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»

Разрабатываемые в настоящее время квантовые вычислительные устройства являются фактором, который потенциально может привести к недопустимости использования для обеспечения информационной безопасности ряда используемых в настоящее время механизмов, протоколов и средств криптографической защиты информации. В частности, алгоритм Шора позволяет эффективно решать на квантовом вычислителе задачи, на которых основывается стойкость схемы обмена ключей Диффи-Хеллмана и применяемых в настоящее время алгоритмов формирования электронной подписи. В случае создания квантового вычислителя, способного успешно реализовывать данный алгоритм при используемых на практике параметрах безопасности, использование применяемых в настоящее время повсеместно вариантов основных протоколов защиты информации (в первую очередь, TLS и IPsec) станет недопустимым для обеспечения информационной безопасности. С учетом этого тема представленной диссертационной работы Андрея Евгеньевича Жиляева является, несомненно, крайне актуальной, а решение поставленных задач квантового распределения ключей для различных топологий сети важно для развития направления синтеза механизмов защиты информации, защищенных относительно квантового вычислительного устройства. Судя по автореферату, поставленные научные задачи автором успешно решены.

В автореферате представлена суть работы, научная новизна и достоверность результатов, степень участия автора в публикациях и внедрениях, что отвечает требованиям ВАК России.

Тем не менее, следует отметить следующие замечания:

1. В автореферате упоминается необходимость «применения вычислительно стойкой аутентификации, например, с применением функции хэширования ГОСТ 34.11-2018». Так как сама по себе функция хэширования не может обеспечивать свойство аутентификации, следовало бы указать, какие механизмы (например, HMAC_GOSTR3411_2012_256) на основе указанной функции хэширования рекомендуется использовать.
2. По тексту неоднократно термин «проблема» применяется не вполне уместным образом, так, в выражениях «принцип «Store now, decrypt later», считающийся одной из основных проблем систем защиты информации» (стр. 3 автореферата),

«важной научной проблемой, не рассмотренной в научной литературе, является собственно передача созданного квантового ключа от квантовой аппаратуры потребителям» (стр. 8 автореферата), «проблемы распределения общих секретов на расстояния, превышающие предельную длину квантового канала» (стр. 9 автореферата) уместнее было бы употребить термин «задача».

3. На стр. 18 автореферата упоминается проект методических рекомендаций ТК 26 «Информационная технология. Криптографическая защита информации. Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ», но не указан статус данного проекта в рамках работ данного Технического комитета.
4. В списке публикаций, написанных с соавторами, отсутствуют сведения о том, какие из результатов указанных работ получены автором лично.

Указанные замечания не снижают общей положительной оценки данной диссертационной работы.

Судя по автореферату и публикациям, диссертация А.Е. Жиляева 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 ему степени кандидата технических наук.

Заместитель генерального директора
ООО «КРИПТО ПРО»,
Доктор физико-математических наук _____Смышляев С.В.

Адрес: 127018, г. Москва, ул. Сущевский Вал, д.18
Телефон: +7 (495) 995-48-20
e-mail: svs@cryptopro.ru

Подпись Смышляева Станислава Витальевича подтверждаю:
Генеральный директор ООО «КРИПТО-ПРО» Чернова Н.Г.