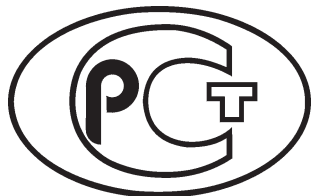

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



ПРЕДВАРИТЕЛЬНЫЙ
НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ПНСТ
829—
2023

КВАНТОВЫЕ КОММУНИКАЦИИ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2023

Предисловие

1 РАЗРАБОТАН Автономной некоммерческой образовательной организацией «Сколковский институт науки и технологий» (Сколтех) и Федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский университет ИТМО» (Университет ИТМО)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 194 «Кибер-физические системы»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 11 июля 2023 г. № 22-пнст

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: 121205 Москва, Инновационный центр Сколково, ул. Нобеля, д. 1, e-mail: info@tc194.ru и/или в Федеральное агентство по техническому регулированию и метрологии по адресу: 123112 Москва, Пресненская набережная, д. 10, стр. 2.

В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

© Оформление. ФГБУ «Институт стандартизации», 2023

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения	1
2 Нормативные ссылки	1
3 Термины и определения	2
4 Сокращения	2
5 Общие положения	2
Библиография	12

Введение

Настоящий стандарт содержит основные положения в области квантовых коммуникаций: принципы передачи информации по квантовым каналам, основные подходы к построению квантовых сетей и их использованию для передачи информации, в том числе для квантового распределения ключей, основные подходы к реализации квантовых сетей различных топологий, а также основные принципы сопряжения сетей квантового распределения ключей с квантовозащищенными сетями связи.

Необходимость разработки стандарта вызвана потребностью в создании информационно-коммуникационных систем на основе квантовых коммуникаций и их интеграции в существующую телекоммуникационную инфраструктуру.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

КВАНТОВЫЕ КОММУНИКАЦИИ

Общие положения

Quantum communications. General principles

Срок действия — с 2023—09—01
до 2026—09—01**1 Область применения**

Настоящий стандарт определяет:

- основные положения и принципы в области квантовых коммуникаций;
- типовые схемы построения квантовых сетей;
- общие принципы использования квантовых сетей для решения задач квантового распределения ключей;
- общие принципы сопряжения сетей квантового распределения ключей с квантовозащищенными сетями связи.

Настоящий стандарт не устанавливает требований:

- к технической реализации и построению систем квантового распределения ключей;
- способу формирования квантового и/или квантовозащищенного ключа.

Примечание — При разработке систем квантового распределения ключей должны быть использованы соответствующие документы, разработанные в рамках ТК 26 «Криптографическая защита информации» и иные документы, определенные действующим законодательством в сфере разработки средств криптографической защиты информации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ПНСТ 830—2023 Квантовые коммуникации. Термины и определения

ПНСТ 799—2022 Информационные технологии. Криптографическая защита информации. Термины и определения

ГОСТ Р 54417 Компоненты волоконно-оптических систем передачи. Термины и определения

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ПНСТ 830—2023, ПНСТ 799—2022 и ГОСТ Р 54417.

4 Сокращения

В настоящем стандарте использованы следующие сокращения:

ДПУ — доверенный промежуточный узел;

ЕТСИ — Европейский институт по стандартизации в области электросвязи;

КДСЧ — квантовый датчик (генератор) случайных чисел;

КЗК — квантовозащищенный ключ;

КЗСС — квантовозащищенная сеть связи;

КК — квантовый ключ;

КРК — квантовое распределение ключей;

МУК — модуль управления ключами;

ПКП — протокол квантовой передачи;

СКЗИ — средство криптографической защиты информации;

СУК — система управления ключами;

CWDM — неплотное мультиплексирование с разделением по длине волны/разреженное спектральное уплотнение (Coarse Wavelength Division Multiplexing);

DWDM — плотное мультиплексирование с разделением по длине волны/плотное спектральное уплотнение (Dense Wavelength Division Multiplexing);

TDM — временное мультиплексирование (Time Division Multiplexing).

5 Общие положения

5.1 Квантовые коммуникации

Квантовые коммуникации — это передача информации посредством прямой передачи квантовых состояний или посредством квантовой запутанности. Основным носителем информации в квантовых коммуникациях являются квантовые системы, состояния которых кодируются (изменяются) в соответствии с передаваемой информацией. Сигнал, описываемый квантовым состоянием, является квантовым сигналом.

В квантовых коммуникациях в настоящее время в качестве квантовой системы для передачи информации используются фотоны, а основными системами передачи квантовой информации являются квантовые оптические системы.

В простейшем случае единицей представления квантовой информации служит кубит. Кубит является кудитом, для которого размерность квантовой системы, которой он описывается, составляет $d = 2$. Математически кудит описывается вектором в комплексном d -мерном гильбертовом пространстве, соответственно кубит — вектором в двухмерном комплексном гильбертовом пространстве.

В квантовых коммуникациях для передачи квантовых сигналов используют квантовые передатчики, квантовые приемники и квантовые каналы.

Квантовый передатчик обеспечивает приготовление и передачу квантовых сигналов по квантовому каналу, а квантовый приемник — прием из квантового канала и обработку квантовых сигналов.

Квантовый канал представляет собой канал связи, по которому передаются квантовые сигналы. В зависимости от схемы реализации квантовый канал может быть однонаправленным или двунаправленным. Передача информации по квантовому каналу выполняется в соответствии с ПКП. На физическом уровне кодирование квантовой информации возможно на дискретных или непрерывных переменных.

В квантовых оптических системах квантовый канал может быть реализован на базе волоконно-оптических каналов связи или беспроводных оптических каналов (например, атмосферно-оптических каналов связи, оптических спутниковых каналов или подводных оптических каналов). Оптический спутниковый квантовый канал может быть реализован на различных спутниках (например, низкоорбитальных, среднеорбитальных, геостационарных спутниках или спутниках на высокоэллиптической орбите).

Для обеспечения функционирования квантового канала необходим канал для синхронизации передающего и приемного оборудования квантового передатчика и квантового приемника (канал син-

хронизации), а также канал для передачи информации, необходимой для работы протокола квантовой передачи (служебный канал).

Квантовые передатчик и приемник совместно с квантовым каналом, каналом синхронизации и служебным каналом образуют систему квантовой коммуникации.

В системе квантовой коммуникации служебный канал и канал синхронизации могут быть реализованы с помощью любых классических (неквантовых) средств связи.

Типовая схема системы квантовой коммуникации представлена на рисунке 1, в [1], [2].

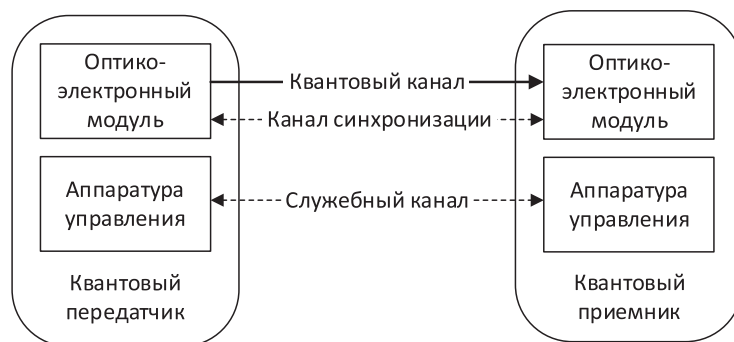


Рисунок 1 — Типовая схема системы квантовой коммуникации

Квантовый передатчик представляет собой программно-аппаратный комплекс, включающий оптико-электронный модуль, обеспечивающий формирование (генерацию и кодирование) квантового сигнала с заданными характеристиками и его передачу в квантовый канал, а также аппаратуру управления, осуществляющую управление элементами квантового передатчика и реализацию ПКП.

Квантовый приемник представляет собой программно-аппаратный комплекс, включающий оптико-электронный модуль, обеспечивающий прием и регистрацию квантового сигнала и его декодирование, а также аппаратуру управления, осуществляющую управление элементами квантового приемника и реализацию ПКП.

В зависимости от конкретной схемы реализации системы квантовой коммуникации допускается совмещение в одном устройстве функций квантового передатчика и квантового приемника, а также использование нескольких квантовых приемников или квантовых передатчиков.

5.2 Квантовые сети

Квантовая коммуникационная сеть (далее — квантовая сеть) — технологическая система, включающая средства и линии связи, предназначенные для передачи квантовой информации.

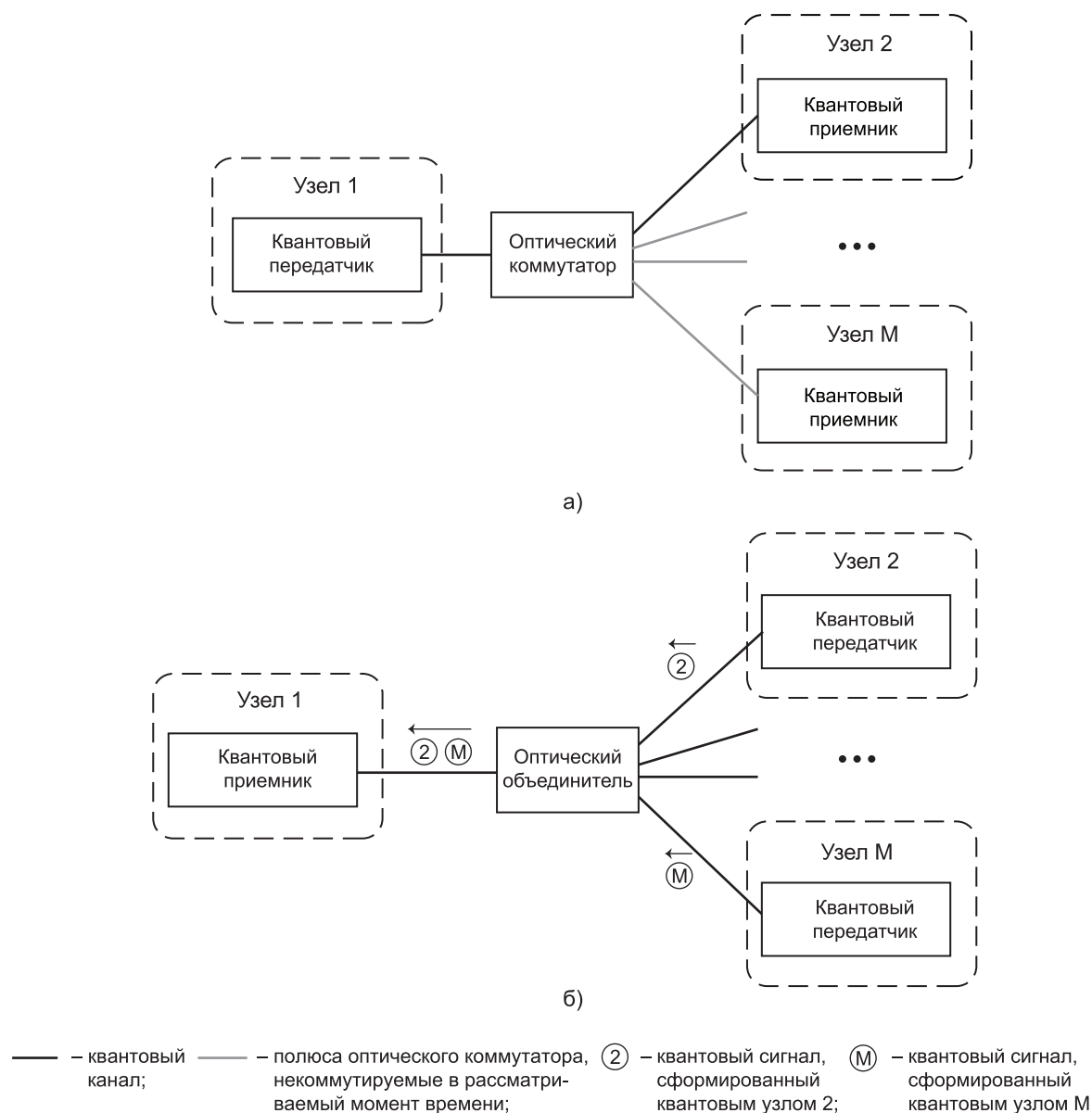
Квантовая сеть образована из узлов, которые могут передавать, принимать или распределять квантовую информацию. Узлы квантовой сети соединены между собой квантовыми каналами и классическими каналами связи для обмена служебной информацией, включая информацию о принимаемых и передаваемых квантовых сигналах, а также для синхронизации квантового оборудования.

Квантовая сеть может реализовывать различные функции передачи квантовой информации, например: квантовую телепортацию, сверхплотное кодирование, квантовое распределение ключей и др. Система квантовой коммуникации, показанная на рисунке 1, является простейшей реализацией квантовой сети из двух узлов топологии «точка—точка».

Для организации квантовых сетей топологии «один-ко-многим» для коммутации квантовых каналов допустимо использование оптических коммутаторов (активные оптические элементы) (см. ГОСТ Р 54417). На рисунке 2 а) показана квантовая сеть топологии «один-ко-многим» в конфигурации $1 \times N$ (N — целое число больше 1). В более общем случае могут быть использованы многопозиционные оптические коммутаторы конфигурации $M \times N$ (M и N целые числа больше 1), а также несколько соединенных между собой оптических коммутаторов. При необходимости, аналогичным образом обеспечивается коммутация каналов синхронизации и служебных каналов.

Для объединения квантовых сигналов, поступающих от нескольких квантовых передатчиков к одному квантовому приемнику, допустимо использование оптических объединителей (пассивные элементы) (см. ГОСТ Р 54417). При этом необходимо, чтобы к входным полюсам оптического объединителя были подключены только квантовые передатчики, а к выходному полюсу оптического объединителя

может подключаться только квантовый приемник. Пример такой схемы квантовой сети показан на рисунке 2 б).



Коммутация служебного канала и канала синхронизации (на рисунке не показаны) может осуществляться аналогично с использованием отдельных оптических коммутаторов или не осуществляться при их прямой передаче между квантовыми приемниками и квантовыми передатчиками

Рисунок 2 — Пример схемы организации соединений квантового канала в квантовой сети с использованием
а) оптических коммутаторов б) оптических объединителей

В случае применения оптического коммутатора и оптического объединителя схема информационного обмена аналогична организации TDM. Коммутатор квантовых каналов может быть реализован как отдельное устройство или входить как составная часть в квантовый передатчик или приемник, квантовый объединитель может быть реализован как отдельное устройство или быть составной частью квантового приемника.

При построении квантовой сети допустимо использование CWDM, DWDM квантовых каналов в одном оптическом канале, а также частотное мультиплексирование квантовых каналов с каналами синхронизации, служебными каналами и иными информационными каналами. Для этого в состав оптических каналов, по которым передаются квантовые сигналы, должны включаться оптические мульт-

типлексоры и демультиплексоры. В квантовых каналах не допускается выполнение преобразований, не предусмотренных ПКП и нарушающих свойства квантовых сигналов (таких как оптическое усиление квантового сигнала или его промежуточное преобразование в электронную форму и обратно).

Квантовый канал имеет предельную дальность, определяемую физическими характеристиками среды передачи квантовых сигналов, характеристиками квантового передатчика и квантового приемника, а также ПКП. Для увеличения дальности передачи квантового сигнала могут быть использованы квантовые повторители, которые представляют собой комплекс устройств, расположенных в одном или нескольких узлах квантовой сети, обеспечивающий ретрансляцию квантового сигнала посредством распределения квантовой запутанности и квантовой телепортации.

Квантовый повторитель может рассматриваться либо как единое устройство, которое получает квантовый сигнал, используя методы квантовой коррекции ошибок, компенсирует потери в канале и передает информацию дальше по исходящему квантовому каналу, как показано на рисунке 3, либо как совокупность нескольких разнесенных в пространстве устройств, например: узла с источником запутанных квантовых состояний и непосредственно узла, в котором осуществляется измерение Белла, за которым следует распределение запутанности.

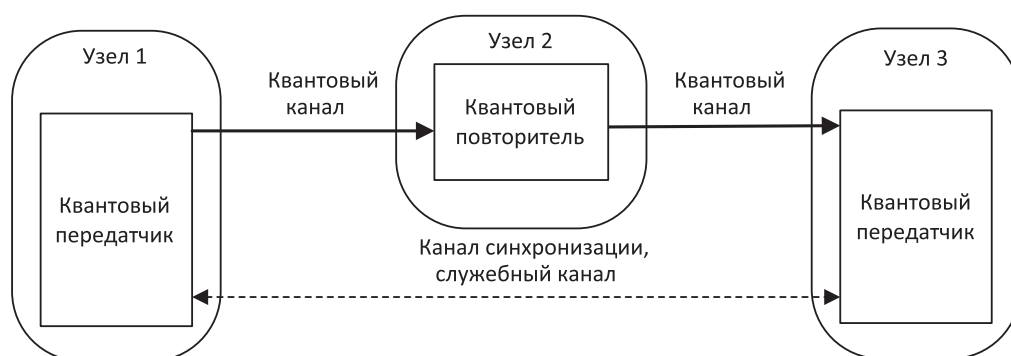


Рисунок 3 — Принципиальная схема квантовой сети типа «точка—точка» с применением квантового повторителя

В общем случае в состав квантовой сети входят:

- узлы квантовой сети, представляющие собой устройства, обрабатывающие квантовую информацию (например, квантовые компьютеры), и связанные с ними квантовые приемники и/или квантовые передатчики;
- узлы квантовой сети с квантовыми повторителями;
- узлы квантовой сети с квантовыми роутерами, представляющие собой квантовые повторители, имеющие несколько входов и/или выходов и обеспечивающие возможность маршрутизации квантовых сигналов;
- узлы квантовой сети с оптическими коммутаторами или оптическими объединителями;
- квантовые каналы (для передачи квантовой информации);
- классические каналы (для организации каналов синхронизации и служебных каналов);
- система управления и мониторинга квантовой сетью.

С использованием квантовых повторителей и квантовых роутеров, а также оптических коммутаторов и оптических объединителей возможно построение квантовых сетей различных топологий: «цепь», «звезда», «кольцо», «дерево», смешанная топология. На рисунке 4 представлена принципиальная схема квантовой сети смешанной топологии.

Несколько последовательно соединенных квантовых повторителей, обеспечивающих увеличение дальности передачи квантовой информации, образуют магистральный сегмент квантовой передачи. В состав квантовой сети может входить несколько отдельных магистральных сегментов квантовой передачи. Различные магистральные сегменты квантовой передачи могут быть объединены с использованием квантовых роутеров или оптических коммутаторов, которые являются управляемыми элементами. В зависимости от команд маршрутизации, поступающих от системы управления и мониторинга квантовой сетью, они обеспечивают связность отдельных магистральных сегментов квантовой передачи.

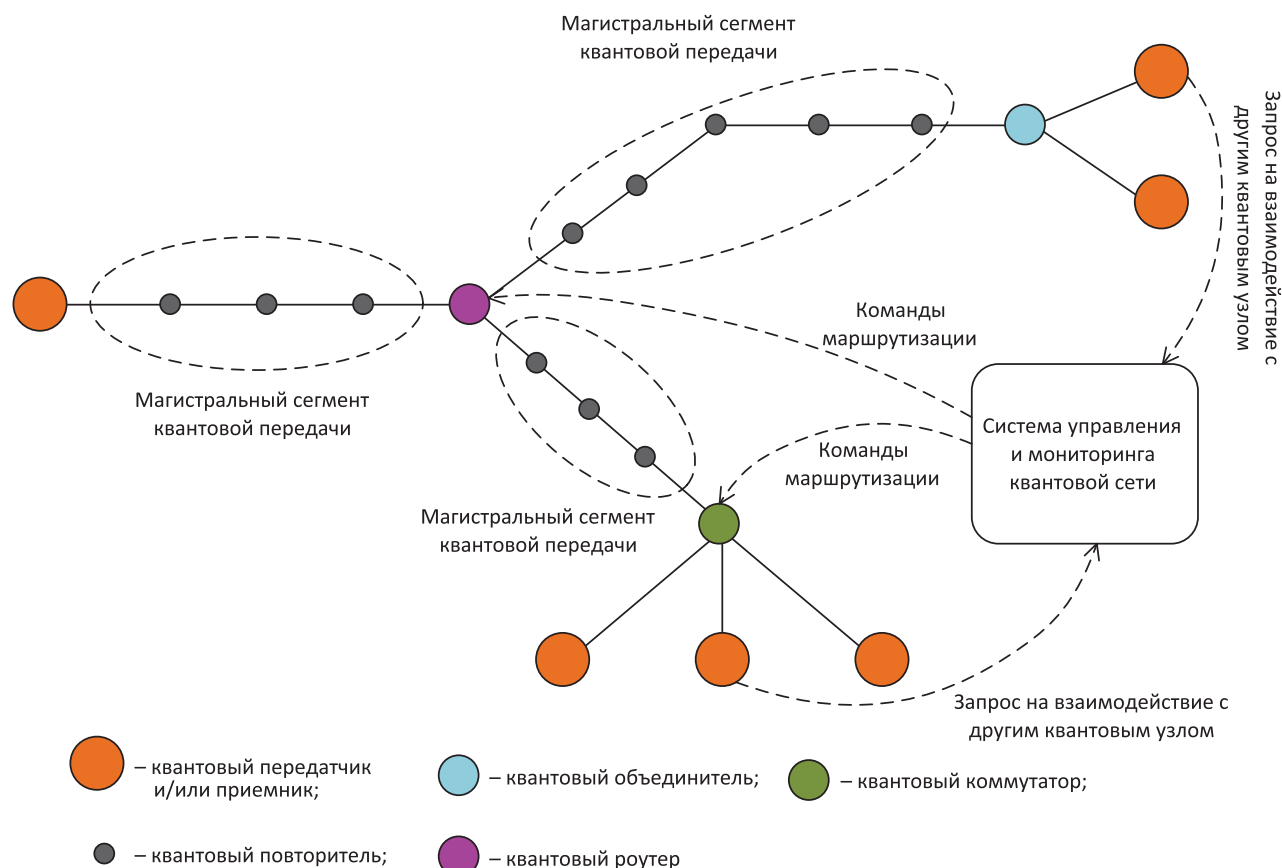


Рисунок 4 — Принципиальная схема квантовой сети смешанной топологии (с квантовыми повторителями и оптическими коммутаторами/объединителями)

Система управления и мониторинга квантовой сетью обеспечивает мониторинг статуса и управление узлами квантовой сети и входящими в них устройствами. В системе управления и мониторинга команды маршрутизации могут формироваться по запросам от узлов квантовой сети на взаимодействие с другими узлами.

5.3 Сети квантового распределения ключей

Сеть КРК — квантовая сеть, реализующая КРК.

Схему расположения и соединения квантовых передатчиков и приемников в сети КРК определяют с учетом выбранного протокола КРК.

Простейшая сеть КРК топологии «точка—точка» состоит из двух модулей КРК, формирующих КК (рисунок 5). Модули КРК соединяются квантовым каналом, каналом синхронизации и служебным каналом. Канал синхронизации необходим для передачи сигнала синхронизации между модулями КРК, а служебный канал — для передачи служебной информации между модулями КРК в соответствии с протоколом КРК.

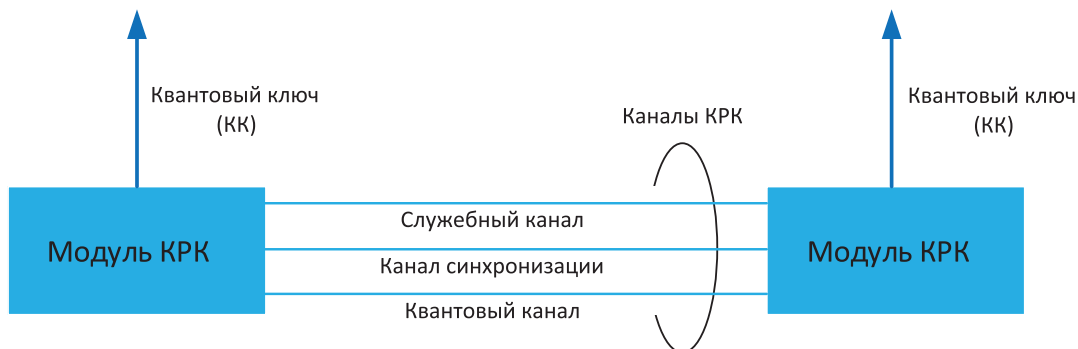


Рисунок 5 — Сеть КРК топологии «точка—точка»

Для организации сетей КРК более сложных топологий и обеспечения многопользовательского взаимодействия, а также в случае расположения узлов на расстоянии, превышающем предельную дальность квантового канала, используют два подхода.

При первом подходе сеть КРК реализуют по принципу квантовой сети на основе квантовых повторителей (рисунок 4). В данном случае квантовые повторители являются недоверенными узлами сети КРК. При этом узлы сети КРК, вырабатывающие в паре с другими узлами сети КРК КК, являются доверенными узлами.

Когда применение квантовых повторителей невозможно, используют построение сетей КРК на основе ДПУ. Эквивалентным термином для ДПУ является термин «промежуточный опорный узел». В сети КРК на основе ДПУ КК формируются только между связанными квантовым каналом узлами сети КРК, а между несвязанным квантовым каналом узлами сети КРК формируются КЗК.

В общем случае в сети КРК на основе ДПУ могут быть выделены следующие уровни:

- уровень квантовых ключей;
- уровень управления ключами;
- уровень управления и мониторинга сетью КРК.

Каждый из уровней сети имеет ограниченный функционал, который может быть реализован отдельными устройствами, в том числе устройствами разных производителей.

Типовая структура сети КРК на основе ДПУ представлена на рисунке 6.

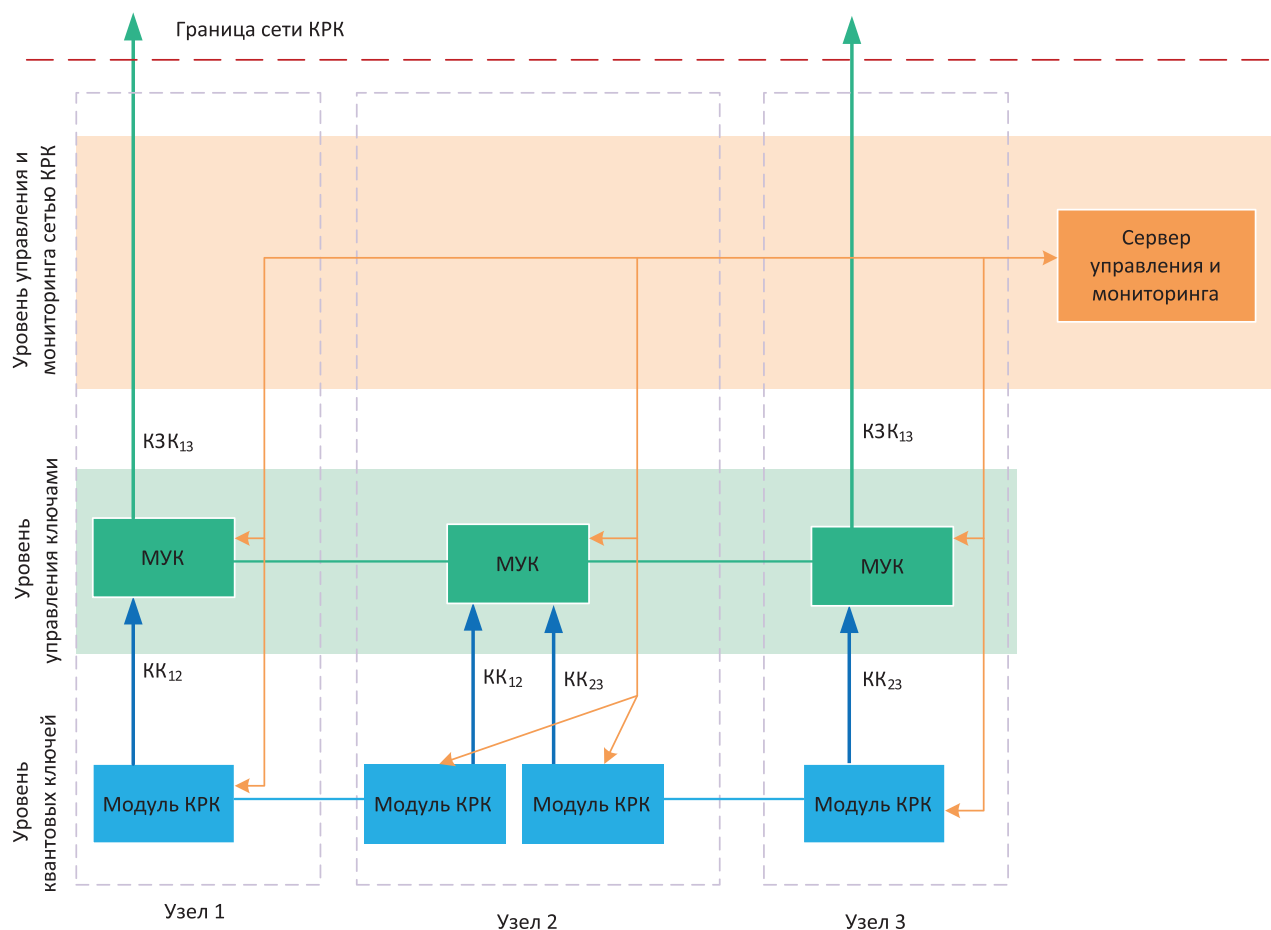


Рисунок 6 — Типовая структура сети КРК на основе ДПУ

На уровне КК осуществляется выработка КК между входящими в состав одной системы КРК модулями КРК, расположенными в разных узлах сети КРК. После выработки КК каждым из модулей КРК осуществляется их выдача в СУК, представленную в виде совокупности отдельных модулей, расположенных в узлах сети КРК — МУК.

МУК относятся к уровню управления ключами и отвечают за формирование КЗК между узлами сети КРК, не имеющими общего квантового канала. Помимо формирования КЗК МУК обеспечивают прием КК от сопряженных с ними модулей КРК, а также управление жизненным циклом КК и КЗК.

Узлы сети КРК, в которых осуществляется выдача КК и/или КЗК потребителям, называются целевыми доверенными узлами (целевые ДУ). Эквивалентным термином для целевых ДУ является термин «опорный узел». ДПУ участвуют в выработке КЗК между целевыми ДУ. Несколько последовательно соединенных ДПУ, объединяющие пару целевых ДУ, образуют магистральный сегмент сети КРК.

Уровень управления и мониторинга сетью КРК обеспечивает управление входящими в состав сети КРК устройствами (МУК, модули КРК, необходимое для функционирования сети КРК телекоммуникационное и вспомогательное инженерно-техническое оборудование) и мониторинг их состояния. Управление может быть осуществлено как централизованно, например с использованием одного сервера управления и мониторинга, так и децентрализованно, в том числе с использованием отдельных систем управления и мониторинга для устройств сети КРК (например, отдельной системы управления и мониторинга для модулей КРК).

В зависимости от архитектуры и назначения сети КРК допускается совмещение функций разных уровней в одном или нескольких устройствах.

В сети КРК с ДПУ КЗК могут формироваться различными способами.

Возможна передача МУК КК, получаемых ими от модулей КРК, по сети КРК в зашифрованном виде (рисунок 7). В данном случае модули КРК генерируют ключи $КК_{12}$ (между узлом 1 и узлом 2) и $КК_{23}$ (между узлом 2 и узлом 3) и передают их в МУК. В узле 2 МУК зашифровывает $КК_{12}$ с помощью $КК_{23}$ и передает его в узел 3. Таким образом, узел 1 и узел 3 получают общий квантовозащищенный ключ $КЗК_{12}$, равный $КК_{12}$.

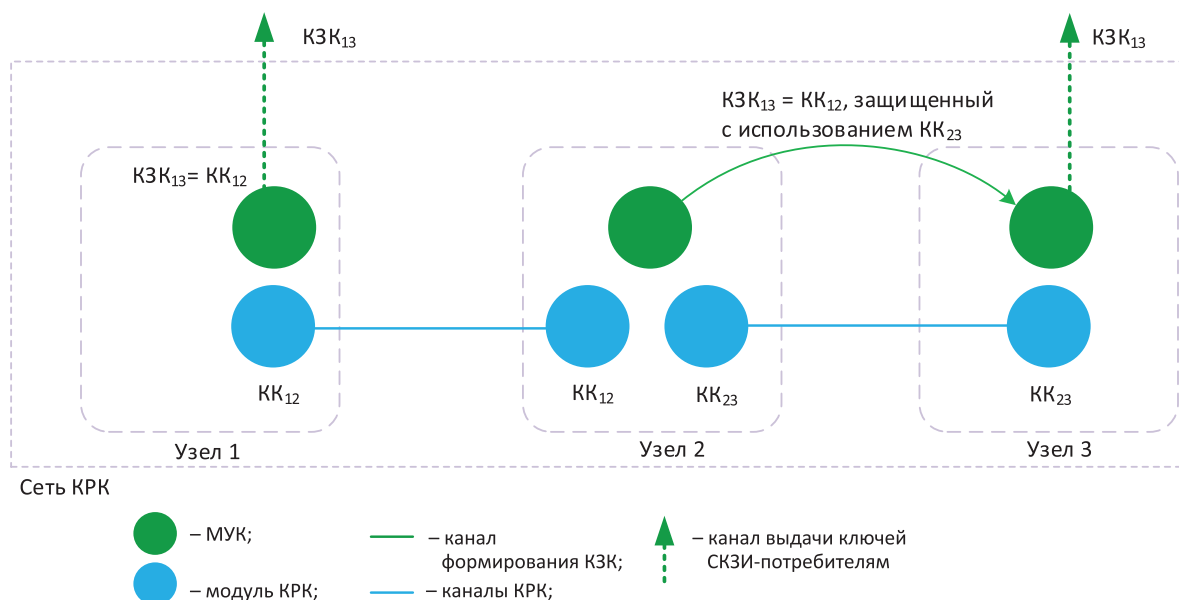


Рисунок 7 — Пример использования ДПУ для формирования КЗК в сети КРК

КЗК может быть сформирован с применением КДСЧ. На рисунке 8 показан пример пересылки выработанного КДСЧ, расположенного в узле 1, ключа $КЗК_{13}$ между узлом 1 и узлом 2 в защищенном виде с использованием для защиты $КК_{12}$, который сформирован между узлом 1 и узлом 2, с дальнейшей пересылкой между узлом 2 и узлом 3 в защищенном виде с использованием для защиты $КК_{23}$, который сформирован между узлом 2 и узлом 3.

Сеть КРК может иметь произвольные топологии, в том числе с наличием нескольких альтернативных возможных путей формирования КЗК между парой узлов сети КРК. Пример такой сети КРК смешанной топологии показан на рисунке 9. Между узлом 2 и узлом 4 $КЗК_{24}$ может быть сформирован по маршруту с наименьшим числом узлов (узел 2) → (узел 3) → (узел 4) или по альтернативному маршруту (узел 2) → (узел 1) → (узел 6) → (узел 4).

Для организации различных произвольных топологий сети КРК между узлами КРК могут быть использованы оптические коммутаторы, обеспечивающие коммутацию оптических каналов (на рисунке 9 коммутатор указан для соединения узла 4 с двумя узлами сети КРК: узлом 6 и узлом 7). Аналогично могут быть использованы оптические объединители.

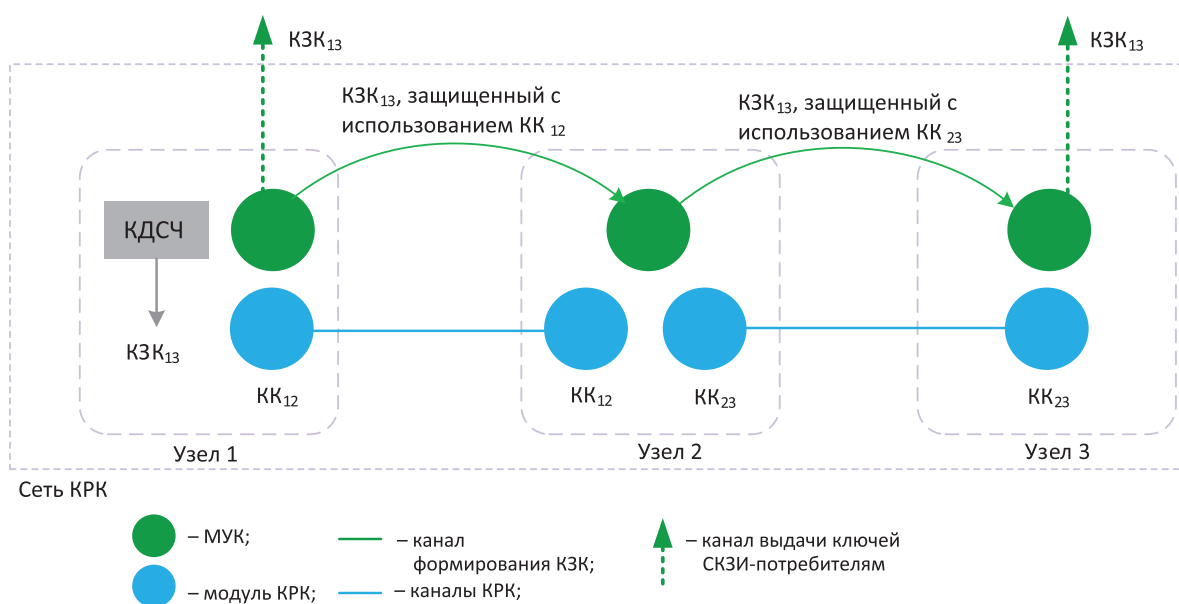


Рисунок 8 — Пример формирования КЗК в сети КРК с использованием КДСЧ

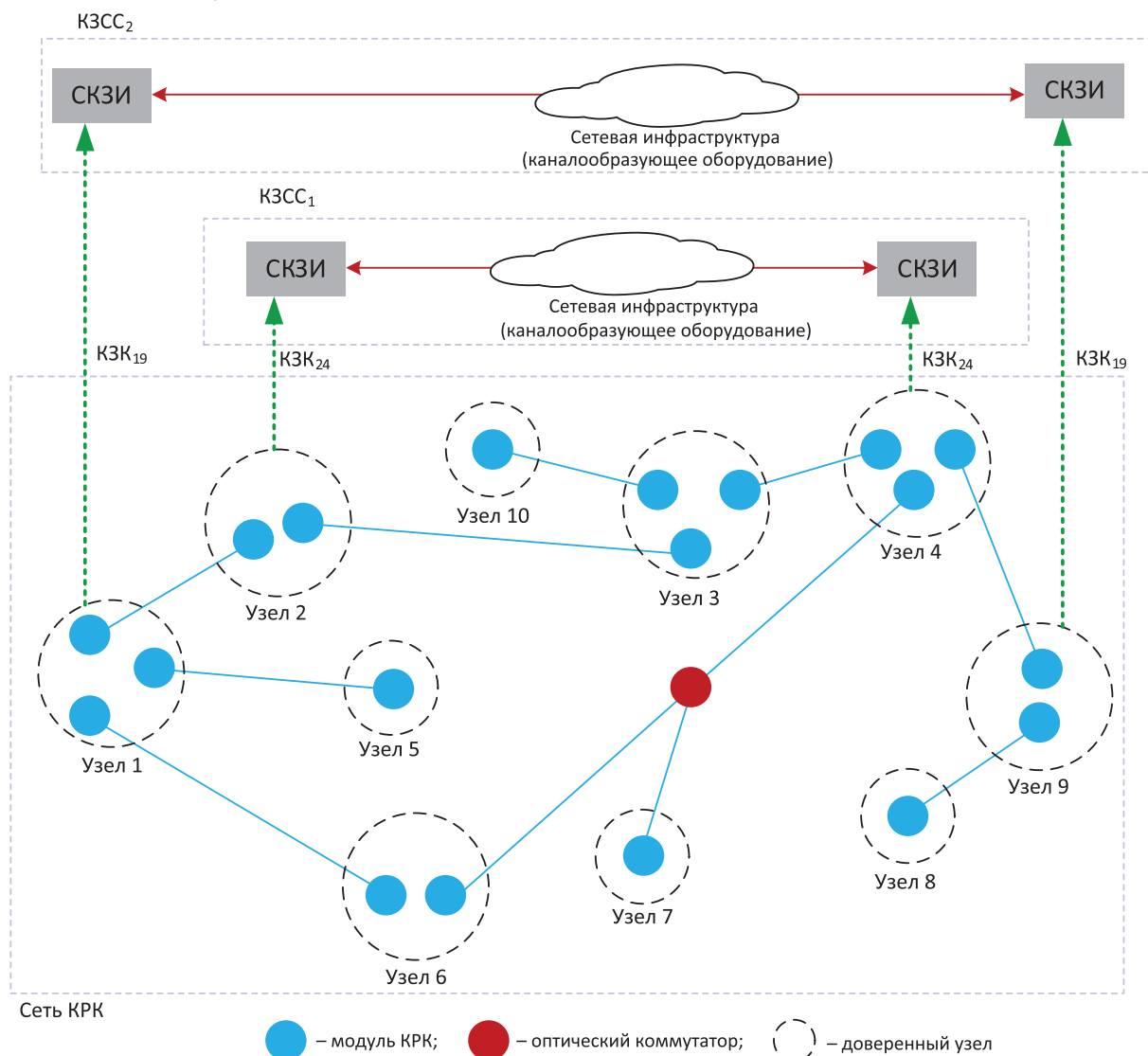


Рисунок 9 — Пример сети КРК произвольной конфигурации, обеспечивающей формирование КЗК для двух КЗСС

Сеть КРК может обеспечивать выдачу КК/КЗК в разные пары СКЗИ (парные СКЗИ—потребители), расположенные в независимых друг от друга КЗСС. На рисунке 9 приведен пример, когда узел 2 и узел 4 сети КРК обеспечивают выдачу $КЗК_{24}$ в парные СКЗИ, расположенные в $КЗСС_1$, а узел 1 и узел 9 обеспечивают выдачу $КЗК_{19}$ в парные СКЗИ, расположенные в $КЗСС_2$.

5.4 Квантовозащищенные сети связи

Сеть связи, в которой обеспечена защищенная передача данных с использованием СКЗИ—потребителей, получающих криптографические ключи от сети КРК, называется КЗСС. В общем случае КЗСС является внешней сетью по отношению к сети КРК.

Можно выделить три способа организации квантовозащищенной передачи данных в КЗСС:

- с использованием КЗК: общий КЗК поступает в парные СКЗИ—потребители КЗСС непосредственно из КРК, которые в дальнейшем осуществляют защищенную передачу данных по произвольному маршруту. Пример такой сети КЗСС показан на рисунке 10 а). В этом случае $КК_{12}$, формируемые между узлом 1 и узлом 2, и $КК_{23}$, формируемые между узлом 2 и узлом 3, используются для защищенной передачи $КЗК_{13}$, которые впоследствии передаются в парные СКЗИ—потребители КЗСС;
- с использованием КК: в сети КРК не формируются КЗК между парными СКЗИ—потребителями КЗСС, а происходит выдача КК в каждом из узлов сети КРК в СКЗИ, расположенные в узлах КЗСС, повторяющей топологию сети КРК. В таком случае защищаемые данные последовательно передаются через цепочку промежуточных узлов КЗСС, в каждом из которых происходит их перешифрование с использованием различных КК. Пример такой КЗСС из трех узлов показан на рисунке 10 б). В этом случае $КК_{12}$, формируемые между узлом 1 и узлом 2, выдаются из узла 1 в СКЗИ₁ и из узла 2 в СКЗИ₂, а $КК_{23}$, формируемые между узлом 2 и узлом 3, выдаются из узла 2 в СКЗИ₂ и из узла 3 в СКЗИ₃. В КЗСС при передаче данных между СКЗИ₁ и СКЗИ₂ они защищаются с использованием $КК_{12}$, а при передаче данных между СКЗИ₂ и СКЗИ₃ они защищаются с использованием $КК_{23}$;
- комбинированный: реализуется комбинация с использованием КЗК и КК на отдельных сегментах сети КЗСС.

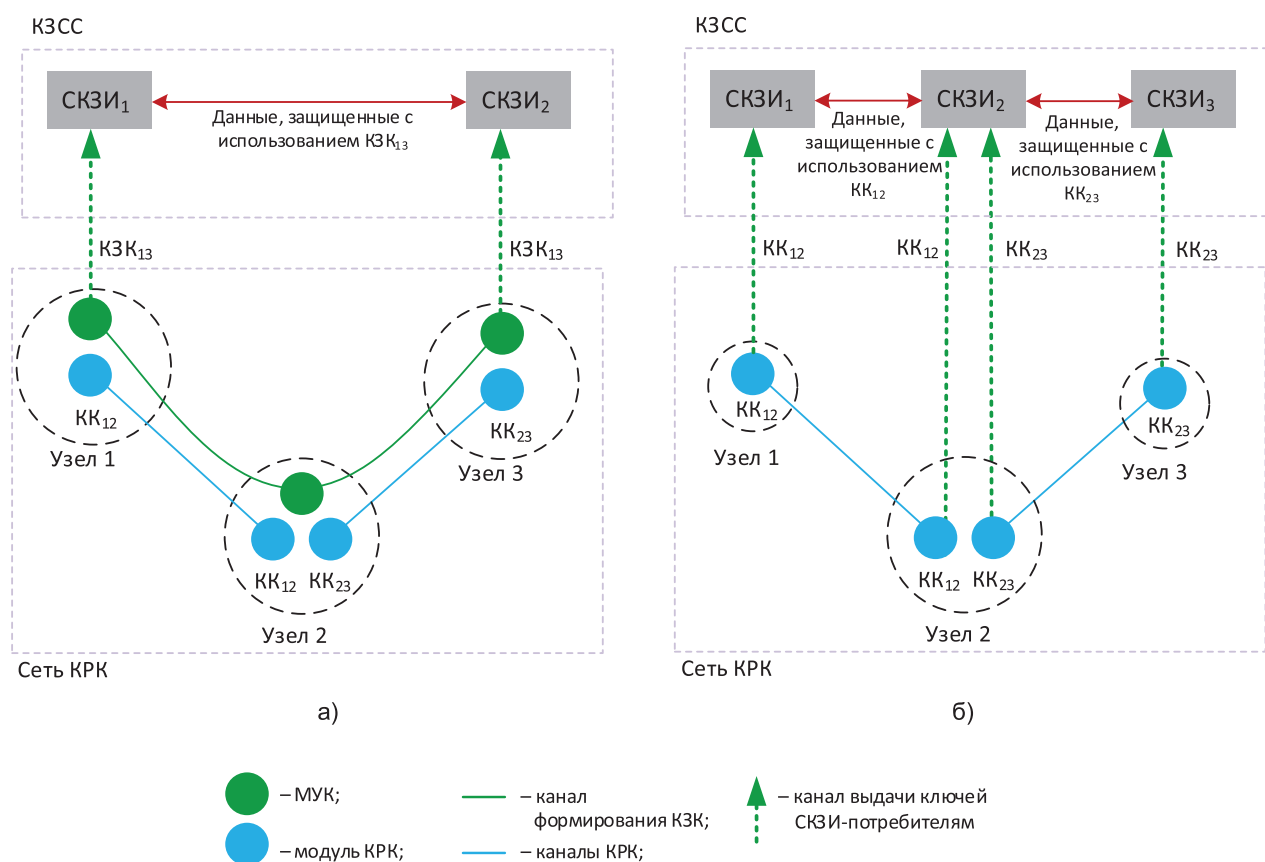


Рисунок 10 — Два варианта использования КК/КЗК в КЗСС

В сети КЗСС дополнительно к функциональным уровням сети КРК реализуются два верхних уровня (рисунок 11):

- уровень передачи данных КЗСС;
- уровень управления и мониторинга КЗСС.

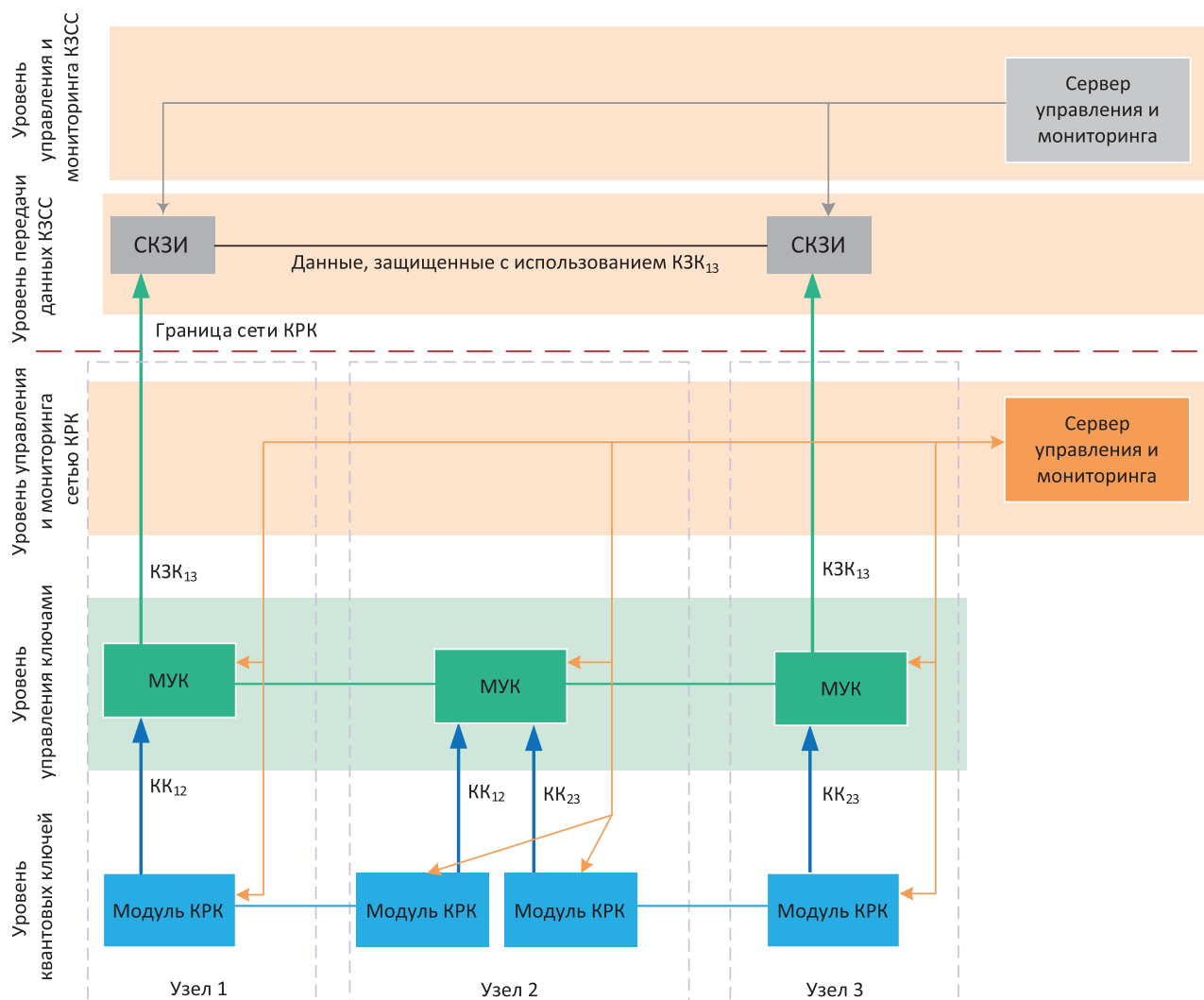


Рисунок 11 — Многоуровневая структура сети КЗСС (красной пунктирной линией показана условная граница между сетью КРК и КЗСС)

На уровне передачи данных КЗСС располагаются СКЗИ—потребители, получающие КЗК/КК от узлов сети КРК, и коммуникационная инфраструктура. На уровне управления КЗСС функционируют устройства управления и мониторинга КЗСС (например, сервер управления и мониторинга).

Библиография

- [1] Спецификация группы Квантовое распределение ключей (КРК). Характеристика компонентов: квантового распределения характеристика оптических компонентов для систем КРК [Quantum Key Distribution (QKD). Component characterization: characterizing optical components for QKD systems] ключей ETSI 011 V1.1.1 (ETSI GS QKD 011 V1.1.1)
- [2] Спецификация группы Квантовое распределение ключей (КРК). Параметры устройства и канала связи квантового распределения для развертывания КРК [Quantum Key Distribution (QKD). Device and Communication Channel Parameters for QKD Deployment] ключей ETSI 012 V1.1.1 (ETSI GS QKD 012 V1.1.1)

УДК 004.738:006.354

ОКС 35.110

Ключевые слова: квантовые коммуникации, общие положения, квантовое состояние, квантовая информация, квантовый канал, квантовая телепортация

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *И.А. Королева*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 12.07.2023. Подписано в печать 18.07.2023. Формат 60×84%. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации» для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru