ДОКЛАД ЭКСПЕРТА

МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МОСКОВСКАЯ МЕЖДУНАРОДНАЯ МОДЕЛЬ ООН ИМ. В.И. ЧУРКИНА

СОДЕЙСТВИЕ ВНЕДРЕНИЮ КВАНТОВОЙ КРИПТОГРАФИИ ДЛЯ ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ ГЛОБАЛЬНЫХ СЕТЕЙ СВЯЗИ И ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....4

ГЛАВА 1. КИБЕРУГРОЗЫ И УЯЗВИМОСТИ ГЛОБАЛЬНЫХ СЕТЕЙ СВЯЗИ.....5
1.1. Информационная безопасность и виды киберугроз.....5
1.2. Уязвимости беспроводных каналов связи и трансграничного трафика.....7

ГЛАВА 2. КВАНТОВАЯ КРИПТОГРАФИЯ И ЕЕ ОСНОВЫ.....8
2.1. Введение в теорию криптографии.....8
2.2. Квантовая криптография: основы и протокол BB84.....9
2.3. Альтернативные протоколы: B92, E91, MDI-QKD, Twin-Field QKD.....13
2.4. Постквантовая криптография.....16

ГЛАВА 3. ТЕХНОЛОГИИ И АРХИТЕКТУРА КВАНТОВОЙ КРИПТОГРАФИИ.....18
3.1. Архитектура квантовой криптографии.....18
3.2. Преимущества квантовой криптографии.....20
3.3. Ограничения и недостатки.....21
3.4. Экономика и масштабирование квантовой криптографии.....22
3.5. Современные мировые технологии и международное сотрудничество.....24
3.5.1. Китайская Народная Республика.....24
3.5.2. Европейский союз.....25
3.5.3. Япония.....26
3.5.4. Соединенные Штаты Америки.....27
3.5.5. Россия.....28

ГЛАВА 4. РОЛЬ МЕЖДУНАРОДНОГО СОЮЗА ЭЛЕКТРОСВЯЗИ (МСЭ) В ПОДДЕРЖКЕ РАЗВИТИЯ КВАНТОВОЙ КРИПТОГРАФИИ.....30
4.1. История и структура Международного союза электросвязи.....30
4.2. Инструменты МСЭ.....32
4.3. Примеры внедрения рекомендаций МСЭ.....33

ЗАКЛЮЧЕНИЕ.....35
ГЛОССАРИЙ.....37

ВВЕДЕНИЕ

На сегодняшний день вопрос защиты информации является особенно актуальным ввиду практически полного перехода к цифровым технологиям и созданию интернета вещей. Основные методы шифрования, используемые в настоящее время, базируются на одном очень уязвимом допущении – вся защищенность (секретность) этих методов опирается на сложности вычислительных алгоритмов, используемых для дешифровки сообщения, или ограниченной вычислительной мощности злоумышленника. Это касается как симметричного шифрования (например, AES, DES), так и асимметричного шифрования (например, RSA). Фундаментальной задачей в области шифрования является необходимость распределения ключей. Именно в этом заключается основное отличие методов шифрования.

Криптография как наука о защите информации с помощью математических методов и алгоритмов является основой современной безопасности коммуникаций и хранения данных. Развитие вычислительных технологий, в том числе появление квантовых компьютеров, создает новые вызовы для существующих криптографических систем. В частности, достаточно мощные квантовые компьютеры потенциально способны взламывать некоторые широко используемые криптографические алгоритмы значительно эффективнее классических вычислительных систем. Это формирует потребность в инновационных подходах к защите информации, устойчивых к квантовым угрозам. Одним из таких подходов является квантовая криптография, использующая свойства квантовых состояний для повышения защищенности передачи данных.

Квантовая криптография возникла как ответ на эту угрозу и представляет собой новый подход к обеспечению безопасности данных. В отличие от классической криптографии, которая использует сложные математические функции для шифрования информации, квантовая криптография использует явления квантовой механики, такие как квантовая запутанность и квантовая суперпозиция, для создания защищенных ключей и обеспечения непрерывной, контролируемой защиты информации.

ГЛАВА 1. КИБЕРУГРОЗЫ И УЯЗВИМОСТИ ГЛОБАЛЬНЫХ СЕТЕЙ СВЯЗИ

1.1. Информационная безопасность и виды киберугроз

Год за годом в мире становится все больше угроз и происходит все больше утечек данных. Статистика шокирует: согласно отчету RiskBased Security, только за первые девять месяцев 2019 года было зафиксировано 7,9 миллиарда случаев утечки данных. Эти цифры превышают показатели за тот же период 2018 года более чем в два раза.

Чаще всего утечке данных подвергаются медицинские и государственные учреждения или организации из сферы розничной торговли. В большинстве случаев причина – действия преступников. Некоторые организации привлекают злоумышленников, так как у них обладают финансовыми и медицинскими данными. Мишенью может стать любая компания, ведь преступники могут охотиться за данными клиентов, шпионить или готовить атаку на одного из клиентов.

Очевидно, что масштаб киберугроз будет расширяться, следовательно, глобальные расходы на решения по кибербезопасности будут увеличиваться. По прогнозам Gartner, в целом расходы на информационную безопасность в мире достигли $188,3 млрд в 2023 году, а к 2026 году превысят $260 млрд. Правительства разных стран борются с преступниками, помогая организациям внедрять эффективные методы кибербезопасности.

Национальный институт стандартов и технологий США (NIST) разработал принципы безопасной ИТ-инфраструктуры. NIST рекомендует проводить постоянный мониторинг всех электронных ресурсов в реальном времени, чтобы выявить вредоносный код, пока он не нанес вреда, и предотвратить его распространение.

Национальный центр кибербезопасности правительства Великобритании выпустил руководство «10 шагов к кибербезопасности». В нем говорится о том, насколько важно вести наблюдение за работой систем. В Австралии рекомендации по борьбе с новейшими киберугрозами регулярно публикует Австралийский центр кибербезопасности.[1]

---

1 Что такое кибербезопасность? : [Электронный ресурс] // Kaspersky : официальный сайт. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security (дата обращения: 10.09.2026)

Под киберугрозами понимают любые потенциальные опасности, которые нацелены на то, чтобы нарушить конфиденциальность, целостность или доступность информационных систем, сетей и информации.[2]

Киберугрозы делятся на несколько категорий. По источнику: внутренние (инсайдерские) и внешние. Инсайдерские исходят от сотрудников, подрядчиков или партнеров, у которых уже есть легальный доступ к системам компании. Это могут быть как умышленные действия, так и случайные ошибки (например, отправка конфиденциального файла не тому адресату). Внешние инициируются злоумышленниками, у которых нет прав доступа. Сюда относятся атаки хакеров, попытки взлома, фишинг и другие методы.

Информационная безопасность борется с тремя видами угроз: **киберпреступление** – действия, организованные одним или несколькими злоумышленниками с целью атаковать систему нарушить ее работу или извлечь финансовую выгоду; **кибератака** – действия, нацеленные на сбор информации, в основном политического характера; **кибертерроризм** – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

В связи с этим нельзя не упомянуть основные виды кибератак:

- **SQL-инъекции** – этот вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL).
- **Фишинг** – атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.
- **Атака Man-in-the-Middle («человек посередине»)** – это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают. Такой атаке можно подвергнуться, если, например, подключитесь к незащищенной сети Wi-Fi.
- **DoS-атаки (атаки типа «отказ в обслуживании»)** – киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так злоумышленники, например, могут повредить важные компоненты инфраструктуры и саботировать деятельность организации.

---

2 Что такое кибербезопасность? : [Электронный ресурс] // Kaspersky : официальный сайт. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security (дата обращения: 10.09.2026)

1.2. Уязвимости беспроводных каналов связи и трансграничного трафика

Радиосигнал передается в открытом пространстве и по определению доступен всем в зоне покрытия.[3] Его можно перехватить (прослушать или скопировать данные), подделать (создать ложную базовую станцию, чтобы телефон «подключился» к ней), заглушить (радиопомехами, чтобы связь пропала).

Известны атаки на протоколы мобильной связи, когда устройство притворяется базовой станцией и собирает идентификаторы телефонов или перехватывает трафик. Для государства это риск утечки данных пользователей и нарушения работы экстренных служб. Это также распространяется на спутниковую связь. Перехват спутникового трафика технически возможен даже с относительно недорогим оборудованием. В условиях международных кризисов это может использоваться для сбора разведданных или для создания ложной информации в навигационных сервисах. Отдельно следует рассмотреть оптоволоконные линии. Само волокно очень надежно: сигнал почти невозможно «снять» без разрыва линии.[3] Но уязвимы точки сопряжения и физическая инфраструктура: береговые станции, где подводные кабели выходят на сушу, узлы коммутации и агрегации трафика, места ремонта и тестирования, где сигнал выводится в активную аппаратуру.[4]

Кроме того, возможны физические атаки: перерезание кабеля, повреждение узла, отключение питания. Это не «кибератака» в чистом виде, но приводит к тем же последствиям – масштабным сбоям связи. Не секрет, что подводные кабели – это основа глобального интернета. Несколько инцидентов с повреждением кабелей (в том числе из-за якорей судов) приводили к отключению связи в целых регионах. В марте 2024 года якорь грузового судна Rubymar разорвал три интернет-кабеля в Красном море после попадания в судно ракеты хуситов. Это привело к падению трафика между Азией и Европой на 90%. В ноябре 2024 года повреждение кабеля C-Lion1 между Финляндией и Германией привело к отключению проходивших по нему услуг связи. Если повреждение целенаправленное, эффект может быть стратегическим: нарушается связь, финансы, государственные услуги. В октябре 2022 года у Шетландских островов (Шотландия) рыболовный траулер повредил подводный кабель, связывавший архипелаг с материковой Британией.

---

[3] Сферы применения кибербезопасности : [Электронный ресурс] // Cyberleninka : официальный сайт. — URL: https://cyberleninka.ru/article/n/sfery-primeneniya-kiberbezopasnosti/viewer (дата обращения 10.09.2026)

[4] Квантовая связь : [Электронный ресурс] // РИА Новости. – URL: https://ria.ru/20190217/1550922530.html (дата обращения: 10.09.2026).

В результате жители островов на сутки лишились интернета и телефонной связи, магазины не могли принимать платежи по банковским картам. В городских сетях узлы агрегации – это узкое место: если злоумышленник получит доступ к оборудованию на узле, он может перенаправить трафик или устроить перехват.[5]

Уязвимы узлы маршрутизации – объекты сети, управляющие потоками трафика.[6] Например, это могут быть ошибки конфигурации, из-за которых трафик уходит «не туда» и может быть перехвачен, компрометация оборудования и атаки на протоколы маршрутизации, которые позволяют злоумышленнику «обмануть» сеть и перенаправить потоки данных.

В опасности может быть и трансграничный трафик – данные, которые передаются по сетям между государствами.[5,6] Они проходят через точки, находящиеся под юрисдикцией другого государства или оператора. Риски в данной сфере носят не только технический, но и правовой и политический характер. Различия в национальном законодательстве, регулирующем перехват, хранение и доступ к данным, затрудняют формирование единых подходов к обеспечению безопасности коммуникаций. При этом правомерные действия государственных органов могут восприниматься участниками обмена информацией как угроза ее конфиденциальности. Отсутствие унифицированных международных норм создает правовые пробелы, повышающие риск несанкционированного доступа к данным и их модификации.

ГЛАВА 2. КВАНТОВАЯ КРИПТОГРАФИЯ И ЕЕ ОСНОВЫ

2.1. Введение в теорию криптографии

Криптография – это область математики и информатики, изучающая методы защиты информации. Первоначально она была направлена на сохранение конфиденциальности сообщений, однако сегодня также обеспечивает целостность данных, аутентификацию и подтверждение подлинности информации.

---

5 Квантовая связь : [Электронный ресурс] // РИА Новости. – URL: https://ria.ru/20190217/1550922530.html (дата обращения: 10.09.2026).

6 TR.SQKDN: Standardization consideration of satellite-based QKDN : technical report. – Geneva : ITU-T, 2025. – [Электронный ресурс]. – URL: https://www.itu.int/epublications/publication/itu-t-tr-sqkdn-2025-03-standardization-consideration-of-satellite-based-qkdn (дата обращения: 10.09.2026).

Классическая криптография возникла задолго до появления компьютеров и основывалась на простых способах преобразования текста.[7] К наиболее известным методам относятся шифр Цезаря, подстановочные и перестановочные шифры. Их принцип заключался в изменении исходного сообщения по определенному правилу. Однако развитие криптоанализа показало уязвимость многих таких методов, что привело к созданию более сложных математических систем.

Основой современной криптографии является использование криптографического алгоритма и ключа. Алгоритм определяет способ преобразования информации, а ключ является параметром, необходимым для шифрования и расшифрования. В современных системах безопасность должна основываться на секретности ключа, а не самого алгоритма.

Выделяют симметричную и асимметричную криптографию.[8] В симметричной криптографии для шифрования и расшифрования используется один секретный ключ. Асимметричная криптография использует пару связанных ключей – открытый и закрытый – и применяется, в частности, для обмена ключами и создания цифровых подписей.

Математическую основу современной криптографии составляют теория чисел, алгебра, теория вероятностей и теория вычислительной сложности.[9] Многие криптографические алгоритмы строятся на математических задачах, решение которых при больших параметрах требует значительных вычислительных ресурсов.

Современная наука развивается с каждым днем точно так же, как и компьютерные системы, поэтому классическая криптография становится более уязвимой для кибератак. Привычные методы не способны защитить большие объемы данных, вследствие чего были созданы новые методы защиты информации, основанные на законах физики, например, квантовая криптография.

---

7 Голубчиков Д. М., Румянцев К. Е. Квантовая криптография: принципы, протоколы, системы. Таганрог : Таганрогский технологический институт Южного федерального университета, 2008. 43 с.

8 Филиппов М. А., Кротова Е. Л. Квантовая криптография. Протоколы квантовой криптографии // Актуальные проблемы кибербезопасности. 2017. № 4 (26). С. 31–35.

9 Иванова Е. Ю., Ларионцева Е. А. Введение в квантовую криптографию: основные понятия, подходы и алгоритмы [Электронный ресурс] // Инженерный журнал: наука и инновации. URL: https://engjournal.bmstu.ru/articles/1000/html/files/assets/basic-html/page1.html

2.2. Квантовая криптография: основы и протокол BB84

Квантовая криптография представляет собой направление криптографии, использующее свойства квантовой механики для защиты информации. Одним из наиболее развитых направлений применения квантовой криптографии является квантовое распределение ключей (Quantum Key Distribution, QKD), предназначенное для безопасного формирования и распределения криптографических ключей между участниками коммуникации. В отличие от традиционных криптографических методов, безопасность которых во многом обусловлена вычислительной сложностью математических задач, QKD использует физические свойства квантовых состояний, позволяющие обнаруживать попытки несанкционированного вмешательства в процесс распределения ключа.[10]

Основными понятиями квантовой механики, используемыми в квантовых коммуникациях, являются суперпозиция, измерение квантового состояния и принцип невозможности клонирования.[11] В классических вычислениях основным элементом информации является бит, принимающий значение 0 или 1. В квантовых системах аналогом бита является кубит, который может находиться в суперпозиции состояний $|0\rangle$ и $|1\rangle$.[12] При измерении кубита в выбранном базисе результатом становится одно из допустимых состояний – 0 или 1, причем вероятность получения каждого результата определяется исходным квантовым состоянием.

Для квантовой криптографии особенно важно то, что измерение квантового состояния может изменить это состояние. Кроме того, неизвестное произвольное квантовое состояние невозможно точно скопировать, что известно как принцип невозможности клонирования. Благодаря этим свойствам попытка злоумышленника получить информацию о передаваемых квантовых состояниях приводит к появлению ошибок, которые затем обнаруживаются легитимными участниками коммуникации.

---

[10] Рекомендация ITU-T X.1811. Руководящие указания по безопасности для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность. Женева : ITU-T, 2021. 54 с.

[11] Бровко С. В., Кондаков О. В. Квантовая механика : учебное пособие. Елец : Елецкий государственный университет им. И. А. Бунина, 2016. 186 с.

[12] Квантовая криптография: определение двух кубитов и операция CNOT. Квантовая криптография для будущего [Электронный ресурс]. URL: https://books.yandex.ru/books/Swe2PBYb

Таким образом, квантовые технологии не делают коммуникацию абсолютно защищенной, а позволяют создать механизм обнаружения определенных видов вмешательства в процесс распределения ключей.

Одним из направлений квантовых коммуникаций является создание защищенных каналов связи на основе QKD[13] – это процедура выработки и распределения секретных ключей, реализуемая с помощью квантовых криптографических протоколов и квантовых каналов связи. Она позволяет двум абонентам создать общий и известный только им ключ, который они могут использовать для шифрования и дешифрования сообщений. Ключевыми преимуществами технологии являются автоматизация процесса генерации и распределения ключей между абонентами, снижение нагрузки на инфраструктуру управления ключами, возможность их регулярного обновления, а также обнаружение попыток перехвата в процессе распределения.

Существует множество протоколов квантовой криптографии, основанных на передаче информации посредством кодирования в состояниях одиночных фотонов.[14] BB84 является первым протоколом квантового распределения ключей, предложенным в 1984 году Чарльзом Беннеттом и Жилем Брассаром. Он основан на идеях поляризации фотонов (направление колебаний электрического поля световой волны), а ключ состоит из биты, закодированные состояниями фотонов.

При рассмотрении протокола будем называть отправителя Алисой, а получателя Бобом. Сегодня у них есть, по сути, два варианта: встретиться и сообща сгенерировать криптографический ключ (надеясь, что никто его не перехватит) или использовать протоколы с открытым ключом, например RSA. В первом случае ключ нужно постоянно обновлять, чтобы снизить риск взлома системы, а во втором случае протокол безопасен, но, если будет создан квантовый компьютер с набором элементов достоной мощности, протокол RSA станет уязвим. Для решения этой проблемы предложен протокол BB84. Алиса и Боб используют два канала: открытый (для зашифрованных данных, без возможности подмены) и закрытый (для ключа, его прослушивание позволяет обнаружить BB84). Рассмотрим этот протокол подробнее.

---

13 Recommendation ITU-T Q.4160. Quantum key distribution networks – Protocol framework. Geneva : ITU-T, 2023. 24 p.

14 Филиппов М. А., Кротова Е. Л. Квантовая криптография. Протоколы квантовой криптографии // Актуальные проблемы кибербезопасности. 2017. № 4 (26). С. 31–35.

В протоколе BB84 используются 4 квантовых состояния фотонов, например направление вектора поляризации, одно из которых Алиса выбирает в зависимости от передаваемого бита: 90° или 135° для «1», 45° или 0° для «0». Одна пара квантовых состояний принадлежит базису «+». Другая пара квантовых состояний принадлежит базису «×» (рисунок 1). Внутри каждого базиса векторы состояний ортогональны, но состояния из разных базисов являются попарно неортогональными (неортогональность необходима для усложнения попыток съема информации).

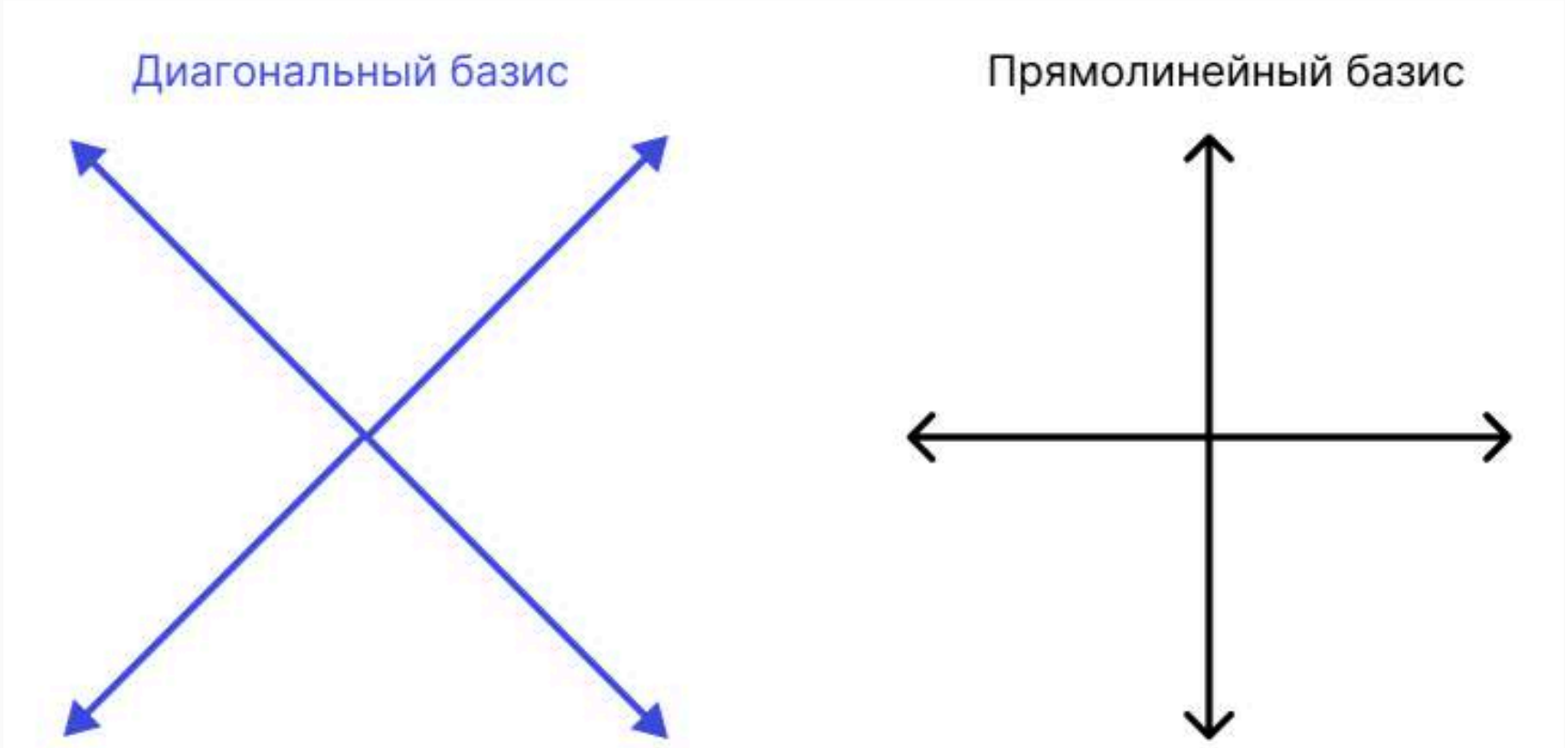


Рисунок 1 — Базисы квантовых состояний

Для генерации ключа отправитель пропускает фотоны через четыре традиционных однонаправленных фильтра (линейных поляризатора). Получатель для определения посылаемых бит (поляризации фотонов) применяет две поляризационные разделительные призмы, работающие в прямолинейном и диагональном базисах. Рассмотрим ситуацию, когда Алиса и Боб передают информацию без прослушивания на примере таблицы 1:

1. Алиса генерирует случайную последовательность бит и для каждого из них случайным образом выбирает один из двух базисов. Полученные фотоны посылает Бобу.
2. Боб получает фотоны и считывает их случайным образом, чередуя базисы, т.к. он не знает, какую последовательность базисов выбрала Алиса. Половина из базисов будет правильно угадана.
3. Боб открыто сообщает Алисе порядок использования им базисов, не сообщая результаты.

4. Алиса открыто сообщает Бобу, какие базисы были выбраны Бобом правильно; биты, полученные в совпавших базисах, формируют ключ.
5. Биты для правильно выбранных базисов используются для проверки целостности переданных данных и формирования ключа.

Таблица 1. Пример обмена ключами по протоколу BB84

Пример обмена ключами по протоколу BB84

Этапы									
	1	Случайным образом сгенерированные биты	1	0	0	1	1	1	0
		Базис, выбранный Алисой	×	×	+	×	+	+	+
		Фотоны	\	/	–	\	|	|	–
	2	Базис, выбранный Бобом	+	×	×	+	+	+	×
		Биты, определенные Бобом	0	0	1	0	1	1	1
	3,4	Проверка правильности применения базисов Бобом		V			V	V	
	5	Биты для контроля целостности и формирования ключа		0			1	1	

В оригинальном протоколе BB84 из этих «правильных» битов выбирается определенная часть и открыто сравнивается. В случае совпадения (канал не прослушивается и данные дошли без искажений), биты, которые открыто сравнивались, удаляются из ключа, и оставшаяся часть используется для формирования ключа требуемой длины.

Рассмотрим ситуацию, при которой Ева пытается перехватить передаваемые Алисой квантовые состояния. В протоколе BB84 Алиса использует два взаимно неортогональных базиса, а Боб случайным образом выбирает один из них для измерения. После сравнения базисов около половины фотонов отбрасывается. Ева также выбирает базис для измерения перехваченного фотона. В половине случаев ее выбор совпадает с базисом Алисы, и состояние фотона не изменяется. В остальных случаях измерение в неправильном базисе изменяет его состояние, поэтому Ева получает случайный результат и передает Бобу измененный фотон. В результате Боб с вероятностью 50% получает ошибочное значение. Таким образом, вмешательство Евы приводит к ошибке примерно в 25 % оставшихся битов ключа. Для ее обнаружения Алиса и Боб сравнивают часть ключа по открытому каналу. Значительная доля несовпадений указывает на возможное вмешательство, и такой ключ не используется.

2.3. Альтернативные протоколы: B92, E91, MDI-QKD, Twin-Field QKD

В квантовой криптографии также используются модификации BB84, например, B92, BB84 (4+2) и их модификации. Кроме того, существует протокол, разработанный для кодирования информации в запутанных состояниях – E91.[15]

Протокол B92 – это упрощенный вариант BB84, предложенный Чарльзом Беннеттом в 1992 году. В отличие от BB84, здесь используются только два неортогональных квантовых состояния, например поляризация фотона под углом 0° и 45°, которые соответствуют битам 0 и 1. Алиса случайно выбирает последовательность битов, кодирует их соответствующими состояниями и отправляет фотоны Бобу. Боб измеряет каждый фотон, но из-за того, что состояния неортогональны, он не всегда может определить, какой бит был передан. Если результат позволяет однозначно исключить одно из состояний, Боб фиксирует соответствующий бит; если определить состояние невозможно, этот результат отбрасывается. После передачи Алиса и Боб по открытому каналу согласовывают, какие результаты оставить, а затем проверяют часть ключа на наличие ошибок. Если ошибок слишком много, это может свидетельствовать о перехвате данных.

Протокол BB84 (4+2) является промежуточным между протоколами BB84 и B92. В протоколе используются 4 квантовых состояния для кодирования «0» и «1» в двух базисах. Состояния в каждом базисе выбираются неортогональными, состояния в разных базисах также попарно неортогональны. Процесс генерации ключа точно такой же, как и в протоколе BB84, который описан выше.

В протоколе E91 используются пары фотонов, рождающиеся в антисимметричных поляризационных состояниях. Отправитель генерирует некоторое количество фотонных пар. Один фотон из каждой пары он оставляет для себя, второй посылает своему партнеру. При получении отправителем значения поляризации «1», его партнер зарегистрирует значение «0», и наоборот. Ясно, что таким образом партнеры всякий раз могут получить идентичные псевдослучайные кодовые последовательности. Предположим, что изначально создается некоторое количество пар фотонов максимально запутанных пар фотонов, чтобы результаты измерений оказались взаимосвязанными, а затем один фотон из каждой пары посылается Алисе, а другой Бобу. Тогда образуется три возможных квантовых состояния для этих пар. Каждое из этих трех состояний кодирует биты «0» и «1» в уникальном базисе.

---

15 Голубчиков Д. М., Румянцев К. Е. Квантовая криптография: принципы, протоколы, системы. Таганрог : Таганрогский технологический институт Южного федерального университета, 2008. 43 с.

Затем Алиса и Боб осуществляют измерения на своих частях разделенных пар фотонов, применяя соответствующие приборы. Алиса записывает измеренные биты, а Боб записывает их дополнения до 1. Результаты измерений, в которых пользователи выбрали одинаковые базисы, формируют «сырой» ключ. Для остальных результатов Алиса и Боб проводят проверку на присутствие Евы.

Также существуют другие протоколы: MDI-QKD и Twin-Field QKD, которые мы рассмотрим ниже.

MDI-QKD (Measurement-Device-Independent Quantum Key Distribution) – это протокол квантового распределения ключей, разработанный для устранения одной из наиболее уязвимых частей традиционных систем QKD – измерительного оборудования, поскольку реальные детекторы и другие устройства могут иметь технические недостатки.[16] Их эксплуатация может позволить злоумышленнику воздействовать на оборудование и получать информацию о ключе, даже если сам протокол QKD теоретически обеспечивает высокий уровень безопасности.

Принцип работы можно представить следующим образом. Алиса и Боб независимо друг от друга подготавливают квантовые состояния и отправляют их на промежуточный узел.[17] Этот узел осуществляет совместное измерение двух сигналов, как правило, измерение Белла (Bell-state measurement).

Ключевой момент заключается в том, что промежуточный узел не должен быть доверенным. Он может даже находиться под контролем потенциального противника. После измерения узел сообщает Алисе и Бобу только классический результат измерения. На основании этой информации они проводят согласование базисов, оценку уровня ошибок и последующую обработку данных – коррекцию ошибок и усиление секретности. В результате они получают общий секретный ключ, при этом безопасность протокола не зависит от того, является ли измерительное устройство исправным или скомпрометированным.

Таким образом, основное преимущество MDI-QKD состоит в том, что атака на измерительный прибор сама по себе не позволяет противнику получить секретный ключ. Это особенно важно для практических сетей, поскольку именно несовершенства детекторов и измерительных компонентов могут создавать уязвимости, которых нет в идеализированной математической модели QKD.

---

[16] Granados G., Velasquez W., Cajo R., Antonieta-Alvarez M. Quantum Key Distribution in Multiple Fiber Networks and Its Application in Urban Communications: A Comprehensive Review // IEEE Access. 2025

[17] Joshi S. K., Aktas D., Wengerowsky S. et al. A trusted node-free eight-user metropolitan quantum communication network // Science Advances. 2020. Vol. 6, № 36. Art. eaba0959

Twin-Field QKD (TF-QKD) – это семейство протоколов, которое помогает решить одну из основных проблем квантовых сетей: с увеличением расстояния скорость передачи секретного ключа снижается.[18]

В TF-QKD Алиса и Боб отправляют слабые световые сигналы на общую центральную станцию. Там два сигнала встречаются и взаимодействуют друг с другом – происходит интерференция. По результату этой интерференции можно определить, насколько согласованы сигналы Алисы и Боба, и получить информацию, необходимую для формирования общего ключа.

Для работы протокола сигналы должны быть хорошо согласованы, прежде всего по фазе. После измерения на центральной станции Алиса и Боб обмениваются необходимой информацией по классическому каналу, оценивают количество ошибок и выполняют дополнительную обработку данных. Если уровень ошибок соответствует требованиям безопасности, из полученной информации формируется секретный ключ.

Главное преимущество TF-QKD заключается в том, что квантовый сигнал не должен проходить все расстояние между Алисой и Бобом. Каждый из них передает сигнал примерно на половину общего расстояния – до центральной станции. Благодаря этому протокол позволяет уменьшить влияние потерь в оптическом волокне и потенциально повысить эффективность QKD при передаче ключей на больших расстояниях.

Таким образом, TF-QKD рассматривается как один из вариантов развития дальних квантовых сетей. Его основная идея достаточно проста: вместо передачи одного квантового сигнала на все расстояние используются два согласованных сигнала, которые встречаются в центральной точке.

Несмотря на высокий потенциал QKD, квантовая криптография не является универсальным решением всех проблем информационной безопасности. Практическое внедрение QKD требует специализированного оборудования, квантовых источников и детекторов, а также каналов связи, способных обеспечивать передачу квантовых состояний.

Одним из основных ограничений являются потери сигнала.[19] При увеличении расстояния между участниками количество зарегистрированных фотонов уменьшается, что ограничивает дальность прямой передачи ключей. Для построения сетей большой протяженности могут потребоваться специальные архитектурные решения, включая доверенные узлы и квантовые ретрансляторы, развитие которых остается отдельным технологическим направлением.

---

[18] Wang S., Yin Z.-Q., He D.-Y. et al. Twin-field quantum key distribution over 830-km fibre // Nature Photonics. 2022. Vol. 16. P. 154–161

[19] Qiu B.-Y., Li Y., Wang G.-Q. et al. 7 km free-space time-bin quantum key distribution // Optics Express. 2025. Vol. 33, № 17. P. 35176–35184.

Кроме того, теоретическая безопасность протокола не гарантирует автоматическую безопасность всей практической системы. Уязвимости могут возникать в оборудовании, программном обеспечении, устройствах генерации и регистрации фотонов, а также в процессе аутентификации классического канала. Поэтому безопасность QKD должна рассматриваться с учетом как математических и физических принципов протокола, так и особенностей его практической реализации.

2.4. Постквантовая криптография

Квантовое распределение ключей следует отличать от постквантовой криптографии (Post-Quantum Cryptography, PQC).[20] PQC предполагает использование классических криптографических алгоритмов, основанных на математических задачах, решение которых должно оставаться вычислительно сложным даже для квантовых компьютеров.[21] Иными словами, алгоритмы специально строятся таким образом, чтобы существующих и возможных в будущем вычислительных возможностей было недостаточно для их быстрого взлома. При этом они работают на обычных вычислительных устройствах и могут внедряться в существующие информационные системы без создания специального квантового канала. QKD, напротив, использует физические свойства квантовых состояний для распределения ключевого материала и позволяет обнаруживать попытки перехвата по изменению параметров квантового сигнала.

Эти подходы не обязательно конкурируют друг с другом. QKD может использоваться для наиболее критичных каналов связи, тогда как PQC обеспечивает защиту широкого спектра информационных систем и сервисов. Их совместное применение позволяет сформировать гибридную модель защиты, в которой безопасность не зависит исключительно от одного криптографического механизма.[22]

Таким образом, перспективы QKD связаны не с полной заменой традиционной криптографии, а с ее интеграцией в комплексную архитектуру кибербезопасности. Сочетание QKD и PQC позволяет одновременно использовать физические механизмы защиты квантового канала и криптографические алгоритмы, устойчивые к квантовым атакам. Это особенно важно для долгосрочной защиты критической инфраструктуры, а также для обеспечения совместимости и устойчивости глобальных коммуникационных сетей.

---

20 Малыгина Е. С., Куценко А. В., Новоселов С. А. [и др.]. Постквантовые криптосистемы: открытые вопросы и существующие решения. Криптосистемы на решетках // Дискретный анализ и исследование операций. 2023. Т. 30, № 4. С. 46–90.

21 Школьный Н. Т., Горохов А. В. Квантовая криптография и постквантовые алгоритмы шифрования // Вестник молодых ученых и специалистов Самарского университета. 2025. № 4 (29). С. 40–47.

22 Рекомендация ITU-T X.1811. Руководящие указания по безопасности для применения в системах IMT-2020 алгоритмов, обеспечивающих квантовую безопасность. Женева : ITU-T, 2021. 54 с.

ГЛАВА 3. ТЕХНОЛОГИИ И АРХИТЕКТУРА КВАНТОВОЙ КРИПТОГРАФИИ

3.1. Архитектура квантовой криптографии

Практическая реализация квантовой криптографии предполагает использование нескольких физических каналов передачи квантовой информации: оптоволоконных, свободно-пространственных и спутниковых.[23] Выбор конкретного канала зависит от расстояния, характеристик среды передачи, уровня потерь, стоимости оборудования и возможностей дальнейшего масштабирования сети.

Наиболее зрелыми считаются оптоволоконные системы, которые применяются прежде всего в городских и региональных сетях. Их преимуществом является возможность использования существующей телекоммуникационной инфраструктуры и совместной работы квантовых и классических каналов связи. Возможности такого подхода демонстрируют эксперименты по передаче квантовой информации по городским оптоволоконным сетям. Например, в Саарбрюккене была продемонстрирована передача запутанных состояний на расстояние 14,4 км с использованием городской оптоволоконной линии.[24] В Берлине была реализована передача квантовой запутанности на расстояние около 82 км одновременно с передачей данных Ethernet по тому же волокну.[25] Дополнительные возможности масштабирования связаны с использованием многожильного оптоволокна, позволяющего разделять квантовый и классический трафик. В одном из экспериментов в Италии по такой инфраструктуре удалось передать до 110 Тбит/с классического трафика.[26]

Основным ограничением оптоволоконных систем являются потери сигнала, которые увеличиваются с расстоянием. В отличие от классических оптических сетей, стандартные усилители нельзя напрямую использовать для усиления неизвестного квантового состояния, поэтому дальность прямой передачи QKD остается ограниченной. Для преодоления этого ограничения применяются различные архитектурные решения. В частности, эксперименты с протоколом Twin-Field QKD продемонстрировали возможность квантовой передачи по оптоволокну на расстояния порядка 830 км.[27] Для построения более протяженных сетей также рассматриваются доверенные промежуточные узлы, MDI-QKD, Twin-Field QKD и перспективные квантовые ретрансляторы. Эти решения позволяют увеличивать дальность передачи, однако различаются по уровню безопасности, технической сложности и стоимости.

---

23 Recommendation ITU-T Q.4160. Quantum key distribution networks – Protocol framework. Geneva : ITU-T, 2023. 24 p.

24 Kucera S., Haen C., Arenskötter E. et al. Demonstration of quantum network protocols over a 14-km urban fiber link [Электронный ресурс] // npj Quantum Information. 2024. Vol. 10. Art. 88. URL: https://www.nature.com/articles/s41534-024-00886-x

25 Sena M., Flament M., Andrewski S. et al. High-fidelity quantum entanglement distribution in metropolitan fiber networks with co-propagating classical traffic // Journal of Optical Communications and Networking. 2025. Vol. 17, № 12. P. 1072–1081. URL: https://opg.optica.org/jocn/fulltext.cfm?uri=jocn-17-12-1072

26 Wu Q., Ribezzo D., Di Sciullo G. et al. Integration of quantum key distribution and high-throughput classical communications in field-deployed multi-core fibers // Light: Science & Applications. 2025.

27 Wang S., Yin Z.-Q., He D.-Y. et al. Twin-field quantum key distribution over 830-km fibre // Nature Photonics. 2022. Vol. 16. P. 154–161.

Другим вариантом являются свободно-пространственные оптические каналы, в которых передача квантовой информации осуществляется через атмосферу без использования физического кабеля.[28] Они могут применяться для связи между зданиями, кампусами и другими близко расположенными объектами. Например, в Афинах была реализована гибридная архитектура, объединяющая свободно-пространственный и оптоволоконный каналы; при различных условиях работы QBER (см. глоссарий) оставался ниже 3,5%.[29] Вместе с тем свободно-пространственная передача зависит от погодных условий, турбулентности атмосферы, облачности, фонового освещения и точности наведения оборудования. Поэтому такие системы требуют автоматической синхронизации, стабилизации и высокоточного позиционирования.

Для передачи квантовой информации на межрегиональные и межконтинентальные расстояния перспективным решением являются спутниковые каналы.[30] Спутник в данном случае выступает источником квантовых состояний: они формируются на борту и передаются непосредственно наземным станциям Алисы и Боба, которые принимают и измеряют фотоны. Таким образом, квантовый сигнал идет от спутника к пользователям, что позволяет снизить потери по сравнению со сверхдлинными оптоволоконными линиями. Важным этапом стало использование спутника «Мо-цзы» для демонстрации квантовой связи между удаленными наземными станциями. Позднее была создана наземно-космическая сеть протяженностью около 4 600 км. Развитие спутниковой QKD также сопровождается международной стандартизацией: в рамках Международного союза электросвязи рассматриваются архитектура квантовых сетей, особенности орбит и взаимодействие космических и наземных сегментов.[31]

Таким образом, для формирования глобальной квантовой сети наиболее реалистичным является гибридный подход. Оптоволоконные каналы целесообразно использовать в городских и региональных сетях, свободно-пространственные технологии – для отдельных наземных и атмосферных участков, а спутниковые системы – для обеспечения связи между удаленными регионами и континентами. Такое сочетание различных технологий позволяет учитывать ограничения каждого типа канала и создавать более устойчивую архитектуру квантовой связи.

---

28 Kržič A., Sharma S., Spiess C. et al. Towards metropolitan free-space quantum networks // npj Quantum Information. 2023. Vol. 9. Art. 95.

29 Stathis A., Ntanos A., Kourelias P. et al. Practical approach to last-mile converged free-space and fiber QKD for secure city-scale networks // Scientific Reports. 2026. Vol. 16. Art. 4073

30 Orsucci D., Kleinpaß P., Meister J. et al. Assessment of practical satellite quantum key distribution architectures for current and near-future missions [Электронный ресурс]. arXiv, 2024. URL: https://arxiv.org/abs/2404.05668

31 Chen Y.-A., Zhang Q., Chen T.-Y. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. 2021. Vol. 589, № 7841. P. 214–219.

3.2. Преимущества квантовой криптографии

Одно из главных преимуществ QKD – возможность обнаружить попытку перехвата квантового состояния. Воздействие на передаваемые фотоны изменяет параметры квантового сигнала и может приводить к росту уровня ошибок. Это позволяет выявлять вмешательство непосредственно при распределении ключа, в отличие от традиционных методов, безопасность которых во многом основана на вычислительной сложности математических задач.

QKD можно интегрировать в существующую телекоммуникационную инфраструктуру, постепенно добавляя квантовые компоненты без полной замены действующих сетей. Эксперимент Стефана Куцеры и соавторов продемонстрировал работу квантовых сетевых протоколов на реальной городской оптоволоконной линии протяженностью 14,4 км.[32] Исследования также подтверждают возможность одновременной передачи квантового и классического трафика по многожильному оптоволокну.

Различные физические каналы позволяют использовать QKD на разных уровнях сети. Оптоволокно подходит для городских и региональных соединений, свободное пространство – для отдельных наземных участков, а спутниковые каналы – для дальних и межконтинентальных соединений. Свободно-пространственная QKD уже рассматривается как дополнение к оптоволоконным сетям.

Спутниковые технологии позволяют уменьшить потери при передаче на очень большие расстояния. В Китае была создана интегрированная космическо-наземная квантовая сеть протяженностью около 4600 км, объединившая спутниковые и оптоволоконные каналы.[33] Это подтверждает возможность сочетания различных технологий в рамках одной сети.

Развитие новых протоколов также расширяет возможности QKD. Twin-Field QKD позволил продемонстрировать передачу ключа по оптоволокну на расстояние 833,8 км при потерях канала более 140 дБ.[34] MDI-QKD снижает требования к доверию к измерительному оборудованию промежуточного узла, а квантовые ретрансляторы в перспективе могут увеличить дальность передачи без использования цепочки полностью доверенных узлов. Кроме того, экспериментальная восьмипользовательская сеть без доверенных промежуточных узлов продемонстрировала возможность перехода от соединений «точка–точка» к более сложным городским архитектурам.

---

32 Chen Y.-A., Zhang Q., Chen T.-Y. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. 2021. Vol. 589, № 7841. P. 214–219.

33 Wang S., Yin Z.-Q., He D.-Y. et al. Twin-field quantum key distribution over 830-km fibre // Nature Photonics. 2022. Vol. 16. P. 154–161.

34 Qiu B.-Y., Li Y., Wang G.-Q. et al. 7 km free-space time-bin quantum key distribution // Optics Express. 2025. Vol. 33, № 17. P. 35176–35184.

3.3. Ограничения и недостатки

Главное техническое ограничение QKD – потери при передаче квантового сигнала.[35] В оптоволокне они увеличиваются с расстоянием, что снижает скорость генерации ключей и ограничивает дальность прямого соединения. Обычные оптические усилители нельзя использовать для усиления неизвестного квантового состояния без нарушения принципов квантовой передачи.

Для увеличения дальности применяются доверенные промежуточные узлы. Они разделяют длинный канал на несколько коротких участков, но каждый узел требует физической защиты, специального оборудования и обслуживания. Поэтому увеличение числа узлов повышает стоимость и сложность сети. MDI-QKD и другие архитектуры без необходимости полного доверия к промежуточному оборудованию позволяют частично решить эту проблему, но требуют более сложных технических решений.

Свободно-пространственные каналы чувствительны к внешним условиям: атмосферной турбулентности, осадкам, облачности и фоновому освещению. Кроме того, необходимы точное наведение, синхронизация и стабилизация передатчика и приемника. Поэтому параметры такого канала могут меняться сильнее, чем в защищенной оптоволоконной линии.

Спутниковая QKD решает проблему очень больших расстояний, но требует сложных оптических систем наведения и сопровождения.[36] Дополнительные ограничения создают атмосферные условия на участке «спутник–Земля» и необходимость поддерживать стабильное соединение с движущимся спутником.

Отдельная проблема – стоимость и сложность оборудования. Для QKD необходимы источники фотонов, высокочувствительные детекторы, системы синхронизации и стабилизации, а также программные средства управления ключами.[37] При масштабировании сети добавляются задачи маршрутизации, управления ключами, мониторинга и защиты сетевых узлов.

Таким образом, основная проблема масштабирования QKD связана не только с увеличением дальности передачи. Необходимо обеспечить физическую устойчивость каналов, безопасность сетевых узлов и оборудования, совместимость с существующей телекоммуникационной инфраструктурой и эффективное управление сетью.

---

35 Qiu B.-Y., Li Y., Wang G.-Q. et al. 7 km free-space time-bin quantum key distribution // Optics Express. 2025. Vol. 33, № 17. P. 35176–35184.

36 Rozenman G. G., Maslennikov A., Gandelman S. P. et al. Free-space and Satellite-Based Quantum Communication: Principles, Implementations, and Challenges [Электронный ресурс]. arXiv, 2026. URL: https://arxiv.org/abs/2602.01426

37 Quantum Key Distribution Deployment Cost: Hardware, Fibre, Trusted Nodes and Total Cost of Ownership [Электронный ресурс]. Quantum Security Defence, 2026. URL: https://quantumsecuritydefence.com/insights/qkd-economics-deployment-cost-roi/

Однако даже при теоретической защищенности квантового протокола уязвимости могут возникать на уровне его физической реализации: например, злоумышленник может воздействовать на характеристики источников или детекторов и использовать особенности их работы для проведения атак. Массовое внедрение технологии поэтому зависит не только от увеличения дальности и снижения стоимости оборудования, но и от разработки защищенных аппаратных решений и методов контроля их безопасности.

3.4. Экономика и масштабирование квантовой криптографии

Экономическая целесообразность внедрения QKD определяется прежде всего высокой стоимостью оборудования и эксплуатации инфраструктуры. В расходы входят не только квантовые передатчики и приемники, но и детекторы одиночных фотонов, системы синхронизации, оптические компоненты, управляющее программное обеспечение, техническое обслуживание и модернизация оборудования. Особенно дорогостоящими остаются высокоэффективные детекторы, включая сверхпроводящие нанопроволочные детекторы одиночных фотонов, использование которых повышает эффективность системы, но одновременно увеличивает ее стоимость.

По отраслевым оценкам, стоимость одного узла QKD может составлять около $100-150 тыс.[38] Однако цена отдельного устройства не отражает реальных затрат на создание сети. Поэтому ключевым показателем является совокупная стоимость владения (Total Cost of Ownership, TCO), включающая первоначальные капитальные вложения, эксплуатационные расходы, обслуживание, энергопотребление, модернизацию и использование телекоммуникационной инфраструктуры.[38]

Существенно снизить первоначальные затраты позволяет использование уже существующих оптических сетей вместо строительства новой инфраструктуры. Это делает интеграцию QKD с действующими телекоммуникационными системами одним из основных способов экономии. При этом пилотные проекты позволяют оценить не только техническую работоспособность технологии, но и фактические расходы на ее установку, эксплуатацию и обслуживание.

---

38 Quantum Key Distribution Deployment Cost: Hardware, Fibre, Trusted Nodes and Total Cost of Ownership [Электронный ресурс]. Quantum Security Defence, 2026. URL: https://quantumsecuritydefence.com/insights/qkd-economics-deployment-cost-roi/

Перспективы коммерциализации отражаются и в отраслевых прогнозах. Согласно оценке Juniper Research, операторы связи могут направить около $6,3 млрд на QKD в 2025–2030 гг.[39] Однако данный показатель является прогнозом, а не гарантированным объемом инвестиций. Коммерческий интерес к технологии связан также с возможностью создания новых услуг для корпоративных клиентов, включая защищенные каналы связи и решения QKD-as-a-Service.[40] Дополнительным фактором является возможность получения конкурентного преимущества за счет предоставления квантово-устойчивых услуг финансовым организациям, государственным структурам и другим компаниям, работающим с критически важными данными.

При оценке экономической эффективности необходимо учитывать не только затраты, но и потенциальный ущерб от компрометации защищаемой информации. Для финансовых организаций, государственных систем и объектов критической инфраструктуры стоимость предотвращенного инцидента может существенно превышать расходы на создание защищенного канала. Поэтому целесообразность внедрения QKD определяется соотношением затрат на защиту и потенциальных потерь от нарушения конфиденциальности.

В долгосрочной перспективе снижение TCO будет зависеть от массового производства компонентов, удешевления детекторов, стандартизации оборудования, автоматизации управления и сокращения затрат на обслуживание. Таким образом, экономическая устойчивость QKD определяется не стоимостью отдельного устройства, а возможностью обеспечить приемлемую совокупную стоимость владения при сохранении требуемого уровня защиты.

---

39 Quantum Key Distribution: Network Operators to Spend $6.3 Billion Over Next Six Years [Электронный ресурс]. – Juniper Research, 2025. – URL: https://www.juniperresearch.com/press/quantum-key-distribution-network-operators-to-spend-6bn/ (дата обращения: 10.09.2026).

40 Quantum Key Distribution Pilots Market Report 2034 [Электронный ресурс]. Dataintelo, 2026. URL: https://dataintelo.com/report/quantum-key-distribution-pilots-market

3.5. Современные мировые технологии и международное сотрудничество

3.5.1. Китайская Народная Республика

«Мо-цзы» — первый спутник в мире, названный в честь древнекитайского философа Мо-цзы, предназначенный для квантовой передачи информации на землю. Это проект Китайской академии наук при участии Австрийской академии наук. Его масса составляет более 600 килограммов.



Рисунок 2 — Спутник «Мо-цзы»

Элементы орбиты составляют большая полуось – 6 873 км, наклонение – 97,4°, период обращения – 94,5 минуты, апоцентр – 511,1 км, перицентр – 494,8 км, высота орбиты – 500 км.

Разработка была инициирована Китайской академией наук в партнерстве с Институтом квантовой оптики и квантовой информации Австрийской академии наук в Вене в 2011 году. Запуск был совершен 16 августа 2016 года в 01:40 по пекинскому времени с космодрома Цзюцюань в пустыне Гоби (северо-западная провинция Ганьсу) с помощью ракеты-носителя «Чанчжэнь-2D»). 18 января 2017 года, после нескольких месяцев испытания на орбите, спутник был сдан в эксплуатацию.

Спутник предназначен для проведения экспериментов по квантовой телепортации, распределения запутанности (от спутника к двум наземным удаленным станциям, расстояние между которыми превышает тысячу километров), проверки свойств запутанности в больших масштабах и нелокальности квантовой механики, квантовому распределению ключей (QKD) и квантово-защищенной связи в глобальном масштабе.

3.5.2. Европейский союз

Европейский проект OpenQKD, который разворачивается под эгидой Еврокомиссии, является первой масштабной попыткой вывести квантовое распределение ключей за пределы лаборатории в реальную коммерческую и административную эксплуатацию. Основные пилотные зоны выбраны далеко не случайно – это банковский сектор, государственные учреждения и крупные телеком-операторы. Для финансистов, например, критически важна защита межфилиальных переводов и биржевых данных на дистанциях до 100–150 км по существующим оптоволоконным линиям, причем особый акцент делается на защите от так называемой стратегии Harvest Now, Decrypt Later («собери сейчас – расшифруй потом»), которая становится все более реальной угрозой по мере развития квантовых компьютеров.

В госсекторе тестируется обмен зашифрованной информацией между посольствами и центральными ведомствами, что требует совершенно иного уровня доверия к аппаратной части. Что касается телеком-операторов, то здесь главная задача – встроить квантовые генераторы ключей в уже работающие магистральные сети с плотным спектральным уплотнением каналов, чтобы квантовые ключи могли спокойно сосуществовать с классическим шифрованием (AES-256), не создавая при этом узких мест по пропускной способности.

Однако, пожалуй, самым сложным и нетривиальным моментом во всем этом проекте является даже не физика распределения одиночных фотонов, а два сугубо инженерных вопроса – совместимость и сертификация. Оборудование разных производителей, будь то швейцарский ID Quantique, японская Toshiba или итальянский ThinkQuantum, должно быть совместимо, поэтому в рамках OpenQKD разрабатываются единые открытые интерфейсы и протоколы, а также создается программно-определяемый сетевой контроллер, который в реальном времени способен переключать трафик между квантовыми и классическими резервными линиями в случае аномалий.

При этом остро стоит проблема встраивания QKD в привычные протоколы TLS и IPsec: решение должно быть таким, чтобы банкам и госкорпорациям не приходилось переписывать свою ИТ-архитектуру с нуля, а достаточно было просто подключить новый модуль как внешний сервис генерации ключей. Что касается сертификации, то здесь проект идёт по пути, не имеющему аналогов в квантовой криптографии – совместно с европейскими регуляторами, такими как ENISA и немецкое BSI, разрабатываются первые формальные стандарты безопасности, аналогичные по духу Common Criteria, с детальными тестами на устойчивость к конкретным типам атак, включая слепую подмену источника, атаки на однофотонные детекторы и измерение потерь в канале.

Параллельно ведется реестр сертифицированного оборудования, что в перспективе даст возможность банкам и госструктурам использовать QKD не как экспериментальную технологию, а как юридически легитимное средство защиты, полностью соответствующее требованиям GDPR и новой директивы NIS-2.

3.5.3. Япония

Японская корпорация Toshiba разработал мультиплексированные QKD-системы, позволяющие передавать квантовые ключи по тем же оптическим волокнам, по которым идет основной трафик данных: для квантового канала используется телекоммуникационный O-диапазон, а C-диапазон остается свободным для клиентского трафика, что устраняет необходимость в дорогостоящих «темных» волокнах и делает внедрение экономически оправданным. Важным компонентом решений выступает система управления квантовыми ключами (Q-KMS), отвечающая за маршрутизацию, распределение и ротацию ключей между узлами сети, обеспечивающая автоматическую доставку ключей к конечным шифраторам и совместимая с существующими средствами криптографической защиты.

В реальных пилотах Toshiba комбинирует QKD с постквантовой криптографией (PQC): QKD защищает физический уровень, гарантируя обнаружение подслушивания и распределение симметричных ключей, а PQC – уровень приложений и протоколов, обеспечивая защиту асимметричных ключей и цифровых подписей, что повышает устойчивость к разным типам атак. Решения спроектированы так, чтобы не требовать полной замены оборудования: квантовые модули можно устанавливать как отдельные устройства на узлах связи, а ключи передавать в стандартные шифраторы через стандартные интерфейсы; при этом системы поддерживают общепринятые протоколы управления и мониторинга, позволяя операторам включать QKD-узлы в свои системы OSS/BSS и управлять ими наравне с другим сетевым оборудованием.

Архитектура решений отличается масштабируемостью и модульностью, что дает возможность поэтапно наращивать сеть – сначала защищать отдельные критические каналы, например между дата-центрами банка, а затем расширять покрытие на всю сеть. В финансовом секторе квантовые ключи применяются для шифрования трафика между головным офисом и филиалами, а также между дата-центрами. Это особенно важно для передачи платежных поручений, персональных данных клиентов и другой конфиденциальной информации.

В телекоммуникационном секторе QKD используют для защиты служебного трафика, каналов синхронизации и передачи ключей между узлами сети, повышая общую устойчивость инфраструктуры к кибератакам и соответствуя требованиям регуляторов по защите критической информационной инфраструктуры. Для японских банков и операторов такие решения обеспечивают соответствие строгим стандартам информационной безопасности, включая международные нормы вроде PCI DSS и ISO/IEC 27001, а также долгосрочную защиту данных за счет фундаментальных законов квантовой физики, гарантирующих стойкость к атакам даже с использованием будущих квантовых компьютеров. При этом интеграция в существующую инфраструктуру и использование общих волокон позволяют сократить капитальные затраты на развертывание и упростить эксплуатацию, демонстрируя, как квантовая криптография может перейти из разряда экспериментальных технологий в практическую плоскость и обеспечивать высокий уровень безопасности при минимальных изменениях в действующей ИТ- и телеком-инфраструктуре.

3.5.4. Соединенные Штаты Америки

В США стратегия в области квантовой и постквантовой криптографии выстроена вокруг стандартизации и поэтапной миграции инфраструктуры – при этом приоритет отдан именно постквантовой криптографии (PQC), а не квантовому распределению ключей (QKD). Ключевую роль здесь играет NIST, который с 2016 года проводил многоэтапный конкурс алгоритмов и к 2024 году утвердил первые федеральные стандарты: FIPS 203 (на базе ML-KEM/CRYSTALS-Kyber) для инкапсуляции ключей, FIPS 204 (ML-DSA/CRYSTALS-Dilithium) для цифровых подписей и FIPS 205 (SLH-DSA/SPHINCS+) как резервную альтернативу на основе хэш-функций.

Эти стандарты уже интегрируются в ключевые программные стеки: Microsoft внедрила PQC-алгоритмы в библиотеку SymCrypt (используемую в Windows, Azure и Microsoft 365), Apple реализовала протокол PQ3 для сквозного шифрования в iMessage, а Zoom добавила постквантовое E2EE-шифрование в свои видеоконференции. Параллельно крупные облачные провайдеры (AWS, Google Cloud, IBM) участвуют в альянсе Post-Quantum Cryptography и развивают открытые реализации (например, библиотеку liboqs в рамках проекта Open QuantumSafe), чтобы ускорить внедрение.

При этом в США активно продвигаются гибридные схемы: в одном сеансе связи одновременно применяются классические алгоритмы (например, RSA или ECDSA) и постквантовые (ML-DSA или SPHINCS+), что снижает риски в случае уязвимости одного из компонентов. Такой подход особенно важен для защиты данных с длительным сроком конфиденциальности (государственные архивы, медицинские записи, интеллектуальная собственность), где актуальна угроза «собери сейчас – расшифруй потом».

Научно-исследовательская деятельность (R&D) сосредоточена в университетах и национальных лабораториях (Массачусетский технологический институт, NIST, Лос-Аламосская лаборатория), а также в партнерствах с индустрией: IBM и Google тестируют устойчивость криптографических протоколов к атакам с использованием собственных квантовых процессоров. При этом масштабное развертывание QKD-сетей в США развивается медленнее, чем PQC-стандартизация, – в первую очередь из-за высокой стоимости инфраструктуры и ограниченной дальности квантовых каналов.

3.5.5. Россия

В России развитие квантовой криптографии идет по пути интеграции в существующую телекоммуникационную инфраструктуру – с упором на магистральные и городские сети. Ключевым координатором выступает ОАО «РЖД», которое строит магистральную квантовую сеть: к концу 2024 года ее протяженность достигла 7 000 км, сеть, соединившая Москву, Санкт-Петербург, Нижний Новгород, Казань, Екатеринбург и другие крупные города. Эта сеть используется не только для передачи квантовых ключей, но и как объект для отработки совместимости с оборудованием операторов связи и корпоративных клиентов.

Параллельно развиваются городские квантовые сети в пилотных проектах с участием «Ростелекома», «ИнфоТеКС» и других компаний: например, тестируются каналы между дата-центрами в Москве и Удомле, а также между офисами банков и их филиалами. Особенность российских пилотов – ориентация на мультиплексирование: квантовые сигналы передаются по тем же волокнам, что и основной трафик, с разделением по длинам волн (DWDM-технологии), что снижает затраты на инфраструктуру.

Важным этапом стало появление сертифицированного оборудования: ФСБ России выдала сертификаты на квантово-криптографические системы от «ИнфоТеКС» и «СМАРТС-Квanттелеком», что позволяет использовать их в защищенных контурах госорганов и финансового сектора. Среди реализованных решений – «квантовый телефон» ViPNet QSS Phone (разработка «ИнфоТеКС» и Центра компетенций НТИ на базе МГУ), который обеспечивает защищенную голосовую связь за счет квантовых ключей. В научно-исследовательской сфере заметную роль играют университетские сети: межуниверситетская квантовая сеть объединяет МГУ, МИСИС, ТУСУР и другие вузы, где студенты и исследователи отрабатывают протоколы QKD, тестируют устойчивость к атакам и разрабатывают собственные алгоритмы. Кроме того, российские специалисты участвуют в международных экспериментах – например, в 2023 году был проведен сеанс квантово-защищенной связи между Россией и Китаем на расстоянии более 3 800 км с использованием спутниковых и наземных каналов.

Нормативно-техническая база формируется в рамках ТК 26 «Криптографическая защита информации» (технический комитет, созданный приказом Ростехрегулирования в 2007 году, где разрабатываются отечественные постквантовые алгоритмы (например, кандидаты «Шиповник» и «Гиперикум»), которые могут дополнить международные стандарты или стать альтернативой мим. При этом стратегия России предполагает комбинированный подход: QKD для защиты критически важных каналов (между дата-центрами, госорганами) и PQC для массовой миграции ИТ-систем, где установка квантового оборудования экономически нецелесообразна.

ГЛАВА 4. РОЛЬ МЕЖДУНАРОДНОГО СОЮЗА ЭЛЕКТРОСВЯЗИ (МСЭ) В ПОДДЕРЖКЕ РАЗВИТИЯ КВАНТОВОЙ КРИПТОГРАФИИ

4.1. История и структура Международного союза электросвязи

История Международного союза электросвязи (МСЭ, International Telecommunication Union, ITU) началась в 1865 году. Это одна из старейших ныне существующих международных организаций, специализирующаяся на вопросах информационно-коммуникационных технологий (ИКТ).

Необходимость в международной координации возникла с бурным развитием телеграфа. К середине XIX века телеграфные линии уже соединяли многие европейские страны, но их работа осложнялась из-за различий в национальных стандартах оборудования, тарифах и правилах обмена сообщениями. 17 мая 1865 года в Париже представители 20 государств, включая Российскую империю, подписали первую Международную телеграфную конвенцию и учредили Международный телеграфный союз. Эта дата позже была объявлена Всемирным днем электросвязи и информационного общества. В 1868 году на конференции в Вене было решено разместить бюро союза в Берне (Швейцария), причём штат бюро поначалу состоял всего из трех сотрудников.

В XX веке происходило расширение сферы деятельности: в 1906 году на Берлинской конференции была подписана первая Международная радиотелеграфная конвенция. В 1932 году на Мадридской конференции произошло слияние Международного телеграфного союза и Международного союза радиосвязи. Организация получила современное название – Международный союз электросвязи. В этот период МСЭ активно занимался распределением радиочастотного спектра, разработкой стандартов для телефонной связи и телевидения, а уже в 1947 году МСЭ получил статус специализированного учреждения ООН.

В 1992 году структура МСЭ была реформирована, и в организации были выделены три специализированных сектора, каждый из которых отвечает за отдельное направление деятельности:

1. **Сектор радиосвязи (ITU-R)** занимается рациональным использованием радиочастотного спектра и спутниковых орбит. В его структуру входят Бюро радиосвязи, выполняющее функции постоянного секретариата, исследовательские комиссии, изучающие технические вопросы и готовящие проекты рекомендаций, а также Радиорегламентарный комитет, который контролирует соблюдение международных правил использования частот и орбит. Деятельность сектора координируется Всемирными и региональными конференциями радиосвязи и Радиорегламентарным комитетом.
2. **Сектор стандартизации электросвязи (ITU-T)** разрабатывает международные технические стандарты и рекомендации в области телекоммуникаций и информационно-коммуникационных технологий.[41] Исследовательские комиссии сектора объединяют представителей государств, компаний и научного сообщества. Их работа охватывает широкий круг вопросов – от волоконно-оптических сетей и интернет-технологий до безопасности связи и квантовых коммуникаций. Деятельность ITU-T направляется Всемирной ассамблеей стандартизации электросвязи.
3. **Сектор развития электросвязи (ITU-D)** сосредоточен на развитии телекоммуникационной инфраструктуры и сокращении цифрового неравенства, прежде всего в развивающихся странах. Он оказывает техническую помощь, содействует подготовке специалистов и реализации проектов по развитию цифровой инфраструктуры. Работой сектора руководит Бюро развития электросвязи, возглавляемое директором, который избирается государствами-членами на Полномочной конференции МСЭ. Деятельность ITU-D определяется Всемирной конференцией по развитию электросвязи.

Исполнительную работу в каждом секторе обеспечивают соответствующие специализированные бюро. Их директора избираются государствами-членами и вместе с генеральным секретарем входят в Координационный комитет МСЭ, который обеспечивает согласованность деятельности всей организации.

Высшим органом управления МСЭ является Полномочная конференция МСЭ, которая созывается раз в четыре года для определения общей политики, принятия стратегических и финансовых планов, а также для проведения выборов высшего руководства организации. В периоды между этими конференциями главным управляющим органом выступает Совет МСЭ, состоящий из представителей государств-членов. Совет собирается ежегодно и осуществляет контроль за текущей деятельностью союза, координирует работу его подразделений и утверждает бюджет.

---

41 Technical Report ITU-T TR.qs-dlt. Guidelines for quantum-safe distributed ledger technology systems. Geneva : ITU-T, 2023. 40 p.

Непосредственное оперативное и административное руководство организацией возложено на генерального секретаря МСЭ, которому помогает заместитель генерального секретаря.

4.2. Инструменты МСЭ

МСЭ играет системообразующую роль в содействии внедрению квантовой криптографии и обеспечении устойчивости глобальных сетей связи перед лицом нарастающих киберугроз. В рамках своей миссии МСЭ консолидирует усилия государств, отраслевых игроков и научно-технического сообщества для формирования согласованной международной повестки в области квантовой и постквантовой безопасности.

Ключевыми инструментами реализации этой работы выступают рекомендации ITU-T, серии международных стандартов и технические отчеты, которые задают единые технические рамки для разработки и развертывания решений на базе QKD и смежных технологий.

Приоритетными направлениями деятельности МСЭ в этой сфере являются стандартизация интерфейсов и протоколов QKD, выработка процедур тестирования и сертификации оборудования, а также формирование рекомендаций по совместимости и интероперабельности – эти меры призваны обеспечить бесшовную интеграцию квантовых решений в существующие телекоммуникационные инфраструктуры и исключить фрагментацию глобального рынка.[42]

МСЭ содействует сбалансированному применению QKD и постквантовой криптографии для обеспечения устойчивости телекоммуникационных сетей к квантовым угрозам. QKD обеспечивает информационно-теоретическую безопасность за счет законов физики: любая попытка перехвата ключа фиксируется из-за изменения квантовых состояний. При этом технология требует специализированной инфраструктуры, ограничена по дальности и скорости генерации ключа и сложна в интеграции с классическими сетями.[43] Постквантовая криптография базируется на математических алгоритмах (на решетках, кодах, хэш-функциях), устойчивых к атакам квантовых компьютеров, и работает на стандартном оборудовании, легко встраиваясь в существующие протоколы (TLS, VPN). Однако ее применение может быть затруднено повышенной вычислительной нагрузкой, особенно на устройствах с ограниченными ресурсами.

---

42 Квантовая связь: использование спутниковых технологий : [Электронный ресурс] // RT. – URL: https://russian.rt.com/science/article/351688-kitai-sputnik-svyaz-kvantovyi-ispolzovanie (дата обращения: 10.09.2026).

43 Кузнецов И. Л. Квантовая криптография: роль в современном мире, перспективы развития / И. Л. Кузнецов, Н. А. Бобырь, С. М. Гурский, И. В. Бережной // 79-я научно-техническая конференция Санкт-Петербургского НТО РЭС им. А. С. Попова, посвященная Дню радио : сборник тезисов докладов. – Санкт-Петербург : СПбГЭТУ «ЛЭТИ», 2024. – С. 1–3.

4.3. Примеры внедрения рекомендаций МСЭ

Международный союз электросвязи также помогает разным странам адаптироваться к квантовым вызовам. Например, в Южной Африке местные исследователи из Стелленбошского университета и Совета по научно-промышленным исследованиям активно изучают квантово-устойчивую криптографию. МСЭ поддержал это направление. Организация помогла экспертам из страны подключиться к международным рабочим группам по стандартизации, чтобы их наработки учитывались при создании глобальных норм (в том числе в рамках ITU-T). В Кении акцент сместился на постквантовую криптографию. Страна начинает работать над стандартами и планирует постепенно внедрять их в уже работающие цифровые системы – в инфраструктуру для электронных платежей или госсервисы. Еще один пример – ОАЭ. В 2023 году телекоммуникационная компания Etisalat при поддержке МСЭ запустила пилотный проект: с партнером ID Quantique они развернули сеть квантовой криптографии внутри страны. Это показало, как МСЭ помогает местным компаниям преодолевать инфраструктурные барьеры – в данном случае интегрировать физически защищенную передачу ключей в коммерческую сеть.

При этом МСЭ не ограничивается лишь продвинутыми странами. Для государств с менее развитой цифровой базой подход иной: МСЭ сначала помогает заложить фундамент. Например, в ряде стран Африки организация акцентирует внимание на том, чтобы сначала расширить доступ к широкополосному интернету и обновить базовую телекоммуникационную инфраструктуру, и только потом переходить к сложным квантовым решениям. Так снижается риск того, что страна потратит ресурсы на высокотехнологичную систему, которая не сможет полноценно функционировать из-за отсутствия стабильной классической основы.

Отдельно стоит упомянуть программу «Bridging the Standardization Gap». Она целенаправленно работает с представителями из развивающихся стран: учит их эффективно участвовать в международных дискуссиях, формулировать позиции и вносить вклад в стандарты по QKD и постквантовой криптографии. Благодаря этому у стран появляется реальный голос в формировании правил игры, а не просто пассивное следование готовым решениям.

В итоге подход МСЭ комплексный: он сочетает обучение кадров, помощь в разработке национальных стратегий, практическую поддержку пилотных проектов и создание площадок для диалога. Это позволяет разным государствам двигаться к квантовой безопасности в своем темпе, опираясь на международные нормы и обмениваясь опытом.

ЗАКЛЮЧЕНИЕ

Таким образом, развитие цифровых технологий одновременно расширяет возможности международных коммуникаций и создает новые риски для их безопасности. Современные сети сталкиваются с большим количеством угроз – от кибератак и перехвата данных до более долгосрочного риска, связанного с развитием квантовых компьютеров. Это заставляет искать новые способы защиты информации и постепенно адаптировать существующую инфраструктуру.

Одним из таких направлений становится квантовая криптография, прежде всего технология квантового распределения ключей – QKD. Ее главное преимущество заключается в том, что безопасность передачи ключей связана не только со сложностью математических вычислений, но и с физическими свойствами квантовых систем. При этом QKD нельзя рассматривать как универсальное решение всех проблем кибербезопасности. Для ее эффективного применения необходимы надежное оборудование, защищенная инфраструктура, аутентификация и грамотная организация сети.

Сегодня основная проблема заключается в том, чтобы перейти от отдельных экспериментальных систем к масштабируемым сетям. Здесь важную роль могут сыграть разные типы каналов: оптоволоконные сети подходят для городских и региональных соединений, свободно-пространственные технологии – для передачи сигнала через атмосферу, а спутниковые системы позволяют создавать более протяженные, в том числе межконтинентальные, соединения. При этом сохраняются технические ограничения, прежде всего потери сигнала и ограниченная дальность передачи.

Не менее важен экономический вопрос. Квантовые технологии пока требуют значительных затрат на оборудование, обслуживание и обеспечение безопасности сетевой инфраструктуры. Поэтому их внедрение, скорее всего, будет происходить постепенно – прежде всего в тех сферах, где защита информации имеет критическое значение. Одновременно перспективным выглядит сочетание QKD с постквантовой криптографией. Такой подход позволяет использовать преимущества обеих технологий и не требует полной замены уже существующей инфраструктуры.

Опыт разных стран показывает, что единой модели развития квантовых коммуникаций пока не существует. Государства делают акцент на разных направлениях: от создания масштабных национальных QKD-сетей и спутниковых систем до разработки постквантовых алгоритмов, стандартов и коммерческих решений. При этом для всех подходов становится все более важной совместимость оборудования и технологий.

Именно поэтому международная стандартизация имеет особое значение. Без общих технических требований и стандартов будет сложно объединить национальные и коммерческие системы в единую глобальную инфраструктуру. В этом направлении важную роль играет Международный союз электросвязи, который способствует разработке стандартов, обеспечению совместимости технологий и формированию общих подходов к развитию квантовых коммуникаций.

Квантовая криптография уже перестала быть исключительно перспективной научной технологией и постепенно становится частью практической политики в сфере информационной безопасности. Однако ее широкое применение зависит не только от дальнейших научных открытий. Необходимы снижение стоимости оборудования, развитие инфраструктуры, международная стандартизация и подготовка к совместному использованию QKD и постквантовой криптографии.

Поэтому наиболее реалистичным сценарием развития методов защиты информации, основанных на квантовых технологиях, является не замена ими существующих систем, а постепенное формирование гибридной модели защиты, в которой классические, постквантовые и квантовые методы дополняют друг друга. Каждый метод и каждый протокол в классической и квантовой криптографии обладает определенными конкурентными преимуществами, обеспечивающими надёжное шифрование в специфических условиях. В то же время именно стремление к комбинированному подходу защиты информации, позволяющему учитывать условия, возможности и ресурсы всех участников диалога, представляет собой главную цель всех усилий в данной области.

ГЛОССАРИЙ

Апоцентр – наиболее удаленная от Земли точка орбиты космического аппарата.

Большая полуось – параметр орбиты, характеризующий ее размер; для эллиптической орбиты равен половине длины ее большой оси.

Высота орбиты – расстояние от поверхности Земли до космического аппарата на орбите.

Гибридная архитектура – архитектура сети, объединяющая несколько технологий передачи и защиты информации, например QKD, PQC, оптоволоконные, свободно-пространственные и спутниковые каналы.

Гибридная криптография – подход, при котором одновременно используются классические и постквантовые или квантовые механизмы защиты информации.

Дешифрование – процесс преобразования зашифрованных данных в открытые для чтения (хранения, использования) без знания ключа.

Доверенный узел – промежуточный сетевой узел, используемый для преодоления ограничений дальности QKD и требующий физической и организационной защиты от компрометации.

Затухание оптического сигнала – постепенное уменьшение мощности оптического сигнала при его распространении по каналу связи.

Интероперабельность – способность оборудования и систем разных производителей взаимодействовать и совместно работать на основе согласованных стандартов и протоколов.

Интерференция – наложение волн друг на друга, при котором они либо усиливают, либо ослабляют друг друга.

Информационно-теоретическая безопасность – уровень безопасности, основанный на фундаментальных свойствах физической системы и не зависящий исключительно от вычислительной сложности математических задач.

Квантовая запутанность – квантовое свойство системы, при котором состояния двух или более частиц связаны между собой настолько, что состояние одной мгновенно определяет состояние другой, даже на огромном расстоянии.

Квантовая криптография – направление криптографии, использующее физические законы квантовой механики для защиты информации.

Квантовое распределение ключей (QKD) – технология безопасного формирования и распределения криптографических ключей между участниками коммуникации с использованием квантовых состояний.

Квантовый канал связи – канал, предназначенный для передачи квантовых состояний между участниками квантовой коммуникации.

Квантовый ретранслятор – перспективное устройство квантовой сети, предназначенное для увеличения дальности передачи квантовой информации.

Кибератака – целенаправленные действия с использованием цифровых технологий для получения информации или воздействия на информационные системы.

Киберпреступление – действия одного или нескольких злоумышленников, направленные на атаку информационной системы с целью нарушения ее работы или получения финансовой выгоды.

Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Киберугроза – потенциальная опасность, направленная на нарушение конфиденциальности, целостности или доступности информационных систем, сетей и информации.

Критическая информационная инфраструктура – информационные и телекоммуникационные системы, нарушение работы которых может существенно повлиять на функционирование государства, экономики и общества.

Кубит – квантовый аналог классического бита, который может находиться в суперпозиции состояний 0 и 1.

Масштабируемость – способность квантовой сети расширяться по числу пользователей, узлов и расстоянию без непропорционального роста сложности и затрат.

МСЭ (ITU) – международная организация системы ООН, специализирующаяся на вопросах информационно-коммуникационных технологий, электросвязи и международной стандартизации.

Мультиплексирование – технология передачи нескольких потоков информации по одному физическому каналу с их разделением, например по длинам волн.

Наклонение орбиты – угол между плоскостью орбиты космического аппарата и плоскостью экватора Земли.

Оптоволоконный канал – канал связи, в котором информация передается посредством оптического сигнала по волоконно-оптическому кабелю.

Ортогональность – свойство, обобщающее понятие перпендикулярности на произвольные линейные пространства с введенным скалярным произведением: если скалярное произведение двух элементов пространства равно нулю, то они называются ортогональными друг другу.

Период обращения – время, необходимое космическому аппарату для совершения одного полного оборота вокруг Земли.

Перицентр – ближайшая к Земле точка орбиты космического аппарата.

Поляризация – это направленность колебаний вектора напряженности электрического поля световой волны в плоскости, перпендикулярной движению фотона.

Постквантовая криптография (PQC) – направление криптографии, использующее классические алгоритмы, устойчивые к атакам с применением квантовых компьютеров.

Принцип невозможности клонирования – фундаментальный принцип квантовой механики, согласно которому неизвестное произвольное квантовое состояние невозможно точно скопировать.

Протокол B92 – протокол квантового распределения ключей, использующий два квантовых состояния для кодирования битов.

Протокол BB84 – протокол квантового распределения ключей, основанный на передаче фотонов в различных состояниях поляризации.

Протокол E91 – протокол квантового распределения ключей, основанный на использовании запутанных пар фотонов и измерении их квантовых состояний.

Расшифрование – процесс преобразования зашифрованного сообщения в открытый текст, при известном ключе шифрования.

Свободно-пространственная оптическая связь (FSO) – передача квантовых сигналов непосредственно через атмосферу без использования физического кабеля.

Сертификация – процесс официального подтверждения соответствия оборудования или системы установленным требованиям безопасности и техническим стандартам.

Совокупная стоимость владения (TCO) – общая стоимость использования системы, включающая первоначальные капитальные затраты, эксплуатацию, обслуживание, модернизацию, энергопотребление и инфраструктурные расходы.

Спутниковая QKD – архитектура квантового распределения ключей, при которой спутник используется как квантовый коммуникационный узел между удаленными наземными станциями.

Стандартизация – процесс разработки и установления единых технических требований, стандартов и правил для обеспечения совместимости и безопасности систем.

Суперпозиция – квантовое состояние, при котором кубит может описываться комбинацией состояний 0 и 1 до момента измерения.

Трансграничный трафик – передача данных через государственную границу, при которой информация проходит через инфраструктуру или юрисдикцию другого государства.

Фишинг – вид атаки, при котором злоумышленник обманом пытается получить конфиденциальные данные пользователя, выдавая себя за доверенную организацию.

Элементы орбиты – параметры, которые описывают положение и движение космического аппарата на орбите.

C-диапазон (C-band) – оптический диапазон телекоммуникационных систем с длинами волн примерно 1530–1565 нм, широко используемый в волоконно-оптических сетях благодаря низким потерям сигнала в оптическом волокне.

DoS-атака – атака, при которой создается избыточная нагрузка на сеть или сервер, в результате чего система становится недоступной или перестает нормально работать.

DWDM – технология спектрального уплотнения каналов, позволяющая передавать несколько информационных потоков по одному оптическому волокну на разных длинах волн.

Harvest Now, Decrypt Later («Собери сейчас – расшифруй потом») – стратегия, при которой злоумышленник заранее собирает зашифрованные данные для их последующей расшифровки после появления более мощных вычислительных возможностей.

ITU-T – сектор стандартизации электросвязи Международного союза электросвязи, разрабатывающий международные технические стандарты в области телекоммуникаций и ИКТ.

Man-in-the-Middle (MITM) – атака, при которой злоумышленник перехватывает данные во время их передачи, выступая скрытым посредником между участниками коммуникации.

MDI-QKD – протокол квантового распределения ключей, разработанный для устранения уязвимостей, связанных с измерительным оборудованием.

O-диапазон (O-band) – оптический диапазон телекоммуникационных систем с длинами волн примерно 1260–1360 нм, используемый, в частности, в волоконно-оптической связи.

Q-KMS – система управления квантовыми ключами, отвечающая за их маршрутизацию, распределение, ротацию и доставку конечным шифраторам.

QBER (Quantum Bit Error Rate) – показатель количества ошибок в переданных квантовых битах, используемый для оценки качества и безопасности квантового канала.

SQL-инъекция – кибератака, при которой злоумышленник использует уязвимости приложений для внедрения вредоносного кода в системы управления базами данных.

Twin-Field QKD (TF-QKD) – семейство протоколов квантового распределения ключей, предназначенных для повышения дальности и скорости распределения ключей за счет использования интерференции оптических полей.