ОТЗЫВ

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

Диссертационная работа Жиляева А. Е. посвящена решению важной задачи практической криптографии – разработке методики распределения ключей между пользователями в криптографических сетях смешанной топологии. Смешанная топология объединяет в себе квантовые и классические каналы связи между узлами сети.

Тема исследований диссертационной работы соответствует паспорту специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

Ознакомление с авторефератом позволяет выделить следующие основные результаты, являющиеся заметным вкладом в решение практических вопросов построения систем распределения ключей с использованием квантовых каналов связи.

1. Введение в рассмотрение конструкции гибридных *квантовозащищенных* ключей для получения конечного общего секрета пользователей.

2. Разработку *структуры* комплекса защищенного обмена данными, интегрированного с аппаратурой квантового распределения ключей, с учетом:

- требований к *целостности* и *конфиденциальности* формируемых общих секретов для средств защиты информации пользователей,

- *контроля идентичности* сформированных секретов.

3. Разработку методики распределения общего секрета - *квантовозащищенного* ключа - в оконечные узлы для *магистральной* сети квантового распределения ключей с обеспечением высокой защищенности распределяемых секретов за счет:

- сохранения *конфиденциальности* распределяемых секретов на *промежуточных* узлах,

- контроля *целостности* секретов при их передаче *между узлами* сети,

- сохранении *конфиденциальности* общего секрета при *компрометации отдельных* квантовых ключей.

4. Разработку методики построения *децентрализованных* сетей квантового распределения ключей смешанной топологии, учитывающей требования к их *целостности* и *конфиденциальности* и имеющей, по сравнению с зарубежными аналогами, большую гибкость при масштабировании сети.

Отдельно следует отметить практическую значимость диссертационной работы, заключающуюся во внедрение разработанной методики в действующую Университетскую квантовую сеть на территории МГУ им. М.В. Ломоносова (ViPNet QTS).

Автореферат диссертации хорошо структурирован и позволяет сделать вывод о научной новизне, теоретической и практической значимости диссертационного исследования. По теме диссертации автором получено 3 патента на изобретения (1 совместно), подготовлено и опубликовано 8 статей (5 совместно), из них 4 – в рецензируемых изданиях, рекомендованных ВАК РФ по специальности 05.13.19 - «Методы и системы защиты информации, информационная безопасность».

По тексту автореферата можно сделать следующие замечания.

1. Утверждение, что *в общем случае* длина необходимого ключа аутентификации должна быть пропорциональна двоичному логарифму длины сообщения (стр.11) представляется не вполне корректным. Если предъявляются требования *к вероятности* навязывания сообщения, то длина необходимого ключа аутентификации будет существенно определяться именно этим параметром.

2. Вывод о том, что для систем квантового распределения ключей, вырабатывающих ключи *недостаточного размера*, неприменимы теоретико-информационные методы оценки стойкости процедуры аутентификации (стр.12), требует уточнения. Системы квантового распределения ключей, такие как ViPNet Quandor (фазовое кодирование квантовых

состояний), ViPNet QSS, QTS Quantel (фазово-временное кодирование), упомянутые в автореферате и приложениях, *принципиально* могут формировать квантовый ключ любой разумной длины. Ограничения на длину, на которые опирается автором, носят *технический* характер, отражая, по существу, уровень *технических* возможностей разработчика систем на *настоящий* момент времени.

3. Представляется также, что процедура *накопления* квантовых ключей малой длины для обеспечения стойкой аутентификации (стр.13) не является обязательной для систем квантового распределения ключей. Малая длина квантовых ключей – это порождение тех же причин *технического* характера, которые отражены в п.2 замечаний.

Вышесказанные замечания носят частный характер и не снижают общей положительной оценки диссертационной работы соискателя.

В целом можно заключить, что представленная диссертация на тему «Методика построения сетей квантового распределения ключей смешанной топологии» на соискание учёной степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки) соответствует критериям п.9 действующего Положения о присуждении учёных степеней, а её автор Андрей Евгеньевич Жиляев заслуживает присуждения искомой степени.

Старший специалист ООО «СФБ Лаб»
кандидат физико-математических наук И.М. Арбеков

Контактные данные:
тел.: +7 916 566 04 71, e-mail: igor.arbekov@sfblaboratory.ru
Адрес места работы:
127273, Москва, ул. Отрадная, д. 2Б, стр. 1, тел: +7 495 645 44 38

Я, Арбеков Игорь Михайлович, даю свое согласие на включение моих персональных данных в документы, связанные с работой диссертационного совета и их дальнейшую обработку.

«23» августа 2022 г.

Подпись Арбекова И.М. удостоверяю

Общество с ограниченной ответственностью ООО «СФБ Лаб» SFB Lab LLC ОГРН 5177746044141 Москва

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
ООО «СФБ ЛАБ»
ЗАЛУНИН О.А.