# ОТЗЫВ

на автореферат диссертации Жиляева Андрея Евгеньевича «Методика построения сетей квантового распределения ключей смешанной топологии», представленной на соискание учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

В современной информационной безопасности актуален вопрос выработки участниками сеанса связи некоторых секретных параметров, необходимых для обеспечения конфиденциальности информации, передаваемой по каналу связи. В большинстве сетевых протоколов используются специальные алгоритмы, построенные на основе некоторых вычислительно-сложных задач – дискретное логарифмирование в конечной группе или разложение больших чисел на множители. Однако такие алгоритмы не являются стойкими, если злоумышленник может использовать квантовый компьютер. В связи с этим актуальны разработка и внедрение протоколов выработки общих секретов, устойчивых в том числе к атакам с использованием квантового компьютера.

Диссертационное исследование посвящено проблематике построения сетей квантового распределения ключей (КРК) смешанной топологии. Автор диссертации предлагает новую методику построения сетей КРК, в которой уточняются мало рассматриваемые ранее аспекты, в том числе возможность построения таких сетей с децентрализованным управлением, методика распределения общих секретов в магистральных сетях квантового распределения ключей, используемая при построении сетей смешанной топологии, структура и способ функционирования комплекса из двух пользовательских устройств и двух экземпляров квантовой аппаратуры, причем такой комплекс неявно используется при конструировании сетей магистральной и смешанной топологии.

Исходя из положений, приведенных в автореферате, можно заключить, что работа имеет последовательную и логичную структуру изложения. Автореферат содержит все необходимые разделы и отличается однозначностью формулировок цели, задач и результатов. К наиболее значимым результатам можно отнести следующие:

- разработана структура системы защищённой передачи секретных данных, в которую входят как квантовая аппаратура, так и целевые пользовательские средства защиты информации;

- предложена методика распределения общего секрета, подразумевающая повышение общего уровня защищённости распределяемых секретов, а также контроль целостности информации при передаче через промежуточные узлы сети;
- сформулирован перечень требований к сетям КРК, которые позволяют конструировать защищённые децентрализованные сети КРК.

Данные результаты имеют научную новизну и практическое значение для разработки и внедрения систем КРК на территории Российской Федерации. Особо стоит отметить соответствие темы исследования и основных результатов дорожной карте, разработанной во исполнение Указа Президента Российской Федерации № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». Разработанные автором методики могут применяться для повышения защищённости систем защиты информации путём построения протяженных сетей квантового распределения ключей. Также к заслугам диссертанта можно отнести полученные патенты на изобретения.

Результаты диссертации прошли достаточную апробацию на российских и международных научных и научно-практических конференциях и использованы при разработке документов национальной системы стандартизации. По теме диссертации опубликовано 8 статей в научных журналах, включая рецензируемые издания из перечня ВАК РФ и индексируемые Scopus.

К автореферату имеются следующие замечания.

1. Неточность формулировки при упоминании квантового алгоритма Гровера в контексте атак на схемы генерации ключей, основанные на сложности вычисления дискретного логарифма или факторизации больших чисел.
2. В автореферате не уделено внимание постквантовым алгоритмам для решения задачи формирования общего секрета двумя устройствами и сравнение с предлагаемым автором решением на основе квантовых технологий.
3. В автореферате не рассматриваются вопросы общей защищённости сети при применении конкретного алгоритма КРК и возможные проблемы при интеграции предложенной сети КРК в уже развёрнутые комплексы.
4. В автореферате не хватает более подробного обоснования выбора семейства функций универсального хэширования Stinson, а также

формализованного описания формирования имитовставки с предлагаемыми функциями универсального хэширования.

Указанные замечания не снижают научной и практической ценности полученных результатов и не влияют на положительную оценку представленной работы.

Судя по автореферату и публикациям, диссертация Жиляева А.Е. «Методика построения сетей квантового распределения ключей смешанной топологии» представляет законченное научное исследование, соответствующее критериям п. 9 Положения о присуждении учёных степеней ВАК РФ, а её автор Андрей Евгеньевич Жиляев заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки).

Коренева Алиса Михайловна,
начальник отдела криптографического анализа
ООО «Код Безопасности»,
кандидат физико-математических наук

«28» 08 2022 г.

Почтовый адрес: 115127, г. Москва, а/я 66
Телефон: +7 495 982 30 20, доб. 404
Эл. почта: A.Koreneva@securitycode.ru

Подпись Кореневой А.М. удостоверяю

Саранова Е.Н.
ведущий менеджер по подбору персонала
28.08.2022 г.