МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
специализированного высшего образования
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Телекоммуникационное оборудование защищенных сетей

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Телекоммуникационное оборудование защищенных сетей» являются обучение принципам построения и эксплуатации различных телекоммуникационных сетей и систем за счет изучения современных телекоммуникационных технологий и технических средств. А также приобретение студентами необходимого объема знаний в области обеспечения безопасности телекоммуникационных сетей и систем, архитектуры беспроводных сетей, стандартов и механизмов защиты, используемых для защиты информации в телекоммуникационных сетях и системах.

Основными задачами дисциплины являются:

- ознакомление основными видами телекоммуникационного оборудования;
- рассмотрение протоколов взаимодействия телекоммуникационного оборудования;
- изучение особенностей использования протокола OSPF;
- изучение особенностей использования протокола BGP;
- изучение основных принципов и подходов к защите информации в разнотипных телекоммуникационных сетях и системах.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-6 - Способность выбирать и применять технические средства защиты информации и обеспечивать их функционирование.

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

Знать:

-виды телекоммуникационных сетей связи;

-основные угрозы безопасности информации в телекоммуникационных сетях связи;

-методы и алгоритмы обеспечения безопасности информации в телекоммуникационных сетях связи;

-основные параметры каналов телекоммуникационных сетей связи;

- технические концепции построения различных телекоммуникационных сетей связи;

-способы организации каналов, доступов в телекоммуникационных сетях связи.

Уметь:

-рассчитывать и выбирать основные параметры аппаратуры телекоммуникационной связи, исходя из требований к качеству канала; эксплуатировать оборудование телекоммуникационных сетей;

-осуществлять выбор оборудования и программного обеспечения для построения защищенных телекоммуникационных сетей связи;

- интегрировать телекоммуникационные сети связи в сетевую инфраструктуру предприятия, учитывая все аспекты обеспечения ее безопасности;

-осуществлять мониторинг телекоммуникационных сетей.

Владеть:

-навыками расчета и выбора основных параметров аппаратуры телекоммуникационной связи, исходя из требований к качеству канала;

-навыками эксплуатации оборудования телекоммуникационных сетей;

- навыками выбора оборудования и программного обеспечения для построения защищенных телекоммуникационных сетей связи;

-навыками интеграции телекоммуникационных сетей связи в сетевую инфраструктуру предприятия, учитывая все аспекты обеспечения ее безопасности; принципами мониторинга телекоммуникационных сетей.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 6 з.е. (216 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 №3
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 184 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	Основы телекоммуникационного оборудования: классификация и назначение — Понятие телекоммуникационного оборудования и его роль в защищённых сетях. — Классификация оборудования по функциональному назначению: активное, пассивное, вспомогательное. — Основные требования к оборудованию в защищённых сетях: надёжность, отказоустойчивость, соответствие стандартам безопасности. — Нормативная база: ГОСТ, ФСТЭК, ФСБ, требования к сертифицированному оборудованию.
2	Активное телекоммуникационное оборудование и его защита — Виды активного оборудования: коммутаторы, маршрутизаторы, межсетевые экраны, шлюзы безопасности. — Функции и особенности работы в защищённых сегментах сети. — Механизмы аутентификации и авторизации пользователей на сетевом оборудовании. — Настройка безопасных протоколов управления (SSH, SNMPv3, HTTPS) и отключение небезопасных (Telnet, HTTP).
3	Пассивное оборудование и его роль в обеспечении защищённости сети Пассивное оборудование и его роль в обеспечении защищённости сети — Состав пассивного оборудования: кабели, патч?панели, розетки, кроссовые шкафы, стойки. — Влияние качества пассивного оборудования на защищённость канала передачи данных. — Способы маркировки и учёта кабельных линий для предотвращения несанкционированного подключения. — Физическая защита пассивного оборудования: запираемые шкафы, системы контроля доступа.
4	Межсетевые экраны и системы обнаружения вторжений (IDS/IPS) — Типы межсетевых экранов: пакетные фильтры, шлюзы сеансового уровня, прикладные шлюзы. — Принципы работы и архитектура IDS/IPS.

№ п/п	Тематика лекционных занятий / краткое содержание
	— Правила фильтрации трафика и сигнатурный анализ атак. — Практические примеры настройки политик безопасности и реагирования на инциденты.
5	Оборудование для криптографической защиты каналов связи — Шифраторы канального и сетевого уровня: назначение и принципы работы. — VPN?шлюзы и их роль в построении защищённых виртуальных сетей. — Протоколы шифрования: IPsec, TLS, DTLS, их сравнительная характеристика. — Управление ключами шифрования: генерация, распределение, хранение, смена ключей.
6	Системы мониторинга и управления сетевой инфраструктурой — Средства централизованного управления сетевым оборудованием (Cisco Prime, HP IMC, Zabbix). — Логирование событий безопасности и анализ журналов (SIEM?системы). — Мониторинг сетевого трафика: NetFlow, sFlow, IPFIX. — Автоматизация реагирования на инциденты: интеграция IDS/IPS с системами управления.
7	Оборудование защищённой беспроводной связи — Точки доступа с поддержкой стандартов WPA3, 802.1X, RADIUS?аутентификации. — Контроллеры беспроводных сетей и их функции в защищённой среде. — Методы защиты Wi?Fi: изоляция гостевых сетей, сегментация трафика, контроль MAC?адресов. — Обнаружение неавторизованных точек доступа и подавление атак типа «злой двойник» (Evil Twin).
8	Отказоустойчивость и резервирование телекоммуникационного оборудования — Принципы построения отказоустойчивых сетей: дублирование каналов, кластеризация, горячее резервирование. — Технологии обеспечения непрерывности связи: VRRP, HSRP, GLBP. — Резервирование питания: ИБП, дизель?генераторы, источники бесперебойного питания с защитой от помех. — Планирование аварийного восстановления (DRP): схемы переключения, тестирование резервных каналов, регламентные процедуры.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Изучение видов активного телекоммуникационного оборудования защищённых сетей В результате выполнения работы студент получит навыки анализа видов активного оборудования (маршрутизаторов, коммутаторов, межсетевых экранов, шлюзов безопасности), научится определять их функциональные возможности и оценивать соответствие требованиям защищённости.
2	Изучение видов пассивного телекоммуникационного оборудования и его роли в защите сети В результате выполнения работы студент получит навыки анализа пассивного оборудования (кабелей, патч?панелей, розеток, кроссовых шкафов), научится оценивать его влияние на защищённость канала передачи данных.

№ п/п	Наименование лабораторных работ / краткое содержание
3	Изучение оборудования криптографической защиты каналов связи В результате выполнения работы студент получит навыки анализа устройств шифрования (шифраторов канального уровня, VPN?шлюзов), научится сопоставлять их характеристики и выбирать оптимальные решения.
4	Изучение беспроводного телекоммуникационного оборудования с функциями защиты В результате выполнения работы студент получит навыки анализа точек доступа, контроллеров Wi?Fi и сопутствующих устройств с поддержкой механизмов защиты.
5	Изучение систем мониторинга и управления сетевой инфраструктурой В результате выполнения работы студент получит навыки анализа средств централизованного управления и мониторинга (SIEM, NetFlow, Zabbix), научится выявлять аномалии в сетевом трафике.
6	Изучение отказоустойчивого телекоммуникационного оборудования В результате выполнения работы студент получит навыки анализа решений для обеспечения непрерывности связи (резервирование каналов, кластеризация, ИБП).
7	Изучение межсетевых экранов и систем обнаружения вторжений (IDS/IPS) Изучение межсетевых экранов и систем обнаружения вторжений (IDS/IPS) В результате выполнения работы студент получит навыки анализа типов межсетевых экранов (пакетные фильтры, шлюзы сеансового уровня, прикладные шлюзы) и IDS/IPS, научится настраивать политики безопасности.
8	Комплексное изучение телекоммуникационного оборудования в защищённой сети В результате выполнения работы студент получит навыки системного анализа всего комплекса оборудования (активного, пассивного, криптографического, мониторингового), научится оценивать общую защищённость инфраструктуры.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к лабораторным работам
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа

1	ГолдовскийЯ.М. ,Желенков Б.В. Маршрутизация в IP-сетях: учеб. пособие для студ. 4 курса спец. Вычислительные машины, комплексы, системы и сети по дисц. Сети ЭВМ и телекоммуникации. - М.: МИИТ, 2007. - 150 с.	https://library.miit.ru/miitpublishing/04-35219.pdf (дата обращения 25.02.2026) 681.3 Г60
2	ГолдовскийЯ.М., Желенков Б.В., Цыганова Н.А. Маршрутизация в компьютерных сетях : учеб. пособие по дисц. "Сети и телекоммуникации" для студ. напр. "Информатика и вычислительная техника"- М. : РУТ(МИИТ), 2017. - 114 с.	https://library.miit.ru/bookscatalog/metod/DC-407.pdf (дата обращения 25.02.2026) 681.3 Г60
3	Желенков Б.В. Основы сетевых технологий. Физический уровень: Метод. указ. к лаб. раб. по дисц. Сети ЭВМ и телекоммуникации для студ. IV курса спец. Вычислительные машины, комплексы, системы и сети. - М.: МИИТ, 2007. - 43 с.	https://library.miit.ru/bookscatalog/metod/04-78203.pdf (дата обращения 25.02.2026) 681.3 Ж51
4	Желенков Б.В. Маршрутизация в глобальных сетях. Протокол BGP: учеб. пособие по дисц. Сети ЭВМ и телекоммуникации для студ. 4 курса спец. Вычислительные машины, комплексы, системы и сети, напр. Информатика и вычислительная техника. - М.: МИИТ, 2011. - 183 с.	https://library.miit.ru/miitpublishing/12-1780.pdf (дата обращения 25.02.2026) 681.3 Ж51

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

- База данных стандартов: https://www.gost.ru/portal/gost/home/standarts
- База данных документов ФСТЭК: https://fstec.ru/dokumenty-filter

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 3 семестре.

10. Оценочные материалы.

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

Авторы:

доцент, к.н. кафедры
«Вычислительные системы и
квантовые коммуникации» Я.М. Голдовский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Андриянова