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)

Квантовая криптография

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 «Квантовая криптография» является формирование профессиональных компетенций по основным разделам дисциплины.

Задачами дисциплины являются:

- изучение методов кодирования в квантовой криптографии;
- изучение протоколов квантовых коммуникаций;
- студенты должны научиться применять методы и средства квантовой криптографии при атаках на защищенные квантовые каналы.

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:

- физические основы процессов, использующихся в квантовых технологиях для шифрования информации;
- методы кодирования в квантовой криптографии;
- протоколы квантового распределения ключей;
- политики информационной безопасности;
- нормативные и методические материалы по вопросам обеспечения информационной безопасности.

Уметь:

- оценивать уровень безопасности объекта защиты;
- применять методы квантовой криптографии для защиты информации.
- применять комплексный подход к обеспечению информационной безопасности объекта защиты;
- осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов;
- составлять обзор по вопросам обеспечения информационной безопасности.

Владеть:

- навыками применения комплексной защиты при атаках на объект информатизации, включая квантовые каналы;

- навыками реализации политики информационной безопасности;

- навыками применения комплексного подхода к обеспечению информационной безопасности объекта защиты с использованием средств квантовой криптографии;

- навыками подбора и составления обзора научно-технической литературы по вопросам обеспечения информационной безопасности.

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 №10
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	МЕТОДЫ КОДИРОВАНИЯ В КВАНТОВОЙ КРИПТОГРАФИИ Рассматриваемые вопросы: - поляризационное кодирование; - фазовое кодирование; - частотное кодирование; - релятивистская квантовая криптография.
2	ТЕХНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ КВАНТОВОЙ КРИПТОГРАФИИ Рассматриваемые вопросы: - источники одиночных фотонов; - квантовые каналы; - детекторы одиночных фотонов; - генераторы случайных чисел.
3	АТАКИ НА ЗАЩИЩЕННЫЕ КВАНТОВЫЕ КАНАЛЫ КОММУНИКАЦИИ Рассматриваемые вопросы: - виды атак; - атака с делением числа фотонов.
4	ОСНОВНЫЕ ПРОТОКОЛЫ КВАНТОВЫХ КОММУНИКАЦИЙ И ИХ ОПИСАНИЕ Рассматриваемые вопросы: - квантовая телепортация; - сверхплотное кодирование; - квантовое распределение ключей.
5	ОДНОРАЗОВЫЕ КЛЮЧИ Рассматриваемые вопросы: - критерий Шеннона абсолютной секретности; - квантово-механические запреты на копирование неизвестного квантового состояния; - основные стадии квантовых протоколов распределения ключей.
6	КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ Рассматриваемые вопросы: - защита посредством неортогональных состояний; - защита посредством перепутывания.
7	КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ С ОДИНОЧНЫМИ ЧАСТИЦАМИ Рассматриваемые вопросы: - поляризованные фотоны; - системы, кодированные по фазе.
8	КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ С ПОМОЩЬЮ ПЕРЕПУТАННЫХ СОСТОЯНИЙ Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- критерии защиты; - квантовое подслушивание; - исправление ошибок; - усиление секретности.
9	ЭКСПЕРИМЕНТАЛЬНЫЕ РЕАЛИЗАЦИИ Рассматриваемые вопросы: - кодирование поляризации; - кодирование фазы; - квантовая криптография, основанная на перепутывании
10	ОСНОВНЫЕ ПРОТОКОЛЫ Рассматриваемые вопросы: - протокол подготовки и измерения; - протоколы, основанные на запутанности; - релятивистское квантовое распределение ключей через открытое пространство с синхронизацией и без синхронизации часов на приемной и передающей стороне.
11	ПРОТОКОЛ BB84 Рассматриваемые вопросы: - используемые квантовые состояния и кодирование состояний; - обнаружение и исправление ошибок, обнаружение вторжения; - криптоанализ протокола; - атака разделения числа фотонов.
12	ПРОТОКОЛ BBM92 Рассматриваемые вопросы: - особенности; - алгоритм; - криптоанализ.
13	ПРОТОКОЛ B92 Рассматриваемые вопросы: - описание; - обнаружение вторжения: - криптостойкость протокола.
14	ЗАЦЕПЛЕННЫЕ СОСТОЯНИЯ. ПРОТОКОЛ E9 Рассматриваемые вопросы: - зацепленные состояния частиц, ЭПР-пара; - неравенство Белла, обобщенная теорема Белла; - описание и обоснование работы протокола; - криптоанализ протокола.
15	ДРУГИЕ ПРОТОКОЛЫ (SARG04, Lo05 и др.) Рассматриваемые вопросы: - описание и обоснование алгоритма; - особенности; - криптоанализ.

№ п/п	Тематика лекционных занятий / краткое содержание
16	АППАРАТНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ КВАНТОВОЙ КРИПТОГРАФИИ Рассматриваемые вопросы: - особенности и общие требования; - примеры работающих квантово-криптографических систем. - процедуры настройки устройства квантовой криптографии.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Исследование классических шифров замены и перестановки (Цезарь, Атбаш, Скитала) В результате работы студентом будут исследованы и проанализированы методы шифрования заменой (Цезарь, Атбаш) и перестановкой (Скитала), выполнено практическое шифрование и дешифрование текстов различной длины, проведен частотный анализ для вскрытия шифра Цезаря, а также подготовлен отчет с выводами о криптостойкости классических алгоритмов к современным методам криптоанализа.
2	Исследование шифра Вижинера и методов его криптоанализа В результате работы студентом будут исследованы и проанализированы принципы работы шифра Вижинера (таблица Вижинера, ключевое слово), выполнено шифрование и дешифрование текстов с различными ключами, проведен криптоанализ с использованием метода Касиски (поиск повторяющихся фрагментов) и индекса совпадений для определения длины ключа, а также подготовлен отчет с выводами об уязвимостях полиалфавитных шифров.
3	Исследование модульной арифметики и её применения в криптографии В результате работы студентом будут исследованы и проанализированы алгоритмы модульной арифметики (расширенный алгоритм Евклида для нахождения обратного элемента, быстрое возведение в степень по модулю, решение сравнений первой степени, китайская теорема об остатках), выполнены практические вычисления, необходимые для реализации криптографических алгоритмов RSA и Диффи-Хэллмана, а также подготовлен отчет с примерами применения модульных вычислений.
4	Исследование алгоритма DES (Data Encryption Standard) и его уязвимостей В результате работы студентом будут исследованы и проанализированы структура алгоритма DES (сеть Фейстеля, S-блоки, расписание ключей), выполнена программная реализация или ручной расчет одного раунда DES, проведен анализ уязвимостей (малый размер ключа 56 бит, возможность дифференциального криптоанализа), а также подготовлен отчет с выводами о причинах замены DES на AES.
5	Исследование алгоритма AES (Advanced Encryption Standard) В результате работы студентом будут исследованы и проанализированы структура и все этапы раунда AES (SubBytes, ShiftRows, MixColumns, AddRoundKey), выполнена реализация одного раунда AES на учебных данных, проведен анализ генерации раундовых ключей (Key Schedule) и исследован лавинный эффект при изменении одного бита ключа или открытого текста, а также подготовлен отчет с обоснованием криптостойкости AES.

№ п/п	Тематика практических занятий/краткое содержание
6	Исследование режимов шифрования блочных алгоритмов (ECB, CBC, CFB, OFB, CTR) В результате работы студентом будут исследованы и проанализированы все основные режимы шифрования блочных алгоритмов, выполнено практическое шифрование графического изображения в режиме ECB (визуализация уязвимости — проявление повторяющихся блоков) и в режиме CBC (скрытие повторяющихся блоков), проведен анализ влияния ошибки в одном блоке шифротекста на расшифрованные блоки для каждого режима, а также подготовлен отчет с рекомендациями по выбору режима в зависимости от области применения.
7	Исследование потоковых шифров (RC4, ChaCha20) В результате работы студентом будут исследованы и проанализированы принципы работы потоковых шифров на примере RC4 (инициализация S-блока, генерация псевдослучайного ключевого потока) и ChaCha20 (структура раунда QR — Quarter Round), выполнено шифрование тестовых сообщений, проведен анализ уязвимостей RC4 (смещение первых байтов, применимость в протоколе WEP), а также подготовлен отчет со сравнением производительности и криптостойкости RC4 и ChaCha20.
8	Исследование кодов аутентификации сообщений (HMAC, CMAC) и режимов аутентифицированного шифрования (AES-GCM, ChaCha20-Poly1305) В результате работы студентом будут исследованы и проанализированы принципы построения HMAC на основе хэш-функций и CMAC на основе блочных шифров, выполнены генерация MAC для сообщений различной длины, а также исследованы режимы аутентифицированного шифрования (AEAD) — AES-GCM и ChaCha20-Poly1305, проведен анализ устойчивости к атакам на целостность (битовые искажения шифротекста), а также подготовлен отчет с выводами о применении MAC и AEAD для обеспечения целостности и подлинности данных.
9	Исследование протокола Диффи-Хэллмана (Diffie-Hellman) и атаки «человек посередине» В результате работы студентом будут исследованы и проанализированы математические основы протокола Диффи-Хэллмана (задача дискретного логарифмирования, выбор простого числа и первообразного корня), выполнена программная реализация выработки общего секретного ключа двумя абонентами, проведена эмуляция атаки «человек посередине» (MITM) на неаутентифицированный протокол, а также подготовлен отчет с выводами о необходимости аутентификации сторон при использовании DH.
10	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 модуля n и функции Эйлера ?(n), выбор открытой экспоненты e, вычисление закрытой экспоненты d), выполнены практическое шифрование и дешифрование числовых сообщений, проведен анализ зависимости криптостойкости RSA от размера ключа (512, 1024, 2048 бит), а также подготовлен отчет с выводами о факторах, влияющих на безопасность RSA.
11	Исследование алгоритмов цифровой подписи (RSA-PSS, DSA, ECDSA) В результате работы студентом будут исследованы и проанализированы принципы работы алгоритмов цифровой подписи RSA-PSS, DSA и ECDSA, выполнены генерация ключевых пар, подписание сообщения (с предварительным хэшированием) и проверка подписи, проведен анализ уязвимости DSA и ECDSA при повторном использовании случайного числа k (возможность

№ п/п	Тематика практических занятий/краткое содержание
	восстановления закрытого ключа), а также подготовлен отчет со сравнением размера подписи, производительности и области применения каждого алгоритма.
12	Исследование эллиптической криптографии (ECC, ECDH, EdDSA) В результате работы студентом будут исследованы и проанализированы основы эллиптической криптографии (эллиптические кривые над конечными полями, операции сложения и удвоения точек, задача дискретного логарифмирования на эллиптической кривой — ECDLP), выполнена программная реализация ECDH для выработки общего ключа и EdDSA для подписи сообщений, проведено сравнение ECC с RSA (размер ключа при одинаковой стойкости, скорость операций), а также подготовлен отчет с выводами о преимуществах ECC для мобильных устройств и встраиваемых систем.
13	Исследование криптографических хэш-функций (MD5, SHA-1, SHA-256) В результате работы студентом будут исследованы и проанализированы свойства криптографических хэш-функций (детерминизм, лавинный эффект, устойчивость к коллизиям), выполнено вычисление хэшей MD5, SHA-1 и SHA-256 для текстовых сообщений и файлов различной длины, проведен эксперимент по поиску коллизий для MD5 (с использованием готовых коллизионных блоков) и анализ лавинного эффекта (изменение одного бита сообщения), а также подготовлен отчет с выводами о непригодности MD5 и SHA-1 для современных криптографических приложений.
14	Исследование хэш-функции SHA-3 (Keccak) и атаки «дней рождения» В результате работы студентом будут исследованы и проанализированы принципы работы SHA-3 (губчатая конструкция — sponge construction, режимы впитывания — absorbing — и отжима — squeezing), выполнено вычисление хэшей SHA-3 для тестовых сообщений, проведен анализ атаки «дней рождения» для поиска коллизий (моделирование с уменьшенной разрядностью хэша 20–30 бит), а также подготовлен отчет с выводами о минимально безопасной длине хэша (256 бит и более) и целесообразности перехода на SHA-3.
15	Исследование инфраструктуры открытых ключей (PKI) и сертификатов X.509 В результате работы студентом будут исследованы и проанализированы компоненты PKI (удостоверяющий центр CA, регистрационный центр RA, репозиторий сертификатов), структура сертификата X.509 v3 (поля subject, issuer, public key, validity, extensions), цепочки доверия (корневой, промежуточный и конечный сертификаты), выполнена генерация самоподписанного сертификата и запроса на сертификат (CSR) с использованием OpenSSL, проведен анализ протоколов отзыва сертификатов (CRL и OCSP), а также подготовлен отчет с выводами о роли PKI в обеспечении безопасных коммуникаций.
16	Исследование протокола TLS (рукопожатие, анализ трафика и уязвимостей) В результате работы студентом будут исследованы и проанализированы этапы рукопожатия TLS 1.2 и TLS 1.3 (согласование шифров, аутентификация сервера, обмен ключами, установление сессионного ключа), выполнен захват и анализ TLS-трафика с помощью Wireshark (идентификация используемых CipherSuites, сертификатов, алгоритмов обмена ключами), проведен анализ уязвимостей устаревших версий (SSL 3.0 — атака POODLE, TLS 1.0 — атака BEAST), а также подготовлен отчет с рекомендациями по безопасной настройке TLS для веб-серверов.

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	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	«Защита информационных систем. Кибербезопасность» (Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург:Лань, 2024. — ISBN 978-5-507-48807-0	https://e.lanbook.com/book/394544
2	Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 400 с. — ISBN 978-5-507-49250-3. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/414947
3	Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/182491
4	Каширская, Е. Н. Криптографические системы : учебное пособие / Е. Н. Каширская, А. П. Кушнир. — Москва : РТУ МИРЭА, 2021. — 66 с. — Текст : электронный // Лань : электронно-библиотечная система.	https://e.lanbook.com/book/182424

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/

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 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, мультимедийное оборудование, доска.

Аудитория подключена к сети «Интернет».

9. Форма промежуточной аттестации:

Экзамен в 10 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