РКЦ | Российский Квантовый Центр

УТВЕРЖДАЮ
Научный директор
«Российского Квантового Центра»
Шляпников Г. В.
«07» июля 2022 г.

ОТЗЫВ

ведущей организации – общества с ограниченной ответственностью «Международный центр квантовой оптики и квантовых технологий»
на диссертацию Жиляева Андрея Евгеньевича
на тему «Методика построения сетей квантового распределения ключей смешанной топологии», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

1. Актуальность темы диссертации

Появление новых угроз безопасности информации, в частности квантового компьютера, требует применения новых методов защиты информации. Использование систем квантового распределения ключей (КРК) позволяет существенно повысить защищенность информационных систем. В работе решается актуальная задача преодоления фундаментального ограничения систем КРК, а именно преодоления максимальной длины квантового канала и распределение общих секретов для географически разнесенных пользовательских устройств защиты информации. Построение магистральных сетей КРК, а также сетей смешанных топологий является несомненно важной задачей для развития и внедрения принципиально новых мер защиты информации, чья стойкость гарантируется физическими принципами. Определение порядка функционирования таких сетей, их рекомендованной архитектуры и способов использования истинной квантовых ключей при формировании секретов для произвольно удаленных друг от друга пользовательских устройств несомненно является актуальной задачей для создания протяженных сетей КРК.

2. Структура и объем работы

Диссертационная работа Жиляева А. Е. содержит введение, четыре главы, заключение, три приложения и список источников из 126 наименований. Объем основной части диссертационной работы составляет 135 страниц, включая 2 таблицы и 27 рисунков.

Результаты диссертационного исследования в достаточной мере изложены в тексте диссертации. Автореферат полностью соответствует основному содержанию диссертации.

Во введении обоснована актуальность темы диссертации, обозначена цель и задачи исследования, отражена научная новизна, практическая и теоретическая значимость полученных результатов, приведены положения, выносимые на защиту.

Первая глава посвящена исследованию современного состояния предметной области. Рассматривается обобщенная структура системы КРК, выделены основные этапы типового протокола КРК. Рассмотрен известный способ распределения секретов в сетях КРК на основе

доверенных промежуточных узлов и сформулированы его недостатки. Проанализированы известные архитектуры сетей КРК.

Во второй главе решаются проблемы для систем КРК топологии точка-точка. Рекомендована функция универсального хэширования для построения классического аутентифицированного канала системы КРК. Разработана структура и способ функционирования комплекса из двух экземпляров аппаратуры КРК и двух средств защиты информации (СЗИ), потребляющих общие секреты, формируемые системой КРК. Такой комплекс назван базовым сегментов для построения протяженных сетей КРК.

В третьей главе автором разработаны способы распределения общего секрета в магистральных сетях КРК и сетях топологии «звезда». Предложены критерии для анализа разработанных в рамках исследования и создаваемых в будущем способов распределения общего секрета. Синтезирована методика распределения общих секретов в магистральных сетях КРК, позволяющая путем использования ключевых подсистем двух типов распределять общие секреты, стойкие даже в случае компрометации одной из подсистем.

Четвертая глава посвящена построению сетей КРК смешанной топологии. По результатам анализа европейских аналогов предложена трехуровневая архитектура сети КРК и структура узла сети. Для каждого уровня сети подробно обоснованы функциональные требования. Разработана методика построения сети КРК смешанной топологии и основные этапы функционирования сети. Разработанная методика опирается на ранее синтезированную методику распределения общих секретов в магистральной сети КРК.

В заключении приведены основные выводы и результаты диссертационного исследования.

Оформление диссертации и автореферата соответствует требованиям ГОСТ Р 7.0.11-2011.

3. Научная новизна исследования и полученных результатов

Полученные результаты диссертационного исследования являются новыми и могут быть классифицированы как изложение научно обоснованных решений, внедрение которых внесет вклад в науку и обеспечение безопасности Российской Федерации, в частности в развитие сетей квантового распределения ключей.

Наиболее важные результаты диссертационной работы, обладающими признаками научной новизны:

1. структура комплекса защищенной передачи данных, интегрированного с аппаратурой квантового распределения ключей, в том числе порядок функционирования такого комплекса для синхронизированной передачи ключевой информации в СЗИ, отличающийся от известных учетом целостности и конфиденциальности общих секретов в процессе передачи в СЗИ и контролем идентичности сформированных секретов, объединением классического канала аппаратуры КРК с транспортным каналом СЗИ для повышения защищенности классического канала аппаратуры КРК;
2. методика распределения общих секретов в сети КРК магистральной топологии, отличающаяся сохранением стойкости распределенных общих секретов при компрометации квантовых ключей, а также возможностью сохранения конфиденциальности распределяемых секретов на промежуточных узлах сети КРК;
3. методика построения сети КРК смешанной топологии, включающая требования к структуре сети КРК, способу ее функционирования, методику распределения квантов защищённых ключей, отличающаяся от известных полностью децентрализованным

управлением при создании квантов защищённых ключей, учетом требований их целостности и конфиденциальности, а также имеющая по сравнению с зарубежными аналогами большую гибкость при масштабировании сети.

4. **Достоверность и обоснованность основных результатов и выводов**

Цель диссертационного исследования и поставленные для ее достижения задачи изложены корректно, являются практически значимыми и реализуемыми. Решения задач доведены до практических приложений. Список литературы показывает полноту изучения соискателем рассматриваемых вопросов.

Достоверность и обоснованность результатов и выводов работы подкрепляется глубоким анализом современного состояния исследований в предметной области, непротиворечивым обоснованием предложенных методик, апробацией полученных результатов в научных публикациях и докладах на различных международных и российских конференциях, а также положительным эффектом внедрения результатов в действующие образцы систем КРК, а также использованием результатов диссертационного исследования в документах национальной системы стандартизации.

5. **Значимость результатов диссертации для соответствующей отрасли науки**

Результаты данной работы представляют развитие теории защиты информации в части применения технологии КРК для регулярной доставки общих секретов, предлагая решение, позволяющее распределять общие секреты на расстояния, превышающие предельные длины квантовых каналов. Как правило в научной литературе по тематике КРК в большинстве случаев рассматривается распределение ключей типа точка-точка, в то время как для сетей КРК алгоритмам и техническим деталям касательно функционирования и взаимодействия улов сети не уделяется должного внимания.

Среди полученных результатов можно выделить следующие:

1. Разработано описание сопряжения и взаимодействия СЗИ с комплектами установок КРК.
2. Разработана методика КРК для пары оконечных узлов для сети магистральной топологии.
3. Сформулированы функциональные требования структуре построения сетей смешанной топологии.

6. **Рекомендации по использованию результатов работы**

Результаты диссертационной работы Жиляева А.Е. могут быть применены при проектировании протяженных сетей квантового распределения ключей, а также комплексов защиты информации с использованием систем квантового распределения ключей.

7. **Публикации по теме диссертации**

По материалам диссертации Жиляевым А.Е. опубликовано 8 научных работ, в том числе 4 работы в изданиях, рекомендованных ВАК РФ, 2 работы в изданиях, индексируемых в базах Scopus и WoS, получены 3 патента на изобретения. Результаты докладывались и обсуждались на различных российских и международных конференциях.

8. **Замечания по диссертации**

Для распределения общего секрета в сети КРК смешанной топологии требуется определить цепочку УКС, на которой будет распределяться этот секрет. Процесс определения цепочки (пути) с учетом скоростей генерации и скоростей потребления секретных ключей является важной нетривиальной оптимизационной задачей. Однако в диссертации этому не уделено должного внимания.

9. Заключение о соответствии диссертации критериям, установленным Положением о порядке присуждения ученых степеней

Диссертация Жиляева А.Е. является завершенной научно-квалификационной работой, в которой даны научно обоснованные решения по построению протяженных сетей квантового распределения ключей сложных топологий, в особенности в части безопасного и стойкого распределения общих секретов в пары средств защиты информации, произвольно подключенных к узлам сети КРК.

Диссертация отвечает требованиям пункта 9 «Положения о порядке присуждения ученых степеней» ВАК РФ по актуальности, научной новизне, значимости, объему выполненных исследований, практической и теоретической значимости, а ее автор, Жиляев Андрей Евгеньевич, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв ведущей организации на диссертацию Жиляева А.Е. рассмотрен и одобрен на научном семинаре «Квантовые коммуникации», который состоялся «01» июля 2022 г.

Отзыв подготовил: Федоров Алексей Константинович

Руководитель научной группы «Квантовые информационные технологии», Российский Квантовый Центр, PhD по теоретической физике, профессор МФТИ.

Адрес: 121205, г. Москва, Территория Инновационного Центра «Сколково», Большой бульвар, д. 30, стр. 1.
+7 916 297-09-77, akf@rqc.ru

Федоров Алексей Константинович

«07» июля 2022г.

Подпись Федорова А.К заверяю
СПЕЦИАЛИСТ ПО КАДРОВОМУ УЧЕТУ Азаров З.В.

Сведения об организации:
Общество с ограниченной ответственностью «Международный центр квантовой оптики и квантовых технологий» (ООО «МЦКТ»), 143026, Московская область, Одинцовский р-н, д Сколково, ул. Новая, д.100, mail@rqc.ru, +7 495 280-12-91.