На правах рукописи

Жиляев Андрей Евгеньевич

МЕТОДИКА ПОСТРОЕНИЯ СЕТЕЙ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ СМЕШАННОЙ ТОПОЛОГИИ

05.13.19 – Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Томск 2022

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники» (ТУСУР)

Научный руководитель –	доктор технических наук доцент Сабанов Алексей Геннадьевич
Официальные оппоненты:	Молотков Сергей Николаевич, доктор физико-математических наук, главный научный сотрудник Института физики твердого тела РАН, г. Черноголовка Московской области
	Корольков Андрей Вячеславович, кандидат технических наук, заместитель командира войсковой части 43753-А, г. Москва
Ведущая организация:	Общество с ограниченной ответственностью «Международный центр квантовой оптики и квантовых технологий» (ООО “МЦКТ”), г. Москва, «Сколково»

Защита диссертации состоится 15.09.2022 в 15-00 на заседании диссертационного совета Д 212.268.03, созданном на базе ТУСУРа, по адресу: 634050, г. Томск, пр. Ленина 40, ауд. 201.

С диссертацией можно ознакомиться в библиотеке ТУСУРа по адресу: 634045, г. Томск, ул. Красноармейская 146, а также на сайте ТУСУРа: https://postgraduate.tusur.ru/urls/g5uxkdc7

Автореферат разослан «___» _____ 2022 г.

Ученый секретарь
диссертационного совета  Костюченко Евгений Юрьевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В системах защищенной связи данные передаются по сетям связи общего пользования, а следовательно, доступны потенциальному нарушителю для проведения различных атак. Нарушитель способен сохранять закодированные данные, передаваемые в канале, а попытку декодирования производить в будущем, когда новые технические возможности и способы атаки на алгоритмы защиты информации позволят провести раскодирование за приемлемое время. В этом заключается принцип «Store now, decrypt later», считающийся одной из основных проблем систем защиты информации.

Возникает потребность регулярной смены используемого ключа, а следовательно, и поиск вариантов доставки и/или генерации таких ключей между двумя устройствами, организующими защищенный канал. Смена ключа на новый, независимый от предыдущего, позволяет добиться защиты передачи будущей информации при компрометации текущего ключа, а также обеспечения свойства *Perfect forward secrecy,* т.е. при компрометации мастер-ключа все последующие ключи должны оставаться не скомпрометированными.

Отдельно стоит отметить угрозу создания квантового компьютера, позволяющего эффективно атаковать известные схемы генерации ключей, основанные на сложности вычисления дискретного логарифма или факторизации больших чисел (например, квантовые алгоритмы Шора и Гровера).

Известные способы доставки секретных ключей: с помощью доверенного курьера; с помощью алгоритмов с секретным ключом; с помощью схем выработки ключа на основе вычислительно сложных задач, – не позволяют добиться регулярной доставки независимых ключей, в условиях нарушителя, обладающего квантовым компьютером и неограниченными вычислительными ресурсами.

Таким образом, проблема распределения ключей между парами пользовательских устройств является актуальной научной проблемой, требующей решения в условиях появления новых угроз, связанных с созданием квантового компьютера.

Перспективным решением является распределение ключей с помощью технологии квантового распределения ключей (КРК). КРК основывается на совершенно иных физических принципах, что предотвращает возможность проведения эффективных атак с применением квантового компьютера. В то же время у технологии КРК есть ряд существенных ограничений, которые необходимо учитывать при проектировании таких систем доставки ключей.

Протоколы КРК для систем топологии «точка-точка» активно разрабатываются и изучаются учеными-физиками. Неоспоримый вклад в развитие технологии КРК внесли Ch. Bennett и G. Brassard, предложив первый протокол КРК BB84. Развитием протоколов КРК занимаются A. Poppe, A. Shields, С.Н. Молотков. В изучение применения технологии КРК в сетях смешанных топологий существенный вклад вносят N. Lütkenhaus, M. Mosca, Группа В. Макарова вносит значимый вклад в анализ безопасности систем КРК, проводя

исследования уязвимости реализаций систем КРК. Устройства, реализующие протоколы КРК, разрабатываются в Китае, США, Европе и России. В России сложилось три крупных центра разработки в области квантовых коммуникаций: МГУ имени М. В.Ломоносова совместно с АО «ИнфоТеКС», Российский квантовый центр совместно с ООО «КуРейт» и Национальный исследовательский университет ИТМО совместно с ООО «СМАРТС-Кванттелеком».

К сожалению, большинство работ, касающихся протоколов КРК и квантовой аппаратуры, посвящены физике процесса и не рассматривают реализацию неотъемлемой части квантовой аппаратуры, а именно классического аутентифицированного канала. Также подробно не рассматривается сопряжение квантовой аппаратуры и пользовательских устройств, средств защиты информации (СЗИ), для которых формируются общие секреты.

Для преодоления ограничения длины квантового канала аппаратура КРК объединяется в так называемые сети КРК с доверенными промежуточными узлами. При данном подходе квантовые ключи вырабатываются только между узлами сети, соединенными напрямую квантовым каналом. На прочие узлы квантовой сети (УКС) одни квантовые ключи передаются под защитой других выработанных квантовых ключей.

Работы в этом направлении осуществляются ведущими организациями по всему миру. В Китае создана и успешно функционирует сеть КРК, протяженностью более 2000 км. Также ведутся работы по стандартизации сетей КРК, в том числе в ETSI и в ITU-T. Международная организация ISO занимается вопросами разработки требований по безопасности к квантовой аппаратуре и сетям КРК. Создан европейский проект OpenQKD, предполагающий развертывание испытательных полигонов для тестирования наработок по созданию крупных сетей КРК и создания практически применимых промышленных образцов. В России, в рамках национальной программы «Цифровая экономика», принятой в соответствии с Указом Президента Российской Федерации от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», утверждена дорожная карта развития «сквозной» цифровой технологии «квантовые технологии». Дорожная карта «разработана с целью получения в среднесрочной и долгосрочной перспективе практически значимых научно–технических и практических результатов мирового уровня по следующим субтехнологиям: квантовые вычисления, квантовые коммуникации и квантовые сенсоры». В исполнение дорожной карты развития «сквозной» цифровой технологии утверждена дорожная карта ОАО «РЖД» развития высокотехнологичной области «Квантовые коммуникации» на период до 2024 года. Целью дорожной карты ОАО «РЖД» является «ускорение технологического развития и достижение РФ позиций одного из лидеров на глобальных технологических рынках в высокотехнологичной области «Квантовые коммуникации».

Целью исследования является развитие методического обеспечения квантовых коммуникаций для повышения защищенности сетей квантового распределения ключей смешанной топологии.

Для достижения поставленной цели необходимо решить следующие задачи:

1. разработать способ построения классического аутентифицированного канала квантовой аппаратуры;
2. создать способ взаимодействия квантовой аппаратуры с пользовательскими СЗИ, уточняющий процессы синхронизации и обеспечения целостности общих секретов при их передаче в СЗИ;
3. разработать методику распределения общего секрета для пары узлов сети КРК магистральной топологии;
4. выработать методику построения сетей КРК смешанной топологии, включающую требования к структуре сети КРК смешанной топологии и способу функционирования такой сети.

Объектом исследования данной работы являются сети квантового распределения ключей смешанной топологии.

Предметом исследования является методика построения сетей квантового распределения ключей смешанной топологии с учетом требований безопасности.

Основные **методы исследования**, примененные в диссертационной работе – это методы системного анализа, теории защиты информации, теории кодирования, теории квантовой физики и квантового распределения ключей.

Научная новизна результатов работы и проведенных исследований:

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 полученным патентом на изобретение [10].

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 решения подтверждается полученным патентом на изобретение [11].

Теоретическая и практическая значимость работы.

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.

В то же время основные положения работы представляют практическую ценность для создания промышленных образцов квантовых сетей, что соответствуют, например, основным направлениям 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.

Достоверность и обоснованность результатов и выводов работы подтверждается 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 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.

Положения, выносимые на защиту:

1. Структура комплекса защищенной передачи данных, состоящего из пары СЗИ и пары квантовой аппаратуры, и способ доставки общих секретов в таком комплексе, позволяющий контролировать идентичность формируемых в квантовой аппаратуре секретов с секретами, полученными парой СЗИ.

Соответствует пункту 6 паспорта специальности 05.13.19: 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.

2. Методика распределения общего секрета в оконечные узлы магистральной сети квантового распределения ключей, позволяющая повысить защищенность распределяемых секретов за счет сохранения конфиденциальности распределяемых секретов на промежуточных узлах сети, контроля целостности

секретов при их передаче между узлами сети, а также сохранении общего секрета нескомпрометированным даже при компрометации квантовых ключей.

Соответствует пункту 8 паспорта специальности: модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.

3. Методика построения сетей КРК смешанной топологии, включая требования к структуре и функциям такой сети, позволяющая конструировать децентрализованные сети КРК.

Соответствует пункту 13 паспорта специальности: принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Апробация работы. Основные и промежуточные результаты исследования докладывались и обсуждались на следующих конференциях:

- Восьмая всероссийская научно-техническая конференция «Безопасные информационные технологии» (Москва, 2017);
- Ежегодная международная молодежная научно-практическая конференция студентов, аспирантов и молодых учёных «Информационная безопасность в банковско-финансовой сфере» (Москва, 2017);
- Ежегодная международная молодежная научно-практическая конференция студентов, аспирантов и молодых учёных «Информационная безопасность в банковско-финансовой сфере» (Москва, 2018);
- XX научно-практическая конференция «РусКрипто’2018» (Солнечногорск, 2018);
- 2018 Moscow Workshop on Electronic and Networking Technologies (MWENT), (Москва, 2018);
- 9th International Conference on Quantum Cryptography (QCrypt-2019), (Монреаль, Канада, 2019);
- 10th International Conference on Quantum Cryptography (QCrypt-2020), (Амстердам, Нидерланды, 2020);
- The 3rd International School on Quantum Technologies (Sochi 2020) (QTS20), (Сочи, 2020);
- IX Симпозиум «Современные тенденции в криптографии» (CTCrypt 2020), (Московская область, 2020).
- XXIV научно-практическая конференция «РусКрипто’2022» (Солнечногорск, 2022)

Реализация результатов работы. Результаты настоящей 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.

Публикации по теме диссертации. По материалам исследования опубликовано 8 работ, в том числе 4 работы в изданиях, рекомендованных ВАК РФ, 2 в изданиях WoS и Scopus. Получено 3 патента на изобретение.

Личный вклад автора состоит в выполнении основного объема приведённых в диссертационной работе исследований. В работах, написанных в соавторстве, автору принадлежит определяющая роль в представленных результатах по теме исследования.

Структура и объем диссертации. Диссертация содержит введение, четыре главы, заключение, список сокращений и условных обозначений, список терминов, список источников из 126 наименований, список иллюстративного материала и 3 приложения. Объем работы: 240 страниц, в том числе 27 рисунков, 2 таблицы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертационного исследования, сформулирована цель, определены задачи, научная новизна, практическая и теоретическая значимость полученных результатов, а также положения, выносимые на защиту.

В первой главе рассматриваются подходы применения технологии квантового распределения ключей для регулярной доставки общих секретов в пары пользовательских устройств, СЗИ-потребителей, в том числе подходы к преодолению принципиального ограничения технологии, обусловленного предельными значениями потерь в квантовом канале, выражающиеся в построении протяженных сетей квантового распределения ключей.

В результате проведенного анализа показана типовая архитектура комплекса квантовой аппаратуры, реализующей протокол КРК. Сервер КРК и Клиент КРК соединены двумя логическими каналами: квантовым и классическим. Квантовый канал предназначен для передачи квантовых информационных состояний, фотонов, обычно реализуется оптоволокном. Система КРК дополнительно имеет логический служебный канал данных, соединяющий Клиент КРК и Сервер КРК, в котором передаются команды и данные управления и мониторинга аппаратуры, не связанные непосредственно с протоколом КРК

Сеанс КРК состоит из трех этапов: подготовка квантового канала, передача одиночных фотонов по квантовому каналу, постобработка переданной последовательности.

Этап постобработки включает в себя три подэтапа: согласование базисов, исправление ошибок и усиление секретности.

На рисунке 1 представлена обобщенная последовательность выполнения протокола КРК.

В работах, описывающих физическую сторону технологии КРК, не уделяется должного внимания построению классического аутентифицированного

канала. Открытым научным вопросом является способ обеспечения аутентификации этого канала.

Другой важной научной проблемой, не рассмотренной в научной литературе, является собственно передача созданного квантового ключа от квантовой аппаратуры потребителям, а точнее пользовательским устройствам, которые будут использовать этот квантовый ключ, в том числе достижение синхронизации передаваемых секретов, сформированных из квантовой гаммы.

Рисунок 1 – Последовательность выполнения протокола КРК

Решение обозначенных научных проблем, проведенных в настоящем исследовании, позволит применять технологию КРК для систем в топологии «точка-точка» для регулярного распределения общих секретов в пользовательские устройства.

Также в работе рассматриваются пути решения проблемы распределения общих секретов на расстояния, превышающие предельную длину квантового канала, с помощью сетей КРК с доверенными промежуточными узлами. В основу таких сетей заложена идея последовательной передачи с перекодированием некоторого квантового ключа, полученного на некотором сегменте сети КРК, через промежуточные узлы на требуемые узлы, на которые необходимо распределить общий секрет. В качестве алгоритма кодирования принято выбирать одноразовый шифроблокнот (One-Time Pad Encryption).

Существенным недостатком предлагаемого подхода при передаче секрета является решение только задачи обеспечения конфиденциальности передачи, но не целостности, а также появление его в открытом виде на каждом УКС. Кроме того, предлагается использовать квантовый ключ некоторого сегмента, т.е. ключ, о котором у нарушителя есть некоторая, пусть малая информация.

Таким образом, известный базовый подход может рассматриваться как начальный шаг при синтезе способов распределения общего секрета для произвольных УКС, но требует дальнейшей проработки и устранения описанных недостатков, что является нерешенной научной задачей.

В работе проанализированы существующие предложения по структуре сетей КРК с доверенными промежуточными узлами. Наиболее проработанными вариантами являются сети КРК, описанные в документах ETSI и ITU-T.

По результатам анализа выявлено, что сети КРК, описываемые в европейских рекомендациях, имеют многоуровневую структуру с централизованным управлением. Все ключи, появляющиеся в сети КРК именуются квантовыми ключами, что вносит дополнительную путаницу и неотличимость квантовых ключей, создаваемых в результате протокола КРК, от общих секретов, полученных в результате дальнейшего функционирования сети КРК. Централизованное управление сетью КРК ведет к возникновению точки отказа из-за повышения нагрузки на единый центр управления.

Таким образом, имеется научная проблема исследования возможности построения децентрализованной сети КРК, а также необходимость решения проблемы распределения общего секрета на произвольные пары УКС с обеспечением не только конфиденциальности, но и целостности передаваемой ключевой информации.

Во второй главе предлагаются решения выявленных проблем для систем КРК в простейшей топологии «точка-точка».

Выделяются два основных подхода к обеспечению аутентификации данных в классическом канале, т.е. обеспечению аутентичности отправителя и целостности переданных данных. Аутентичность отправителя достигается наличием секретного ключа у отправителя и получателя. Причем ключ формируется из квантового ключа предыдущего сеанса КРК путем разбиения квантового ключа KK на ключи для пользователей $K_{\text{Полз}}$ и ключи аутентификации $K_{\text{Аут}}$ следующего сеанса КРК размера, требуемого для выбранной функции аутентификации (см. рис. 2).

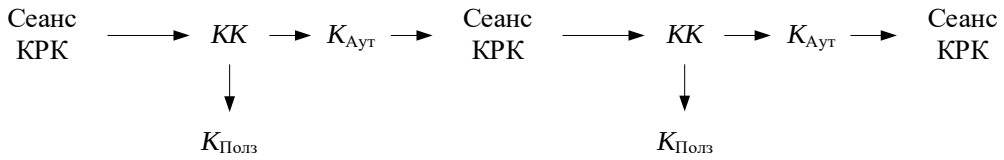

Рисунок 2 – Схема диверсификации квантовых ключей протокола КРК

Для обеспечения целостности данных вычисляется имитовставка от передаваемого сообщения.

В качестве аутентификации, стойкой в теоретико-информационном смысле, для систем КРК рассматриваются классы функций универсального хэширования $\varepsilon - ASU_2$ (Almost Strong Universal Hashing). Параметр ε является параметром стойкости класса хэш-функций.

По результатам проведенного анализа наименьшими размерами ключей обладают функции семейств Stinson, der Boer, Bierbrauer. Однако, использование семейства функций Bierbrauer сопряжено с построением кода Рида-Соломона большой размерности, а стойкость семейства функций der Boer существенно зависит от длины обрабатываемых сообщений. Наиболее целесообразным является применение функций семейства Stinson. При малом расходе ключа они

обладают простотой конструкции и параметром стойкости, зависящим от логарифма длины обрабатываемых сообщений.

Фундаментальной проблемой теоретико-информационно стойкой аутентификации является необходимость использования новых различных независимых ключей аутентификации для каждого аутентифицируемого сообщения.

В работе проведена оценка требуемого объема ключей аутентификации. Расчет произведен на основе объемов данных, передаваемых в классическом аутентифицированном канале, для комплекса ViPNet Quandor в процессе выполнения работ по проекту 03.G25.31.0254 при финансовой поддержке Министерства образования и науки Российской Федерации. Длина квантового канала составляет 100 км и длина квантового ключа, получаемого в результате одного сеанса КРК, не менее 256 бит.

Рассматривались четыре подхода вычисления имитовставки:

1. от каждого сообщения при первичной передаче его в классическом аутентифицируемом канале;
2. от всех сообщений, переданных в течение одного этапа сеанса КРК в одну сторону в конце этапа сеанса КРК;
3. от всех сообщений в обе стороны, переданных в течение одного этапа сеанса КРК;
4. от всех сообщений, переданных в течение всех трех этапов протокола КРК по окончании сеанса КРК.

В общем случае длина необходимого ключа аутентификации пропорциональна двоичному логарифму длины сообщения согласно формуле (1):

$$k_j = \sum_i \log_2 m_i, \qquad (1)$$

где i – номер аутентифицируемого сообщения;

m_i – длина аутентифицируемого сообщения;

j – номер подхода аутентификации.

Если применять хэш-функцию на базе кода Рида-Соломона, обладающую наименьшей длиной ключа из рассмотренных, длина ключа вычисляется по формуле (2):

$$k' = 2\log_2 m + 3t, \qquad (2)$$

где t – длина метки аутентификации, m – длина аутентифицируемого сообщения. Согласно рекомендациям SECOQC длина метки аутентификации должна быть не менее 64 бит.

Получены следующие нижние оценки длин ключа аутентификации для подходов $2 - 4$, соответственно: $k_2' = 1346$ бит, $k_3' = 686$ бит, $k_4' = 236$ бит. Оценки получены для размера данных классического аутентифицированного канала комплекса ViPNet Quandor при длине квантового канала 100 км.

Расчеты для подхода аутентификации 1 не производились в силу того, что данный подхода еще более затратный, чем подход аутентификации 2. Согласно произведенным расчетам при фактически полученной длине квантового ключа 400 бит для квантового канала длиной 100 км, следует, что только подход аутентификации 4 потенциально возможен: число бит, необходимых на ключ аутентификации, меньше, чем число бит получаемого квантового ключа. Однако при таком подходе аутентификации останется всего 164 бита квантового ключа, который можно использовать для формирования общего секрета пользователей. Если при расчете длины ключа аутентификации принимать, что за один сеанс КРК выработается 256 бит квантового ключа, что соответствует заявленным характеристикам комплекса ViPNet Quandor, то ни один из предложенных подходов не позволит выделять часть квантового ключа в качестве ключа аутентификации, и необходимо применять иные методы доставки ключей аутентификации в квантовую аппаратуру для удовлетворения потребности в ключах аутентификации множества сеансов КРК.

Малая скорость генерации квантовых ключей при большом объеме данных для аутентификации вызвана высокой степенью сжатия на этапе усиления секретности протокола КРК. Для конкретной системы, использованной для расчета, возможно уменьшение фактической длины квантового канала, что приведет к уменьшению ошибки в квантовом канале и, соответственно, уменьшению степени сжатия на этапе усиления секретности.

В общем случае, для систем КРК, обладающих недостаточным размером вырабатываемых квантовых ключей из-за высокого уровня стойкости вырабатываемых квантовых ключей (высокой степени сжатия на этапе усиления секретности), применение теоретико-информационно стойкой аутентификации оказывается невозможным. Для таких систем необходимо применение вычислительно стойкой аутентификации, например, с применением функции хэширования ГОСТ 34.11-2018.

В то же время, если степень сжатия на этапе усиления секретности позволяет получить необходимый объем ключа для формирования ключа аутентификации, необходимо применение универсальных функций хэширования для сохранения теоретико-информационной стойкости вырабатываемых квантовых ключей. Функции универсального хэширования, построенные по принципу Stinson обладают высоким показателем стойкости при низком расходе ключа аутентификации и простой конструкции используемых примитивов.

В данной главе также рассматривается решение проблемы доставки общих секретов в СЗИ-потребители. В частности, решается научная задача формирования общих секретов из квантовой последовательности, полученной в результате выполнения протокола КРК, последующей согласованной передачи идентичных секретов в пару СЗИ и контроля успешной передачи.

В результате выполнения протокола КРК на двух концах квантового канала получается идентичная случайная последовательность некоторой длины. Вариативность длины последовательности обусловлена неидеальностью

квантового канала и этапами исправления ошибок и усиления секретности протокола КРК.

В результате анализа выявленных недостатков предлагаются следующие решения для комплекса, представленного на рисунке 3.

В предлагаемом комплексе используется только одна классическая линия связи (транспортная линия связи), соединяющая как два СЗИ, так и два узла системы КРК, следовательно, не требуется отдельный канал для обмена служебными данными узлов системы КРК при выработке квантовых ключей, вместо этого используется единый канал для передачи служебных сообщений системы КРК и передачи закодированных пользовательских данных, что позволяет снизить затраты на создание, развертывание и эксплуатацию комплекса, а также повысить безопасность системы КРК за счет обеспечения конфиденциальности данных служебного канала системы КРК.

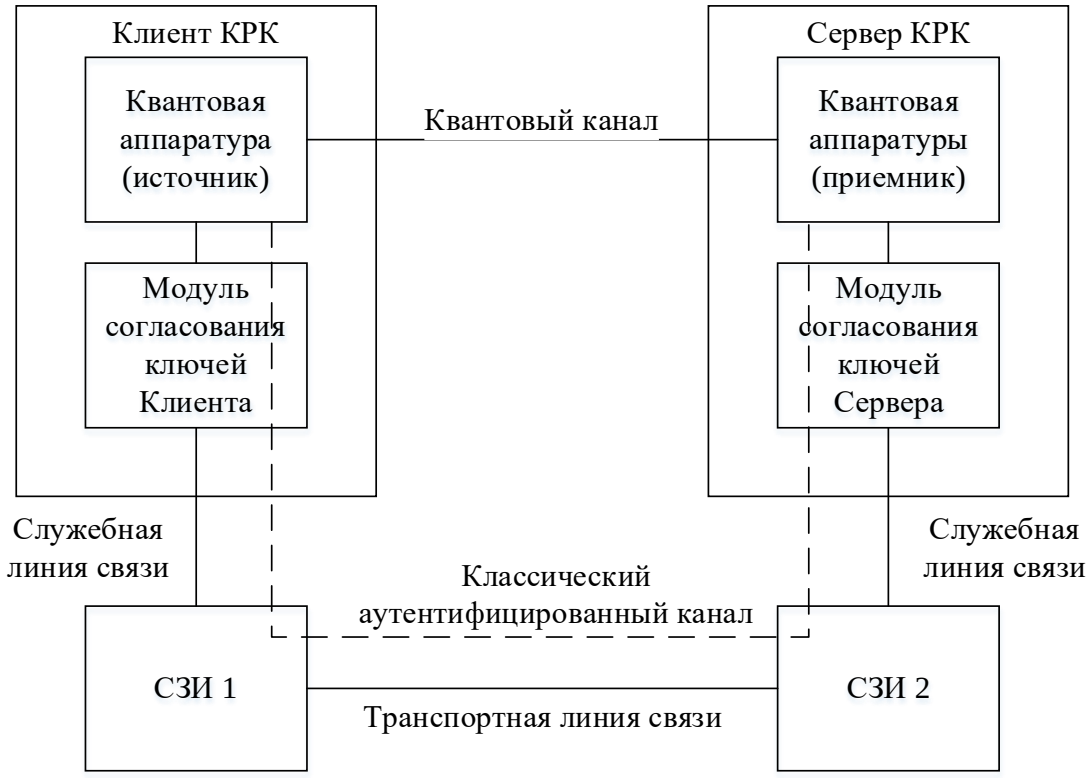

Рисунок 3 – Схема комплекса квантовой аппаратуры защиты информации

В квантовой аппаратуре предлагается реализация дополнительных модулей согласования ключей, выполняющих функции накопления случайной последовательности и формирования квантовых ключей для последующей их диверсификации на ключи аутентификации и пользовательские общие секреты. Накопление квантовых ключей сохраняет работоспособность комплекса в случае непредвиденных кратковременных сбоев системы КРК, выражающихся во временном прекращении генерации квантовых ключей или вызванных, например, атаками нарушителя на квантовый канал связи. Также работоспособность комплекса сохраняется в случае выработки системой КРК квантовых ключей, длина которых недостаточна для формирования новых ключей кодирования и ключей аутентификации. В этом случае происходит накопление ключей для

формирования требуемых общих секретов и ключей аутентификации уже из совокупности накопленных квантовых ключей.

Контроль идентичности производится двумя способами. В модели, полагающей квантовую аппаратуру и канал связи с СЗИ надежными, осуществляется только сравнение идентификатором формируемых и передаваемых общих секретов. В модели, допускающий сбои в работе аппаратуры дополнительно производится сравнение хэш-значений от сформированных секретов и их идентификаторов. Идентификаторы и хэш-значения передаются с обеспечением конфиденциальности в транспортной линии между СЗИ. В случае не совпадения хэш-значений, отбрасывается не только сформированный общий секрет, но и оставшаяся часть накопленной квантовой гаммы для исключения дальнейших расхождений общих секретов.

Третья глава посвящена решению основной научной проблемы распределения общего секрета на пары СЗИ, удаленные друг от друга на существенно большие расстояния, чем предельная длина квантового канала, т.е. распределение общего секрета на неограниченные расстояния.

Главной научной задачей является задача распределения общего секрета для произвольных пар УКС. Согласно базовому способу распределения общего секрета необходимо передать квантовый ключ по цепочке УКС. Следовательно, для распределения общего секрета необходимо определить цепочку УКС, соединяющую требуемую пару УКС, после чего на определенной цепочке произвести распределения общего секрета.

Каждую цепочку УКС можно рассматривать как подсеть магистральной топологии некоторой сети КРК. Такая магистральная подсеть представлена на рисунке 4. Подключение внешних СЗИ производится к оконечным УКС. Магистральная сеть будет рассматриваться как основной конструктив для распределения общих секретов между оконечными УКС в сетях смешанной топологии.

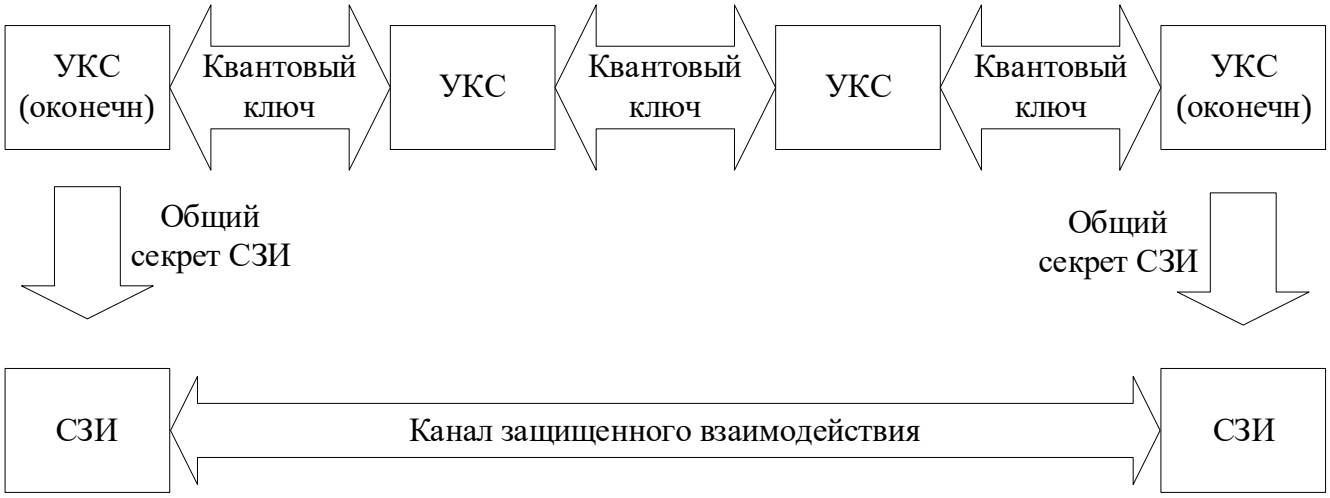

Рисунок 4 – Схема сети КРК топологии «магистраль»

Для решения общей задачи определения цепочек УКС предлагается первым шагом рассмотреть ее решение для простых топологий. Наиболее простой топологией после магистральной топологии является топология «звезда».

Сеть топологии «звезда» можно рассматривать как совокупность подсетей магистральной топологии, каждая из которых состоит из трех УКС: некоторого периферийный УКС, УКС Клиент; центрального УКС, УКС Сервер; и другого УКС Клиент.

Для сетей КРК магистральной топологии в работе разработаны способы распределения общего секрета на оконечные УКС.

Важно понимать, что общий секрет, распределенный на пару целевых УКС, в отличие от квантового ключа, получен не в результате протокола КРК, а путем передачи ключевого материала под защитой на квантовых ключах. То есть общий секрет целевых УКС – ключ, созданный сетью КРК, передаваемый по сети КРК с защитой на квантовых ключах, а не созданный на основе принципов квантовой физики. Для различения распределяемого общего секрета и истинно квантового ключа вводится термин «квантовозащищенный ключ (КЗК)». **Квантовозащищенный ключ** (КЗК) – ключ, созданный сетью КРК, ключевой материал для создания которого передавался по сети КРК с защитой на квантовых ключах. КЗК является результатом выполнения способа распределения общего секрета для двух целевых ДПУ.

Решая научную задачу распределения КЗК, необходимо определить те свойства данного объекта, которыми он будет обладать в зависимости от способа его распределения.

1. Неотличимость КЗК от случайного числа:
   - для нарушителя с любыми вычислительными ресурсами;
   - для нарушителя с ограниченными вычислительными ресурсами;
   - для нарушителя с ограниченными вычислительными ресурсами даже при компрометации всех квантовых ключей в системе;
2. Недоступность КЗК на промежуточных узлах;
3. Непредсказуемость КЗК в вычислительном смысле даже в случае, когда один из целевых УКС доступен нарушителю.
4. Сохранение защиты от чтения назад для КЗК.

Обязательными для КЗК, полученного в результате реализации некоторого способа распределения являются первое и четвертое свойство. Наличие второго и третьего свойства обеспечивает сохранение защищенности системы в условиях нарушителя, обладающего дополнительно возможностью влиять на некоторый УКС.

Разработаны несколько способов распределения КЗК, каждый из которых устраняет некоторые недостатки базового способа.

Способ **одновременной доставки секрета** предназначен для быстрого распределения КЗК между двумя целевыми УКС. Для этого цепь УКС длины n

делится на две подцепи длин $\left\lfloor \frac{n}{2} + 1 \right\rfloor$ и $\left\lfloor \frac{n}{2} \right\rfloor$. Квантовый ключ расцепленных УКС становится общим секретом целевых УКС.

Способ позволяет производить параллельные вычисления и легко масштабируется на большее число узлов. Для цепи из n узлов нужно совершить $n - 1$ защищенную передачу ключей. В предположении, что одна передача происходит за t секунд и узел способен одновременно принять до $\left\lfloor \frac{n}{2} + 1 \right\rfloor$ защищенных ключей, получаем, что распределить общий секрет между двумя целевыми узлами можно за t секунд. Если узел может одновременно принимать m сообщений, тогда процесс распределения займет $\left\lceil \frac{\left\lfloor \frac{n}{2}+1 \right\rfloor}{m} \right\rceil \cdot t$ секунд.

Способ **передачи секрета в ключевом контейнере** обобщает базовый способ распределения КЗК, заменяя конкретную передачу с защитой одноразовым шифроблокнотом на передачу в ключевом контейнере, т.е. в конструкции, обеспечивающей конфиденциальность и целостность. В общем случае конкретные примитивы, из которых формируется ключевой контейнер, должны выбираться для каждой сети КРК с учетом модели нарушителя и требуемых свойств безопасности, предъявляемых к создаваемым КЗК.

Способ **предварительного формирования ключей** перекодирования является вариантом решения проблемы появления передаваемой ключевой информации на промежуточных УКС в открытом виде. При применении одноразового шифроблокнота для кодирования общего секрета при передаче по цепочке УКС необходимо предварительно вычислить ключи перекодирования. В результате вместо последовательного раскодирования и кодирования в УКС производится одно преобразование и общий секрет не появляется в открытом виде. Однако в случае сетей КРК с топологией, отличной от топологии «магистраль», существенно вырастает количество квантовых ключей, которые необходимо предварительно выработать квантовой аппаратуре. Так как в случае соединения некоторого УКС с более чем двумя соседними УКС существует C_n^2 способов выбрать пару квантовых каналов для формирования суммарного ключа перекодирования. Т.е. вместо n квантовых ключей необходимо хранить C_n^2 уникальных пар.

Способ **распределения КЗК с применением коммутативных функций кодирования** также призван решить проблему появления передаваемых КЗК на промежуточных УКС в открытом виде. Способ основан на свойстве коммутативности применяемой функции кодирования по формуле (3):

$$X = \mathrm{D}_{K1}\big(\mathrm{E}_{K1}(X)\big) = \mathrm{D}_{K2}\big(\mathrm{E}_{K2}(X)\big) = \mathrm{D}_{K1}\left(\mathrm{D}_{K2}\left(\mathrm{E}_{K1}\big(\mathrm{E}_{K2}(X)\big)\right)\right) = \cdots, \qquad (3)$$

Где D_{Ki} – функция раскодирования на ключе Ki,
E_{Ki} – функция кодирования на ключе Ki,
Ki – используемый ключ кодирования,
X – сообщение.

При специальной структуре УКС и наличия свойства (3) на УКС сначала производится кодирование на квантовом ключе следующего сегмента, а затем раскодирование на квантовом ключе предыдущего сегмента. Применение способа показано на рисунке 5.

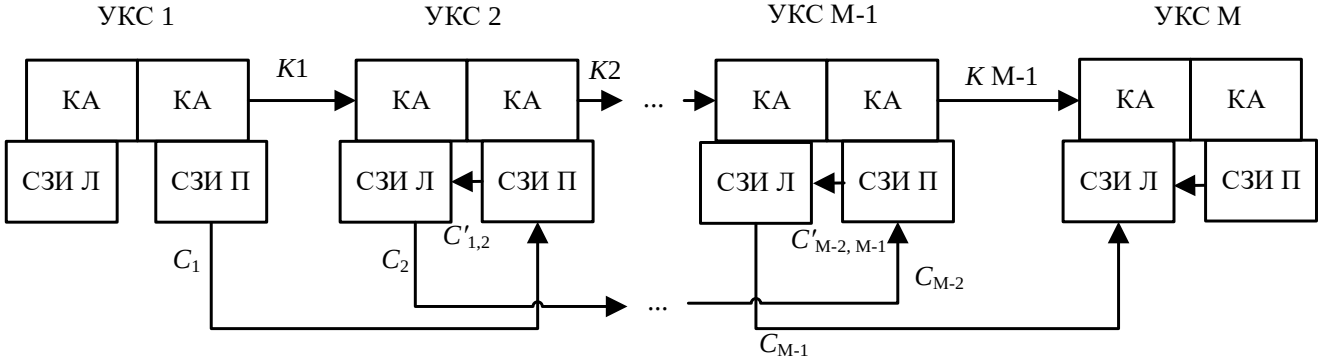

Рисунок 5 – Схема передачи ключа по цепочке УКС

На описываемый способ получен патент РФ № 2708511.

Способ **на основе схемы разделения секрета** предполагает разделение ключевых систем таким образом, чтобы при полном взломе защиты с применением одной ключевой системы, защита на второй ключевой системе сохранялась и обеспечивала достаточный уровень стойкости формируемых КЗК. В отличие от простого разделения секрета и передачи долей секрета с защитой на разных квантовых ключах в предлагаемом способе повышается безопасность КЗК, так как нарушителю необходимо осуществлять принципиально разные атаки: атаки на квантовую аппаратуру и протоколы КРК, а также атаки на вторую используемую ключевую систему, которая может быть реализована на предварительно распределенных ключах, на постквантовых алгоритмах или иных принципах, стойких к атакам нарушителя, обладающего квантовым компьютером.

Более того, схема разделения на независимые ключевые подсистемы может быть выполнена путем передачи разных частей КЗК полностью на ключах разных подсистем с последующим финальным смешиванием уже на целевых УКС.

В целях анализа будущих способов решения задачи распределения общего секрета на целевые УКС предложены **критерии классификации** таких способов.

Критерии классификации разделены на три группы:

– критерии, относящиеся к конструктивным особенностям, предъявляемым к системе;
– критерии, относящиеся к эксплуатационным свойствам способа;
– критерии, относящиеся к свойствам безопасности, достигаемым при применении способа.

По результатам анализа проведенной классификации разработанных способов выявлено, что способы, предъявляющие меньше требований к используемым примитивам, не предоставляют защиты передаваемых КЗК непосредственно на УКС и требуют повышенного доверия к УКС, что на

практике приводит к реализации дополнительных организационно-технических мер защиты и особых правил размещения и/или эксплуатации УКС. Если способ обеспечивает защиту передаваемых КЗК в том числе и при обработке на УКС, то появляются дополнительные ограничения к допустимым примитивам и ухудшаются эксплуатационные характеристики способа.

На основе разработанных способов распределения общего секрета синтезирована методика распределения КЗК, сочетающая основные преимущества разных способов, при этом позволяющая достичь следующих свойств:

– ни один из участников формирования КЗК не имеет возможность предсказать его значение до начала формирования;
– компрометация только квантовых ключей или только классических ключей не приводит к компрометации КЗК;
– промежуточные УКС не могут восстановить КЗК только с использованием передаваемой через них информации.

Методика распределения КЗК на магистральной линии из N УКС, целевыми из которых являются УКС 1 и УКС N, состоит в следующем.

Для распределения КЗК должны быть выполнены предусловия.

1. Между всеми парами соседних УКС в цепочке от УКС 1 до УКС N создано достаточное количество квантовых ключей. Достаточность определяется выбранными алгоритмами формирования ключевых контейнеров квантовой части КЗК.
2. На УКС 1 и УКС N загружен классический ключ для осуществления выбранного способа передачи классической части КЗК (далее ключей защиты КЗК).

Непосредственно методика распределения КЗК заключается в следующем.

1. Два целевых УКС формируют каждый по две части КЗК. Назовем их $Rand_{1,N}$ и $QRand_{1,N}$ для частей, формируемых УКС 1 в адрес УКС N и $Rand_{N,1}$ и $QRand_{N,1}$ для частей, формируемых УКС N в адрес УКС 1, соответственно.
2. УКС 1 передает часть КЗК $Rand_{1,N}$ с защитой на ключе защиты КЗК в адрес УКС N. УКС N передает часть КЗК $Rand_{N,1}$ с защитой на ключе защиты КЗК в адрес УКС 1. Передача осуществляется защищенным образом в ключевом контейнере с обеспечением конфиденциальности и целостности передаваемой ключевой информации, а также с обеспечением целостности необходимых дополнительных данных
3. УКС 1 передает часть КЗК $QRand_{1,N}$ с последовательным перекодированием по цепочке УКС с защитой на квантовых ключах соответствующих сегментов магистральной подсети КРК. Требования к защите передаваемой ключевой информации аналогичны шагу 2 описываемой методики. Передача части КЗК $QRand_{N,1}$ от УКС N до УКС 1 производится аналогично.

4. УКС 1 и УКС N получают полный комплект частей КЗК, который смешивают в КЗК с помощью некоторой функции. Назовем ее функцией гибридизации.

Предложенная методика 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».

В четвертой главе формулируются требования к структуре и функциям составных частей сети КРК смешанной топологии. Сеть КРК описывается в уровневой модели.

Предлагается трехуровневое деление сети КРК, включающее уровень выработки квантовых ключей, уровень выработки КЗК и уровень управления КЗК. Дополнительно для дальнейших пояснений введен уровень потребителей, представленный парами СЗИ-потребителей, в том числе не объединенных в единую сеть. Уровень потребителей является внешним по отношению к сети КРК.

Сеть КРК в виде совокупности уровней сети представлена на рисунке 6.

Уровень потребителей реализует запрос КЗК, возможно с указанием желаемых или требуемых параметров запрашиваемого ключа; получение КЗК согласно запросу; использование ключа согласно предписанию в устройствах этого уровня.

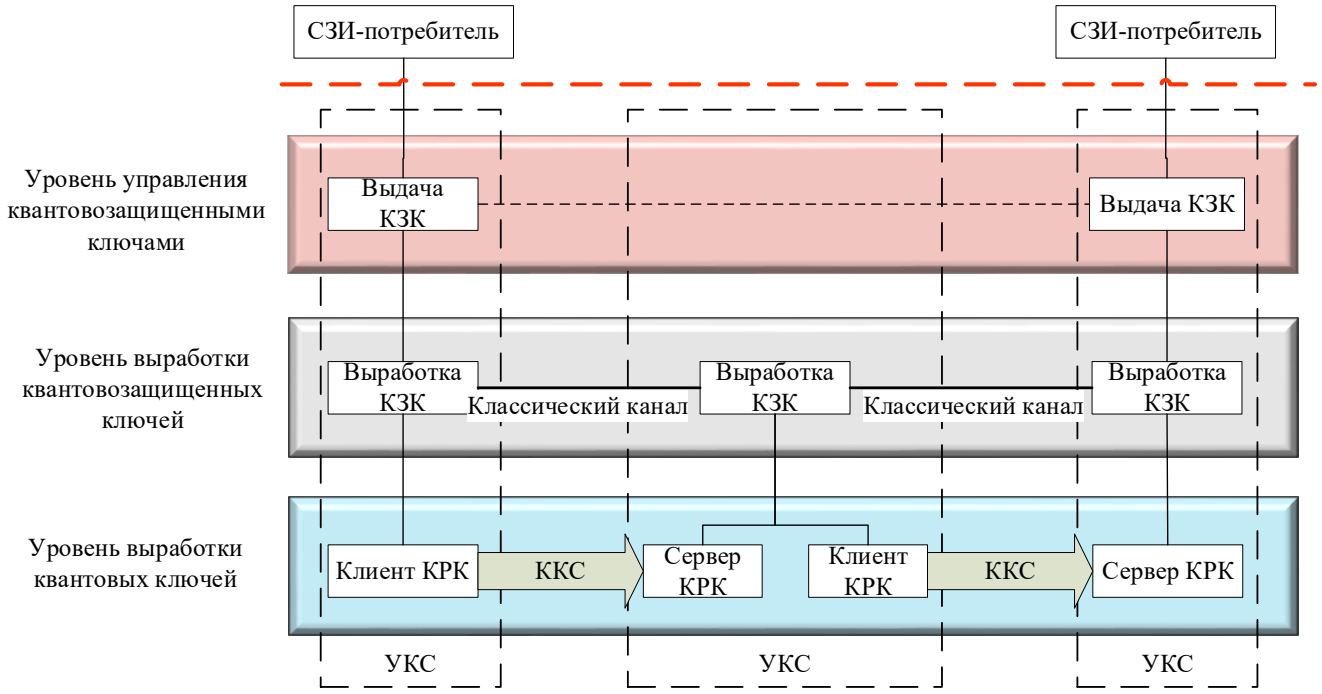

Рисунок 6 – Структура сети КРК (по уровням)

Уровень управления КЗК должен обладать следующими функциями:

– организация и синхронизация хранилищ КЗК;
– мониторинг запросов на КЗК (прогнозирование);
– обработка запросов КЗК от внешних СЗИ и передача КЗК в ответ;

– поддержание актуальной базы соответствия СЗИ-потребителей и УКС, к которым они подключены;
– формирование запросов КЗК к уровню выработки КЗК и получение КЗК в ответ;

Уровень выработки КЗК должен обладать следующими функциями:

– поддержание актуальной карты сети;
– построение оптимальных цепочек УКС для формирования КЗК;
– распределение КЗК на определенных цепочках УКС, в том числе организацию каналов с защитой на квантовых ключах;
– организация хранилищ квантовых ключей;
– построение аутентифицированного канала для уровня выработки квантовых ключей (опционально);
– организация запросов квантовых ключей к уровню выработки квантовых ключей и получение в ответ квантовых ключей;
– передача КЗК на уровень управления КЗК в ответ на запрос таких ключей.

Уровень выработки квантовых ключей должен обладать следующими функциями:

– выработка квантовых ключей;
– передача квантовых ключей на уровень выработки КЗК.

На основе разработанных требований к структуре сети КРК и методики распределения КЗК в сети магистральной топологии сформулирована методика построения сети КРК смешанной топологии. Графическое изображение методики в нотации IDEF0 приведено на рисунке 7

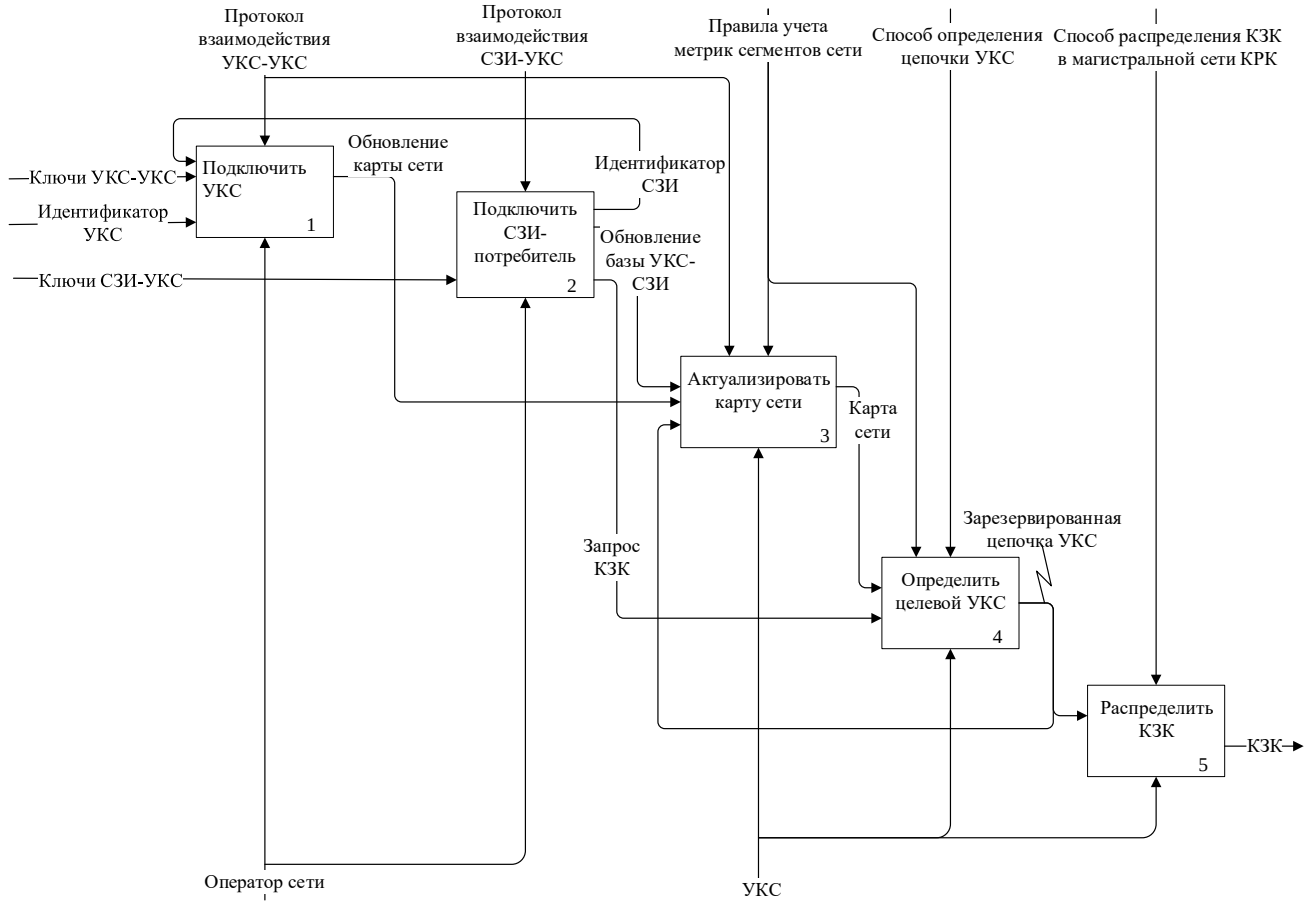

Рисунок 7 – Методика построения сети КРК

Сеть КРК строится из доверенных узлов, к каждому из которых могут подключаться внешние пользовательские устройства, СЗИ-потребители. Каждый УКС содержит не менее одного полукомплекта квантовой аппаратуры и соединен квантовым каналом связи не менее чем с одним соседним УКС. Граф связей квантовыми каналами сети КРК должен быть связным.

УКС должен содержать модули трех уровней, реализующие функции согласно сформулированным требованиям. Каждый УКС содержит один или более модулей выработки квантовых ключей, реализованных квантовой аппаратурой. На текущий момент из-за отсутствия единого полностью стандартизованного протокола КРК на двух концах каждого квантового канала должна располагаться аппаратура, реализованная одним производителем и выполняющая один протокол КРК. На каждом сегменте сети КРК возможно применение различной квантовой аппаратуры. Максимальная длина квантового канала каждого сегмента определяется предельными значениями потерь квантового канала, выбранного на этом сегменте протокола КРК.

Для начала работы сети КРК, а именно начала выработки квантовых ключей для дальнейшей возможности распределения КЗК, необходимо предварительно распределить требуемые наборы ключей, в частности для аутентификации классического канала квантовой аппаратуры, на пары соседних УКС, соединенных квантовым каналом.

Распределение КЗК между парами УКС осуществляется согласно сформулированной ранее методике распределения общего секрета в сети КРК магистральной топологии. Расчет магистральной подсети производится тем узлом, на который поступил запрос КЗК на основе актуальной карты сети КРК, включающей метрики сегментов сети. Для определения пар целевых УКС, на которые необходимо распределить КЗК в соответствии с запросом СЗИ-потребителя, необходимо поддерживать актуальную базу соответствия УКС и подключенных к ним СЗИ-потребителей для всей сети. При этом идентификация всех УКС в сети должна быть уникальной для однозначного определения целевых УКС.

Сеть КРК может строится итерационно, путем подключения новых УКС к существующей сети КРК.

Для подключения нового УКС к существующей сети КРК необходимо выполнить следующие условия.

– Соединить новый УКС с существующим квантовым каналом.
– Загрузить в существующий и новый УКС предварительно распределенные ключи для построения классического аутентифицированного канала квантовой аппаратуры в составе этой пары УКС. Предварительно распределяемые ключи могут создаваться с помощью датчика случайных чисел из состава УКС с последующей доставкой до нового УКС доверенным курьером. После успешного сеанса КРК с новым УКС данный УКС считается подключенным к сети КРК.

Таким образом, сформулированы требования к структуре сети КРК и функциям ее составных частей. На основе данных требований сформирована методика построения сетей КРК смешанной топологии, отличающаяся децентрализованным управлением и учетом требований целостности и конфиденциальности распределяемых КЗК.

В заключении приведены основные результаты и выводы по проделанной работе.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В работе выявлены и решены научные проблемы, препятствующие построению сетей КРК смешанной топологии. Разработано решение задачи сопряжения пары СЗИ с парой экземпляров квантовой аппаратуры для согласованной выработки общих секретов в простейшей сети «точка-точка». Такой комплекс устройств предложен в качестве базового элемента для построения сетей квантового распределения ключей смешанной топологии.

Выявлены научные проблемы, возникающие в сетях квантового распределения ключей простых топологий «магистраль» и «звезда». Введено понятие квантовозащищенного ключа (КЗК), соответствующее общему секрету, распределяемому между парами оконечных узлов магистральной сети КРК. Введение нового понятия позволяет различать квантовые ключи, создаваемые квантовой аппаратурой из состава сети КРК, и общие секреты, передаваемые

внешним парам внешних пользовательских устройств, распределенных без непосредственного использования принципов квантовой механики. Разработана методика распределения квантовозащищенных ключей для пар оконечных узлов сети КРК магистральной топологии. Данная методика решает существующую проблему появления в открытом виде передаваемых КЗК на промежуточных узлах. Решение для магистральной сети квантового распределения ключей предложено в качестве базовой логической единицы в сетях смешанной топологии. В результате внедрения методики распределения квантовозащищенных ключей сокращен процесс разработки проекта методических рекомендаций ТК26 на 30%.

Проведен анализ существующих мировых решений, касающихся структур, способов функционирования и сценариям применения сетей квантового распределения ключей. Выявлены недостатки рассмотренных решений. На основе проанализированных структур сетей, а также разработанных способа взаимодействия квантовой аппаратуры с СЗИ и методики распределения квантовозащищенных ключей сформулированы требования к структуре и функциям сети КРК смешанной топологии. В результате сформирована методика построения сетей КРК смешанной топологии.

Внедрение методики построения сетей КРК позволило сократить время развертывания Университетской квантовой сети на 20%, ускорило процесс эскизного проектирования аппаратуры сетей квантового распределения ключей с использованием доверенных узлов на 15% и позволило унифицировать аппаратную платформу доверенных узлов.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ РАБОТЫ

Статьи в ведущих рецензируемых журналах, рекомендованных Высшей аттестационной комиссией (ВАК) для публикации результатов кандидатских и докторских диссертационных работ:

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. Испытание комплекса квантовой криптографической аппаратуры защиты информации на городских волоконно-оптических линиях связи / А.В. Борисова, А.Е. Жиляев, С.В. Алферов, В.Л. Елисеев, Ю.В. Кармазиков, А.Н. Климов, К.А. Балыгин // Вестник российского нового университета. Серия: сложные системы: модели, анализ и управление. – 2019. – № 4. – С. 100–110.

3. 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.

4. Подход к формированию уровней доверия для оценки рисков ошибок аутентификации / А.Е. Жиляев, А.Г. Сабанов, П.А. Шелупанова, Д.С. Брагин,

А.А. Мицель, М.Ю. Катаев // Вопросы защиты информации. –2022. – № 1. – С. 17–22.

В изданиях WoS и Scopus:

5. Zhilyaev A.E. On the question of the authentication tag length based on reed-solomon codes / A.E. Zhilyaev, E.B. Gurova // Moscow Workshop on Electronic and Networking Technologies, MWENT 2018 - PROCEEDINGS. – 2018. –P. 1–5.

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

В других изданиях, сборниках трудов и тезисов конференций:

7. Жиляев А.Е. К вопросу об аутентификации классического канала в системах квантового распределения ключей // Безопасные информационные технологии : Сборник трудов Восьмой всероссийской научно-технической конференции. – Москва. – 2017. – С. 202–205.

8. Жиляев А.Е. Квантовое распределение ключей для защиты информации в городской сети банкоматов / А.Е. Жиляев, А.С. Николаева // Сборник научных работ участников ежегодной международной молодежной научно-практической конференции в рамках V Международного форума «Как попасть в пятерку?». Москва. – 2018. – С. 161–163.

Патенты на изобретения**:**

9. 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.

10. Пат. 2 736 870 РФ МПК H 04 L 9/08. Комплекс для защищенной передачи данных в цифровой сети передачи данных с использованием однопроходной системы квантового распределения ключей и способ согласования ключей при работе комплекса / А.Г. Втюрина, А.Е. Жиляев. – № 2019144324: заявл. 27.12.2019: опубл. 23.11.2020, Бюл. № 33. – 6 с.

11. Пат. 2 752 844 РФ, МПК H 04 L 9/08. Система выработки и распределения ключей и способ распределенной выработки ключей с использованием квантового распределения ключей (варианты) / А.Е. Жиляев. – № 2020140774: заявл. 10.12.2020: опубл. 11.08.2021, Бюл. №23. – 9 с.