УДК 004.72

РАЗРАБОТКА СТРУКТУРНОЙ СХЕМЫ КОМПЛЕКСА ТЕХНИЧЕСКИХ СРЕДСТВ УЗЛА ПРОГРАММНО-КОНФИГУРИРУЕМОЙ СЕТИ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Яшин Д.А. (Университет ИТМО)
Научный руководитель – Егоров В.И (Университет ИТМО)

Введение. В настоящее время активно ведется развитие квантовых сетей различного масштаба и топологий. Архитектура квантовых сетей включает в себя различное оборудование, такое как системы квантового распределения ключей (системы КРК), средства криптографической защиты информации (СКЗИ), а также вспомогательное сетевое оборудование, такое как сетевые и оптические коммутаторы и маршрутизаторы. На данный момент большинство параметров квантовых сетей устанавливаются при первичной настройке и остаются постоянными в процессе работы. Любые изменения требуют ручных действий со стороны администратора, что может стать проблемой при масштабировании сети и увеличении числа абонентов и участков сетей КРК. Исходя из этого, разработка эффективных систем управления сетями КРК, способных автоматизировать изменение параметров и устранять необходимость в ручных действиях, представляется ключевой задачей. При масштабировании технологии сетей КРК и увеличении количества участков и абонентов, автоматизированный подход к управлению становится тем более критически важным для обеспечения эффективности и масштабируемости сети, а также управления межвендорным взаимодействием.

Задача автоматизированного управления классической коммуникационной сетью решается переходом к парадигме программно-конфигурируемых сетей (далее – SDN, от англ. Software Defined Network). В связи с этим интеграция данной технологии в архитектуру сетей КРК является перспективным решением. В мировом научном сообществе тематика применения технологии SDN является широко распространенной и исследуемой, при этом основной импульс развития она получила в последние годы после выхода целой серии стандартов о применении данной технологии в рамках деятельности комитетов по стандартизации, входящих в состав Европейского института телекоммуникационных стандартов (ETSI) [1]. Особенностью данных стандартов является формирование общих архитектурных принципов и перспективности применения технологии SDN в задачах управления сетями КРК, однако конкретных решений по обеспечению жизненного цикла функций аппаратуры сетей КРК в данных стандартах не представлено. К перспективным работам можно отнести исследования научных групп из Китайской Народной Республики и Республики Корея, в которых развитие данной технологии осуществляется в тесной кооперации между научными исследовательскими группами, компаниями-производителями систем КРК и крупнейшими национальными телекоммуникационными операторами. В частности, среди ключевых научных центров развития данной технологии можно выделить лабораторию «Информационной фотоники и оптической связи» в Пекинском университете почты и телекоммуникаций [2], а также исследовательское подразделение компании SK Telekom [3, 4]. В Университете ИТМО также уже проводились предварительные научно-исследовательские работы, направленные на оценку возможности применения технологии SDN для задач управления сетями КРК на основе систем КРК на боковых частотах фазомодулированного излучения [5]. Однако данные исследования требуют дальнейшего развития, расширения и адаптации под современные принципы построения квантовых сетей и их архитектурные особенности, в том числе с учетом возможности использования произвольных систем КРК, помимо систем на боковых частотах.

Основная часть. В рамках данной работы разработана структурная схема комплекса технических средств узла программно-конфигурируемой сети КРК для решения задач управления сетью КРК в следующих сценариях, ранее не применимых в существующих решениях:

– управления коммутацией каналов в абонентской сети топологии «звезда» для поочередного соединения абонентских модулей системы КРК с модулем КРК, расположенным в центральном узле;
– оптимизации маршрутов распределения ключей при наличии в квантовой сети альтернативных маршрутов между целевыми узлами квантовой сети для распределения нагрузки на используемое оборудование;
– резервирования квантовых каналов при наличии аварийных ситуаций или вмешательстве злоумышленника в квантовый канал, в том числе при проведении атак на квантовую аппаратуру (системы КРК в целом или ее отдельные элементы);

На структурной схеме отображены необходимые функциональные блоки и раскрыты функциональные связи между блоками, входящими в состав узла программно-конфигурируемой сети КРК.

Выводы. Предлагаемый состав комплекса технических средств, описанный в данной работе, позволит эффективно воплотить все внутренние функциональные особенности узлов и взаимосвязи. Решение установленной проблемы позволит обеспечить независимое развитие различных сегментов квантовых сетей, которые будут интегрированы на едином уровне управления и предоставления итоговых сервисов с потенциалом дальнейшего масштабирования, не ограниченного возможностями по ручному администрированию сетей. Полученные результаты предполагают возможность их практической верификации в рамках взаимодействия с лидирующим исследовательским центром «Национальный центр квантового интернета» ИТМО, а также с производителями реальных систем КРК и сопряженных СКЗИ ООО «СМАРТС-Кванттелеком» и ООО «Амикон» в качестве разработчиков реальных архитектурных решений и средств, заинтересованных в интеграции результатов работы в свои решения.

Список использованных источников:

1. ETSI GS QKD 015 v 2.1.1 (2022-04) Quantum Key Distribution (QKD); Control Interface for Software Defined Networks
2. Cao Y. et al. SDQaaS: Software defined networking for quantum key distribution as a service //Optics express. – 2019. – Т. 27. – №. 5. – С. 6892-6909.
3. Cao Y. et al. Demonstration of SDN-Based Heterogeneous Quantum Key Distribution Chain Orchestration over Optical Networks //arXiv preprint arXiv:2209.09528. – 2022.
4. Sim D. H., Shin J., Kim M. H. Software-Defined Networking Orchestration for Interoperable Key Management of Quantum Key Distribution Networks //Entropy. – 2023. – Т. 25. – №. 6. – С. 943.
5. Chistyakov V. V. et al. Software-defined subcarrier wave quantum networking operated by OpenFlow protocol //arXiv preprint arXiv:1709.09081. – 2017.