15. *Pal'chevskiy E.V.* Prognozirovanie ugroz v slozhnykh raspredelennykh sistemakh na osnove intellektual'nogo analiza bol'shikh dannykh avtomatizirovannykh sredstv monitoringa [Forecasting threats in complex distributed systems based on intelligent analysis of big data of automated monitoring tools], *Programmnye produkty i sistemy* [Software Products and Systems], 2021, No. 2, pp. 230-236. Available at: https://swsys.ru/index.php?page=article&id=4811&ysclid=m8k65v2fsd994246327.
16. Informatsionnaya bezopasnost' i tsifrovaya transformatsiya. Bezopasnost' funktsionirovaniya informatsionnykh resursov. Otchet PAO «RusGidro» [Information security and digital transformation. Security of functioning of information resources. Report of PJSC RusHydro]. Available at:https://ar2023.rushydro.ru/strategic-review/information-security.html (accessed 24 March 2025).
17. Rol' bezopasnosti v tsifrovoy transformatsii biznesa [The role of security in digital business transformation]. Available at: https://infars.ru/blog/rol-bezopasnosti-v-tsifrovoy-transformatsii-biznesa/ (accessed 24 March 2025).
18. Tekhnologii informatsionnoy bezopasnosti, vazhnye dlya tsifrovoy transformatsii krupnogo biznesa [Information security technologies important for the digital transformation of large businesses]. Available at: https://www.nic.ru/help/tehnologii-informacionnoj-bezopasnosti-vazhnye-dlya-cifrovoj-transformacii-krupnogo-biznesa_14011.html.
19. *Lobkova E.V., Ki-Yuan A.A.* Tsifrovaya transformatsiya sistem obespecheniya bezopasnosti [Digital transformation of security systems], *Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski* [State and Municipal Administration. Scientific Notes], 2023, No. 2, pp. 115-127. Available at: https://doi.org/10.22394/2079-1690-2023-1-2-115-127.
20. Tsifrovaya transformatsiya, strategiya i protsessy IT [.Available at: https://kept.ru/services/tsifrovaya-transformatsiya-strategiya-i-protsessy-it [Digital transformation, strategy and IT processes] (accessed 24 March 2025).
21. Kiberbezopasnost' i tsifrovaya transformatsiya: 3 glavnykh tendentsii zashchity dannykh [Cybersecurity and digital transformation: 3 main trends in data protection]. Available at: https://cloudnetworks.ru/analitika/kiberbezopasnost-i-tsifrovaya-transformatsiya-3-glavnyh-tendentsii-zashhity-dannyh/ (accessed 24 March 2025).

Якименко Кирилл Викторович – Сибирский государственный университет науки и технологии имени академика М.Ф. Решетнева; e-mail: Yakimenko.KV@yandex.ru; г. Красноярск, Россия; аспирант; ORCID: 0009-0003-3374-1569.

Золотарев Вячеслав Владимирович – Сибирский государственный университет науки и технологии имени академика М.Ф. Решетнева; e-mail: zolotorev@mail.sibsau.ru; г. Красноярск, Россия; к.т.н.; зав. кафедрой безопасности информационных технологий; ORCID: 0000-0002-8054-8564.

Yakimenko Kirill Viktorovich – Reshetnev Siberian State University of Science and Technology; e-mail: Yakimenko.KV@yandex.ru; Krasnoyarsk, Russia; graduate student; ORCID: 0009-0003-3374-1569.

Zolotarev Vyacheslav Vladimirovich – Reshetnev Siberian State University of Science and Technology; e-mail: zolotorev@mail.sibsau.ru; Krasnoyarsk, Russia; cand. of eng. sc.; head of Information Technologies Security Department; ORCID: 0000-0002-8054-8564.

УДК 621.396.624 DOI 10.18522/2311-3103-2025-3-256-264

А.П. Плёнкин

ЭНЕРГЕТИЧЕСКАЯ МОДЕЛЬ МАГИСТРАЛЬНОЙ КВАНТОВОЙ СЕТИ

Уже сегодня в России и во всём мире активно разворачиваются и создаются сети квантовых коммуникаций, разрабатываются стандарты в области квантовых технологий. В рамках дорожной карты по развитию квантовых коммуникаций в России реализуется протяженность квантовых сетей более 7 тыс. км, а к 2030 году планируется более 15 тыс. км. Квантовые коммуникации сегодня – это, по сути, технология квантового распределения ключей, которая находятся на стадии интенсивного научного исследования и развития. Применительно к магистральным квантовым сетям технология распределения секретных ключей нуждается в новых подходах реализации, так как использование аппаратуры различных вендоров и протяженность волоконно-оптических линий связи накладывают преодолимые ограничения на топологии магистральных сетей. Немаловажным аспектом при проектировании квантовых сетей является расчет потерь в

оптических каналах связи. Затухания, вносимые различными пассивными и активными элементами, как правило, рассчитываются индивидуально для каждого участка сети и в итоге формируют комплексную энергетическую модель. В статье рассматривается несколько топологий магистральных квантовых сетей и приводится расчет оптических потерь для волоконно-оптического канала связи. В общем виде описан способ обнаружения оптического сигнала в сетях квантовых коммуникаций. Целью статьи является сравнительный анализ энергетических моделей топологий магистральных квантовых сетей и представление варианта реализации участка городской квантовой сети. В работе описывается применимость системы квантового распределения ключей, как в двухпроходном варианте исполнения, так и в однопроходной конфигурации. Приведены результаты анализа энергетической модели и расчет усредненных потерь в квантовом канале. В заключении мы предлагаем к рассмотрению возможный вариант топологии квантовой сети.

Квантовые коммуникации; квантовый ключ; фотонный импульс; вероятность обнаружения; доверенные узлы.

A.P. Pljonkin

ENERGY MODEL OF THE QUANTUM BACKBONE NETWORK

Already today, quantum communications networks are being actively deployed and created in Russia and around the world, and standards in the field of quantum technologies are being developed. As part of the roadmap for the development of quantum communications in Russia, the length of quantum networks is more than 7 thousand km, and by 2030 it is planned to be more than 15 thousand km. Quantum communications today are, in fact, a technology of quantum key distribution, which is at the stage of intensive scientific research and development. With regard to backbone quantum networks, the technology of secret key distribution requires new approaches to implementation, since the use of equipment from various vendors and the length of fiber-optic communication lines impose surmountable restrictions on the topology of backbone networks. An important aspect in the design of quantum networks is the calculation of losses in optical communication channels. Attenuations introduced by various passive and active elements are usually calculated individually for each section of the network and ultimately form a comprehensive energy model. The article considers several topologies of backbone quantum networks and presents the calculation of optical losses for fiber-optic communication channels of these topologies. In general, a method for detecting an optical signal in quantum communication networks is presented. The purpose of the article is a comparative analysis of energy models of backbone quantum networks and a presentation of a variant of implementing a section of an urban quantum network. The work describes a generalized principle of operation of a quantum key distribution system both in a two-pass version and in a single-pass configuration. The results of the analysis of the energy model and the calculation of average losses in a quantum channel are presented. In conclusion, we propose for consideration a possible variant of the topology of a quantum network.

Quantum communications; quantum key; photon pulse; detection probability; trusted nodes.

Введение. Квантовые коммуникации сегодня технически сводятся к квантовому распределению ключей [1, 2]. В простейшей конфигурации квантовое распределение представляет собой отправителя и получателя, которые обмениваются сигналами по оптическому каналу связи, соединяющему их. Такая простая топология именуется «точка-точка» и на практике является базовой топологией при конфигурации сложных сетей квантовых коммуникаций, включая магистральные сети. Известно, что топология «точка-точка» имеет ряд ограничений на использование в реальных условиях эксплуатации, например, максимальное расстояние передачи оптического сигнала, которое обусловлено особенностями распространения света в волокне и работой квантовых протоколов. Большинство протоколов квантового распределения ключей требуют использования оптических сигналов, ослабленных до уровня одного фотона или слабее – 0,1 фотона. Последнее означает, что в среднем каждый импульс света содержит 0,1 фотона. Это понятие используется в квантовой криптографии и указывает на то, что в среднем только один из десяти импульсов содержит фотон. Остальные девять импульсов не содержат фотонов. Это связано с вероятностной природой квантовой механики: фотоны в импульсе подчиняются статистике Пуассона. В квантовых сетях такие слабые сигналы используются для передачи квантовых состояний между узлами. Однако из-за затухания в оптических во-

локнах сигнал может становиться ещё слабее, что требует использования повторителей или других методов для увеличения дальности передачи. Использование повторителей или квантовой памяти при квантовом распределении ключей на сегодняшний день невозможно. Данные технологии в обозримом будущем не имеют перспектив достаточной степени реализации. Предел допустимого расстояния, на котором могут работать системы квантового распределения ключей в топологиях магистральных сетей требует наличия доверенных промежуточных узлов (ДПУ). Через ДПУ секретные ключи передаются по цепочке к нужным узлам сети [3]. В России также применяется подход с использованием ДПУ при построении квантовых сетей. Технически доверенный узел – это защищённое помещение, оснащённое оборудованием для квантовой криптографии. В последнее десятилетие активно исследуются методы квантового распределения ключей, которые основаны на перепутанных парах фотонов (TF QKD). Такая технология теоретически позволяет использовать конфигурацию сети с недоверенными промежуточными узлами (НПУ). В таких недоверенных узлах допускается, что злоумышленник обладает всей информацией о работе аппаратуры и имеет к ней доступ. Топология сети с НПУ представляет собой конфигурацию «точка-НПУ-точка». Квантовое распределение в такой сети реализуется по протоколу MDI (Measurement Device Independent) [4].

Обзор топологий магистральных квантовых сетей. Рассмотрим несколько примеров реализованных топологий квантовых сетей. В работе [5] продемонстрирована система квантового распределения ключей по оптическому кабелю в городской телекоммуникационной сети методом квантовой коммуникации на боковых частотах. Топология сети – «точка-точка». Длина линии ВОЛС составляла 1 км, собственные потери в ВОЛС – 1,63 дБ, марка волокна – SMF-28e. Оптическая синхронизация осуществлялась по отдельному волокну в том же кабеле. Для обмена данными по открытому каналу между станциями было установлено соединение по локальной сети. Ориентировочные суммарные потери с учетом вносимых элементами станций системы КРК затуханий составили ~ 50 дБ. В статье [6] предложена схема синхронизации квантовых часов для нескольких пользователей, которая реализована на основе источника запутанных фотонов. Сервер распределяет запутанные фотоны среди нескольких пользователей с помощью мультиплексирования. Разделение происходит по длине волны. Длина ВОЛС в эксперименте составила 75 км с собственными потерями 15 дБ. В работе не описывается энергетическая модель системы, но по составу элементов можно предположить, что суммарные потери составляют порядка 75 дБ. Статья [7] описывает систему квантового распределения ключей на основе квантовой запутанности. Источник запутанности расположен на расстоянии 32,6 км от одной станции и на расстоянии 15,2 км от другой. Результаты экспериментальных исследований показывают работу системы при потерях в 32 дБ и теоретические расчеты работы СКРК при потерях 48дБ. Исследование в [8] показывает работу системы КРК на базе протокола BB84 с предельными потерями 71,2 дБ. Отметим, что более детальная энергетическая модель или значения вносимых потерь отдельными элементами квантовой сети в статьях [7, 8] также не представлены.

Рассматривая магистральные квантовые сети с точки зрения оптических потерь, можно составить обобщенную энергетическую модель сети, основанную на сегментировании отдельных участков. В работах [9, 10] описаны основные топологии магистральных квантовых сетей и предложены способы распределения ключей, а в исследовании [11] рассматривается нестандартная топология сети и рассчитана ее энергетическая модель. На рис. 1 приведена модель магистральной квантовой сети, которая сочетает в себе несколько различных топологий. Особенностью такой структуры является возможность использования оборудования различных вендоров.

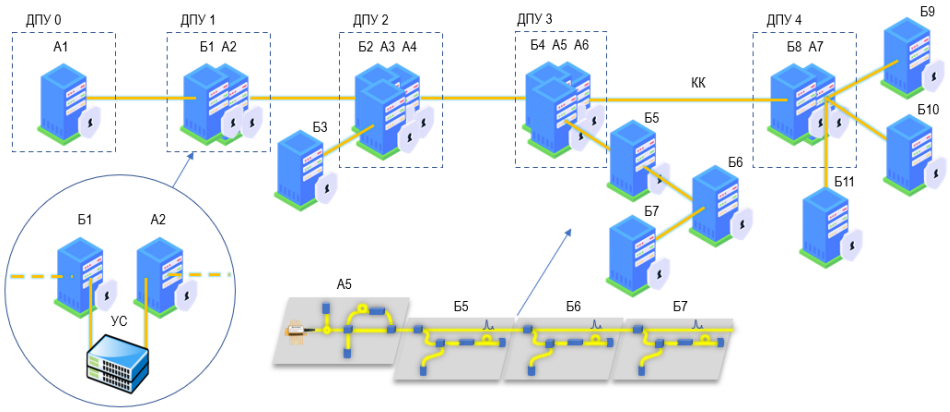

Рис. 1. Схема магистральной квантовой сети смешанной топологии

Предположим, что общая магистральная протяженность сети от ДПУ0 до ДПУ4 (рис. 1) составляет 200 км. Для удобства сеть разбита на равные по длине квантового канала сегменты (ДПУ0 – ДПУ1, ДПУ1 – ДПУ2, ДПУ2 – ДПУ3, ДПУ3 – ДПУ4), каждый из которых имеет конфигурацию «точка-точка». А – станция «Алиса», Б – станция «Боб». В каждом из доверенных промежуточных узлов станции КРК соединены физически с управляющим сервером (УС). *Напомним, что задача систем КРК заключается в выработке случайной последовательности, которую далее можно преобразовать в секретный ключ (с набором атрибутов)*. Обработкой последовательностей, формированием ключей и их использованием занимается управляющий сервер. Способы передачи секретного ключа от сегмента к сегменту описаны в [10–12]. Отметим, что подобная конфигурация сети позволяет использовать оборудование квантовой криптографии разных производителей. При рассмотрении сегмента сети с ДПУ2 видно, что узел содержит три станции СКРК, две из которых (Б2, А4) отвечают за взаимодействие с предшествующим и последующим сегментами магистральной сети. Предположим, что участок А3 – Б3 представляет собой «вертикальное» подключение к магистральной сети с длиной ВОЛС 30 км. На этом участке применяются системы КРК с односторонним квантовым протоколом [13]. Последнее означает, что Б3 содержит в своем составе лавинные фотодетекторы (ОЛФД) и при расчете потерь актуально учитывать распространение оптического сигнала только в одном направлении (от А3 к Б3). Для ДПУ2 также необходим УС, который будет взаимодействовать с тремя СКРК. В качестве УС может быть комплекс устройств, включающий, например, сервер взаимодействия с системой КРК, шифратор, коммутатор и т.д. Конфигурация участка с ДПУ3 показывает нестандартную топологию сети, в которой предполагается использование одной станции Алиса (А5) и нескольких станций Боб (Б5 – Б7). Особенностью схемы является то, что станции Боб соединены последовательно через волоконно-оптические ответвители [11]. На участке А5 – Б5 – Б6 – Б7 используется двухпроходная схема распространения оптического излучения. Это связано с тем, что станции Б5 – Б7 не содержат дорогостоящих ОЛФД, а удаленность станций позволяет использовать схему с автоматической компенсацией поляризационных (фазовых) искажений.

Рассмотрим более детально участок сети с ДПУ4 (рис. 2).

На данном сегменте предполагается использование нестандартной топологии, при которой конечными пользователями являются, как и в случае [11], устройства без ОЛФД. Отличительная особенность конфигурации заключается в наличии одной станции Алиса (А7) и нескольких систем КРК Боб (Б9 – Б11), соединенных параллельно друг другу через оптический разветвитель. Так как источник излучения и ОЛФД расположены в одной станции (А7), то возможно использование автокомпенсационного принципа с распространением оптического сигнала по одному волокну в двух направлениях. Расстояние от А7 до каждой станции Б примем равным 30 км.

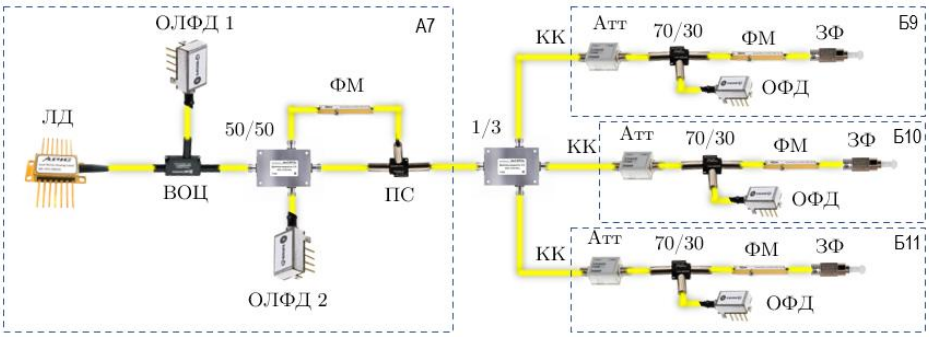

Рис. 2. Топология квантовой сети с разветвителем 1/3. ЛД – лазерный диод; ОЛФД – лавинный фотодиод; ПС – поляризационный сплиттер; КК – квантовый канал; Атт – аттенюатор управляемый

Анализ прохождения сигнала. Работа квантового протокола представляет собой одну из завершающих стадий в функционировании систем КРК, которые не могут работать без предварительных процедур настройки и синхронизации. Канал синхронизации (или калибровки) в некоторых случаях является отдельным волоконно-оптическим каналом, предназначенным для согласования и периодической настройки компонентов системы КРК. Квантовый канал и канал синхронизации могут быть объединены, то есть физически реализованы в одном оптическом волокне. В последнем случае все влияющие на оптическое волокно факторы будут одинаково отражаться как на работе квантового протокола, так и на процессе синхронизации. Общедоступный канал – это сеть передачи данных, используемая для процессов аутентификации, шифрования и дешифрования. Подавляющее большинство исследований сосредоточено на обеспечении защищенности квантовых протоколов, и лишь малая часть работ описывает процессы тактовой синхронизации. В исследовании [14] показано, что незащищенность синхронизации может быть потенциальным каналом несанкционированного доступа к системе КРК и злоумышленник, имея информацию о процессе синхронизации, может навредить работе системы. Обратимся к рис. 2. Оптический сигнал с длиной волны 1550 нм от источника излучения (ЛД) поступает на циркулятор (ВОЦ), где полностью перенаправляется против часовой стрелки на светоделитель (50/50). Далее равными долями сигнал распределяется в плечи интерферометра Маха-Цендера. В процессе синхронизации часть элементов схемы КРК не функционируют и не влияют на процесс, поэтому мы не будем акцентировать на них внимание. После интерферометра сигнал в одном волокне поступает на светоделитель 1/3. Конструктивно удобнее интегрировать светоделитель в станцию А7 или сразу после нее (в пределах ДПУ). Далее сигнал распространяется по параллельным квантовым каналам (КК) на станции Б. В каждой станции на светоделителе (70/30) сигнал поступает на фотодетектор (ОФД) и распространяется к зеркалу Фарадея (ЗФ) через фазовый модулятор (ФМ). Классический фотодетектор выполняет функцию регистрации момента поступления импульсов и фиксирует точные временные отрезки времени. Эта информация в последствии используется, например, для прикладывания напряжения к фазовому модулятору в определенный момент времени. Отраженный от ЗФ сигнал следует в обратном направлении по тому же оптическому пути к станции А7, где регистрируется ОЛФД. Мы не фокусируем внимание на способе кодирования, так как для синхронизации это не имеет значения. Отметим, что в подобных двухпроходных схемах можно использовать как поляризационное, так и фазовое кодирование состояний фотонов. Технически обнаружение синхросигнала выполняется путем последовательного анализа временных интервалов, которые измеряются в наносекундах и пикосекундах [15, 16]. Отправляя сигналы синхронизации с частотой, например, 800 Гц, и фиксируя отраженные сигналы, станция Алиса будет знать, в какой момент времени необходимо активировать ОЛФД для каждой станции Б. Исследуемая топология предполагает наличие трех параллельно со-

единенных станций Б. Последнее может вызывать следующие вопросы при физической реализации: *какова вероятность события, когда отраженные от станций Б импульсы поступят на ОЛФД А7 в один момент времени?* Предположим, что расстояние от ЛД до ЗФ у двух станций одинаковое с точностью (во временном выражении) до 1 нс. Тогда на разветвителе 1/3 при обратном распространении произойдет интерференция излучения и электроника А7 не сможет различить принадлежность сигнала к определенной станции. На практике вероятность такого события стремится к нулю, так как длительность оптического импульса в процессе калибровки составляет 1 нс, что соответствует в выражении расстояния 20 сантиметрам оптического волокна (с учетом коэффициента преломления). Кроме того, ситуацию с абсолютно равной длиной КК можно исключить путем измерения длины ВОЛС при помощи, например, оптического рефлектометра.

Нужно ли станции А7 идентифицировать станции Б, т.е. в процессе синхронизации станция А7 должна знать, какой отраженный импульс следует от какой станции Б? С одной стороны, эта задача решается классическими способами, применяемыми в топологии «точка-точка». Но рассмотрим иную сторону вопроса. При работе квантового протокола, несомненно, станции должны быть идентифицированы и аутентификация должна осуществляться до квантового распределения. Задачей синхронизации является обнаружение точных моментов регистрации импульсов в станциях А7, Б9 – Б11. Для А7 – это момент подачи напряжения на ОЛФД для активации однофотонного режима, а для станций Б – это тактовый счетчик импульсов и момент подачи напряжения, например, на фазовый модулятор. *Последнее позволяет выдвинуть гипотезу о том, что процесс синхронизации в схеме с несколькими параллельными станциями Б не нуждается в предварительной идентификации станций.* Еще один инженерный вопрос, который может возникнуть при реализации схемы: *какова вероятность того, что отраженный импульс встретится с вновь испускаемым импульсом?* Вероятность этого события исключается достаточно тривиальным способом: в реализованных системах КРК интервал между тактовыми импульсами составляет более 1 мс, что вдвое превышает предельно допустимое рабочее расстояние, даже с учетом обратного пути следования.

Отметим, что мы описываем задачу обнаружения оптического сигнала в конфигурации, когда отраженный сигнал с вероятностью 100% поступит на фотодетектор. Смешанная топология магистральной квантовой сети может содержать оборудование КРК, которое функционирует по односторонней схеме. В таком случае задача синхронизации сохраняется и, более того, алгоритм обнаружения оптического сигнала практически не изменяется. В схеме, когда квантовое распределение функционирует по одностороннему протоколу, ОЛФД расположены в удаленной станции. Обнаружение оптического синхросигнала в двухпроходной и односторонней схемах осуществляется последовательным анализом временных интервалов. В открытых источниках встречается несколько вариантов реализации пошагового поиска сигнала [15–21].

Энергетическая модель сети. Проведем усредненный анализ потерь оптического сигнала для непрерывной магистральной сети (рис. 1). Принимаем потери на сварных соединениях *(lw) = 0.03 дБ,* собственные потери в КК для одномодового волокна *(lk)* и потери на разъемных соединениях *(lf)* принимаем равными *0.2 дБ/км.* При физической реализации квантового канала схема соединения оборудования для сегментов будет выглядеть следующим образом: оптическая розетка станции соединена патч-кордом с оптическим кроссом; кросс соединен с переходной муфтой сварным соединением; далее, с учетом строительной длины кабеля, расположены проходные муфты; вводная муфта соединена с оптическим кроссом, который патч-кордом связан с розеткой станции. Отметим, что данная конфигурация является обобщенной, но в тоже время она применима к большинству топологий оптических сетей.

Суммарные потери в сегментах рассчитаем по формулам:

$$L_{\text{а1б1}} = 0.2\ (lf) * 4 + 0.03(lw) * 14 + 0.2(lk) * 50 = 11.22 \text{ дБ}.$$

$$L_{\text{а3б3}} = 0.2(lf) * 4 + 0.03(lw) * 10 + 0.2(lk) * 30 = 7.1 \text{ дБ}.$$

$$L_{\text{а5б7}} = 0.2(lf) * 8 + 0.03(lw) * 61 + 0.2(lk) * 45 = 12.43 \text{ дБ}.$$

Строительную длину кабеля ВОЛС принимаем равной 1 км. Расстояние в сегменте ДПУ3 на участках А5 – Б5, Б5 – Б6, Б6 – Б7 составляет по 15 км. Так как длина КК между сегментами ДПУ0 – ДПУ1, ДПУ1 – ДПУ2, ДПУ2 – ДПУ3, ДПУ3 – ДПУ4 одинаковая, то расчет потерь $L_{\text{а1б1}}$ справедлив и для остальных сегментов, а $L_{\text{а3б3}} = L_{\text{а7б9}} = L_{\text{а7б10}} = L_{\text{а7б11}}$ (за исключением делителя оптической мощности 1/3, вносимые затухания которого в данном случае можно отнести к погрешности). Отметим, что для всех сегментов сети, кроме А3 – Б3 необходимо учитывать обратное распространение сигнала, следовательно, потери будут вдвое больше.

Выводы и дискуссия. В исследовании рассмотрена магистральная квантовая сеть, состоящая из нескольких нестандартных топологий. Проведен расчет потерь для оптической части непрерывной квантовой сети. В общем виде описан способ обнаружения оптического сигнала в сетях квантовых коммуникаций и принцип функционирования системы квантового распределения ключей, как в двухпроходном варианте исполнения, так и в однопроходной конфигурации. Предложена модель нестандартной топологии абонентской квантовой сети, в которой одна станция Алиса взаимодействует с тремя параллельно соединенными станциями Боб. Для описанной топологии предлагается двухпроходная схема работы, когда источник излучения и ОЛФД расположены в станции Алиса.

Переходя к дискуссии, можно акцентировать внимание на нескольких актуальных проблемах по мнению автора при технической реализации квантовых сетей смешанной топологии: *защищенность каналов аутентификации* (как обеспечить безусловную защищенность процесса предварительной аутентификации удаленных станций и возможно ли это осуществить без использования классической криптографии? *Возможна ли физическая реализация предложенных в статье топологий и будет ли это эффективным решением для частных случаев?* (как в этом случае можно реализовать распределение квантовых ключей на различных принципах и протоколах – перепутанных парах фотонов, боковых частотах?). *Если злоумышленник имеет доступ к процессу тактовой синхронизации и аутентификации, то как это отражается на комплексной защищенности сети?*

Автор статьи благодарен читателю и приглашает дать обратную связь по приведенным вопросам.

Исследование выполнено за счет гранта Российского научного фонда № 25-29-00007, https://rscf.ru/project/25-29-00007/.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145-195.
2. *Bennett C.H., Brassard G., & Ekert A.K.* Quantum Cryptography // Scientific American. – 1992. – 267 (4). – P. 50-57. – http://www.jstor.org/stable/24939253.
3. *Chen Y. . et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. – 2021. – Vol. 589, No. 7841. – P. 214-219.
4. *Кулик С.П., Молотков С.Н.* MDI–Measurement Device Independent квантового распределения ключей // Письма в Журнал экспериментальной и теоретической физики. – 2023. – Т. 118, № 1. – С. 62-70.
5. *Gleĭm A.V., Chistyakov V.V., Bannik O.I. [et al.].* Sideband quantum communication at 1 Mbit/s on a metropolitan area network // Journal of Optical Technology. – 2017. – Vol. 84, No. 6. – P. 362-367.
6. *Tang B.Y. et al.* Demonstration of 75 km-fiber quantum clock synchronization in quantum entanglement distribution network // EPJ Quantum Technology. – 2023. – Vol. 10, No. 1. – P. 1-10.
7. *Pelet Y. et al.* Entanglement-based clock syntonization for quantum key distribution networks. Demonstration over a 50 km-long link // arXiv preprint arXiv:2501.16796. – 2025.
8. *Krause J. et al.* Clock offset recovery with sublinear complexity enables synchronization on low-level hardware for quantum key distribution // arXiv preprint arXiv:2404.04081. – 2024.
9. *Пленкин А.П.* Обзор топологий сетей квантовых коммуникаций // Инженерный вестник Дона. – 2024. – № 9 (117). – С. 87-97.
10. *Сабанов А.Г., Шелупанов А.А.* Идентификация и аутентификация в цифровом мире. – М.: Горячая Линия–Телеком, 2022.

11. *Пленкин А.П.* Способ обнаружения оптического сигнала в квантовых сетях // Известия ЮФУ. Технические науки. – 2024. – № 5 (241). – С. 254-260.
12. *Поздняков А.М.* Способ передачи сообщения через вычислительную сеть с применением аппаратуры квантового распределения ключей. – 2019.
13. *Кравцов К.С. и др.* Система релятивистской квантовой криптографии. – 2018.
14. *Pljonkin A., Petrov D., Sabantina L., Dakhkilgova K.* Nonclassical attack on a quantum keydistribution system // Entropy. – 2021. – Vol. 23, No. 5.
15. *Pljonkin A., Rumyantsev K., Kumar Singh P.* Synchronization in quantum key distribution systems // Cryptography. – 2017. – Vol. 1, No. 3. – P. 18.
16. *Гальярди Р.М., Карп Ш.* Оптическая связь: пер. с англ. / под ред. А.Г. Шереметьева. – М.: Связь, 1978. – 424 с.
17. *Румянцев К.Е., Рудинский Е.А.* Двухэтапный временной алгоритм синхронизации в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Известия ЮФУ. Технические науки. – 2017. – № 5 (190). – С. 75-89.
18. *Прудников В., Плёнкин А., Юшицына В.* Квантово-криптографические сети. – Litres, 2024.
19. *Румянцев К.Е., Миронов Я.К., Миронова П.Д.* Сравнительный анализ временных характеристик алгоритмов обнаружения синхроимпульса в системе квантового распределения ключа // IV Всероссийская научно-практическая конференция "Digital Era", Грозный, 01 марта 2024 года. – Грозный: Чеченский государственный университет имени Ахмата Абдулхамидовича Кадырова, 2024. – С. 139-141.
20. *Миллер А.В.* Синхронизация времени в спутниковом квантовом распределении ключей // Проблемы передачи информации. – 2023. – Т. 59, №. 4. – С. 13-27.
21. *Андреев С.А., Свистунова А.И.* Системы синхронизации для квантового канала связи в открытом пространстве // Наука, техника, педагогика в высшей школе: Матер. Всероссийской научно-практической конференции, Москва, 20–27 февраля 2023 года. – М.: Московский Политех, 2023. – С. 398-404.

REFERENCES

1. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography, *Reviews of Modern Physics,* 2002, Vol. 74, No. 1, pp. 145-195.
2. *Bennett C.H., Brassard G., & Ekert A.K*. Quantum Cryptography, *Scientific American,* 1992, 267 (4), pp. 50-57. Available at: http://www.jstor.org/stable/24939253.
3. *Chen Y.A. et al.* An integrated space-to-ground quantum communication network over 4,600 kilometres, *Nature,* 2021, Vol. 589, No. 7841, pp. 214-219.
4. *Kulik S.P., Molotkov S.N.* MDI–Measurement Device Independent kvantovogo raspredeleniya klyuchey [MDI–Measurement Device Independent of Quantum Key Distribution], *Pis'ma v Zhurnal eksperimental'noy i teoreticheskoy fiziki* [Letters to the Journal of Experimental and Theoretical Physics], 2023, Vol. 118, No. 1, pp. 62-70.
5. *Gleĭm A.V., Chistyakov V.V., Bannik O.I. [et al.].* Sideband quantum communication at 1 Mbit/s on a metropolitan area network, *Journal of Optical Technology,* 2017, Vol. 84, No. 6, pp. 362-367.
6. *Tang B.Y. et al.* Demonstration of 75 km-fiber quantum clock synchronization in quantum entanglement distribution network, *EPJ Quantum Technology,* 2023, Vol. 10, No. 1, pp. 1-10.
7. *Pelet Y. et al.* Entanglement-based clock syntonization for quantum key distribution networks. Demonstration over a 50 km-long link, *arXiv preprint arXiv:2501.16796,* 2025.
8. *Krause J. et al.* Clock offset recovery with sublinear complexity enables synchronization on low-level hardware for quantum key distribution, *arXiv preprint arXiv:2404.04081,* 2024.
9. *Plenkin A.P.* Obzor topologiy setey kvantovykh kommunikatsiy [Review of quantum communications network topologies], *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don], 2024, No. 9 (117), pp. 87-97.
10. *Sabanov A.G., SHelupanov A.A.* Identifikatsiya i autentifikatsiya v tsifrovom mire [Identification and authentication in the digital world]. Moscow: Gorya-chaya Liniya–Telekom, 2022.
11. *Plenkin A.P.* Sposob obnaruzheniya opticheskogo signala v kvantovykh setyakh [Method for detecting an optical signal in quantum networks], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2024, No. 5 (241), pp. 254-260.
12. *Pozdnyakov A.M.* Sposob peredachi soobshcheniya cherez vychislitel'nuyu set' s primeneniem apparatury kvantovogo raspredeleniya klyuchey [Method for transmitting a message through a computer network using quantum key distribution equipment], 2019.
13. *Kravtsov K.S. i dr.* Sistema relyativistskoy kvantovoy kriptografii [Relativistic quantum cryptography system], 2018.

14. *Pljonkin A., Petrov D., Sabantina L., Dakhkilgova K.* Nonclassical attack on a quantum keydistribution system, *Entropy,* 2021, Vol. 23, No. 5.
15. *Pljonkin A., Rumyantsev K., Kumar Singh P.* Synchronization in quantum key distribution systems, *Cryptography,* 2017, Vol. 1, No. 3, pp. 18.
16. *Gal'yardi R.M., Karp Sh.* Opticheskaya svyaz' [Optical communications]: trans. from engl, ed. by A.G. Sheremet'eva. Moscow: Svyaz', 1978, 424 p.
17. *Rumyantsev K.E., Rudinskiy E.A.* Dvukhetapnyy vremennoy algoritm sinkhronizatsii v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoy kompensatsiey polyarizatsionnykh iskazheniy [Two-stage time synchronization algorithm in a quantum key distribution system with automatic compensation of polarization distortions], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2017, No. 5 (190), pp. 75-89.
18. *Prudnikov V., Plenkin A., Yushitsyna V.* Kvantovo-kriptograficheskie seti [Quantum cryptographic networks], Litres, 2024.
19. *Rumyantsev K.E., Mironov Ya.K., Mironova P.D.* Sravnitel'nyy analiz vremennykh kharakteristik algoritmov obnaruzheniya sinkhroimpul'sa v sisteme kvantovogo raspredeleniya klyucha [Comparative analysis of temporal characteristics of sync pulse detection algorithms in a quantum key distribution system], *IV Vserossiyskaya nauchno-prakticheskaya konferentsiya "Digital Era", Groznyy, 01 marta 2024 goda* [IV All-Russian scientific and practical conference "Digital Era", Grozny, March 01, 2024]. Groznyy: Chechenskiy gosudarstvennyy universitet imeni Akhmata Abdulkhamidovicha Kadyrova, 2024, pp. 139-141.
20. *Miller A.V.* Sinkhronizatsiya vremeni v sputnikovom kvantovom raspredelenii klyuchey [Time synchronization in satellite quantum key distribution], *Problemy peredachi informatsii* [Problems of Information Transmission], 2023, Vol. 59, No. 4, pp. 13-27.
21. *Andreev S.A., Svistunova A.I.* Sistemy sinkhronizatsii dlya kvantovogo kanala svyazi v otkrytom prostranstve [Synchronization systems for a quantum communication channel in open space], *Nauka, tekhnika, pedagogika v vysshey shkole: Materialy Vserossiyskoy nauchno-prakticheskoy konferentsii, Moskva, 20–27 fevralya 2023 goda* [Science, technology, pedagogy in higher education: Proceedings of the All-Russian scientific and practical conference, Moscow, February 20-27, 2023]. Moscow: Moskovskiy Politekh, 2023, pp. 398-404.

Плёнкин Антон Павлович – Южный федеральный университет; e-mail: pljonkin@sfedu.ru; г. Таганрог, Россия; тел.: 89054592158; кафедра ИБТКС; к.т.н.; доцент.

Pljonkin Anton Pavlovich – Southern Federal University; e-mail: pljonkin@sfedu.ru; Taganrog, Russia; phone: +79054592158; the Department of Information Security of Telecommunication Systems; cand. of eng. sc.; associate professor.

УДК 004.089 DOI 10.18522/2311-3103-2025-3-264-273

П.Д. Борисов, Ю.В. Косолапов

О ФУНКЦИИ ПОХОЖЕСТИ ГРАФИЧЕСКИХ ПРЕДСТАВЛЕНИЙ ИСПОЛНЯЕМЫХ ФАЙЛОВ В МОДЕЛИ ОЦЕНКИ ОБФУСЦИРУЮЩИХ ПРЕОБРАЗОВАНИЙ

Обфускация программного кода используется с целью затруднения его анализа в модели, когда аналитик имеет полный доступ к программе. Обычно обфускация делится на криптографически стойкую и эвристически стойкую. В первом случае сложность анализа сопоставима с трудностью решения некоторой известной математической задачи. Во втором случае стойкость обосновывается, как правило, отсутствием известных на момент создания метода обфускации эффективных техник ее анализа. Криптографически стойкая обфускация пока не нашла применения на практике, в то время как эвристически стойкая широко применяется. Ранее авторами была предложена модель оценки эффективности и стойкости эвристических обфусцирующих преобразований, в основе которой лежит применение функции похожести. В настоящей работе с помощью методов машинного обучения строится такая функция похожести на основе сравнения графического представления исполняемых файлов программ. В частности, сравнение выполняется с помощью сверточной сети с четырьмя сверточными слоями, оптимизатором RMSprop, функцией потерь NLLLoss и двумя выходами полносвязного слоя. Предложенная функция применяется в