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 РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Техническая защита каналов передачи данных

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (в сфере связи, информационных и коммуникационных технологий)

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целью дисциплины «Техническая защита каналов передачи данных» является формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умения применять специальные знания для решения конкретных научно-практических задач. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Основными задачами дисциплины являются:

- изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- изучение современных телекоммуникационных технологий, применяемых при построении телекоммуникационных сетей и систем;
- организационно-правовое обеспечение деятельности по получению, накоплению, обработке, анализу, использованию информации и защите объектов информатизации, информационных технологий и ресурсов;
- разработка и контроль эффективности осуществления системы мер по формированию и использованию информационных ресурсов, систем обеспечения информационной безопасности;
- контроль соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ПК-1 - Способность анализировать и оценивать защищенность программно-аппаратных средств защиты информации;

ПК-7 - Способность выбирать и применять технические средства защиты информации, обеспечивать их функционирование, проводить восстановление и замену отказавших компонентов.

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

Знать:

- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы ФСБ России, ФСТЭК России в данной области;

- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.

Уметь:

- анализировать и оценивать угрозы информационной безопасности объекта;

- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;

- пользоваться нормативными документами по защите информации.

Владеть:

- навыками работы с нормативными правовыми актами;

- методами и средствами выявления угроз безопасности автоматизированным системам;

- методами технической защиты информации;

- методами формирования требований по защите информации;

- методами расчета и инструментального контроля показателей технической защиты информации;

- методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов;

- профессиональной терминологией.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 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 №9
Контактная работа при проведении учебных занятий (всего):	64	64

В том числе:		
Занятия лекционного типа	32	32
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 116 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 технической защиты каналов передачи данных. Классификация угроз Содержание учебного материала: - Определение технической защиты информации (ТЗИ) на каналах связи - Классификация каналов передачи данных: проводные, волоконно-оптические, радиоканалы, спутниковые, инфракрасные - Основные угрозы: перехват, навязывание, модификация, ретрансляция, анализ трафика - Модель нарушителя на канальном уровне - Принципы защиты: конфиденциальность, целостность, доступность, аутентичность
2	Физическая природа побочных электромагнитных излучений и наводок (ПЭМИН) Содержание учебного материала: - Источники ПЭМИН в кабельных системах и радиотрактах - Параметры опасных сигналов: амплитуда, частота, длительность - Дифференциальный и синфазный режимы наводок - Перекрестные помехи (crosstalk) в многопарных кабелях - Дальность перехвата ПЭМИН в зависимости от типа линии и среды распространения
3	Методы перехвата информации в проводных линиях связи Содержание учебного материала: - Прямое подключение (таппинг) к витой паре и коаксиальному кабелю - Индукционный (бесконтактный) съем сигнала с помощью датчиков Холла и токовых клещей - Емкостной съем информации

№ п/п	Тематика лекционных занятий / краткое содержание
	- Анализ отраженных сигналов (TDR) для определения места несанкционированного подключения - Использование высокоомных усилителей для необнаружимого перехвата
4	Защита каналов от несанкционированного подключения и прослушивания Содержание учебного материала: - Экранирование проводных линий: типы экранов (фольга, оплетка), требования к заземлению - Скретка пар (скрутка различного шага) как метод повышения помехоустойчивости - Использование ферритовых фильтров и подавителей синфазной помехи - Обнаружение устройств перехвата: рефлектометрия, анализ шумов, внесение тестовых сигналов - Организация физической охраны кабельной инфраструктуры
5	Волоконно-оптические линии связи (ВОЛС): уязвимости и методы перехвата Содержание учебного материала: - Принципы передачи по ВОЛС: отражение, преломление, затухание - Способы несанкционированного съема сигнала: изгиб оптического волокна (макро- и микроизгибы), полировка поверхности, вварка отвода - Обнаружение факта съема через мониторинг уровня оптической мощности и рефлектограммы (OTDR) - Пассивные и активные системы контроля целостности ВОЛС - Особенности защиты многомодовых и одномодовых волокон
6	Криптографическая защита каналов передачи данных на физическом уровне Содержание учебного материала: - Шифрование на канальном уровне: технологии MACsec (IEEE 802.1AE) - Формат кадра MACsec: тег безопасности, ICV (Integrity Check Value) - Управление ключами в MACsec (MKA протокол) - Аппаратная реализация шифрования (криптомодули в коммутаторах и NIC) - Сравнение MACsec с шифрованием на сетевом (IPsec) и транспортном (TLS) уровнях
7	Квантовое распределение ключей (QKD) для защиты каналов передачи данных Содержание учебного материала: - Принципы квантовой криптографии: состояние фотона, теорема о невозможности клонирования - Протоколы BB84, E91, B92: процедура согласования и проверки на подслушивание - Аппаратные реализации QKD для ВОЛС (коммерческие системы: ID Quantique, QRate) - Ограничения QKD: дальность, влияние шумов, скорость генерации ключа - Интеграция QKD с классическим шифрованием (гибридные схемы)
8	Защита радиоканалов передачи данных. Анализ уязвимостей Содержание учебного материала: - Диапазоны радиосвязи (HF, VHF, UHF, SHF) и их уязвимость к перехвату - Методы перехвата: сканирующие приемники, SDR (программируемые радиосистемы), направленные антенны - Анализ протоколов: Bluetooth, Wi-Fi, ZigBee, LoRa - общие уязвимости - Атака «человек посередине» в радиоканалах (ретрансляция, подмена сигнала) - Обнаружение работающих радиозакладок и скрытых передатчиков
9	Способы защиты радиоканалов: скрытность и помехозащищенность

№ п/п	Тематика лекционных занятий / краткое содержание
	Содержание учебного материала: - Псевдослучайная перестройка рабочей частоты (ППРЧ / FHSS) - Шумоподобные сигналы (ШПС) и их обнаружение на фоне шумов - Пространственная фильтрация: применение узконаправленных антенн и умных антенных решеток - Экранирование помещений (клетка Фарадея) для предотвращения утечки через радиоканал - Уменьшение мощности передатчика до минимально необходимого уровня
10	Защита каналов спутниковой связи Содержание учебного материала: - Принципы работы спутниковых каналов: прямое и обратное распространение, зоны покрытия - Угрозы: перехват сигнала всенаправленной антенной, постановка помех (jamming), подмена спутника (meaconing) - Шифрование спутникового трафика: DVB-S2 с поддержкой AES, решения на базе IPsec - Ограничение зоны приема (Spot beam) как метод физической защиты - Противодействие несанкционированному доступу к спутниковым терминалам
11	Аппаратные средства защиты каналов передачи (шифраторы, сканеры поля) Содержание учебного материала: - Классификация аппаратных шифраторов каналов: для проводных, ВОЛС и радиоканалов - Требования ФСБ и ФСТЭК к сертифицированным средствам криптографической защиты (СКЗИ) - Сканеры электромагнитного поля (СЭМП) и анализаторы спектра для контроля утечек - Генераторы шума (подавители диктофонов и закладок) активного типа - Аппаратные детекторы подключения к витой паре (Reflectometer)
12	Организация защищенных каналов с использованием VPN на канальном уровне L2TP/IPsec Содержание учебного материала: - Принципы построения защищенных туннелей L2TP поверх IPsec - Режимы работы IPsec: транспортный и туннельный, их применение для защиты канала - Обмен ключами IKEv1/IKEv2, использование сертификатов X.509 - Аппаратные ускорители шифрования для высокоскоростных линий (10 Гбит/с и выше) - Примеры настройки L2TP/IPsec на маршрутизаторах Cisco, MikroTik, Linux
13	Защита каналов передачи в автоматизированных системах управления технологическим процессом (АСУ ТП) Содержание учебного материала: - Специфика каналов связи в АСУ ТП: протоколы Modbus, DNP3, IEC 61850, Profinet - Уязвимости промышленных протоколов: отсутствие шифрования, слабая аутентификация - Методы защиты: шлюзы безопасности (Security Gateway), однонаправленные устройства (диоды данных) - Использование глубокого анализа пакетов (DPI) для контроля технологических команд - Изоляция сетей АСУ ТП от корпоративной сети и интернета (воздушный зазор)
14	Анализ защищенности каналов передачи данных. Тестовые методы Содержание учебного материала: - Пассивный анализ: захват трафика (sniffing) в контрольных точках - Активный анализ: внесение тестовых искажений, попытки несанкционированного подключения - Оценка уровня затухания и соотношения сигнал/шум как параметров защищенности - Использование сетевых анализаторов (Wireshark, tcpdump, CommView) для выявления

№ п/п	Тематика лекционных занятий / краткое содержание
	незашифрованных данных - Методология «пентраста» (penetration testing) для каналов передачи данных
15	Правовое регулирование технической защиты каналов передачи в РФ Содержание учебного материала: - Федеральный закон «Об информации, информационных технологиях и о защите информации» (149-ФЗ) - Федеральный закон «О связи» (126-ФЗ): требования к операторам связи по защите каналов - Приказы ФСТЭК России о сертификации средств ТЗИ - Лицензирование деятельности по технической защите каналов передачи данных - Ответственность за несанкционированный перехват информации (УК РФ, ст. 138, 272)
16	Перспективные направления защиты каналов передачи данных Содержание учебного материала: - Применение искусственного интеллекта для обнаружения аномалий в канале (аномальное изменение задержки, битовых ошибок) - Постквантовая криптография для защиты каналов на дальнюю перспективу - Защита каналов в квантовых сетях связи (квантовая телепортация состояния) - Автономные адаптивные системы защиты (изменение режима шифрования при попытке атаки) - Развитие стандартов: IEEE 802.1AE-202x, новый профиль MACsec с постквантовыми алгоритмами

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Идентификация каналов передачи данных и анализ их уязвимостей В результате выполнения лабораторной работы студент получит навыки классификации типов каналов передачи данных (витая пара, коаксиал, оптоволокно, радиоканал), построения схемы локальной сети с выделением всех каналов передачи, идентификации критичных к перехвату участков (магистральные линии, резервные каналы, беспроводные сегменты), проведения анализа уязвимостей для каждого типа канала на основе модели угроз, а также оформления карты угроз каналов передачи данных.
2	Обнаружение несанкционированного подключения к витой паре с помощью рефлектометра (TDR) В результате выполнения лабораторной работы студент получит навыки подключения временного рефлектометра (TDR) к кабелю витой пары, измерения длины кабеля и расстояния до обрывов, обнаружения несанкционированного отвода (тройника, таппа) по появлению дополнительных отраженных импульсов, идентификации местоположения отвода с точностью до 1 метра, а также составления протокола проверки целостности кабельной линии.
3	Перехват и анализ трафика в незащищенной сети Ethernet (сниффинг) В результате выполнения лабораторной работы студент получит навыки организации пассивного перехвата трафика в сегменте локальной сети с использованием Wireshark и переключения сетевой карты в режим promiscuous, выделения из захваченных пакетов логинов и паролей в протоколах HTTP, FTP, Telnet, POP3, идентификации передаваемых файлов и извлечения их из трафика, а также формулирования выводов о необходимости шифрования каналов.

№ п/п	Наименование лабораторных работ / краткое содержание
4	Защита канала передачи с помощью шифрования на канальном уровне (MACsec) В результате выполнения лабораторной работы студент получит навыки настройки MACsec (IEEE 802.1AE) на двух коммутаторах (например, Cisco или MikroTik) с использованием предварительного общего ключа (CAK), анализа защищенного трафика в Wireshark (обнаружение тега безопасности SecTAG и поля ICV), проверки невозможности дешифрации кадра без ключа, сравнения производительности канала с включенным и выключенным MACsec, а также настройки ротации ключей через MKA (MACsec Key Agreement).
5	Моделирование перехвата сигнала в волоконно-оптической линии связи (метод изгиба) В результате выполнения лабораторной работы студент получит навыки создания практического стенда с ВОЛС (передатчик - оптоволокно - приемник), реализации метода макроизгиба оптического волокна для отвода части оптической мощности, измерения уровня отведенного сигнала с помощью оптического детектора, обнаружения факта съема с помощью контроля уровня мощности на приемнике (оптический рефлектометр в режиме реального времени), а также формулирования рекомендаций по защите ВОЛС от несанкционированного съема.
6	Анализ побочных электромагнитных излучений и наводок (ПЭМИН) от кабельной линии В результате выполнения лабораторной работы студент получит навыки размещения измерительной антенны вблизи неэкранированного кабеля витой пары, подключения анализатора спектра для регистрации ПЭМИН в диапазоне от 10 кГц до 1 ГГц, идентификации информативного сигнала (например, передача тестового файла приводит к появлению спектральных пиков), оценки отношения сигнал/шум для разных частот, а также подбора ферритовых фильтров для подавления синфазной составляющей ПЭМИН.
7	Обнаружение и локация радиозакладки (жучка) в помещении В результате выполнения лабораторной работы студент получит навыки использования портативного сканера электромагнитного поля для поиска работающего радиопередатчика (жучка) на частотах 433 МГц, 900 МГц, 2,4 ГГц, метода триангуляции для определения местоположения источника сигнала с помощью направленной антенны, измерения уровня мощности сигнала (мкВт/м?), а также составления карты электромагнитного фона помещения с зонами повышенного риска.
8	Перехват и дешифрование WPA2/WPA3 в беспроводной сети (этический взлом) В результате выполнения лабораторной работы студент получит навыки захвата WPA2 4-way handshake с помощью инструмента aircrack-ng в контролируемой среде, проведения словарной атаки (например, rockyou.txt) на захваченный хэш, анализа стойкости пароля (слабый vs. сильный), выполнения аналогичных действий для сети WPA3 (захват SAE handshake), а также формулирования рекомендаций по настройке безопасного Wi-Fi (длина пароля, WPA3, управление через RADIUS).
9	Настройка защищенного туннеля L2TP/IPsec для канала «удаленный офис - ЦОД» В результате выполнения лабораторной работы студент получит навыки настройки L2TP-сервера на маршрутизаторе (MikroTik, OpenSwan или StrongSwan), генерации самоподписанных сертификатов X.509 для аутентификации сторон, настройки клиента L2TP/IPsec на операционной системе Windows/Linux, проверки шифрования трафика через Wireshark (ESP-пакеты, отсутствие L2TP в открытом виде), измерения пропускной способности туннеля и сравнения с открытым каналом.

№ п/п	Наименование лабораторных работ / краткое содержание
10	Защита промышленного канала передачи (Modbus/TCP) с помощью шлюза безопасности В результате выполнения лабораторной работы студент получит навыки эмуляции промышленной сети с ПЛК (например, Modbus-сервер на Raspberry Pi) и HMI (клиент), организации перехвата и модификации кадров Modbus с использованием инструмента Modbuspal или Metasploit, настройки промышленного шлюза безопасности (например, Cisco IE 3000 или программный аналог Opal), создания правил белых списков (разрешены только команды чтения, запрещена запись), а также проверки блокировки несанкционированных команд через шлюз.
11	Квантовое распределение ключей (QKD) - симуляция протокола BB84 В результате выполнения лабораторной работы студент получит навыки запуска симулятора квантового распределения ключей (например, QKD Simulator или пакет NetSquid), настройки параметров канала (длина ВОЛС, уровень шумов, эффективность детекторов), выполнения протокола BB84 (отправка фотонов в четырех поляризациях, согласование баз, проверка на подслушивание), анализа процента ошибок (QBER) и вычисления финального секретного ключа, а также сравнения с классическим распределением ключей по уязвимости к MITM.
12	Сканирование радиоканала и анализ протокола Bluetooth Low Energy (BLE) В результате выполнения лабораторной работы студент получит навыки использования SDR-приемника (например, HackRF или RTL-SDR) для захвата спектра в диапазоне 2,4 ГГц, идентификации BLE-пакетов (рекламные кадры, данные характеристик), декодирования передаваемых значений с помощью инструментов (Ubertooth, Wireshark с модулем BLE), обнаружения незашифрованных BLE-устройств (датчики температуры, замки, брелоки), а также формулирования рекомендаций по защите BLE-каналов (шифрование, парная связь, смена MAC).
13	Обнаружение подмены спутникового сигнала (GPS/GNSS спуфинг) В результате выполнения лабораторной работы студент получит навыки генерации поддельного GPS-сигнала с помощью SDR (например, GPS-SDR-SIM и HackRF) в контролируемой экранированной среде, анализа реакции GPS-приемника (смещение координат, времени), обнаружения спуфинга через мониторинг отношения сигнал/шум и числа видимых спутников, настройки защищенных GPS-приемников с функцией антиспуфинга (проверка корреляции сигналов разных созвездий), а также составления протокола проверки целостности навигационного канала.
14	Использование псевдослучайной перестройки частоты (ППРЧ) для защиты радиоканала В результате выполнения лабораторной работы студент получит навыки настройки двух SDR-модулей в режиме приемопередатчиков с ППРЧ по заданному закону (например, 50 скачков в секунду в диапазоне 868–928 МГц), перехвата сигнала широкополосным приемником без знания последовательности (получен шум), синхронизации приемника с передатчиком при известном псевдослучайном коде, оценки отношения сигнал/шум для фиксированной частоты против ППРЧ в условиях помех, а также формулирования выводов о скрытности передачи.
15	Анализ утечек информации через наводки на смежные кабели (cross-talk) В результате выполнения лабораторной работы студент получит навыки прокладки двух кабелей витой пары (информационный и «наводящий») в одном кабель-канале с расстоянием 5–10 см, передачи информационного сигнала (например, 1 МГц меандр или Ethernet-трафик) по первому кабелю, измерения наведенного напряжения на втором кабеле с помощью осциллографа и анализатора спектра, оценки затухания перекрестной помехи (Near-End/ Far-End Crosstalk), а также

№ п/п	Наименование лабораторных работ / краткое содержание
	демонстрации метода защиты - увеличения расстояния или использования экранированной витой пары (FTP/SFTP).
16	Разработка политики технической защиты каналов передачи для предприятия В результате выполнения лабораторной работы студент получит навыки проведения инвентаризации всех каналов передачи данных на условном предприятии (3 отдела, ЦОД, удаленный филиал), классификации каналов по степени конфиденциальности передаваемой информации (открытые, служебные, секретные), выбора средств защиты для каждого типа канала (MACsec, IPsec, радиошумоподавление, экранирование), расчета бюджета на внедрение и эксплуатацию, а также составления итогового документа «Политика технической защиты каналов передачи данных» с графиком внедрения и зонами ответственности.

4.3. Самостоятельная работа обучающихся.

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

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

№ п/п	Библиографическое описание	Место доступа
1	Желенков, Борис Владимирович. Канальный уровень модели OSI : метод. указ. к лаб. раб. по дисц. "Сети ЭВМ и телекоммуникации" для студ. 4 курса спец. "Вычислительные машины, комплексы, системы и сети", напр. "Информатика и вычислительная техника" / Б.В. Желенков ; МИИТ. Каф. "Вычислительные	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-41547.pdf.(дата обращения 09.06.2026).Текст : непосредственный.Полочный шифр 004-Ж51

	системы и сети". - М. : МИИТ, 2011. - 50 с. : ил. с. 49. - 100 экз. - (в пер.) : 42.60 р. - Текст : непосредственный.	
2	Голдовский Я.М., Желенков Б.В., Сафонова И.Е. Криптографическая защита компьютерной информации : метод. указ. к лаб. раб. по дисц. "Теоретические основы компьютерной безопасности" для студ., обуч. по напр. "Информационная безопасность" / МИИТ. Каф. "Вычислительные системы и сети". - М. : МГУПС(МИИТ), 2013. - 36 с. : ил. - Библиогр.: с. 46. - 100 экз. - (в пер.) : 39.78 р.	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-42764.pdf. (дата обращения 09.06.2026)Текст : непосредственный. 004 Г60

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).

Microsoft Windows
Microsoft Office

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

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

- компьютер преподавателя, мультимедийное оборудование, рабочие станции студентов, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Зачет в 9 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