АННОТАЦИЯ

диссертационной работы, на тему**:**
«МЕТОДЫ БЕЗОПАСНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА БАЗЕ ПРОТОКОЛОВ КВАНТОВОЙ КРИПТОГРАФИИ»
представленной на соискание степени доктора философии (PhD) по специальности 6D070400 – «Вычислительная техника и программное обеспечение»

ЮБУЗОВА ХАЛИЧА ИБРАГИМОВНА

Актуальность темы исследования. В современных информационных и коммуникационных системах основным из методов обеспечения конфиденциальности данных является криптография. В настоящее время, как правило, используются методы симметричной и ассиметричной криптографии, которые помимо преимуществ имеют определенные недостатки. Симметричные криптосистемы обладают достаточно высоким быстродействием и криптостойкостью к атакам, но при их использовании возникает сложная проблема распределения секретных ключей.

Существует несколько способов решения этой проблемы, например, применение ассиметричных систем криптографии. Но методам асимметричной криптографии также присущи существенные недостатки. Ассиметричные криптосистемы относительно симметричных медленные, а их криптостойкость к атакам объясняется невозможностью эффективного вычислительного решения NP-сложных задач (факторизация, логарифмирование в дискретных полях большого размера и т.п.). Однако с развитием технологий, быстрым увеличением производительности и одновременным удешевлением вычислительных средств, а также с открытием новых, более эффективных алгоритмов решения некоторых NP-сложных задач (алгоритмы Шора, Гровера и т.п.) ставит под угрозу обеспечение конфиденциальности и надежности, обеспеченные традиционной криптографией.

Также угрозой секретности современным классическим шифрам является возможность появления устойчивых многокубитных квантовых вычислительных систем, квантовых компьютеров.

В связи с этим, большой интерес вызывает квантовая криптография (КК), которая основана на использовании специфических свойств квантовых систем, служащих носителями информации в протоколах квантовой криптографии. КК при решении некоторых задач защиты информации дает возможность добиться теоретико-информационной стойкости, не зависящей как от вычислительных, так и от других возможностей злоумышленника. За последние десятилетия КК прошла путь от лабораторных экспериментов до внедрения полноценных коммерческих решений.

Ряд работ, ведущих отечественных и зарубежных ученых, посвящены развитию теории и практики квантовой криптографии, среди них Ахметов Б.,

Беннет Ч., Брассар Ж., Василиу Е., Гнатюк С., Диаманти Е., Жмурко Т., Завадски П., Зеневич А., Килин С., Лам П., Люткенхаус Н., Реннер Р., Румянцев К., Холево А.С., Явич М. и др.

Большая часть результатов исследований связанны с повышением стойкости (до теоретико-информационного уровня) и скорости передачи данных с использованием протоколов КК. Как правило, эти показатели являются взаимозависимыми и повышение уровня стойкости непременно приводит к понижению скорости обработки и передачи данных. Это снижает эффективность распределения ключей шифрования в режиме реального времени. В связи с этим, разработка современных методов повышения эффективности распределения ключей шифрования на базе протоколов квантовой криптографии является актуальной научно-технической задачей, которая имеет теоретическое и практическое значение для развития КК.

Цель исследования. Целью данной работы является разработка моделей безопасного распределения секретных ключей и повышение эффективности их распределения за счет использования комбинированной модели на базе протоколов квантовой криптографии.

Поставленная цель определила основные задачи диссертации.

1. Анализ современных методов, моделей и коммерческих систем распределения ключей шифрования по критериям безопасности (защищенности) и скорости.
2. Разработка модели угроз и модели нарушителя в квантово-криптографических системах.
3. Разработка и исследование модели квантового детерминистического протокола в режиме контроля подслушивания.
4. Разработка и исследование модели квантового детерминистического протокола в режиме передачи сообщений.
5. Разработка комбинированной модели с режимом контроля подслушивания и режимом передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов.
6. Предложить новый метод безопасного распределения ключей комбинированной модели с режимом контроля подслушивания и режимом передачи сообщений квантового детерминистического протокола.

Объект исследования – процесс распределения ключей шифрования для обеспечения конфиденциальности передачи данных в ИКС**.**

Предмет исследования – методы и модели безопасного распределения ключей на базе протоколов квантовой криптографии.

Методы исследования – методы теории защиты информации; теории криптографии и криптоанализа; квантовая теория информации; теория квантовой механики.

Использовались современные пакеты прикладных программ:

- MatlabR2018a;
- Microsoft Visual Studio 2016;
- Wolfram Mathematica 7;
- C++.

Научная новизна полученных результатов.

В диссертационной работе получены следующие результаты:

- на основе результатов анализа современного состояния в области квантовой криптографии и связи, выявлены недостатки существующих методов распределения ключей, расширена классификация квантово-криптографических методов, которая позволяет расширить возможности по выбору необходимых квантово-криптографических методов для построения безопасных систем распределения ключей шифрования;

- разработана модель квантового детерминистического протокола в режиме контроля подслушивания, учитывающая особенности квантового канала и вероятности возникновения в нем ошибки, что позволяет обеспечить безопасное и быстрое распределение ключей, сформулировать практические рекомендации по разработке квантово-криптографических систем в условиях использования деполяризационного квантового канала и присутствия нарушителя;

- разработана модель квантового детерминистического протокола в режиме передачи сообщений, которая дает возможность повысить уровень доступности квантового канала при передаче ключа детерминистическим протоколом при небольшом уровне природных шумов;

- предложен метод усиления секретности с использованием квантовых перепутанных состояний и сгенерированных троичных псевдослучайных последовательностей, что позволяет повысить скорость передачи без потерь стойкости детерминистических протоколов квантовой криптографии с использованием пар кутритов к некогерентной атаке;

- впервые реализована комбинированная модель 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, что позволило усовершенствовать метод безопасного распределения ключей, повысить скорость и обеспечить помехоустойчивость деполяризационного квантового канала.

Практическое значение полученных результатов.

Полученные научные результаты и разработанные модели квантового детерминистического протокола с режимом контроля подслушивания и режимом передачи сообщений с парами перепутанных кутритов имеют практическую ценность для решения проблемы распределения ключей, для повышения эффективности систем криптографической защиты информации.

Также разработанные:

- модель угроз позволяет сформировать концептуальные аспекты предупреждения атак и формализовать возможности превентивных систем в процессе их разработки или усовершенствования;

- абстрактная модель нарушителя в системах КК позволяет определить совокупность мероприятий различного характера, которые необходимо дополнительно внедрить для обеспечения надежной защиты применяя специфические квантовые системы;

- программное обеспечение и проведенное имитационное моделирование квантового детерминистического протокола:

- модель в режиме контроля подслушивания позволила повысить скорость распределения ключей шифрования минимум в 1,52 раза при обеспечении защищенности от некогерентной атаки;

- модель в режиме передачи сообщений, позволила получить подтверждение возможности применения предложенной системы помехоустойчивого кодирования над полем Галуа *GF* (3^2) при уровне природных шумов до 10%, повысить уровень доступности квантового канала при передаче ключа детерминистическим протоколом минимум на 3,8%.

Результаты исследования были использованы в учебном процессе кафедры Кибербезопасность, обработка и хранение информации КазНИТУ имени К.И. Сатпаева (акт внедрения от 02.09.2018), Национального авиационного университета (Киев, Украина) (акт внедрения от 05.09.2018), УО «Белорусская государственная академия связи» (Минск, Беларусь) (акт внедрения от 02.11.2018) и компании AxxonSoft (Киев, Украина) (акт внедрения от 29.10.2018).

Личный вклад автора состоит:

- разработаны модели квантового детерминистического протокола в режиме контроля подслушивания и модели в режиме передачи сообщений;

- первая модель обеспечивает безопасное и быстрое распределение ключей, а также формулирование практических рекомендации по разработке квантово-криптографических систем в условиях использования деполяризационного квантового канала и присутствия нарушителя (как показали эксперименты, удалось повысить скорость распределения ключей шифрования минимум в 1,52 раза при обеспечении защищенности от некогерентной атаки);

- вторая модель обеспечивает повышение уровня доступности квантового канала при передаче ключа детерминистическим протоколом при небольшом уровне природных шумов (по результатам экспериментов с применением предложенной соискателем системы помехоустойчивого кодирования над полем Галуа *GF* (3^2) при уровне природных шумов до 10% повышение уровня доступности квантового канала минимум на 3,8%);

- новый метод усиления секретности тритовых детерминистических протоколов, статистически стойкий алгоритм генерации тритовых псевдослучайных последовательностей, а также практические рекомендации по использованию квантовых детерминистических протоколов в квантово-криптографических системах в условиях использования деполяризационного квантового канала и присутствия нарушителя.

Апробация работы. Основные результаты исследования докладывались и обсуждались на научных семинарах института Информационных и телекоммуникационных технологий, на кафедре «Компьютерная и программная инженерия» КазНИТУ им. К.И. Сатпаева, в научно-исследовательской работе «Квантово-криптографические методы защиты критической информационной инфраструктуры государства» №161-ДБ17

(госрегистрация 0117U006770) Национального авиационного университета (**Украина, Киев,**), на Международном форуме, посвященного 80-летию КазНТУ имени К.И. Сатпаева «Инженерное образование и наука в XXI веке: Проблемы и перспективы» (**Алматы, 2014**), на Международных Сатпаевских чтениях «Роль и место молодых учены в реализации стратегии «Казахстан-2050» (**Алматы, 2014**), на II Международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика» (**Алматы, 2015**); на II Международной научно-практической конференции «Актуальные вопросы обеспечения кибербезопасности и защиты информации» (**Украина, Киев, 2016, 2017, 2018**); на Международной научно-практической конференции ITSEC: Безопасность информационных технологий (**Украина, Киев, 2016**); на Международной научной конференции УНИТЕХ'16 (**Болгария, Габрово, 2016**); на III Международной научно-практической конференции «Информационная безопасность и компьютерные технологии» (**Украина, Кропивницкий, 2018**); на XIV Международной конференции по ИКТ в образовании. «Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer» (**Украина, Киев, 2018**); на Международной конференции «Information and Telecommunication Technologies and Radio Electronics - UkrMico» (**Украина, Одесса, 2018**); на XVII International Conference on Computer Information Systems and Industrial Management Applications (**Россия, Москва, 2018**); на Международной научной конференции «Современные средства связи» (**Белоруссия, Минск, 2018**); на VIII Всемирном конгрессе «Aviation in the XXI-st century – Safety in Aviation and Space Technologies» (**Украина, Киев, 2018**); на VIII Международной научно-технической конференции «Инфокоммуникации – современность и будущее» (**Украина, Одесса, 2018**); на IIV Международной научно-практической конференции «Актуальні питання забезпечення кібербезпеки та захисту інформації» (**Украина, Киев, 2021**); на VII Международной научно-практической конференции «Актуальні питання забезпечення кібербезпеки та захисту інформації» (**Украина, Киев, 2021**); на IV Международной научно-практической конференции «Department of Information Systems and Technologies. Integration of information systems and intelligent technologies in the conditions of information society transformation» (**Украина, Полтава, 2021**).

Публикации. По результатам исследований по теме диссертационной работы было опубликовано 36 работ, из них 6 статей, входящих в базу данных Scopus/Web of Science, 3 статьи в журналах, рекомендованных Комитетом по обеспечению качества в сфере образования и науки МОН РК, 3 статьи в зарубежных журналах и 21 статья опубликованы в сборниках трудов международных научно-практических конференций в Казахстане и за рубежом.

Объем и структура диссертации. Диссертационная работа состоит из введения, четырех разделов, заключения и списка использованных источников и 3 приложений. Работа изложена на 144 страницах

машинописного текста, содержит 54 рисунка, 24 таблиц, список использованных источников из 103 наименований.

Краткое содержание диссертации.

Во введении раскрывается актуальность темы исследования, приведены цели и задачи исследования, методы исследования, научная новизна и практическая значимость полученных результатов, личный вклад и апробация работы.

В первом разделе диссертационной работы проведен литературный обзор и анализ современного состояния методов, моделей и коммерческих систем распределения ключей шифрования по критериям безопасности (защищенности) и скорости. По результатам обзора и анализа получена классификация квантово-криптографических методов, которая позволяет расширить возможности при выборе необходимых квантово-криптографических методов для построения безопасных систем распределения ключей шифрования.

Во втором разделе работы приведена разработанная расширенная классификация квантово-криптографических методов распределения ключей шифрования, предложены абстрактные модели угроз и нарушителя в системах квантовой криптографии, особенности реализации некогерентной атаки в системах квантовой криптографии на базе детерминистических протоколов. Полученные модели позволяют определить и выбрать наиболее защищенные методы распределения криптографических ключей.

В третьем разделе представлены разработанные модели: квантового детерминистического протокола в режиме контроля подслушивания; квантового детерминистического протокола в режиме передачи сообщений; предложен новый метод усиления секретности с использованием квантовых перепутанных состояний и сгенерированных троичных псевдослучайных последовательностей; реализована комбинированная модель на основе разработанных моделей режима контроля подслушивания и режима передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов с использованием предложенного метода усиления секретности.

В четвертом разделе приведены практические реализации в среде MATLAB имитационного моделирования квантового детерминистического протокола в режиме контроля подслушивания; имитационного моделирования квантового детерминистического протокола в режиме передачи сообщений; имитационного моделирования, комбинированного квантового детерминистического протокола с режимом контроля подслушивания и режимом передачи сообщений, с усилением секретности. Сформулированы практические рекомендации по использованию квантовых детерминистических протоколов в квантово-криптографических системах в условиях использования деполяризационного квантового канала и присутствия нарушителя.

В заключении отражены основные результаты и выводы по диссертационной работе.