ОТЗЫВ ЗАРУБЕЖНОГО НАУЧНОГО КОНСУЛЬТАНТА

доктора технических наук, профессора, зам. декана ф-та Кибербезопасности компьютерной программной инженерии Национального авиационного университета (г. Киев, Украина) Гнатюка Сергея Александровича на диссертационную работу докторанта PhD Юбузовой Халичи Ибрагимовны по теме «Методы безопасного распределения ключей на базе протоколов квантовой криптографии», представленной на соискание степени доктора философии (PhD) по специальности 6D070400 «Вычислительная техника и программное обеспечение»

Диссертационная работа Юбузовой Халичи Ибрагимовны посвящена решению актуальной научно-технической задачи разработки и исследования современных методов повышения эффективности распределения ключей шифрования на базе протоколов квантовой криптографии. Исследования выполнялись во время трехлетнего обучения соискателя в докторантуре Казахского Национального исследовательского университета имени К.И. Сатпаева, в том числе и научных стажировок в лабораториях Института информационно-диагностических систем Национального авиационного университета (г. Киев, Украина) и лаборатории квантовой криптографии и оптоволоконных систем связи УО Белорусской государственной академии связи (г. Минск, Беларусь).

Проведенные исследования заключались в анализе текущего состояния в области квантовой криптографии, выявлении недостатков и нерешенных задач с целью дальнейшего усовершенствования в контексте повышения эффективности распределения ключей шифрования, за счет использования предложенных в работе методов и моделей на базе протоколов квантовой криптографии. Диссертант определила, что наиболее эффективным альтернативным решением проблемы распределения ключей в криптографии является применение квантовой криптографии, но и эти методы имеют ряд недостатков, связанных с необходимостью внедрения процедур предобработки и постобработки с целью обеспечения необходимого уровня стойкости к различным атакам. В частности, большое внимание в работе отведено так называемой некогерентной атаке, которая является наиболее актуальной угрозой детерминистическим протоколам квантовой криптографии.

С моей точки зрения, научная новизна результатов работы состоит в следующем:

- впервые реализована комбинированная модель реализации режимов контроля подслушивания и передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов и применением предложенного не квантового метода усиления секретности, что позволило усовершенствовать метод безопасного распределения ключей, повысить скорость и обеспечить помехоустойчивость деполяризованного квантового канала;

- усовершенствована модель квантового детерминистического протокола в режиме контроля подслушивания, что позволило обеспечить безопасное и быстрое распределение ключей в условиях реализации некогерентной атаки, а также сформулировать практические рекомендации по разработке квантово-криптографических систем в условиях использования деполяризационного квантового канала и присутствия нарушителя (нарушителей);

- усовершенствована модель квантового детерминистического протокола в режиме передачи сообщений, которая дала возможность повысить уровень доступности квантового канала (используя корректирующие коды) при передаче ключа по детерминистическому протоколу при небольшом уровне природных шумов;

- усовершенствован метод усиления секретности, который позволяет повысить скорость передачи без потерь стойкости детерминистических протоколов с использованием пар кутритов к некогерентной атаке;

- получила дальнейшее развитие классификация квантово-криптографических методов, которая позволяет расширить возможности по выбору необходимых квантово-криптографических методов для построения безопасных систем распределения ключей шифрования и квантовой безопасной связи.

Среди практических результатов, прежде всего, следует выделить:

- модели угроз и нарушителя в квантово-криптографических системах, которые учитывают специфику и уязвимости систем квантовой криптографии, а также вычислительные и другие возможности нарушителей;

-специализированное программное обеспечение для проведения имитационного моделирования квантового детерминистического протокола;

- практические рекомендации по использованию квантового детерминистического прокола в условиях использования деполяризационного квантового канала и присутствия нарушителя (нарушителей).

Научные положения, гипотезы, выводы и практические рекомендации являются полностью обоснованными, а достоверность и точность результатов подтверждены математической корректностью предложенных моделей и методов, имитационным моделирование режимов работы детерминистического протокола, использованием реального лабораторно оборудования, корректной методики проведения экспериментов в области квантовой криптографии и статической обработки полученных экспериментальных данных. Полученные во время экспериментов данные соответствуют теоретическим выводам работы и полностью подтверждают их, в работе корректно применены методы теории защиты информации, теории криптографии и криптоанализа, квантовой теории информации, квантовой механики, теории программирования и имитационного моделирования.

Диссертант Юбузова Х.И. во время написания диссертационной работы проявила себя как высококвалифицированный специалист в области защиты информации (в частности, квантовой криптографии), способный генерировать новые научные идеи, а также оперативно и корректно решать поставленные научные задачи. Знания английского языка позволили обработать

значительное количество англоязычных источников, участвовать в международных научных конференциях.

Результаты диссертационной работы докладывались и обсуждались на различных специализированных научных конференциях и семинарах, в том числе и у нас, в Национальном авиационном университете, во время прохождения диссертанткой стажировки в 2016 году. Кроме того, результаты Юбузовой Х.И., отображены в отчетах научно-исследовательского проекта «Квантово-криптографические методы защиты критической информационной инфраструктуры государства», в котором диссертант выступала в качестве исполнителя (на протяжении 2017-2018 гг.).

Соискателем опубликовано 36 научных работ, в том числе 3 - в изданиях, рекомендованных Комитетом по обеспечению качества в сфере образования и науки МОН Республики Казахстан, 6 – в базе данных Scopus и Web of Sciences, 1 раздел в коллективной монографии на английском языке, 3 - в зарубежных журналах и 21 – в сборниках международных научных конференций, семинаров и симпозиумов.

Резюмируя вышеизложенное, считаю, что диссертационная работа Юбузовой Халичи Ибрагимовны «Методы безопасного распределения ключей на базе протоколов квантовой криптографии» подготовлена на высоко научном уровне, отвечает всем требованиям, предъявляемым к докторским диссертациям и рекомендуется к защите для присвоения ей степени доктора философии (PhD) по специальности 6D070400 «Вычислительная техника и программное обеспечение».

Зарубежный научный консультант
д.т.н., профессор, заместитель декана Факультета
кибербезопасности, компьютерной и программной инженерии
Национального авиационного университета

Сергей ГНАТЮК

«05» апреля 2022 г.

Особистий підпис гр*
ЗАСВІДЧУЮ
Заступник начальника відділу кадрів
Національного авіаційного університету