ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 212.268.03, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР), МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____
решение диссертационного совета от 15 сентября 2022г. № 12

О присуждении Жиляеву Андрею Евгеньевичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методика построения сетей квантового распределений ключей смешанной топологии» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 26 мая 2022 г. (протокол N 10) диссертационным советом Д 212.268.03, созданным на базе ТУСУРа (634050, г. Томск, пр. Ленина, 40). Приказ о создании диссертационного совета № 105/нк от 11 апреля 2012.

Соискатель Жиляев Андрей Евгеньевич, 8 сентября 1993 года рождения, в 2016 г. окончил МГТУ им. Н. Э. Баумана. С 2016 по 2020 г. обучался в аспирантуре МГТУ им. Н. Э. Баумана. Работает младшим научным сотрудником в институте системной интеграции и безопасности (ИСИБ) ТУСУРа.

Диссертация выполнена на кафедре комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа.

Научный руководитель – доктор технических наук, доцент Сабанов Алексей Геннадьевич, ведущий научный сотрудник научно-инжинирингового центра «Доверенные системы на основе АПК» ТУСУРа.

Официальные оппоненты: Молотков Сергей Николаевич, доктор физико-математических наук, главный научный сотрудник Института физики твердого тела РАН (г. Черноголовка Московской обл.); Корольков Андрей Вячеславович, кандидат технических наук, заместитель командира войсковой части 43753-А

(г. Москва), дали положительные отзывы на диссертацию.

Ведущая организация – общество с ограниченной ответственностью «Международный центр квантовой оптики и квантовых технологий» (г. Москва), в своем положительном отзыве, составленном Федоровым А.К., PhD по теоретической физике, руководителем научной группы «Квантовые информационные технологии», утвержденном Шляпниковым Г.В., д.ф.-м.н., научным директором «Российского квантового центра», указала, что диссертация Жиляева А.Е. является завершенной научно-квалификационной работой, в которой даны научно обоснованные решения по построению протяженных сетей квантового распределения ключей (КРК) сложных топологий, в особенности в части безопасного и стойкого распределения общих секретов в пары средств защиты информации, произвольно подключенным 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.

Соискатель имеет 11 опубликованных работ по теме диссертации, в том числе 4 работы, опубликованные в журналах, входящих в список ВАК, и 2 работы, опубликованные в журналах, индексируемых Scopus и/или Web of Science. Общий объем – 2,8 п.л., авторский вклад – 1,8. Получены 3 патента на изобретение.

Наиболее значимые работы:

1. Реализация средства криптографической защиты информации, использующего квантовое распределение ключей / А.Г. Втюрина, В.Л. Елисеев, А.Е. Жиляев, А.С. Николаева, В.Н. Сергеев, А.В. Уривский// Доклады ТУСУР. – 2018. – Т. 21. – № 2. – С. 15–21.

2. Жиляев А.Е. Классификация схем выработки и распределения ключей в сетях квантового распределения ключей произвольной топологии // Доклады ТУСУР. – 2021. – Т. 24. – № 4. –С. 33–39.

3. Пат. 2 708 511 РФ, МПК H 04 L 9/08, G 06 F 21/72. Способ формирования ключа между узлами вычислительной сети с использованием системы квантового распределения ключей / А.Е. Жиляев. – № 2019102923: заявл. 04.02.2019: опубл. 09.12.2019, Бюл. № 34. – 2 с.

4. Borodin, M., Zhilyaev A., Urivskiy A. Key generation schemes for channel authentication in quantum key distribution protocol // IET Quant. Comm. – 2021. – Vol. 2 – № 3. – P. 90– 97. – doi: 10.1049/qtc2.12020.

На диссертацию и автореферат поступило 7 положительных отзывов из следующих организаций: ООО «СФБ Лаб», г. Москва (Арбеков И.М., к.ф.-м.н., старший специалист); АО «Конструкторское бюро «Корунд-М», г. Москва (Баранов А.П., д.ф.-м.н, зам. генерального директора); ООО «Код Безопасности», г. Москва (Коренева А.М., к.ф.-м.н., начальник отдела криптографического анализа; ООО «КРИПТО ПРО», г. Москва (Смышляев С.В., д.ф.-м.н., зам. генерального директора); Нижегородский государственный университет им. Н.И. Лобачевского (Ротков Л.Ю., к.т.н. доц., зав. кафедрой безопасности информационных систем); Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск (Новиков С.Н., д.т.н., доцент, зав. кафедрой «Безопасность и управление в телекоммуникациях»); Омский государственный технический университет (Ложников П.С., д.т.н., профессор, зав. кафедрой «Комплексная защита информации»).

В отзывах на автореферат указаны следующие основные замечания: вывод о том, что для систем КРК, вырабатывающих ключи недостаточного размера, неприменимы теоретико-информационные методы оценки стойкости процедуры аутентификации, требует уточнения, системы КРК, упомянутые в автореферате, принципиально могут формировать квантовый ключ любой разумной длины, ограничения на длину носят технический характер, отражая, по существу, уровень технических возможностей разработчика системы на настоящий момент времени; в автореферате указано, что для распределения общего секрета необходимо определить цепочку узлов сети КРК, по которой будет производиться распределение, способ формирования такой цепочки и возможность ее

технической реализации не показан в тексте автореферата; не уделено внимания постквантовым алгоритмам для решения задачи формирования общего секрета двумя устройствами и сравнению с предлагаемым автором решением на основе квантовых технологий; не рассматриваются вопросы общей защищенности сети при применении конкретного алгоритма КРК и возможные проблемы при интеграции предложенной сети КРК в уже развернутые комплексы; приведены три группы критериев для классификации способов решения задачи распределения общего секрета на целевые узлы квантовой сети, в то же время не представлены сами предложенные критерии из данных групп; в автореферате недостаточно подробно представлен анализ существующих решений по сетям КРК и подходов к увеличению расстояния между оконечными устройствами.

Выбор официальных оппонентов обосновывается тем, что д.ф.-м.н. Молотков С.Н. является известным специалистом в области квантовых коммуникаций; к.т.н. Корольков А.В. является признанным специалистом в области информационной безопасности, что подтверждается списками опубликованных работ по теме диссертации.

Выбор ведущей организации обосновывается тем, что ООО «МЦКТ» имеет общепризнанные достижения в области квантовых коммуникаций, безопасности систем КРК и способна определить и аргументированно обосновать научную и практическую значимость работы Жиляева А.Е.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

– ***разработана*** новая методика распределения общих секретов в сети КРК магистральной топологии, отличающаяся от известных сохранением стойкости распределенных общих секретов при компрометации квантовых ключей, а также возможностью сохранения конфиденциальности распределяемых секретов на промежуточных узлах сети КРК;

– ***разработана*** новая методика построения сети КРК смешанной топологии, отличающаяся от известных полностью децентрализованным управлением при создании квантовозащищенных ключей, учетом требований их целостности

и конфиденциальности;

– ***введено*** новое понятие квантовозащищенного ключа, позволяющее 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 при анализе их стойкости.

Теоретическая значимость исследования обоснована тем, что:

– ***доказана*** эффективность предложенных методики распределения общих секретов в магистральных сетях КРК и построения сетей КРК смешанных топологий, вносящих вклад в развитие методического обеспечения квантовых коммуникаций для повышения защищенности сетей КРК.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

– ***разработаны и внедрены*** способ построения классического аутентифицированного канала квантовой аппаратуры и способ взаимодействия квантовой аппаратуры и средств защиты информации при передаче квантовых ключей в комплексе ViPNet Quandor при выполнения НИОКТР 03.G25.31.0254 при финансовой поддержке Министерства образования и науки Российской Федерации. *Разработанная* методика распределения квантовозащищенных ключей *положена* в основу ключевой системы ViPNet QSS. *Разработанная* структура сети КРК и методика построения сетей КРК смешанной топологии *внедрена* при реализации комплексного проекта «Разработка технологии и аппаратуры сетей квантового распределения криптографических ключей с использованием доверенных узлов», выполняемого по соглашению с Министерством промышленности и торговли Российской Федерации № 020-11-2019-933 от 19.11.2019, что ускорило на 15% процесс эскизного проектирования и позволило унифицировать аппаратную платформу узлов сети КРК. Методика распределения квантовозащищенных ключей повысила безопасность протяженных квантовых сетей на базе изделия «Квазар-СКР» за счет использования функции гибридизации двух компонент, переданных по независимым каналам связи. Методика постро-

ения сети КРК смешанной топологии *внедрена* в Университетской квантовой сети МГУ им. М.В.Ломоносова, что сократило на 20 % процесс развертывания сети. Методика распределения квантовозащищенных ключей *положена* в основу проекта методических рекомендаций ТК 26 «Информационная технология. Криптографическая защита информации. Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ», что сократило на 30% процесс разработки проекта. Результаты внедрения подтверждаются соответствующими актами о внедрении.

Оценка достоверности результатов исследования выявила:

– ***теория*** построена на известных методах теории защиты информации, системного анализа, квантовых коммуникаций;

– ***идея*** распределения общих секретов в магистральной сети КРК, основанная на методе разделения секрета, и построения сетей КРК с использованием доверенных промежуточных узлов *базируется* на анализе практики и обобщении передового опыта построения сетей КРК;

– ***использовано*** сравнение результатов применения авторских методик с опубликованными ранее методик иных авторов в отечественных и зарубежных публикациях и стандартизующих документах.

Личный вклад соискателя состоит в самостоятельной разработке и реализации методики распределения квантовозащищенного ключа в сети КРК магистральной топологии и методики построения сети КРК смешанной топологии, проведении апробации разработанных методик.

В ходе защиты диссертации были высказаны следующие критические замечания: не понятно где внедрена методика в реальных системах; каким образом оценивается и подтверждается внедрение результатов; какие имеются подтверждающие факторы, что предложенные новые результаты не только отличаются от известных, но и позволяют говорить об улучшении; если действия описанных методик формализованы, то это алгоритм, а не методика; не понятно как обосновывается достоверность исследования; не ясно как доказывается стойкость получаемых квантовых ключей и невозможность по свободно рас-

пределяемой части определить оставшуюся часть, отводимую на аутентификацию канала; стойкость и надежность передачи в сети зависит не только от ключа, но и от того, какие атаки будут осуществляться, этот вопрос вообще не касается вашей области исследований.

Соискатель Жиляев А.Е. ответил на задаваемые ему в ходе заседания вопросы и сформулированные замечания и привел собственную аргументацию: методики реализованы в существующих сетях, например в Университетской квантовой сети МГУ имени М.В.Ломоносова, результаты внедрения на реальном объекте подтверждаются соответствующими актами; на основные защищаемые положения и пункты новизны получены патенты на изобретения, по патентуемым объектам проводился патентный поиск и мной и экспертами Роспатента; полученные патенты, положительные эффекты внедрения, а также полученные разрешения на эксплуатацию от регулятора в области информационной безопасности подтверждают достоверность полученных результатов; представленные методики содержат не конкретизированные шаги, так методика распределения квантовозащищенных ключей требует фиксирования способа распределения квантовой компоненты и функции гибридизации, для того чтобы стать алгоритмом, соответствующие алгоритмы были реализованы после уточнения этапов методики в проекте методических рекомендаций Технического комитета 26; непосредственно стойкость квантового протокола, а также безопасности его технической реализации – выход за рамки моего исследования, полученные результаты верны при условии, что создаваемые квантовые ключи стойкие, в том числе случайные, равновероятные, независимые; стойкость квантовых протоколов доказана специалистами в области квантовой физики и квантовых коммуникаций.

На заседании 15 сентября 2022 г. диссертационный совет постановил за решение научной задачи построения сетей квантового распределения ключей смешанной топологии, имеющей значение для развития методического обеспечения квантовых коммуникаций в части защищенности сетей квантового распределения ключей присудить Жиляеву А.Е. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 19 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовал: за – 19, против – 0, недействительных бюллетеней – 0.

Председатель
диссертационного совета Шелупанов Александр Александрович

Ученый секретарь
диссертационного совета Костюченко Евгений Юрьевич

16.09.2022