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)

Криптографическая защита информации

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 освоения учебной дисциплины «Криптографическая защита информации» является формирование профессиональных компетенций по основным разделам дисциплины.

Задачами дисциплины являются:

- изучение основных методов и средств криптографической защиты информации, стандартов в этой области;
- получение представления о математических методах криптографической защиты информации;
- студенты должны научиться применять современные методы и средства криптографической защиты информации на практике.

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.

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

Знать:

- математические методы и основополагающие документы в области криптографической защищенности компьютерных систем (КС) и сетей;
- международные и национальные стандарты по оценке безопасности в области информационных технологий.
- порядок тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации

Уметь:

- оценивать уровень безопасности КС и сетей;
- применять стандарты и другие нормативные документы по информационной безопасности для оценки защищенности КС.
- проводить контроль показателей и процесса функционирования программных и программно- аппаратных (в том числе криптографических) средств защиты информации.

Владеть:

- навыками работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации.

- навыками поддержания бесперебойной работы программных и программно- аппаратных (в том числе криптографических) средств защиты информации в ИТКС

- навыками использования средств криптографической и технической защиты информации для решения задач профессиональной деятельности.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 8 з.е. (288 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	
		№5	№6
Контактная работа при проведении учебных занятий (всего):	128	64	64
В том числе:			
Занятия лекционного типа	64	32	32
Занятия семинарского типа	64	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 160 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	5 СЕМЕСТР Введение в криптографическую защиту информации Содержание учебного материала: - Определение криптографии и криптоанализа - Основные термины: шифрование, дешифрование, ключ, открытый текст, шиф-ротекст - Цели криптографической защиты: конфиденциальность, целостность, аутентич-ность, неотказуемость - Принцип Керкгоффса (безопасность определяется только секретностью ключа) - Классификация криптографических алгоритмов: симметричные и асимметрич-ные
2	Криптоанализ и виды атак на криптоалгоритмы Содержание учебного материала: - Классификация атак: атака по шифротексту (Ciphertext-Only) - Атака с известным открытым текстом (Known-Plaintext) - Атака с выбранным открытым текстом (Chosen-Plaintext, CPA) - Атака с выбранным шифротекстом (Chosen-Ciphertext, CCA) - Атака «человек посередине» (Man-in-the-Middle, MITM) - Атаки по побочным каналам (время, питание, электромагнитное излучение)
3	Математические основы криптографии Содержание учебного материала: - Теория чисел: простые числа, взаимно простые числа, наибольший общий дели-тель (алгоритм Евклида) - Модульная арифметика (mod) и свойства сравнений - Китайская теорема об остатках и её применение в криптографии - Функция Эйлера ?(n) и теорема Эйлера - Дискретные логарифмы и задача дискретного логарифмирования
4	Классические шифры (исторические) Содержание учебного материала: - Шифр Цезаря: принцип, уязвимость к частотному анализу - Шифр Атбаш (обратный алфавит) - Шифр Вижинера: таблица, ключевое слово, вскрытие методом Касиски - Шифр Плейфера (биграммная замена) - Шифр Энигмы: устройство, принцип работы, вскрытие (Тьюринг)
5	Современные методы шифрования: блочные и потоковые шифры Содержание учебного материала: - Блочные шифры: принцип работы с блоками фиксированной длины - Режимы шифрования блочных шифров (ECB, CBC, CFB, OFB, CTR, GCM) - Потоковые шифры: генерация ключевого потока, XOR с открытым текстом - Сравнение блочных и потоковых шифров (области применения, скорость) - Требования к синхронизации для потоковых шифров
6	Алгоритм DES (Data Encryption Standard)

№ п/п	Тематика лекционных занятий / краткое содержание
	Содержание учебного материала: - История создания DES, размер блока (64 бита) и ключа (56 бит) - Сеть Фейстеля: структура раунда, функция Фейстеля - Начальная и конечная перестановки IP и IP?? - S-блоки (таблицы замены) и их роль в нелинейности - Расписание ключей: генерация 16 раундовых ключей
7	Криптоанализ DES и алгоритм 3DES Содержание учебного материала: - Уязвимости DES: малый размер ключа (56 бит) - Атака грубой силы (Deep Crack, EFF) - время перебора - Дифференциальный криптоанализ DES (Бихан, Шамир) - Линейный криптоанализ DES (Мацуи) - Алгоритм 3DES (тройной DES): режимы EDE (шифрование-дешифрование-шифрование) - Эффективная стойкость 3DES (112 бит), область применения и статус (устарева-ние)
8	Алгоритм AES (Advanced Encryption Standard) Содержание учебного материала: - Конкурс NIST на новый стандарт, требования - Структура AES: блок 128 бит, ключи 128/192/256 бит - Раунд AES: SubBytes (S-блок), ShiftRows, MixColumns, AddRoundKey - Генерация раундовых ключей (Key Schedule) - Стойкость AES к линейному и дифференциальному криптоанализу - Аппаратная и программная производительность AES (инструкции AES-NI)
9	Режимы шифрования блочных алгоритмов (ECB, CBC, CFB, OFB, CTR) Содержание учебного материала: - Режим ECB (Electronic Codebook): параллелизм, уязвимость к выявлению повторяющихся блоков - Режим CBC (Cipher Block Chaining): вектор инициализации (IV), связанность блоков - Режимы CFB и OFB (превращение блочного шифра в потоковый) - Режим CTR (Counter): счетчик, параллелизм, произвольный доступ к блокам - Режимы с аутентификацией (GCM, CCM, OCB)
10	Потоковые шифры: RC4, Salsa20, ChaCha20 Содержание учебного материала: - Принцип работы потокового шифра: генератор псевдослучайного ключевого потока (PRNG) - Алгоритм RC4: инициализация S-box, генерация байтов ключевого потока - Уязвимости RC4 (смещение первых байтов, WEP-атаки) - Семейство Salsa20 / ChaCha20 (Daniel Bernstein): структура раунда QR (Quarter Round) - ChaCha20-Poly1305: сочетание шифрования и аутентификации (AEAD) - Применение в протоколах TLS 1.3, WireGuard, OpenSSH
11	Коды аутентификации сообщений (MAC) и режимы AEAD Содержание учебного материала: - Отличие MAC от цифровой подписи (симметричный vs. асимметричный ключ) - Построение MAC на основе хэш-функций: HMAC (RFC 2104) - Построение MAC на основе блочных шифров: CMAC, OMAC - Режимы с аутентификацией (AEAD): AES-GCM, AES-CCM, ChaCha20-Poly1305 - Атака на неаутентифицированное шифрование (Padding Oracle Attack на CBC)
12	Управление ключами в симметричной криптографии

№ п/п	Тематика лекционных занятий / краткое содержание
	Содержание учебного материала: - Проблема распределения ключей в симметричной криптографии - Центры распределения ключей (KDC): протоколы Needham-Schroeder, Kerberos - Протоколы согласования ключей: Diffie-Hellman (как гибридный подход) - Периодическая смена ключей (key rotation) - Атаки на управление ключами (replay attack, reflection attack)
13	Принципы асимметричного шифрования (криптография с открытым ключом) Содержание учебного материала: - Пара ключей: публичный (шифрование) и приватный (дешифрование) - Односторонние функции с «лазейкой» (trapdoor function) - Сравнение с симметричной криптографией (скорость, безопасность, управление ключами) - Основные задачи: шифрование, распределение ключей, цифровая подпись
14	Алгоритм Диффи-Хэллмана (Diffie-Hellman) Содержание учебного материала: - Протокол выработки общего секретного ключа через открытый канал - Математическая основа: модульное возведение в степень, задача дискретного логарифмирования - Атака «человек посередине» на DH без аутентификации - Эллиптические кривые в Diffie-Hellman (ECDH) - Применение: IKE в IPsec, TLS, SSH
15	Алгоритм RSA (Rivest-Shamir-Adleman) Содержание учебного материала: - Генерация ключей: выбор простых чисел p и q, вычисление n = p?q и ?(n), выбор e и d - Шифрование: c = m? mod n, дешифрование: m = c? mod n - Стойкость RSA (разложение n на множители - задача факторизации) - Рекомендуемые размеры ключей (2048 бит, 4096 бит) - Padding в RSA: PKCS#1 v1.5, OAEP (Optimal Asymmetric Encryption Padding) - Атаки на RSA (низкая экспонента e=3, атака Винера, Блейхенбахера)
16	Криптосистема Эль-Гамаля (ElGamal) Содержание учебного материала: - Математическая основа: задача дискретного логарифмирования в конечных по-лях - Генерация ключей: простое число p, первообразный корень g, секретный ключ x, публичный y = g? mod p - Процедура шифрования: эфемерный ключ k, шифротекст (c? = g? mod p, c? = m ? y? mod p) - Дешифрование: m = c? ? (c??)?? mod p - Сравнение RSA и ElGamal (размер шифротекста, скорость) - Эллиптическая версия ECElGamal
17	6 СЕМЕСТР Криптографические хэш-функции Содержание учебного материала: - Определение хэш-функции, требования: детерминизм, быстродействие, лавин-ный эффект - Свойства: устойчивость к нахождению прообраза (preimage resistance) - Устойчивость к нахождению второго прообраза (second preimage resistance) - Устойчивость к коллизиям (collision resistance) - Конструкция Меркла-Дамгора (MD5, SHA-1, SHA-2) - Атака «дней рождения» на нахождение коллизий
18	Хэш-алгоритмы: MD5, SHA-1, SHA-2

№ п/п	Тематика лекционных занятий / краткое содержание
	Содержание учебного материала: - MD5: структура, раунды, результат 128 бит, статус (скомпрометирован) - SHA-1: структура, результат 160 бит, уязвимость (атака Шамбира на коллизии) - Семейство SHA-2: SHA-224, SHA-256, SHA-384, SHA-512 - Внутреннее устройство SHA-256 (блоки, константы, сжатие) - Применение SHA-2 в современных протоколах (TLS, SSH, PGP)
19	Хэш-алгоритм SHA-3 (Keccak) Содержание учебного материала: - Конкурс NIST на новый стандарт (2007–2012), победитель - Keccak - Структура: губчатая функция (sponge construction) - Внутреннее состояние, операции впитывания (absorbing) и отжима (squeezing) - Параметры: размеры выхода 224/256/384/512 бит - Сравнение SHA-3 и SHA-2 (безопасность против квантовых атак, производи-тельность)
20	Цифровая подпись (ЭЦП): принципы и алгоритмы Содержание учебного материала: - Требования к цифровой подписи: подлинность, целостность, неотказуемость - Схема подписи: подпись (приватным ключом) и проверка (публичным ключом) - Хэш перед подписанием (hash-then-sign) - Алгоритм RSA-PSS (Probabilistic Signature Scheme) - Алгоритм DSA (Digital Signature Algorithm) - Алгоритм ECDSA (Elliptic Curve DSA): преимущества меньших ключей - Сравнение RSA и ECDSA (скорость генерации, размер подписи)
21	Эллиптическая криптография (ECC) Содержание учебного материала: - Основы эллиптических кривых над конечными полями (Weierstrass форма: y? = x? + ax + b) - Операция сложения точек и удвоения точки - Задача дискретного логарифмирования на эллиптической кривой (ECDLP) - Выбор параметров кривой (SECP256k1, Curve25519) - ECDH, ECDSA, EdDSA (Edwards-curve Digital Signature Algorithm) - Преимущества ECC перед RSA (меньший размер ключа при той же стойкости)
22	Инфраструктура открытых ключей (PKI) Содержание учебного материала: - Компоненты PKI: удостоверяющий центр (CA), регистрационный центр (RA), репозиторий сертификатов - Цепочки доверия: корневой сертификат, промежуточные CA, конечный серти-фикат - Формат сертификата X.509 v3: поля (subject, issuer, public key, validity, extensions) - Протоколы отзыва сертификатов: CRL (Certificate Revocation List), OCSP (Online Certificate Status Protocol) - Самоподписанные сертификаты vs. сертификаты от CA
23	Протокол TLS/SSL (Transport Layer Security) Содержание учебного материала: - Назначение TLS: защита канала связи (конфиденциальность, целостность, аутен-тификация) - Архитектура TLS: Record Protocol и Handshake Protocol - Рукопожатие TLS 1.3: согласование шифров, аутентификация сервера, выработ-ка сессионного ключа - Используемые криптографические алгоритмы в TLS 1.3 (AES-GCM, ChaCha20-Poly1305, ECDHE,

№ п/п	Тематика лекционных занятий / краткое содержание
	ECDSA) - Уязвимости устаревших версий: POODLE (SSL 3.0), Heartbleed (OpenSSL), FREAK, Logjam
24	Криптографическая защита в протоколах SSH, IPsec Содержание учебного материала: - Протокол SSH: аутентификация по ключам, туннелирование, шифрование сессии - Архитектура IPsec: ESP (Encapsulating Security Payload), AH (Authentication Header) - Режимы IPsec: транспортный и туннельный - Управление ключами в IPsec: протокол IKEv1/IKEv2 (Internet Key Exchange) - Применение: VPN-решения на базе IPsec (site-to-site, remote access)
25	Гомоморфное шифрование Содержание учебного материала: - Определение гомоморфного шифрования: выполнение операций над зашифро-ванными данными - Частично гомоморфные системы (PHE): RSA (умножение), Paillier (сложение) - Полностью гомоморфное шифрование (FHE): схема Gentry (2009) - Современные схемы: BGV, CKKS, TFHE - Применение: облачные вычисления, конфиденциальные транзакции, медицин-ские данные
26	Квантовая криптография (QKD) Содержание учебного материала: - Принципы квантовой криптографии: состояние фотона (поляризация, фаза) - Теорема о невозможности клонирования (no-cloning theorem) - Протокол BB84 (Bennett & Brassard 1984): передача и согласование баз - Обнаружение подслушивания: уровень ошибок QBER (Quantum Bit Error Rate) - Коммерческие системы QKD (ID Quantique, QRate) и ограничения (дальность, стоимость) - Интеграция QKD с классическим шифрованием (гибридные схемы)
27	Постквантовая криптография (PQC) Содержание учебного материала: - Угрозы квантовых компьютеров: алгоритм Шора (факторизация, дискретные ло-гарифмы), алгоритм Гровера (ускорение перебора) - Семейства постквантовых алгоритмов: на основе решеток (lattice-based) - На основе хэш-функций (hash-based): схема SPHINCS+ - На основе многомерных квадратичных уравнений (multivariate) - На основе кодов с коррекцией ошибок (code-based): McEliece - Стандартизация NIST: Kyber (KEM), Dilithium (подпись), Falcon, SPHINCS+
28	Криптографические протоколы электронного голосования Содержание учебного материала: - Требования к протоколам голосования: анонимность, корректность, устойчивость к повторному голосованию - Протоколы на основе слепой подписи (схема Фудзиока–Окамото–Оты) - Гомоморфное шифрование для суммирования голосов (схема Эль-Гамаля) - Голосование с использованием блокчейна (анализ преимуществ и угроз) - Реальные системы: Helios Voting, Voatz (криптоанализ и критика)
29	Блокчейн и криптовалюты (криптографические основы) Содержание учебного материала: - Криптографическая основа блокчейна: хэш-функции для связывания блоков (Proof-of-Work) - Цифровая подпись (ECDSA/EdDSA) для подтверждения транзакций

№ п/п	Тематика лекционных занятий / краткое содержание
	- Дерево Меркла для эффективной проверки транзакций в блоке - Консенсусные механизмы: Proof-of-Work, Proof-of-Stake, их криптографические аспекты - Криптографические примитивы в Bitcoin, Ethereum (Keccak-256, secp256k1)
30	Стеганография и криптография (комбинированные методы защиты) Содержание учебного материала: - Определение стеганографии, отличие от криптографии (сокрытие факта переда-чи) - Классические методы: LSB (младший бит) в изображениях и аудио - Стеганография в сетевых протоколах (TCP-опции, поля IP ID, временные за-держки) - Обнаружение стеганографии (стегоанализ) - Комбинация: сначала шифрование, затем встраивание в контейнер
31	Правовое регулирование криптографической защиты информации 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 - Приказы ФСТЭК России о сертификации средств криптографической защиты информации (СКЗИ) - Приказы ФСБ России о применении криптографических алгоритмов (ГОСТ) - Лицензирование деятельности по распространению шифровальных средств - Ответственность за незаконное использование криптографии (УК РФ, КоАП РФ)
32	ГОСТ криптографические стандарты РФ Содержание учебного материала: - ГОСТ 28147-89 (симметричное шифрование): блок 64 бита, ключ 256 бит, сеть Фейстеля, режимы - ГОСТ Р 34.10-2012 (цифровая подпись на эллиптических кривых): параметры кривых - ГОСТ Р 34.11-2012 (хэш-функция Стрибог): конструкция, размер выхода 256/512 бит - Сравнение ГОСТ с международными стандартами (AES, RSA, ECDSA, SHA-2/3) - Использование ГОСТ в системах государственной и коммерческой тайны - Переход на постквантовые стандарты в РФ (перспективные разработки)

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	5 СЕМЕСТР Реализация и криптоанализ классических шифров (Цезарь, Атбаш, Вижинер) В результате работы студентом будут исследованы и проанализированы методы шифрования Цезаря, Атбаш и Вижинера, выполнено практическое шифрование и дешифрование текстов с различными ключами, проведен частотный крипто-анализ для вскрытия шифров, а также подготовлен отчет с выводами о стойко-сти классических алгоритмов к современным методам атак.
2	Частотный криптоанализ моноалфавитных и полиалфавитных шифров В результате работы студентом будут исследованы и проанализированы методы частотного анализа символов, построены гистограммы распределения частот для зашифрованных текстов на русском и английском языках, выполнено вскрытие неизвестного шифра с использованием индекса

№ п/п	Тематика практических занятий/краткое содержание
	совпадений, определены длина ключа шифра Вижинера, а также подготовлен отчет с обоснованием выбора ме-тодов криптоанализа.
3	Модульная арифметика и её применение в криптографии В результате работы студентом будут исследованы и проанализированы алго-ритмы модульной арифметики (расширенный алгоритм Евклида, быстрое возве-дение в степень, китайская теорема об остатках), выполнены вычисления обрат-ных элементов и решение систем сравнений, а также подготовлен отчет с при-мерами применения модульных вычислений в криптографических алгоритмах.
4	Исследование алгоритма DES и его уязвимостей В результате работы студентом будут исследованы и проанализированы струк-тура алгоритма DES (сеть Фейстеля, S-блоки, расписание ключей), выполнена программная или ручная реализация одного раунда DES, проведен анализ уяз-вимостей (малый размер ключа, дифференциальный криптоанализ), а также под-готовлен отчет об эффективности атаки грубой силы на DES.
5	Исследование алгоритма 3DES (тройной DES) В результате работы студентом будут исследованы и проанализированы режимы работы 3DES (EDE2, EDE3), выполнено сравнение стойкости 3DES с одно- и двухключевыми вариантами, проведена оценка производительности 3DES на различных объемах данных, а также подготовлен отчет с выводами о целесооб-разности применения 3DES в современных системах.
6	Исследование алгоритма AES (Advanced Encryption Standard) В результате работы студентом будут исследованы и проанализированы все этапы раунда AES (SubBytes, ShiftRows, MixColumns, AddRoundKey), выполнена реализация одного раунда AES вручную или с использованием учебного кода, проведен анализ генерации раундовых ключей (Key Schedule), а также подготовлен отчет с обоснованием стойкости AES к линейному и дифференциальному криптоанализу.
7	Исследование режимов шифрования блочных алгоритмов (ECB, CBC, CFB, OFB, CTR) В результате работы студентом будут исследованы и проанализированы все ос-новные режимы шифрования блочных алгоритмов, выполнено практическое шифрование изображения в режиме ECB (визуализация уязвимости) и CBC (скрытие повторяющихся блоков), проведен анализ влияния ошибки в одном блоке на последующие блоки для каждого режима, а также подготовлен отчет с рекомендациями по выбору режима в зависимости от области применения.
8	Исследование потоковых шифров (RC4, ChaCha20) В результате работы студентом будут исследованы и проанализированы прин-ципы работы потоковых шифров RC4 и ChaCha20, выполнена генерация ключе-вого потока и шифрование тестовых сообщений, проведен анализ уязвимостей RC4 (смещение первых байтов, применимость в WEP), а также подготовлен от-чет со сравнением производительности и безопасности RC4 и ChaCha20.
9	Исследование кодов аутентификации сообщений (HMAC, CMAC) В результате работы студентом будут исследованы и проанализированы прин-ципы построения HMAC на основе хэш-функций и CMAC на основе блочных шифров, выполнена генерация MAC для сообщений различной длины, проведен анализ уязвимости к атакам на подделку подписи (forgery attacks), а также подго-товлен отчет с выводами о применении MAC для обеспечения целостности и аутентичности данных.

№ п/п	Тематика практических занятий/краткое содержание
10	Исследование режимов с аутентификацией (AES-GCM, ChaCha20-Poly1305) В результате работы студентом будут исследованы и проанализированы режимы аутентифицированного шифрования (AEAD) - AES-GCM и ChaCha20-Poly1305, выполнено практическое шифрование с одновременной аутентификацией дан-ных, проведен анализ устойчивости к атакам на целостность (битовые искаже-ния), а также подготовлен отчет с рекомендациями по применению AEAD-режимов в сетевых протоколах (TLS 1.3, WireGuard).
11	Управление ключами в симметричной криптографии (KDC, Kerberos) В результате работы студентом будут исследованы и проанализированы модели управления ключами с использованием центра распределения ключей (KDC), выполнена эмуляция протокола Kerberos (аутентификация и выдача билетов), проведен анализ уязвимостей (replay attack, атака на временные метки), а также подготовлен отчет с выводами о безопасности симметричного распределения ключей.
12	Исследование протокола Диффи-Хэллмана (Diffie-Hellman) В результате работы студентом будут исследованы и проанализированы матема-тические основы протокола Диффи-Хэллмана (задача дискретного логарифми-рования), выполнена программная реализация выработки общего секретного ключа, проведена эмуляция атаки «человек посередине» (MITM) на неаутенти-фицированный протокол, а также подготовлен отчет с выводами о необходимо-сти аутентификации сторон.
13	Исследование алгоритма RSA (генерация ключей, шифрование, дешифрование) В результате работы студентом будут исследованы и проанализированы все этапы алгоритма RSA: генерация простых чисел p и q, вычисление n и ?(n), выбор открытой и закрытой экспонент, выполнено практическое шифрование и де-шифрование сообщений, проведен анализ стойкости для различных размеров ключей (512, 1024, 2048 бит), а также подготовлен отчет с выводами о факторах, влияющих на безопасность RSA.
14	Атаки на алгоритм RSA (малая экспонента, атака Винера, Блейхенбахера) Атаки на алгоритм RSA (малая экспонента, атака Винера, Блейхенбахера) В результате работы студентом будут исследованы и проанализированы классические атаки на RSA: атака с малой открытой экспонентой (e=3), атака Винера (цепные дроби), атака Блейхенбахера на адаптивно выбранный шифротекст, вы-полнены практические сценарии эксплуатации уязвимостей при неправильной настройке параметров, а также подготовлен отчет с рекомендациями по безопас-ному использованию RSA (OAEP-паддинг, выбор e=65537).
15	Исследование криптосистемы Эль-Гамаля (ElGamal) В результате работы студентом будут исследованы и проанализированы принципы работы криптосистемы Эль-Гамаля, основанной на задаче дискретного логарифмирования, выполнена генерация ключей, шифрование и дешифрование сообщений, проведено сравнение с RSA по размеру шифротекста и скорости операций, а также подготовлен отчет с выводами об областях применения ElGamal.
16	Исследование алгоритмов цифровой подписи (RSA-PSS, DSA, ECDSA) В результате работы студентом будут исследованы и проанализированы алгоритмы цифровой подписи RSA-PSS, DSA и ECDSA, выполнены генерация ключевых пар, подписание сообщения и проверка подписи, проведен анализ уязвимостей (повторное использование случайного числа k в DSA), а также под-готовлен отчет со сравнением размера подписи и производительности алгорит-мов.

№ п/п	Тематика практических занятий/краткое содержание
17	6 СЕМЕСТР Исследование эллиптической криптографии (ECC, ECDH, EdDSA) В результате работы студентом будут исследованы и проанализированы основы эллиптической криптографии (операции сложения и удвоения точек на кривой, задача ECDLP), выполнена реализация ECDH для выработки общего ключа и EdDSA для подписи сообщений, проведено сравнение ECC с RSA (размер клю-ча, стойкость, скорость), а также подготовлен отчет с выводами о преимуще-ствах ECC для мобильных и встраиваемых систем.
18	Исследование эллиптической криптографии (ECC, ECDH, EdDSA) В результате работы студентом будут исследованы и проанализированы основы эллиптической криптографии (операции сложения и удвоения точек на кривой, задача ECDLP), выполнена реализация ECDH для выработки общего ключа и EdDSA для подписи сообщений, проведено сравнение ECC с RSA (размер клю-ча, стойкость, скорость), а также подготовлен отчет с выводами о преимуще-ствах ECC для мобильных и встраиваемых систем.
19	Исследование хэш-функции SHA-3 (Keccak) В результате работы студентом будут исследованы и проанализированы прин-ципы работы SHA-3 (губчатая конструкция sponge, впитывание и отжим), вы-полнены вычисления хэшей для тестовых сообщений, проведено сравнение SHA-3 с SHA-2 по производительности и устойчивости к атакам, а также подго-товлен отчет с выводами о целесообразности перехода на SHA-3.
20	Исследование атак на хэш-функции (атака «дней рождения», поиск коллизий) В результате работы студентом будут исследованы и проанализированы методы атак на хэш-функции (атака «дней рождения» для поиска коллизий, атака на по-иск прообраза), выполнено практическое моделирование атаки «дней рождения» с уменьшенной разрядностью хэша (20–30 бит), проведен анализ вычислитель-ной сложности атаки, а также подготовлен отчет с выводами о минимально без-опасной длине хэша (256 бит и более).
21	Исследование инфраструктуры открытых ключей (PKI) и сертификатов X.509 В результате работы студентом будут исследованы и проанализированы струк-тура сертификата X.509 v3, цепочки доверия, процедуры выпуска и отзыва сер-тификатов, выполнена генерация самоподписанного сертификата и запроса на сертификат (CSR) с помощью OpenSSL, проведен анализ CRL и OCSP для про-верки статуса сертификата, а также подготовлен отчет с выводами о роли PKI в защищенных коммуникациях.
22	Исследование протокола TLS (рукопожатие, анализ трафика) В результате работы студентом будут исследованы и проанализированы этапы рукопожатия TLS 1.2 и TLS 1.3, выполнен захват и анализ TLS-трафика с помо-щью Wireshark (идентификация CipherSuites, сертификатов, ключевого обмена), проведен анализ уязвимостей устаревших версий (SSL 3.0, TLS 1.0), а также подготовлен отчет с рекомендациями по безопасной настройке TLS.
23	Исследование протоколов SSH и IPsec (криптографические аспекты) В результате работы студентом будут исследованы и проанализированы крипто-графические механизмы SSH (аутентификация по ключам, шифрование сессии) и IPsec (ESP, AH, IKE), выполнены настройка SSH-соединения с использовани-ем RSA/ECDSA-ключей, настройка IPsec-туннеля между двумя узлами, проведен анализ захваченного трафика (ESP-пакеты, невозможность дешифровки без ключа), а также подготовлен отчет со сравнением областей применения SSH и IPsec.
24	Исследование гомоморфного шифрования (на примере схемы Пайе)

№ п/п	Тематика практических занятий/краткое содержание
	В результате работы студентом будут исследованы и проанализированы прин-ципы частично гомоморфного шифрования на примере криптосистемы Пайе (свойство аддитивности), выполнены операции сложения зашифрованных чисел без расшифрования, проведен анализ вычислительной сложности и размера шифротекста, а также подготовлен отчет с выводами о применимости гомо-морфного шифрования в облачных вычислениях.
25	Исследование протокола квантового распределения ключей (BB84) - симуляция В результате работы студентом будут исследованы и проанализированы прин-ципы протокола BB84 (передача фотонов в различных поляризациях, согласова-ние баз, обнаружение подслушивания), выполнена программная симуляция ра-боты протокола с моделированием канала связи и наличия Eve, проведен анализ уровня ошибок QBER (Quantum Bit Error Rate) и доли успешно переданных би-тов, а также подготовлен отчет с выводами о перспективах и ограничениях квантового распределения ключей.
26	Исследование постквантовых криптографических алгоритмов (Kyber, Dilithium) В результате работы студентом будут исследованы и проанализированы постквантовые алгоритмы Kyber (KEM) и Dilithium (цифровая подпись), осно-ванные на задачах на решетках (LWE, MLWE), выполнена генерация ключей, шифрование и подпись с использованием открытых реализаций (liboqs), прове-ден сравнительный анализ размера ключей и подписей с классическими алго-ритмами (RSA, ECDSA), а также подготовлен отчет с выводами о готовности PQC к внедрению.
27	Исследование криптографических протоколов электронного голосования (Helios) В результате работы студентом будут исследованы и проанализированы крипто-графические принципы протокола Helios Voting (гомоморфное шифрование, слепая подпись), выполнена эмуляция процесса голосования (регистрация, голо-сование, верификация, подсчет), проведен анализ требований к анонимности и корректности, а также подготовлен отчет с выводами о безопасности протоколов электронного голосования.
28	Исследование криптографических основ блокчейна (Bitcoin, Ethereum) В результате работы студентом будут исследованы и проанализированы крипто-графические примитивы, используемые в блокчейне (хэш-функции SHA-256, деревья Меркла, цифровая подпись ECDSA, Proof-of-Work), выполнена верифи-кация транзакции и построение дерева Меркла, проведен анализ уязвимостей (атака 51%, атака на энтропию ключей), а также подготовлен отчет с выводами о роли криптографии в обеспечении децентрализованного консенсуса.
29	Исследование стеганографии в сочетании с криптографией (LSB в изображениях) В результате работы студентом будут исследованы и проанализированы методы стеганографии (метод младшего бита LSB в изображениях и аудио), выполнено встраивание зашифрованного текста в контейнер (графический файл) и после-дующее извлечение, проведен стегоанализ для обнаружения скрытых данных (визуальный, статистический), а также подготовлен отчет с выводами о комби-нированном применении стеганографии и криптографии.
30	Исследование атак на реализацию криптоалгоритмов (атаки по времени, по питанию) В результате работы студентом будут исследованы и проанализированы атаки по побочным каналам (timing attack на сравнение строк, атака по энергопотреб-лению на S-блоки AES), выполнена программная симуляция измерения времени выполнения операций для разных входных данных, проведен анализ корреляции времени и секретного ключа, а также подготовлен отчет с выводами о методах защиты (постоянное время выполнения, маскирование операций).

№ п/п	Тематика практических занятий/краткое содержание
31	Исследование российских криптографических стандартов (ГОСТ) Исследование российских криптографических стандартов (ГОСТ) В результате работы студентом будут исследованы и проанализированы россий-ские криптографические стандарты (ГОСТ 28147-89 - симметричное шифрование, ГОСТ Р 34.10-2012 - электронная подпись на эллиптических кривых, ГОСТ Р 34.11-2012 - хэш-функция Стрибог), выполнены тестовые расчеты (имитация работы ГОСТ 28147-89 на учебных данных), проведено сравнение с междуна-родными стандартами (AES, ECDSA, SHA-2), а также подготовлен отчет с выводами о применении ГОСТ в системах государственной и коммерческой тай-ны.
32	Комплексный анализ криптографической защищенности информационной системы В результате работы студентом будут исследованы и проанализированы все этапы построения криптографической защиты для типовой информационной си-стемы (выбор алгоритмов шифрования, управление ключами, цифровая под-пись, хэширование, защита каналов связи), выполнено проектирование крипто-системы (с обоснованием выбора алгоритмов и параметров), проведен анализ возможных угроз и уязвимостей, а также подготовлен итоговый отчет с предло-жениями по внедрению криптографических средств защиты.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы
2	Работа с лекционным материалом
3	Подготовка к практическим занятиям
4	Выполнение курсовой работы.
5	Выполнение курсовой работы.
6	Подготовка к промежуточной аттестации.
7	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

- Реализация алгоритма Ривеста.

- Реализация алгоритма DES – режим сцепления блоков в CBC шифре.

- Реализация алгоритма DES – режим работы ECB (электронный блокнот).

- Реализация алгоритма DES – режим работы CFB – обратная связь по шифротексту.

- Реализация алгоритма DES – OFB – обратная связь по выходу.

- Алгоритм федерального стандарта x9.9.

- Алгоритм криптографического преобразования – общий.

- Алгоритм криптографического преобразования в режиме простой замены.

- Алгоритм криптографического преобразования в режиме гаммирования с обратной связью

- Алгоритм криптографического преобразования в режиме имитовставки.

- Алгоритм, основанный на схеме шифрования Эль Гамаля.

- Алгоритм, основанный на комбинированном методе шифрования

- Открытое распределение ключей Диффи-Хеллмана

- Алгоритм электронной подписи RSA.

- Алгоритм электронной подписи DSA.

- Отечественный стандарт электронной подписи.

- Алгоритм цифровой подписи с дополнительными функциями по схеме «слепой подписи».

- Алгоритм цифровой подписи с дополнительными функциями по схеме «неоспоримой подписи».

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

№ п/п	Библиографическое описание	Место доступа
1	Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург: Изд-во Урал. ун-та, 2019.- 204 с. - ISBN 978-5-7996-2677-8.	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf (дата обращения: 16.05.2026). - Текст:электронный
2	Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального	https://book-pc.ru/bezopasnost/1882-programmno-apparatnye-sredstva-zaschity-informacii.html (дата обращения: 16.05.2026). - Текст:электронный.

	образования / О. В. Казарин, А. С. Забабурин. - Москва: Издательство Юрайт, 2022. - 312 с. - (Профессиональное образование). - ISBN 978-5-534-13221-2.	
3	Голиков А. М. Защита информации в инфоком-муникационных системах и сетях: учебное посо-бие / А. М. Голиков. - Москва: ТУСУР, 2015. - 284 с. // Лань: электронно-библиотечная система.	https://e.lanbook.com/book/110336 (дата обращения: 03.05.2026). - Режим доступа: для авториз. пользователей. - Текст: электронный
4	Нестеров С. А. Основы информационной без-опасности: учебное пособие / С. А. Нестеров. - 5-е изд., стер. - Санкт-Петербург: Лань, 2022. - 324 с. - ISBN 978-5-8114-4067-2.	https://www.litres.ru/book/s-a-nesterov/osnovy-informacionnoy-bezopasnosti-66007377/ (дата обра-щения: 16.05.2026). - Режим доступа: для авториз. пользователей. Текст:электронный.
5	Лось А. Б., Нестеренко, А. Ю., Рожков, М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр. - М.: Издательство Юрайт,	https://azon.market/image/catalog/v_1/product/pdf/378/3777079.pdf (дата обращения: 17.05.2026). - Режим до-ступа: для авториз. пользователей. - Текст: электронный

	2019. - 473 с. - (Серия: Бакалавр. Академический курс). - ISBN 978-5-534-12474-3.	

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

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Поисковые системы: Yandex, Google, Mail.

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).

Операционная система Microsoft Windows.

Microsoft Office.

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:

Зачет в 5 семестре.

Курсовая работа в 6 семестре.

Экзамен в 6 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