Письменный отзыв официального рецензента
на диссертационную работу
Юбузовой Халичи Ибрагимовны
на тему «Методы безопасного распределения ключей на базе протоколов квантовой криптографии», представленную на соискание степени доктора философии (PhD) по специальности 6D070400 – «Вычислительная техника и программное обеспечение»

№ п/п	Критерии	Соответствие критериям (необходимо отметить один из вариантов ответа)	Обоснование позиции официального рецензента
1.	Тема диссертации (на дату ее утверждения) соответствует направлениям развития науки и/или государственным программам	1.1 Соответствие приоритетным направлениям развития науки или государственным программам: 1) Диссертация выполнена в рамках проекта или целевой программы, финансируемого(ой) из государственного бюджета (указать название и номер проекта или программы) 2) Диссертация выполнена в рамках другой государственной программы (указать название программы) 3) Диссертация соответствует приоритетному направлению развития науки, утвержденному Высшей научно-технической комиссией при Правительстве Республики Казахстан (указать направление)	Соответствует. Тема диссертации связана с научно-исследовательскими работами, выполняемыми в рамках Концепции кибербезопасности «Киберщит Казахстана». Данная концепция разработана в соответствии с Посланием Президента Республики Казахстан «Третья модернизация Казахстана: Глобальная конкурентоспособность» с учетом подходов Стратегии «Казахстан-2050» по вхождению Казахстана в число 30-ти самых развитых государств мира. А также результаты данной работы соответствуют целям и задачам Государственной программы «Информационный Казахстан-2020». Кроме этого, работа связана с научно-исследовательской работой «Квантово-криптографические методы защиты критической информационной инфраструктуры государства» №0117U006770, выполнялась на протяжении 2017-2019 в Национальном авиационном университете (Киев, Украина).
2.	Важность для науки	Работа вносит/не вносит существенный вклад в науку, а ее важность хорошо раскрыта/не раскрыта	Полученные в диссертационной работе результаты могут быть использованы для решения проблемы распределения ключей, а также для повышения эффективности систем криптографической защиты информации. В диссертационной работе разработаны эффективные модели квантового детерминистического протокола в режиме контроля подслушивания и в режиме передачи сообщений, предложен новый метод усиления секретности с использованием квантовых перепутанных состоя-

			ний пар кутритов и сгенерированных троичных псевдослучайных последовательностей, разработана комбинированная модель на основе разработанных эффективных моделей квантового детерминистического протокола с парами перепутанных кутритов и метода усиления секретности. В качестве замечания можно указать следующее. Определения таких понятий, используемых в работе, как детерминистический протокол, некогерентная атака, деполяризующий канал – не совсем полны.
3.	Принцип самостоятельности	Уровень самостоятельности: 1) Высокий; 2) Средний; 3) Низкий; 4) Самостоятельности нет	Диссертационная работа Юбузовой Х.И. является законченным научным трудом, который содержит новые научно обоснованные теоретические и экспериментальные результаты, которые в совокупности существенны для развития теории и практики систем защиты информации. Автором самостоятельно проведены все исследовательские работы.
4.	Принцип внутреннего единства	4.1 Обоснование актуальности диссертации: 1) Обоснована; 2) Частично обоснована; 3) Не обоснована.	Учитывая внедрение современных информационно-коммуникационных технологий (ИКТ) во все сферы жизнедеятельности, а также увеличение количества и мощности кибератак на них, обеспечение кибербезопасности является одним из ключевых вопросов государства. Традиционные методы безопасности (в частности, криптографические алгоритмы) не позволяют в полной мере обеспечить защиту от всех известных сегодня атак, а именно они потенциально уязвимы к атакам на основе квантовых алгоритмов (Шора, Гровера, Ксионга-Ванга, Дойча-Йожи и т.д.). Указанные методы основываются на принципиальной невозможности злоумышленником решить сложную математическую задачу за полиномиальное время, но увеличение вычислительных мощностей ИКТ ставит под сомнение эффективность защиты (в случае, если квантовый компьютер окажется в руках злоумышленника) и побуждает к поиску альтернативных методов безопасности, которые будут оставаться устойчивыми в постквантовый период. Такими подходами могут быть методы квантовой криптографии, на разработку которых и направлена работа соискателя.
		4.2. Содержание диссертации отражает тему диссертации: 1) Отражает; 2) Частично отражает; 3) Не отражает	Содержание диссертации в полном объёме отображает тему, цель и задачи диссертации. Начиная с введения, четырех разделов и заключения в диссертации в полном объеме излагается содержание полученных результатов соответственно теме научно-исследовательской работы. Общий объем дис-

			сертации: 144 страницы, машинописного текста, содержащего 54 рисунка, 24 таблицы, список использованных источников, состоящий из 103 наименований.
		4.3. Цель и задачи соответствуют теме диссертации: 1) соответствуют; 2) частично соответствуют; 3) не соответствуют	Цели и задачи исследования соответствуют теме диссертации. Цель исследований – разработка моделей безопасного распределения секретных ключей и повышение эффективности их распределения за счет использования комбинированной модели на базе протоколов квантовой криптографии. Для достижения цели были решены следующие логически связанные задачи: 1) проведен анализ современных методов, моделей и коммерческих систем распределения ключей шифрования по критериям безопасности (защищенности) и скорости; 2) разработана модель угроз и модель нарушителя в квантово-криптографических системах; 3) разработана и исследована модель квантового детерминистического протокола в режиме контроля подслушивания; 4) разработана и исследована модель квантового детерминистического протокола в режиме передачи сообщений; 5) разработана комбинированная модель с режимом контроля подслушивания и режимом передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов; 6) предложен новый метод безопасного распределения ключей комбинированной модели с режимом контроля подслушивания и режимом передачи сообщений квантового детерминистического протокола
		4.4 Все разделы и положения диссертации логически взаимосвязаны: 1) полностью взаимосвязаны; 2) взаимосвязь частичная; 3) взаимосвязь отсутствует	Структурно диссертация состоит из введения, 4 разделов и заключения. Все разделы и положения диссертации логически связаны. Во *введении* изложено обоснование актуальности темы диссертационной работы, сформулированы цель, объект и предмет научно-исследовательской работы. Также представлены научная новизна и практическая значимость работы. Приведены сведения об апробации и публикации результатов исследовательских работ. *В первом разделе* проведен детальный анализ методов распределения криптографических ключей, представлены теоретические основы квантовой криптографии, а также изложен обзор коммерческих решений квантовой криптографии, на основании чего представлена классификация квантовых методов защиты информации. *Во втором разделе* разработана расширенная классификация квантово-криптографических методов распределения ключей шифрования, описана абстрактная модель

			нарушителя в системах квантовой криптографии, а также представлена модель угроз в системах квантовой криптографии. *В третьем разделе* представлены разработанные модели квантового детерминистического протокола в разных режимах работы. Автором предложен новый метод усиления секретности, а также реализован синтез комбинированной модели на основе разработанных модели режима контроля подслушивания и модели режима передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов с использованием предложенного метода усиления секретности. В *четвертом разделе* приведены результаты экспериментального исследования, практические реализации и рекомендации по использованию квантовых детерминистических протоколов в квантово-криптографических системах. В *заключении* формулируются основные выводы и результаты работы.
		4.5 Предложенные автором новые решения (принципы, методы) аргументированы и оценены по сравнению с известными решениями: 1) критический анализ есть; 2) анализ частичный; 3) анализ представляет собой не собственные мнения, а цитаты других авторов	В работе проведен многокритериальный анализ квантовых систем и методов защиты. Как следствие получена классификация квантово-криптографических методов, которая позволяет расширить возможности при выборе необходимых квантово-криптографических методов для построения безопасных систем распределения ключей шифрования, а также приведена разработанная расширенная классификация квантово-криптографических методов распределения ключей шифрования. Достоверность каждого научного результата, решения и вывода, сформулированных в диссертации, подтверждается экспериментальными исследованиями (имитационным моделированием).
5.	Принцип научной новизны	5.1 Научные результаты и положения являются новыми? 1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	Научные результаты и принципы диссертации являются полностью новыми. Подтверждением является публикация результатов работы в рейтинговых научных изданиях, в том числе в тех что включены в науко-метрическую базу Scopus (Q2-Q3).
		5.2 Выводы диссертации являются новыми? 1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	Выводы диссертации являются полностью новыми.
		5.3 Технические, технологические, экономические или управленческие решения являются новыми и обоснованными:	Технические и технологические решения диссертационной работы являются новыми и обоснованными.

		1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	
6.	Обоснованность основных выводов	Все основные выводы основаны/не основаны на весомых с научной точки зрения доказательствах либо достаточно хорошо обоснованы (для qualitative research и направлений подготовки по искусству и гуманитарным наукам)	Результаты исследования диссертанта являются полностью обоснованными. Достоверность предложенных диссертантом теоретических положений, гипотез и математических моделей подтверждается соответствующими экспериментальными данными и результатами верификации предложенных методов и протоколов.
7.	Основные положения, выносимые на защиту	Необходимо ответить на следующие вопросы по каждому положению в отдельности: 7.1 Доказано ли положение? 1) доказано; 2) скорее доказано; 3) скорее не доказано; 4) не доказано 7.2 Является ли тривиальным? 1) да; 2) нет 7.3 Является ли новым? 1) да; 2) нет 7.4 Уровень для применения: 1) узкий; 2) средний; 3) широкий 7.5 Доказано ли в статье? 1) да; 2) нет	На защиту вынесены следующие положения: **1. Разработанные эффективные модели квантового детерминистического протокола в режиме контроля подслушивания и в режиме передачи сообщений, позволяющие повысить уровень доступности квантового канала и обеспечить безопасное и быстрое распределение ключей;** 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да, Ahmetov B., Gnatyuk S., Kinzeryavyy V., Yubuzova Kh. Model of simulation of operation of the deterministic protocol of safe communication in the quantum channel with noise, Bulletin of National Academy of Sciences of the Republic of Kazakhstan, 2018, Vol.2, Number 372, pp. 6-16. **2. Новый метод усиления секретности с использованием квантовых перепутанных состояний пар кутритов и сгенерированных троичных псевдослучайных последовательностей, позволяющий повысить скорость передачи детерминистических протоколов квантовой криптографии без потери стойкости к некогерентной атаке.** 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да,

			Zhengbing Hu, Gnatyuk S., Zhmurko T., Yubuzova Kh. High-speed privacy amplification method for deterministic quantum cryptography protocols using pairs of entangled qutrits, CEUR Workshops Proceedings. Vol. 2393, 2019, pp. 810-821. **3. Разработанная комбинированная модель на основе разработанных эффективных моделей квантового детерминистического протокола с парами перепутанных кутритов и метода усиления секретности, позволяющая усовершенствовать метод безопасного распределения ключей, обеспечить помехоустойчивость деполяризационного квантового канала.** 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да, Akhmetov B., Gnatyuk S., Okhrimenko T., Kinzeryavyy V., Yubuzova Kh. Experimental research of the corrective ability of interference stable Reed-Solomon codes over the GF(3^2) Galois field at transferring information on a deterministic quantum and cryptographic protocol, VESTNIK KazNRTU. No2(132), 2019. Алматы, P.61-69. Akhmetov B., Gnatyuk S., Kinzeryavyy V., Yubuzova Kh. Studies on practical cryptographic security analysis for block ciphers with random substitutions, International Journal of Computing, 19 (2) 2020, pp. 298-308 *(Q2, процентиль – 56).*
8.	Принцип достоверности Достоверность источников и предоставляемой инфор-	8.1 Выбор методологии – обоснован или методология достаточно подробно подробно описана 1) да; 2) нет	Выбранная диссертантом методология обоснована и подробно описана. В диссертационной работе использованы критический анализ; современные научные методы анализа и исследований; современные методы теории защиты информации; теория криптографии и криптоанализа; квантовая теории информации; квантовая механика; имитационное моделирование.

	мации	8.2 Результаты диссертационной работы получены с использованием современных методов научных исследований и методик обработки и интерпретации данных с применением компьютерных технологий: 1) да; 2) нет	Результаты диссертации были получены с использованием современных методов научного исследования, обработки и интерпретации данных с использованием компьютерных технологий. В работе использовались современные пакеты прикладных программ: MATLAB; Microsoft Visual Studio 2016; Wolfram Mathematica 7; C++.
		8.3 Теоретические выводы, модели, выявленные взаимосвязи и закономерности доказаны и подтверждены экспериментальным исследованием (для направлений подготовки по педагогическим наукам результаты доказаны на основе педагогического эксперимента): 1) да; 2) нет	Теоретические выводы, модели были доказаны и подтверждены экспериментальными исследованиями, а также имитационным моделированием.
		8.4 Важные утверждения подтверждены/частично подтверждены/не подтверждены ссылками на актуальную и достоверную научную литературу	Важные утверждения подтверждаются ссылками на актуальную и достоверную научную литературу.
		8.5 Использованные источники литературы достаточны/не достаточны для литературного обзора	Список использованной литературы включает 103 ссылки на английском, украинском, русском и казахском языках.
9	Принцип практической ценности	9.1 Диссертация имеет теоретическое значение: 1) да; 2) нет	Диссертация имеет теоретическое значение, достоверность теоретических положений подтверждается корректным применением известного математического аппарата, экспериментальными данными и результатами верификации предложенных методов.
		9.2 Диссертация имеет практическое значение и существует высокая вероятность применения полученных результатов на практике: 1) да; 2) нет	Результаты, полученные в ходе исследовательских работ, имеют высокую практическую ценность и могут быть использованы для решения проблемы распределения ключей, а также для повышения эффективности систем криптографической защиты информации. Практические результаты роботы, подтверждены соответствующими актами внедрения.
		9.3 Предложения для практики являются новыми?	Практические решения являются полностью новыми.

		1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%)	
10.	Качество написания и оформления	Качество академического письма: 1) высокое; 2) среднее; 3) ниже среднего; 4) низкое.	Диссертационная работа Юбузовой Халичи Ибрагимовны на тему «Методы безопасного распределения ключей на базе протоколов квантовой криптографии», предоставленную на соискание степени доктора философии (PhD) по специальности 6D070400 – «Вычислительная техника и программное обеспечение» подготовлена в соответствии с требованиями. Диссертация написана грамотным научно-техническим языком, формулировки научных положений, выводов четкие и лаконичные, имеют законченный характер.

Заключение

Считаю, что рецензируемая диссертационная работа Юбузовой Халичи Ибрагимовны на тему «Методы безопасного распределения ключей на базе протоколов квантовой криптографии» по своей актуальности, научной новизне, важности для теории и практики, объёму экспериментальных исследований полностью соответствует требованиям, которые предъявляются к диссертациям на соискание степеней PhD Комитетом по обеспечению качества в сфере образования и науки МОН Республики Казахстан, а ее автор Юбузова Халича Ибрагимовна заслуживает присуждения степени доктора философии (PhD) по специальности 6D070400 – «Вычислительная техника и программное обеспечение».

Рецензент, доктор технических наук, профессор каф.
Кибербезопасность и техническая защита информации
Государственный университет интеллектуальных технологий и связи
(Одесса, Украина) **Василиу Евгений Викторович**

Підпис затверджую
Вчений секретар Вченої ради ДУІТЗ Т. Казарян