Экз. № 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЁННОЕ УЧРЕЖДЕНИЕ «ВОЙСКОВАЯ ЧАСТЬ 43753»

25 августа 2022 г. № 149/3-7814

121351, г. Москва, в/ч 43753

Ученому секретарю
Диссертационного совета
Д 212.268.03 на базе ТУСУР

Е.Ю. Костюченко

634050, г. Томск, пр. Ленина, д. 40

О направлении отзыва
официального оппонента

Уважаемый Евгений Юрьевич!

Направляю Вам отзыв Королькова А.В. - официального оппонента по диссертации Жиляева А.Е.

Приложение: 1. Отзыв, экз. № 1 и 2, несекретно, № 149/3-7815, на 7 листах каждый.

Приложение только в адрес.

Командир войсковой части 43753-А М.В. Федоров

Экз. № 1

Отзыв

официального оппонента на диссертацию 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»

Актуальность. В последние десятилетия активно разрабатываются подходы к построению квантового компьютера. Ряд алгоритмов, реализуемых на квантовых компьютерах, несут угрозу секретности повсеместно используемых криптографических методов обеспечения защиты данных. В настоящее время рассматривается два варианта обеспечения стойкости криптографических систем с точки зрения создания квантового оборудования: постквантовая криптография и квантовая криптография для целей безопасного распределения ключей. Квантовое распределение ключей (КРК) обеспечивает формирование одинакового секретного ключа у пары географически разнесенных абонентов и является перспективной областью не только исследований, но и практических разработок. С этой точки зрения работа Жиляева Андрея Евгеньевича посвящена актуальной проблеме регулярной доставки общих секретов на пользовательские устройства. Судя по содержанию диссертационной работы и автореферату, автором достаточно подробно рассмотрены методические проблемы применения систем КРК и протяженных сетей, построенных на их основе. В результате диссертационного исследования разработана методика формирования общего секрета в сетях простых топологий (магистраль, звезда), а также методика построения сети КРК смешанной топологии. Данные методики закрывают ряд недостаточно глубоко освещенных ранее вопросов при применения квантовых технологий в области защиты информации.

Структура диссертации. Работа состоит из введения, четырех глав, заключения по основным результатам работы, списка литературы, списка сокращений и условных обозначений, списка терминов, списка иллюстративных материалов и одного приложения.

Научная новизна диссертационной работы состоит в следующем:

1. Разработана структура комплекса защищенной передачи данных, интегрированного с аппаратурой квантового распределения ключей, в том числе способ функционирования такого комплекса для синхронизированной

передачи ключевой информации в СКЗИ, отличающаяся от известных учетом целостности и конфиденциальности общих секретов в процессе передачи в СКЗИ, объединением классического канала аппаратуры КРК с транспортным каналом СКЗИ для повышения защищенности классического канала аппаратуры КРК, оптимизации числа каналов между частями комплекса и упрощения развертывания такого комплекса. Новизна предлагаемого решения подтверждается патентом на изобретение.

2. Впервые предложено новое понятие квантовозащищенного ключа, определяющее результат функционирования сети КРК. Для квантовозащищенных ключей сформулированы свойства безопасности, которыми могут обладать эти ключи в зависимости от способа их распределения в сети КРК.

3. Разработаны новые методы распределения квантовозащищенных ключей в сети КРК магистральной топологии и проведен их анализ. На основе разработанных методов синтезирован способ распределения квантовозащищенных ключей, позволяющий повысить их стойкость за счет применения технологии КРК, при этом сохраняя квантовозащищенные ключи не скомпрометированными в том числе при компрометации квантовых ключей.

4. Предложены структура и способ функционирования сети КРК произвольной топологии, отличающиеся от известных полностью децентрализованным управлением при создании квантовозащищенных ключей, имеющие по сравнению с зарубежными аналогами большую гибкость при масштабировании сети, и возможности построения сети с использованием оборудования различных производителей. Новизна предлагаемого решения подтверждается патентом на изобретение.

Достоверность сведений в представленной диссертационной работе подтверждена анализом современного состояния исследований в предметной области, обоснованием предложенных методик, не противоречащих известным положениям других авторов, корректностью проведенных математических преобразований, апробацией полученных результатов в научных публикациях и докладах на международных и российских научных и научно-практических конференциях, а также положительным эффектом внедрения результатов в экспериментальные макеты сетей КРК (Университетская квантовая сеть, ViPNet QTS), промышленные комплексы

систем КРК (ViPNet Quandor, ViPNet QSS, Квазар-СКР), а также использованием результатов работы в проектах документов национальной системы стандартизации.

Теоретическая и практическая значимость. Результаты данной работы представляют развитие теории защиты информации в части применения технологии КРК для регулярной доставки общих секретов, в том числе в устройства, расположенные на расстояниях, существенно превышающих предельные длины квантовых каналов.

Введенное автором понятие квантовозащищенных ключей позволяет различать общий секрет, распределяемый в сети КРК, и квантовые ключи, создаваемые непосредственно в результате выполнения протокола КРК, в связи с чем уменьшается путаница при описании квантовой аппаратуры, сетей КРК, а также анализе их стойкости.

Основные положения работы представляют практическую ценность для создания промышленных образцов квантовых сетей во исполнение дорожной карты ОАО «РЖД» по развитию сквозной цифровой технологии квантовых коммуникаций. Предложенная структура базового сегмента сети КРК топологии «точка-точка» позволяет минимизировать число каналов между географически разнесенными узлами, что приводит к упрощению развертывания таких пар узлов. Разработанная методика распределения общего секрета в магистральной сети КРК существенно ускорила процесс разработки проектов документов национальной системы стандартизации в части ключевых систем сетей КРК.

Обзор диссертационной работы. Во **введении** автор обосновывает актуальность темы диссертации, обозначает цель и задачи исследования, приводит научную новизну, практическую и теоретическую значимость полученных результатов, положения, выносимые на защиту.

В **первой главе** описывается типовая структура системы КРК и основные этапы протокола КРК. Показана недостаточная проработанность способов аутентификации служебного канала систем КРК. Также выявлено принципиальное ограничение систем КРК, связанное с предельно допустимой длиной квантового канала связи. В работе подробно рассматриваются различные известные подходы к увеличению максимальной дальности распределения общих секретов и обоснованно делается вывод о необходимости построения сетей КРК на основе доверенных промежуточных

узлов. Проводится анализ известных сетей КРК, описанных в зарубежных источниках, и предлагаемых способов распределения общих секретов на пользовательские устройства, подключаемые к таким сетям и системам КРК. По результатам анализа сформированы основные проблемы и задачи проводимого исследования.

Во **второй главе** решаются выявленные проблемы для систем КРК топологии точка-точка. Рассматривается применение семейств функций универсального хэширования для вычисления имитовставки от сообщений служебного канала системы КРК. По каждому из рассмотренных семейств функций хэширования описаны принципы их построения, требуемый размер ключа для формирования имитовставки и ее стойкость в теоретико-информационном смысле.

На основе данных об объемах трафика служебного канала системы КРК ViPNet Quandor автором получены оценки размера ключа, необходимого при различных подходах вычисления теоретико-информационно стойкой имитовставки. В результате показана невозможность применения такого класса имитовставок для рассмотренной системы КРК.

Также в данной главе представлена структура и способ функционирования комплекса, состоящего из пары СЗИ и системы КРК, защищающий от проблемы сбоев в система КРК и выравнивающий длины формируемой квантовой гаммы. Дополнительно вводится контроль идентичность формируемых общих секретов как в системе КРК, так и в подключенных СЗИ.

В третьей главе автором разрабатываются способы распределения общего секрета в магистральных сетях КРК. Для этого подробно проанализирован основной известный способ, называемый в работе базовым. Каждый из предлагаемых способов нацелен на устранение некоторых недостатков базового. В **результате** сформированы критерии классификации способов распределения общего секрета, позволяющие проводить сравнительный анализ предложенных способов, а также применимые для анализа создаваемых в будущем. На основе разработанных способов распределения общего секрета синтезируется методика распределения общих секретов в магистральных сетях КРК, сочетающая способы разделения секрета, передачи защищаемой информации в ключевом контейнере, дополнительно позволяющая в равной степени обоим узлам сети КРК

участвовать в процессе распределения. Для этого вводятся функции симметризации и гибридизации частей общей секрета.

Четвертая глава посвящена построению сетей КРК смешанной топологии. На основе проведенного анализа существующих решений предлагается новая трехуровневая структура сети КРК, не требующая централизованного управления. Для каждого уровня сети подробно обоснованы требования к функциям каждого уровня.

Также на основе структуры узла сети КРК и архитектуры сети в целом сформирована методика построения сети КРК смешанной топологии и основные этапы ее функционирования. Ключевым этапом при распределении каждого общего секрета является выделение магистральной подсети, соединяющей два требуемых узла сети, и дальнейшей распределение общего секрета с применением ранее разработанной методики.

В **заключении** приведены основные выводы и результаты диссертационного исследования.

Приложение содержит иллюстративный материал по теме работы. **Список использованных источников** содержит 126 наименований.

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

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

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 работы были представлены на различных российских и международных конференциях. Значительный объём публикаций результатов в ведущих научных изданиях, доклады на перечисленных конференциях, подтверждают высокий спрос научной информации, полученной соискателем. Полученные патенты на изобретения и эффекты внедрения предлагаемых соискателем решений свидетельствуют о высокой степени достоверности полученных результатов исследования.

Тем не менее следует отметить следующие замечания по представленной работе:

1. В функциях уровня выработки КЗК указана опциональная функция по построению аутентифицированного канала для выработки квантовых ключей. У уровня выработки квантовых ключей такая функция отсутствует. Не ясно, какими средствами строится данный канал, если опциональная функция не реализуется и почему она обозначена опциональной.

2. Указано свойство разработанной методики распределения общего секрета: ни один из участников формирования КЗК не имеет возможности предсказать результат формирования КЗК до начала его формирования. Это свойство выполняется только при ограничении вычислительных мощностей оконечного УКС, иначе он способен подобрать такую компоненту КЗК, которая вместе с полученной компонентой от второго оконечного УКС сформирует требуемый КЗК.

3. Из предложенной методики распределения КЗК не ясно, как оконечные УКС будут определять, кому необходимо передать свою компоненту КЗК.

4. Целевые УКС в предлагаемой методике распределения общего секрета расположены на концах магистральной сети КРК. Однако СЗИ-потребители могут располагаться и в середине магистральной линии. Целесообразно было бы предложить модификацию методики для этого случая.

Соответствие темы диссертации заявленной научной специальности. Тема диссертации и положения, выносимые на защиту, соответствуют паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по пунктам:

- модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования (п. 6);

- модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем (п. 8);

- принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности (п. 13).

Оценка диссертационной работы. 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.

Официальный оппонент,

Заместитель командира войсковой части 43753-А
кандидат технических наук
старший научный сотрудник Корольков Андрей Вячеславович

Подпись Королькова А.В. подтверждаю.

Уполномоченный сотрудник К.Е.Скоробогатов

25.08.2022