

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ))



Рабочая программа дисциплины (модуля),
как компонент образовательной программы
базового высшего образования
по направлению подготовки
02.03.02 Фундаментальная информатика и
информационные технологии,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Квантовая криптография

Направление подготовки: 02.03.02 Фундаментальная информатика и
информационные технологии

Направленность (профиль): Квантовые вычислительные системы и сети

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде
электронного документа выгружена из единой
корпоративной информационной системы управления
университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис
Владимирович
Дата: 07.06.2026

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):

ПК-3 - Способность применять физические основы процессов, использующихся в квантовых технологиях для шифрования информации.

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 3 з.е. (108 академических часа(ов)).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №6
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
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 60 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	МЕТОДЫ КОДИРОВАНИЯ В КВАНТОВОЙ КРИПТОГРАФИИ - поляризованное 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: - критерии защиты; - квантовое подслушивание; - исправление ошибок; - усиление секретности.
9	ЭКСПЕРИМЕНТАЛЬНЫЕ РЕАЛИЗАЦИИ Рассматриваемые вопросы: - кодирование поляризации;

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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.
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	АНАЛИЗ МЕТОДОВ КОДИРОВАНИЯ В КВАНТОВОЙ КРИПТОГРАФИИ В результате работы студентом будут исследованы и проанализированы методы кодирования и подготовлен отчет.

№ п/п	Тематика практических занятий/краткое содержание
2	ИССЛЕДОВАНИЕ ВИДОВ АТАК НА ЗАЩИЩЕННЫЕ КВАНТОВЫЕ КАНАЛЫ В результате работы студентом будут исследованы и проанализированы виды атак и подготовлен отчет.
3	КРИПТОСТОЙКОСТЬ ПРОТОКОЛА BB84 В результате работы студентом будет проанализирован криптоанализ протокола и подготовлен отчет.
4	АЛГОРИТМ РАБОТЫ ПРОТОКОЛА BBM92 В результате работы студентом будет подготовлен отчет, где представлен алгоритм работы протокола.
5	ОПИСАНИЕ ПРОТОКОЛА B92 В результате работы студентом будет подготовлен отчет с описанием протокола.
6	ПРОТОКОЛ E9 В результате работы студентом будет подготовлен отчет с описанием и обоснованием работы протокола.
7	ПРОТОКОЛ SARG04 В результате работы студентом будет подготовлен отчет, где представлен алгоритм работы протокола.
8	КВАНТОВО-КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ В результате работы студентом будет подготовлен отчет, где проанализированы квантово-криптографические системы, и применим комплексный подход к обеспечению информационной безопасности объекта 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	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:

Зачет в 6 семестре.

10. Оценочные материалы.

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

Авторы:

заведующий кафедрой, доцент, к.н.
кафедры «Вычислительные системы
и квантовые коммуникации»

Б.В. Желенков

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической
комиссии

Н.А. Андриянова