Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ

М.М. Лаврентьев
«18» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Квантовый криптоанализ, квантовая и постквантовая криптография

Направление подготовки: 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА
Направленность (профиль): Квантовые технологии и криптография

Форма обучения: очная
Год обучения: 2, семестр: 3

№	Вид деятельности	Семестр
		3
1	Лекции, час.	32
2	Практические занятия, час.	32
3	Лабораторные занятия, час.	
4	Занятий в контактной форме без учета промежуточной аттестации, час, из них	64
5	в электронной форме, час.	
6	из них аудиторных занятий, час.	64
7	из них в активной и интерактивной форме, час.	64
8	консультаций, час.	
9	Самостоятельная работа, час.	150
10	в том числе на выполнение письменных работ, час	75
11	Форма аттестации (экзамен, зачет, дифференцированный зачет), час	ДЗ 2
12	Всего зачетных единиц[1]	6

Новосибирск 2022

[1] С учетом выделенных часов на промежуточную аттестацию

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта (ФГОС) высшего образования - магистратура по направлению подготовки 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Федеральный государственный образовательный стандарт (ФГОС) высшего образования по направлению подготовки магистрантов 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА введен в действие приказом Минобрнауки 19.09.2017 № 918.

Место дисциплины в структуре учебного плана: Блок 1 Дисциплины (модули), обязательная дисциплина.

Рабочая программа дисциплины утверждена решением Ученого совета факультета информационных технологий от 28.03.2022, протокол № 84.

Программу разработали:

ассистент кафедры теоретической кибернетики ММФ НГУ
кандидат физико-математических наук  А.В. Куценко

Заведующий кафедрой систем информатики ФИТ,
доктор физико-математических наук  М.М. Лаврентьев

Ответственный за образовательную программу:

доцент КвЭл ФФ НГУ ФФ НГУ
кандидат физико-математических наук  И.И.Бетеров

Аннотация к рабочей программе дисциплины
«Квантовый криптоанализ, квантовая и постквантовая криптография»

Дисциплина «Квантовый криптоанализ, квантовая и постквантовая криптография» реализуется в рамках образовательной программы высшего образования – программы магистратуры 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА, направленность (профиль): КВАНТОВЫЕ ТЕХНОЛОГИИ И КРИПТОГРАФИЯ по очной форме обучения на английском языке.

Место в образовательной программе: Дисциплина **«Квантовый криптоанализ, квантовая и постквантовая криптография»** развивает знания, умения и навыки, сформированные у обучающихся по результатам изучения следующих дисциплин: «Теория вероятностей и математическая статистика».

Дисциплина «Квантовый криптоанализ, квантовая и постквантовая криптография» реализуется в 3 семестре в рамках базовой части дисциплин (модулей) Блока 1 и является обязательной дисциплиной.

Дисциплина **«Квантовый криптоанализ, квантовая и постквантовая криптография»** является базовой для выполнения работы в рамках практики и выполнением выпускной квалификационной работы.

Дисциплина **«Квантовый криптоанализ, квантовая и постквантовая криптография»** направлена на формирование компетенций:

Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте (ОПК-1), в части следующих индикаторов достижения компетенции:

ОПК-1.1. Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности

ОПК-1.2. Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний

ОПК-1.3. Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте

Перечень основных разделов дисциплины:

Тема 1. Математические основы квантовой информатики.
Тема 2. Основные понятие квантовой теории информации.
Тема 3. Протоколы квантового распределения ключей. Алгоритмы классической пост-обработки.
Тема 4. Атаки на протоколы квантового распределения ключей.
Тема 5. Основы квантовых вычислений.
Тема 6. Квантовый криптоанализ асимметричных шифров.
Тема 7. Квантовый криптоанализ симметричных шифров.
Тема 8. Основные направления постквантовой криптографии.
Тема 9. Криптография, основанная на кодах, исправляющих ошибки.
Тема 10. Криптография, основанная на решётках.

При освоении дисциплины студенты выполняют следующие виды учебной работы: лекции, практические занятия, самостоятельная работа. В учебном процессе предусматривается использование активных и интерактивных форм проведения занятий.

Самостоятельная работа включает: подготовку к практическим занятиям по разделам дисциплины, выполнение заданий, подготовку к дифференцированному зачету.

Общий объем дисциплины – 6 зачетных единиц (216 часов).

Правила аттестации по дисциплине. Текущий контроль по дисциплине «Квантовый криптоанализ, квантовая и постквантовая криптография» осуществляется на практических занятиях на основании оценки за портфолио (задания по темам практических занятий). По результатам защиты портфолио выставляется оценка «зачтено» или «не зачтено».

Промежуточная аттестация по дисциплине «Квантовый криптоанализ, квантовая и постквантовая криптография» проводится по завершению периода ее освоения (семестра). Промежуточная аттестация по дисциплине включает 2 этапа:

1) портфолио (задания по темам практических занятий);

2) дифференцированный зачет.

Оценка «зачтено» за портфолио является необходимым условием для прохождения промежуточной аттестации. Результаты промежуточной (итоговой по дисциплине) аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Учебно-методическое обеспечение дисциплины.

Учебно-методические материалы по дисциплине выкладываются на электронный ресурс, создаваемый для каждого нового набора

1. **Внешние требования к дисциплине**

Таблица 1.1

Компетенция ОПК-1 Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте, в части следующих индикаторов достижения компетенции:	
ОПК-1.1	Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности
ОПК-1.2	Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний
ОПК-1.3	Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте

2. Требования к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**		
	Лекции	**Практики / семинары**	**Самостоятельная работа**
ОПК-1.1 Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности			
1. Знать основной набор понятий квантовой информатики, квантовой теории информации, квантового криптоанализа, постквантовой криптографии, квантового распределения ключей;	+	+	+
ОПК-1.2 Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний			
2. Уметь решать актуальные задачи криптографии и криптоанализа с использованием современных методов квантовых технологий;	+	+	+
ОПК-1.3 Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте			
3. Владеть навыками общего выбора методов для решения конкретных задач квантового криптоанализа и разработки постквантовых криптосистем.	+	+	+

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час. (входит в общее кол-во часов)	Часы	Ссылки на результаты обучения
Семестр: 3			
Тема 1. Математические основы квантовой информатики.	6	6	1, 2, 3
Тема 2. Основные понятия квантовой теории информации.	6	6	1, 2, 3
Тема 3. Протоколы квантового распределения ключей. Алгоритмы классической пост-обработки.	4	4	1, 2, 3
Тема 4. Атаки на протоколы квантового распределения ключей.	2	2	1, 2, 3
Тема 5. Основы квантовых вычислений.	2	2	1, 2, 3
Тема 6. Квантовый криптоанализ асимметричных шифров.	2	2	1, 2, 3
Тема 7. Квантовый криптоанализ симметричных шифров.	4	4	1, 2, 3
Тема 8. Основные направления постквантовой криптографии.	2	2	1, 2, 3
Тема 9. Криптография, основанная на кодах, исправляющих ошибки.	2	2	1, 2, 3
Тема 10. Криптография, основанная на решётках.	2	2	1, 2, 3
Итого:	**32**	**32**	

Таблица 3.2

Темы практических занятий	Активные формы, час. (входит в общее кол-во часов)	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 3				
Тема 1. Математические основы квантовой информатики. История развития квантовой механики. Чистое и смешанное квантовое состояние. Квантовые измерения общего вида, проективные измерения (измерения фон Неймана). Теорема о неразличимости неортогональных квантовых состояний. Теорема о невозможности копирования произвольного квантового состояния.	6	6	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 2. Основные понятия квантовой теории информации. Понятие квантового бита (кубита). Энтропия фон Неймана. Система из двух кубитов. Запутанность (сцепленность) квантовых состояний. Квантовая	6	6	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы

телепортация. Очищение квантовых состояний, теорема Шмидта. Квантовое сверхплотное кодирование. Квантовые коды, исправляющие ошибки.				
Тема 3. Протоколы квантового распределения ключей. Алгоритмы классической пост-обработки. История вопроса. Общая схема протокола BB84. Доказательство стойкости протокола. Описание протоколов E91, B92, 4+2, SARG04, DPS, COW. Исправление ошибок в просеянном ключе. Верификация исправленного ключа. Оценка уровня ошибок. Усиление секретности. Аутентификация классического канала связи.	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 4. Атаки на протоколы квантового распределения ключей. Атака типа “прием-перепосыл”. Прозрачное индивидуальное подслушивание. Коллективная атака. Когерентная атака. Атака с разделением по числу фотонов (PNS-атака). Общее описание PNS-атаки. PNS-атака на протоколы BB84, B92, 4+2, SARG04. Критическая длина связи.	2	2	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 5. Основы квантовых вычислений. История вопроса. Эволюция квантового состояния во времени. Уравнение Шрёдингера. Вентиль Адамара. Универсальные наборы квантовых вентилей. Алгоритм Дойча. Алгоритм Дойча-Йожа. Модели Q1 и Q2 квантовых вычислений.	2	2	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 6. Квантовый криптоанализ асимметричных шифров. Криптосистемы Диффи-Хеллмана и RSA. Задачи факторизации, дискретного логарифмирования. Алгоритмы Шора решения задач факторизации и дискретного лагарифмирования. Криптография с открытым ключом на эллиптических кривых.	2	2	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 7. Квантовый криптоанализ симметричных шифров. Алгоритм Саймона. Квантовая атака на криптосистему Even-	4	4	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы

Mansour. Квантовая атака на режим шифрования CBC-MAC. Алгоритм Гровера. Квантовый линейный криптоанализ. Алгоритм Бернштейна-Вазирани. Квантовый разностный криптоанализ.				
Тема 8. Основные направления постквантовой криптографии. История вопроса и современное состояние. Общий обзор криптосистем, основанных на хеш-функциях; на кодах, исправляющих ошибки; на решетках; на суперсингулярных изогениях; на системах уравнений от многих переменных. Этапы стандартизации постквантовой криптографии.	2	2	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 9. Криптография, основанная на кодах, исправляющих ошибки. Коды, исправляющие ошибки. Линейный код. Задача декодирования линейного кода. Криптосистема Мак-Элиса. Криптосистема Нидеррайтера. Атака на основе процедуры Information set decoding.	2	2	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Тема 10. Криптография, основанная на решётках. Основные сведения из теории решеток. Задача нахождения ближайшего вектора (CVP). Задача нахождения кратчайшего вектора в решетке (SVP). Задача обучения с ошибками в кольце. Криптосистема NTRU, известные атаки на нее.	2	2	1, 2, 3	Разбор представленного теоретического материала, решение задач, практическое применение изученной темы
Итого:	**32**	**32**		

4. Самостоятельная работа студентов

Таблица 4.1

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 3				
1	Изучение разделов дисциплины по учебной литературе, в том числе вопросов, не освещаемых на лекциях	1, 2, 3	45	
	Изучение предлагаемых теоретических разделов в соответствии с настоящей Программой. Учебно-методические материалы по дисциплине выложены на странице курса в сети Интернет			
2	Подготовка к практическим занятиям, к текущему контролю знаний	1, 2, 3	75	
	Выполнение заданий			

3	Подготовка к дифференцированному зачету	1, 2, 3	30	
	Повторение теоретического материала по вопросам, совпадающим с темами лекций			
	Итого		150	

5. Образовательные технологии

В ходе реализации учебного процесса по дисциплине проводятся лекционные и практические занятия. Темы, рассматриваемые на лекциях и изучаемые самостоятельно, закрепляются на практических занятиях. Применяются такие формы проведения практических занятий, как обсуждение и защита результатов работы, а также используются следующие интерактивные формы обучения (таблица 5.1).

Таблица 5.1

Технологии проблемного обучения	ОПК-1
Формируемые умения: уметь ориентироваться в современных методах квантового криптоанализа и постквантовой криптографии;	
Краткое описание применения: Постановка под руководством преподавателя проблемных задач и активная самостоятельная деятельность обучающихся по их разрешению, сопровождающаяся обсуждением результатов.	
Портфолио	ОПК-1
Формируемые умения: Уметь ориентироваться в современных методах квантового криптоанализа и постквантовой криптографии; владеть навыками общего выбора методов для решения конкретных задач квантового криптоанализа и разработки постквантовых криптосистем.	
Краткое описание применения: студенты ведут портфолио (коллекцию работ), которое является основой для проведения аттестации по дисциплине.	

Для организации и контроля самостоятельной работы студентов, а также проведения консультаций применяются информационно-коммуникационные технологии (таблица 5.2).

Таблица 5.2

Практические занятия	www.crypto.nsu.ru
Информирование	www.crypto.nsu.ru
Консультирование	www.crypto.nsu.ru
Контроль	www.crypto.nsu.ru
Размещение учебных материалов	www.crypto.nsu.ru

6. Правила аттестации студентов по учебной дисциплине

По дисциплине «Квантовый криптоанализ, квантовая и постквантовая криптография» проводится текущая и промежуточная аттестация (итоговая по дисциплине).

Текущая аттестация по дисциплине «Квантовый криптоанализ, квантовая и постквантовая криптография» осуществляется на практических занятиях и представлена защитой заданий на практических занятиях. В ходе обучения каждый студент должен выполнить задания. По результатам текущей аттестации выставляется оценка «зачтено»

или «не зачтено». Оценка «зачтено» по результатам защиты заданий является одним из условий успешного прохождения промежуточной аттестации.

Для получения оценки «зачтено» каждое задание должно быть выполнено и защищено в полном соответствии с предъявляемыми требованиями.

Промежуточная аттестация по дисциплине «Квантовый криптоанализ, квантовая и постквантовая криптография» проводится по завершению периода ее освоения (семестра). Промежуточная аттестация по дисциплине включает 2 этапа:

1) портфолио (задания по темам практических занятий);

2) дифференцированный зачет.

Оценка «зачтено» за портфолио является необходимым условием для прохождения промежуточной аттестации. Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

В таблице 6.1 представлено соответствие форм аттестации заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.1

Коды компетенций ФГОС	**Результаты обучения**	**Формы аттестации**	
		1 этап - портфолио	**2 этап – дифференцированный зачет**
ОПК-1	**ОПК-1.1.** Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности	+	+
	ОПК-1.2. Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний	+	+
	ОПК-1.3. Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте	+	+

Требования к структуре и содержанию портфолио, оценочные средства, а также критерии оценки сформированности компетенций и освоения дисциплины в целом, представлены в Фонде оценочных средств, являющемся приложением 1 к настоящей рабочей программе дисциплины.

7. Перечень учебной литературы

1. Нильсен, Майкл А. Квантовые вычисления и квантовая информация / М. Нильсен, И. Чанг ; пер. с англ. под ред. М.Н. Вялого, П.М. Островского / с предисл. К.А. Валиева. М. : Мир, 2006. 822 с. : ил. ; 25 см. ISBN 5-03-003524-9. (2 экз.)

8. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения дисциплины

При освоении дисциплины используются следующие ресурсы:

- электронная информационно-образовательная среда НГУ (ЭИОС);

- образовательные интернет-порталы;
- информационно-телекоммуникационная сеть Интернет.

Взаимодействие обучающегося с преподавателем (синхронное и (или) асинхронное) осуществляется через личный кабинет студента в ЭИОС

Таблица 8.1

№ п/п	Наименование Интернет-ресурса	Краткое описание
1	www.crypto.nsu.ru	Cryptographic center (Novosibirsk) Sobolev Institute of Mathematics Mathematical Center in Akademgorodok Novosibirsk State University

9. Учебно-методическое и программное обеспечение дисциплины

9.1. Перечень учебно-методических материалов по самостоятельной работе обучающихся

Для обеспечения самостоятельной работы обучающихся при изучении дисциплины используются следующие учебно-методические материалы:

1. Рабочая программа дисциплины, соответствующие разделы.
2. Учебники, учебные пособия и дополнительные материалы, указанные в соответствующих разделах настоящей рабочей программы
3. Перечень ресурсов информационно-коммуникационной сети «Интернет», указанные в соответствующих разделах настоящей рабочей программы.
4. Методические указания для обучающихся по освоению дисциплины, обеспечивающие самостоятельную работу студента при подготовке к учебным занятиям, выполнении домашних работ, подготовке к контрольным мероприятиям и аттестациям, приведенные в соответствующих разделах настоящей рабочей программы и приложения к ней.

9.2. Программное обеспечение

Для обеспечения реализации дисциплины используется стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MS Office.

Перечень специализированного программного обеспечения для изучения дисциплины представлен в таблице 9.1.

Специализированное программное обеспечение

Таблица 9.1

№	Наименование ПО	Назначение
1	Microsoft Visual Studio 2013	Среда разработки приложений

10. Профессиональные базы данных и информационные справочные системы

1. Полнотекстовые электронные ресурсы Freedom Collection издательства Elsevier (Нидерланды) (2 предметные коллекции – Computer Science, Mathematics)
2. БД Scopus (Elsevier)

11. Материально-техническое обеспечение

Для реализации дисциплины используются специальные помещения:

1. Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля, промежуточной и итоговой аттестации;

2. Помещения для самостоятельной работы обучающихся;

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду НГУ.

Для проведения занятий лекционного типа предлагаются следующие наборы демонстрационного оборудования и учебно-наглядных пособий:

- комплект лекций-презентаций по темам дисциплины;

Таблица 11.1

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Для проведения лекционных и практических занятий
2	Компьютерный класс (с выходом в Internet)	Для организации самостоятельной работы обучающихся

Материально-техническое обеспечение образовательного процесса по дисциплине для обучающихся из числа лиц с ограниченными возможностями здоровья осуществляется согласно «Порядку организации и осуществления образовательной деятельности по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья в Новосибирском государственном университете».

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования «Новосибирский национальный исследовательский
государственный университет» (Новосибирский государственный университет, НГУ)

Факультет информационных технологий

СОГЛАСОВАНО
Декан ФИТ НГУ
_____ М.М. Лаврентьев

«18» апреля 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ
по дисциплине Квантовый криптоанализ, квантовая и постквантовая криптография

Направление подготовки: 09.04.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА.

Направленность (профиль): Квантовые технологии и криптография
Квалификация: Магистр

Форма обучения: очная

Год обучения: 2, семестр 3

Форма аттестации	Семестр
Дифзачет	3

Новосибирск 2022

Фонд оценочных средств промежуточной аттестации является **Приложением 1** к рабочей программе дисциплины «Квантовый криптоанализ, квантовая и постквантовая криптография», реализуемой в рамках образовательной программы высшего образования – программы магистратуры 09.04.01 Информатика и вычислительная техника, направленность (профиль): Квантовые технологии и криптография

Фонд оценочных средств промежуточной аттестации по дисциплине утвержден решением Ученого совета факультета информационных технологий протокол № 84 от 28.03.2022 г.

Разработчик:
ассистент кафедры теоретической кибернетики ММФ НГУ
кандидат физико-математических наук А.В. Куценко

Заведующий кафедрой систем информатики ФИТ,
доктор физико-математических наук М.М. Лаврентьев

Ответственный за образовательную программу:
Доцент кафедры квантовой электроники ФФ,
кандидат физико-математических наук И.И.Бетеров

1. Содержание и порядок проведения промежуточной аттестации по дисциплине

1.1. Общая характеристика содержания промежуточной аттестации

Промежуточная аттестация по дисциплине «Квантовый криптоанализ, квантовая и постквантовая криптография» проводится по завершению периода освоения образовательной программы (семестра) для оценки сформированности компетенций в части следующих индикаторов достижения компетенции (таблица П1.1).

Таблица П1.1

Коды компетенций ФГОС	Компетенции, формируемые в рамках дисциплины «Квантовый криптоанализ, квантовая и постквантовая криптография»	Семестр 3	
		портфолио	дифзачет
ОПК-1 Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте			
ОПК-1.1	Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности	+	+
ОПК-1.2	Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний	+	+
ОПК-1.3	Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте	+	+

Тематика вопросов к диф.зачету соответствует избранным разделам (темам) дисциплины «Квантовый криптоанализ, квантовая и постквантовая криптография»

Тема 1. Математические основы квантовой информатики.
Тема 2. Основные понятие квантовой теории информации.
Тема 3. Протоколы квантового распределения ключей. Алгоритмы классической пост-обработки.
Тема 4. Атаки на протоколы квантового распределения ключей.
Тема 5. Основы квантовых вычислений.
Тема 6. Квантовый криптоанализ асимметричных шифров.
Тема 7. Квантовый криптоанализ симметричных шифров.
Тема 8. Основные направления постквантовой криптографии.
Тема 9. Криптография, основанная на кодах, исправляющих ошибки.
Тема 10. Криптография, основанная на решётках.

Промежуточная аттестация включает 2 этапа:

1. Портфолио.
2. Дифзачет.

Все компетенции, формируемые в рамках дисциплины, оцениваются как через портфолио, так и на дифзачете.

1.2. Порядок проведения промежуточной аттестации по дисциплине

Промежуточная аттестация проводится в форме дифзачета и включает 2 этапа: портфолио и дифзачет. Необходимым условием для прохождения промежуточной аттестации является оценка «зачтено» по результатам выполненного портфолио. Для оценивания портфолио студенту необходимо сдать все работы, входящие в структуру портфолио.

Портфолио включает выполнение заданий по темам практических занятий.

Дифзачет проводится в устной форме, в аудитории, студентам разрешено пользоваться бумагой для записей и авторучкой. Во время проведения дифзачета студенту разрешается использовать справочники, учебную и научную литературу, компьютеры. В процессе ответа на вопросы дифзачета студенту могут быть заданы дополнительные вопросы по темам дисциплины.

2. **Требования к структуре и содержанию фонда оценочных средств промежуточной аттестации по дисциплине**

Перечень оценочных средств, применяемых на каждом этапе проведения промежуточной аттестации по дисциплине, представлен в таблице П1.2.

Таблица П1.2

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Этап 1 - портфолио			
1.	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах	Структура портфолио
Этап 2 – Дифзачет			
2	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины

2.1. Требования к структуре и содержанию оценочных средств аттестации в семестре

Текущая аттестация по дисциплине «Квантовый криптоанализ, квантовая и постквантовая криптография» проводится в форме портфолио. Промежуточная аттестация проводится в формате дифзачета.

2.1.1 Требования к структуре и содержанию портфолио

Портфолио включает защиту заданий на практических занятиях.

Оценка за курс выставляется по результатам дифзачета. Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

2.1.2 Перечень вопросов дифзачета 1 семестра

Тема 1. Математические основы квантовой информатики. История развития квантовой механики. Чистое и смешанное квантовое состояние. Квантовые измерения общего вида, проективные измерения (измерения фон Неймана). Теорема о неразличимости неортогональных квантовых состояний. Теорема о невозможности копирования произвольного квантового состояния.

Тема 2. Основные понятия квантовой теории информации. Понятие квантового бита (кубита). Энтропия фон Неймана. Система из двух кубитов. Запутанность (сцепленность) квантовых состояний. Квантовая телепортация. Очищение квантовых состояний, теорема Шмидта. Квантовое сверхплотное кодирование. Квантовые коды, исправляющие ошибки.

Тема 3. Протоколы квантового распределения ключей. Алгоритмы классической пост-обработки. История вопроса. Общая схема протокола BB84. Доказательство стойкости протокола. Описание протоколов E91, B92, 4+2, SARG04, DPS, COW. Исправление ошибок в просеянном ключе. Верификация исправленного ключа. Оценка уровня ошибок. Усиление секретности. Аутентификация классического канала связи.

Тема 4. Атаки на протоколы квантового распределения ключей. Атака типа “прием-перепосыл”. Прозрачное индивидуальное подслушивание. Коллективная атака. Когерентная атака. Атака с разделением по числу фотонов (PNS-атака). Общее описание PNS-атаки. PNS-атака на протоколы BB84, B92, 4+2, SARG04. Критическая длина связи.

Тема 5. Основы квантовых вычислений. История вопроса. Эволюция квантового состояния во времени. Уравнение Шрёдингера. Вентиль Адамара. Универсальные наборы квантовых вентилей. Алгоритм Дойча. Алгоритм Дойча-Йожа. Модели Q1 и Q2 квантовых вычислений.

Тема 6. Квантовый криптоанализ асимметричных шифров. Криптосистемы Диффи-Хеллмана и RSA. Задачи факторизации, дискретного логарифмирования. Алгоритмы Шора решения задач факторизации и дискретного лагарифмирования. Криптография с открытым ключом на эллиптических кривых.

Тема 7. Квантовый криптоанализ симметричных шифров. Алгоритм Саймона. Квантовая атака на криптосистему Even-Mansour. Квантовая атака на режим шифрования CBC-MAC. Алгоритм Гровера. Квантовый линейный криптоанализ. Алгоритм Бернштейна-Вазирани. Квантовый разностный криптоанализ.

Тема 8. Основные направления постквантовой криптографии. История вопроса и современное состояние. Общий обзор криптосистем, основанных на хеш-функциях; на кодах, исправляющих ошибки; на решетках; на суперсингулярных изогениях; на системах уравнений от многих переменных. Этапы стандартизации постквантовой криптографии.

Тема 9. Криптография, основанная на кодах, исправляющих ошибки. Коды, исправляющие ошибки. Линейный код. Задача декодирования линейного кода. Криптосистема Мак-Элиса. Криптосистема Нидеррайтера. Атака на основе процедуры Information set decoding.

Тема 10. Криптография, основанная на решётках. Основные сведения из теории решеток. Задача нахождения ближайшего вектора (CVP). Задача нахождения кратчайшего вектора в решетке (SVP). Задача обучения с ошибками в кольце. Криптосистема NTRU, известные атаки на нее.

Набор вопросов к дифзачету формируется и утверждается в установленном порядке в начале учебного года при наличии контингента обучающихся, завершающих освоение дисциплины «Квантовый криптоанализ, квантовая и постквантовая криптография» в текущем учебном году.

3. **Критерии оценки сформированности компетенций в рамках промежуточной аттестации по дисциплине**

Таблица П1.5

Шифр компетенций	**Структурные элементы оценочных средств**	**Показатель сформированности**	**Не сформирован**	**Пороговый уровень**	**Базовый уровень**	**Продвинутый уровень**
ОПК-1	Портфолио (этап 1), Дифзачет (этап 2)	ОПК-1.1 Знать: математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности	Не знает математические, естественнонаучные и социально-экономические методы для использования в профессиональной деятельности	Допускает грубые ошибки, слабо знает основной набор понятий квантовой информатики, квантовой теории информации, квантового криптоанализа, постквантовой криптографии, квантового распределения ключей	Знает основной набор понятий квантовой информатики, квантовой теории информации, квантового криптоанализа, постквантовой криптографии, квантового распределения ключей	Уверенно знает основной набор понятий квантовой информатики, квантовой теории информации, квантового криптоанализа, постквантовой криптографии, квантового распределения ключей
ОПК-1	Портфолио (этап 1), Дифзачет (этап 2)	ОПК-1.2 Уметь: решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний	Не умеет решать нестандартные профессиональные задачи с применением математиче-	Демонстрирует ошибки, слабо умеет решать актуальные задачи криптографии и криптоанализа с использованием современных	Умеет решать актуальные задачи криптографии и криптоанализа с использованием современных методов квантовых технологий, допускает незначительные погреш-	Умеет грамотно решать актуальные задачи криптографии и криптоанализа с использованием современных методов квантовых технологий

			ских, естественнонаучных, социально-экономических и профессиональных знаний	методов квантовых технологий	ности	
ОПК-1	Портфолио (этап 1), Дифзачет (этап 2)	ОПК-1.3 Владеть: навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте	Не владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, в том числе в новой или незнакомой среде и в междисциплинарном контексте	Слабо владеет навыками общего выбора методов для решения конкретных задач квантового криптоанализа и разработки постквантовых криптосистем	Владеет навыками общего выбора методов для решения конкретных учебных задач квантового криптоанализа и разработки постквантовых криптосистем	Уверенно владеет навыками общего выбора методов для решения задач квантового криптоанализа и разработки постквантовых криптосистем

4. **Критерии выставления оценок по результатам промежуточной аттестации по дисциплине**

Результаты промежуточной аттестации определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение промежуточной аттестации.

Оценка «отлично» соответствует продвинутому уровню сформированности компетенции.

Оценка «хорошо» соответствует базовому уровню сформированности компетенции.

Оценка «удовлетворительно» соответствует пороговому уровню сформированности компетенции.

Оценка «неудовлетворительно» выставляется, если хотя бы одна компетенция не сформирована.

Итоговая оценка результатов промежуточной аттестации выставляется как оценка за дифзачет.