технологий защиты сетевого и транспортного уровней, включая конфигурирование межсетевых экранов (NGFW), систем обнаружения и предотвращения вторжений (IDS/IPS), а также механизмов безопасной маршрутизации и коммутации;
- формирование практических навыков развертывания систем мониторинга информационной безопасности, анализа защищенности сетей, выявления уязвимостей и автоматизированного реагирования на инциденты (SIEM/SOC);
- приобретение умений по обеспечению кибербезопасности специализированных сегментов, включая системы мобильной связи (4G/5G), беспроводные сети доступа, IoT-устройства и транспортные инфокоммуникационные системы;
- развитие компетенций в области нормативно-правового регулирования информационной безопасности, защиты критической информационной инфраструктуры (КИИ) и применения современных концепций (Zero Trust, SASE) в корпоративных сетях связи.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-12 - Способен осуществлять руководство группой специалистов, обеспечивающих функционирование инфокоммуникационных систем и/или их составляющих;

УК-3 - Способен организовать работу команды для достижения поставленной цели.

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

Знать:

- архитектуру и современные стандарты защиты инфокоммуникационных систем, включая транспортные и мобильные сегменты, а также нормативные требования к кибербезопасности и защите критической информационной инфраструктуры (КИИ);
- принципы организации работы команд информационной безопасности, регламенты управления уязвимостями и процессы реагирования на инциденты (Incident Response) в условиях непрерывной эксплуатации сетей.

Уметь:

- планировать и координировать действия группы специалистов по развертыванию и эксплуатации средств сетевой защиты, систем мониторинга (SIEM/SOC) и механизмов Zero Trust в гетерогенных средах;
- организовывать процессы аудита безопасности, оценки рисков и управления инцидентами, обеспечивая отказоустойчивость и непрерывность функционирования транспортных и мобильных инфокоммуникационных систем.

Владеть:

- методиками технического руководства и распределения задач при внедрении NGFW, IDS/IPS и систем оркестрации безопасности (SOAR) на объектах транспортной отрасли;
- навыками разработки стратегий кибербезопасности, нормативно-технической документации и организации учений по реагированию на кибератаки для подчиненных подразделений и команд эксплуатации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 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 №7
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	16	16
Занятия семинарского типа	32	32

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 60 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	Введение в кибербезопасность сетей связи. Рассматриваемые вопросы: - эволюция угроз, архитектура современных систем защиты, модель «эшелонированной обороны», стандарты ISO 27001, NIST, требования регуляторов РФ (ФСТЭК, ФСБ).
2	Криптографические методы защиты информации. Рассматриваемые вопросы: - симметричные и асимметричные шифры, электронная подпись, PKI-инфраструктура, сертификаты, хеширование, протоколы TLS/SSL и их применение в сетях связи.
3	Межсетевые экраны нового поколения (NGFW). Рассматриваемые вопросы: - архитектура, типы фаерволов (packet-filter, stateful, proxy, NGFW), политики безопасности, глубокий анализ пакетов (DPI), интеграция с каталогами пользователей.
4	Системы обнаружения и предотвращения вторжений (IDS/IPS). Рассматриваемые вопросы: - сигнатурный и поведенческий анализ, сетевые и узловые IDS/IPS, методы обхода защиты, интеграция с фаерволами, современные решения (Snort, Suricata).
5	Защита транспортной и сетевой инфраструктуры. Рассматриваемые вопросы: - защита транспортной и сетевой инфраструктуры. Безопасность протоколов маршрутизации (OSPF,

№ п/п	Тематика лекционных занятий / краткое содержание
	BGP), защита MPLS/SD-WAN, механизмы аутентификации соседей, предотвращение атак на плоскость управления.
6	Кибербезопасность беспроводных и мобильных сетей. Рассматриваемые вопросы: - угрозы в Wi-Fi (WPA2/WPA3), защита корпоративного беспроводного доступа (802.1X, RADIUS). Специфика уязвимостей сетей 4G/5G, сигнальные атаки (SS7, Diameter).
7	Защита IoT и транспортных инфокоммуникационных систем. Рассматриваемые вопросы: - угрозы для промышленных и транспортных сетей (ICS/SCADA), сегментация IoT-сегментов, безопасность подвижных объектов, телематических и спутниковых каналов.
8	SIEM/SOC, Zero Trust и нормативное регулирование. Рассматриваемые вопросы: - архитектура центра управления безопасностью, сбор и корреляция логов, концепция Zero Trust (SASE), защита критической информационной инфраструктуры (КИИ), организация работы команды ИБ.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Развертывание лабораторной среды для отработки навыков ИБ. Рассматриваемые вопросы: - установка GNS3/EVE-NG/Packet Tracer, подготовка топологии корпоративной сети, базовое харденирование устройств (пароли, SSH, отключение неиспользуемых сервисов).
2	Контроль доступа на канальном и сетевом уровнях. Рассматриваемые вопросы: - настройка расширенных ACL, Port Security, защита от ARP-spoofing (Dynamic ARP Inspection), DHCP snooping, IP Source Guard на управляемых коммутаторах.
3	Конфигурация межсетевого экрана (NGFW). Рассматриваемые вопросы: - создание зон безопасности, базовых политик доступа, настройка NAT (SNAT/DNAT), ведение журналов соединений, анализ логов фаервола.
4	Расширенные функции NGFW и DPI. Рассматриваемые вопросы: - фильтрация трафика по приложениям, пользователям и URL-категориям, настройка антивирусной защиты и защиты от эксплойтов, интеграция с Active Directory/LDAP.
5	Развертывание и настройка IDS/IPS. Рассматриваемые вопросы: - установка Snort/Suricata в сетевой сегмент, написание пользовательских правил (Snort rules), настройка режимов обнаружения и предотвращения, тестирование на синтетических атаках.
6	Анализ сетевого трафика и выявление аномалий. Рассматриваемые вопросы: - работа с Wireshark: фильтрация, разбор заголовков, поиск признаков сканирования портов, DNS-туннелирования, эксфильтрации данных и вредоносной активности.
7	Организация защищенных VPN-туннелей (site-to-site). Рассматриваемые вопросы:

№ п/п	Тематика практических занятий/краткое содержание
	- настройка IPsec VPN между удаленными филиалами, выбор алгоритмов шифрования (IKEv2, AES-GCM), обмен ключами, тестирование отказоустойчивости туннеля.
8	Безопасный удаленный доступ сотрудников. Рассматриваемые вопросы: - развертывание SSL/TLS VPN, настройка многофакторной аутентификации (MFA), политик доступа по принципу наименьших привилегий, контроль конечных точек.
9	Защита протоколов динамической маршрутизации. - настройка аутентификации OSPF (MD5/SHA) и BGP (TCP MD5/TCP-AO), защита от инъекций ложных маршрутов, анализ устойчивости к BGP-hijacking.
10	Безопасность беспроводной инфраструктуры. Рассматриваемые вопросы: Настройка WPA3-Enterprise, развертывание RADIUS-сервера, конфигурация 802.1X с различными методами EAP, обнаружение rogue-точек доступа.
11	Анализ защищенности мобильных сетей 4G/5G. Моделирование сигнальных атак в эмуляторе, анализ уязвимостей абонентского оборудования, настройка IPsec между базовыми станциями и ядром сети (X2/N3 интерфейсы).
12	Сегментация и защита IoT-сегмента. Рассматриваемые вопросы: - выделение изолированного VLAN для IoT-устройств, настройка микросегментации, контроль горизонтальных соединений, мониторинг аномальной активности датчиков.
13	Развертывание SIEM-системы. Рассматриваемые вопросы: - установка Wazuh/ELK Stack, настройка сбора логов с фаерволов, маршрутизаторов, серверов и конечных точек, нормализация событий, визуализация в дашбордах.
14	Корреляция событий и реагирование на инциденты. Рассматриваемые вопросы: - создание правил корреляции в SIEM, настройка алертов на типовые атаки (brute-force, DDoS, перемещение злоумышленника), отработка сценариев Incident Response.
15	Автоматизация реагирования (SOAR) и Threat Intelligence. Рассматриваемые вопросы: - интеграция внешних источников данных об угрозах (TI-feeds), написание плейбуков автоматического блокирования IOC, оркестрация действий между средствами защиты.
16	Комплексный аудит безопасности сети. Рассматриваемые вопросы: - проведение сканирования уязвимостей (Nmap, OpenVAS), анализ результатов, подготовка отчета с рекомендациями для руководства, формирование плана устранения недостатков и дорожной карты развития системы защиты.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к текущему контролю.
2	Подготовка к практическим занятиям
3	Подготовка к промежуточной аттестации.
4	Работа с лекционным материалом, литературой, самостоятельное изучение разделов (тем) дисциплины(модуля)

5	Подготовка к промежуточной аттестации.
6	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Калмыков И. А. [и др.] Криптографические методы защиты информации : учебное пособие. — Ставрополь : СКФУ, 2015.	e.lanbook.com/book/111765
2	Воробьев С. П., Широбокова С. Н., Литвяк Р. К. Компьютерные сети и сетевая безопасность : учебное пособие. — Новочеркасск : ЮРГПУ (НПИ), 2022.	e.lanbook.com/book/292247
3	Корниенко А. А., Корниенко С. В. Риск-модели информационной безопасности : учебное пособие. — Ставрополь : СКФУ, 2016.	e.lanbook.com/book/191006

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

Информационный портал Научная электронная библиотека eLIBRARY.RU (www.elibrary.ru);

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

Поисковые системы «Яндекс» для доступа к тематическим информационным ресурсам;

Электронно-библиотечная система издательства «Лань» – http://e.lanbook.com/;

https://www.reddit.com/ - международное сообщество сетевых инженеров;

https://tryhackme.com/ - сетевая безопасность, анализ трафика, основы администрирования;

https://www.virtualbox.org/ - запуск виртуальных машин для лабораторных работ;

https://www.wireshark.org/ - анализ сетевого трафика, разбор пакетов;

https://www.netdata.cloud/ - мониторинг производительности сетей и серверов;

https://man7.org/linux/man-pages/ - справка по командам и системным вызовам;

https://habr.com/ru/hub/network/ - статьи практиков: от базовых концепций до сложных кейсов;

https://adminvps.ru/blog/ - практические руководства по администрированию.

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

Программное обеспечение для выполнения практических заданий включает в себя программные продукты общего применения: операционная система Windows, Microsoft Office 2003 и выше, Браузер Internet Explorer 8.0 и выше с установленным Adobe Flash Player версии 10.3 и выше, Adobe Acrobat

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

Для проведения аудиторных занятий и самостоятельной работы требуется:

1. Рабочее место преподавателя с персональным компьютером, подключённым к сети INTERNET.
2. Специализированная лекционная аудитория с мультимедиа аппаратурой и проектором.
3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сети INTERNET
4. Для проведения практических занятий: компьютерный класс

9. Форма промежуточной аттестации:

Зачет в 7 семестре.

10. Оценочные материалы.

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

Авторы:

руководитель образовательной программы А.С. Киселёва

Согласовано:

Директор Д.В. Паринов

Руководитель образовательной программы А.С. Киселёва

Председатель учебно-методической комиссии Д.В. Паринов