Отзыв

научного руководителя на диссертационную работу Жиляева Андрея Евгеньевича «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

Актуальность темы исследования обоснована тем, что проблема распределения ключей между парами пользовательских устройств требует решения в условиях появления новых угроз, связанных с развитием квантовых вычислений, при этом перспективным решением является распределение ключей с помощью технологии квантового распределения ключей, что предотвращает возможность проведения эффективных атак с применением квантового компьютера.

Научная новизна. В работе получены следующие новые результаты:

1. Разработана 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. Новизна предлагаемого решения подтверждается авторским патентом на изобретение.

2. Разработана 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. Предложена методика построения сети КРК смешанной топологии, включающая требования к структуре сети КРК, способу ее функционирования, методику распределения квантовозащищенных ключей (п. 2 новизны), отличающаяся от известных полностью децентрализованным управлением при создании квантовозащищенных ключей, учетом требований их целостности и конфиденциальности, а также имеющая по сравнению с зарубежными аналогами большую гибкость при масштабировании сети. Новизна предлагаемого автором решения подтверждается патентом на изобретение.

Методы исследования. Для решения поставленных задач в диссертационном исследовании использовались методы системного анализа, теории защиты информации, теории кодирования, теории квантовой физики и квантового распределения ключей.

Достоверность и обоснованность разработанных научных положений, результатов и выводов работы подкрепляются анализом современного состояния исследований в предметной области, обоснованием предложенных методик, не противоречащих известным положениям других авторов, 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 квантового распределения ключей (Университетская квантовая сеть, ViPNet QTS), промышленные комплексы систем квантового распределения ключей (ViPNet Quandor, ViPNet QSS, Квазар-СКР).

Теоретическая ценность работы состоит в развитии теории защиты информации в части применения технологии квантового распределения ключей 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 квантового

распределения ключей, и проводить анализ стойкости квантовых ключей.

Практическая ценность работы состоит в использовании основных положений диссертации для создания промышленных образцов квантовых сетей в соответствии с основными направлениями дорожной карты ОАО РЖД по развитию сквозной цифровой технологии квантовых коммуникаций. Предложенная структура базового сегмента сети квантового распределения ключей топологии «точка-точка» позволяет минимизировать число каналов между географически разнесенными узлами, что приводит к упрощению развертывания таких пар узлов.

Внедрение. Результаты представленной работы использовались при реализации проекта 03.G25.31.0254, выполняемого при финансовой поддержке Министерства образования и науки Российской Федерации и комплексного проекта «Разработка технологии и аппаратуры сетей квантового распределения криптографических ключей с использованием доверенных узлов», выполняемого по соглашению с Министерством промышленности и торговли РФ № 020-11-2019-933 от 19.11.2019.

Полнота опубликования результатов работы. По материалам представленного исследования опубликовано им 8 статей (из них 4 работы в изданиях, рекомендованных ВАК РФ, 2 работы - в изданиях WoS и Scopus) и получено три патента, в которые непосредственно вошли научные результаты диссертационной работы.

Жиляев Андрей Евгеньевич успешно закончил МГТУ им. Н.Э. Баумана с присвоением диплома математика по специальности «Компьютерная безопасность» в 2016 году. В этом же году поступил в аспирантуру МГТУ им. Н.Э. Баумана на кафедру ИУ-8, которую окончил в 2020 году. С апреля 2022 года работает в должности младшего научного сотрудника Института системной интеграции и безопасности ТУСУР, продолжая научные исследования по теме диссертации. Научная работа, представленная в диссертации, была выполнена на кафедре комплексной информационной безопасности электронно-вычислительных систем ТУСУР.

Андрей Евгеньевич Жиляев во время подготовки и написания

диссертационной работы проявил себя настойчивым, целеустремленным, глубоко разбирающимся в поставленных задачах научных исследований сотрудником. Жиляев А.Е. начал исследовать проблему распределения квантовых ключей для общепринятых топологий сети и достиг значимых результатов на этапе подготовки кандидатской диссертации. Важной отличительной чертой Жиляева А.Е. является стремление довести результаты научных исследований до практического применения и защиты своих результатов путем получения патентов на изобретения. Результаты, полученные им, успешно внедрены в ведущих предприятиях России в области исследования квантовых систем: МГУ имени М.В. Ломоносова и АО «ИнфоТеКС». Некоторые положения диссертационной работы Жиляева А.Е. используются в Техническом комитете по стандартизации № 26 при разработке проектов стандартов, входящих в систему национальных стандартов Российской Федерации.

На этапе работы над кандидатской диссертацией Жиляев А.Е. провел значительный объем исследований по распределению квантовозащищенных ключей для систем смешанной топологии, что является его несомненно существенным вкладом в развитие теории защиты информации.

Считаю соискателя степени кандидата технических наук Жиляева А.Е. сформировавшимся исследователем, способным самостоятельно ставить и решать актуальные прикладные научные задачи. Его диссертационная работа является законченным научно-квалификационным трудом, в котором решена важная научно-техническая задача создания сетей квантового распределения ключей произвольной топологии.

Научная новизна полученных результатов, их обоснованность и достоверность, теоретическая и практическая значимость позволяют считать, что представленная диссертационная работа соответствует требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по форме, содержанию и оформлению, а соискатель Жиляев Андрей Евгеньевич заслуживает присвоения ему ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты

предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по форме, содержанию и оформлению, а соискатель Жиляев Андрей Евгеньевич заслуживает присвоения ему ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Научный руководитель,
ведущий научный сотрудник ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники»
доктор технических наук, доцент А.Г. Сабанов
09.04.2022

634050, г. Томск, пр. Ленина, 40
Тел.: +7 (3822) 90-71-55, e-mail: sag@fb.tusur.ru

Подпись А.Г. Сабанова удостоверяю
Ученый секретарь совета ТУСУРа Е.В. Прокопчук