



ПРЕДВАРИТЕЛЬНЫЙ
НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ПНСТ
830—
2023

КВАНТОВЫЕ КОММУНИКАЦИИ

Термины и определения

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. № 23-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

II

Содержание

1 Область применения1

2 Термины и определения.1

Алфавитный указатель терминов на русском языке9

Алфавитный указатель эквивалентов терминов на английском языке.12

Приложение А (справочное) Термины, применяемые в классических и квантовых коммуникациях . . 14

Приложение Б (справочное) Терминосистема в области квантовых коммуникаций15

Библиография18

Введение

Настоящий стандарт устанавливает термины и определения в области квантовых коммуникаций. Для каждого понятия установлен один стандартизованный термин.

Термины-синонимы приведены в качестве справочных данных и не являются стандартизованными.

Заключенная в круглые скобки часть термина может быть опущена при использовании термина в документах по стандартизации, при этом не входящая в круглые скобки часть термина образует его краткую форму.

Наличие квадратных скобок в терминологической статье означает, что в нее включены два термина, имеющие общие терминологические элементы.

В алфавитном указателе данные термины приведены отдельно с указанием номера статьи.

В стандарте приведен алфавитный указатель на русском языке, а также алфавитный указатель эквивалентов терминов на английском языке.

Стандартизованные термины набраны полужирным шрифтом, их краткие формы, представленные аббревиатурой или словосочетанием на основе аббревиатуры, — светлым, синонимы — курсивом.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

КВАНТОВЫЕ КОММУНИКАЦИИ

Термины и определения

Quantum communications. Terms and definitions

Срок действия — с 2023—09—01
до 2026—09—01

1 Область применения

Настоящий стандарт устанавливает основные термины и определения в области квантовых коммуникаций.
Термины, установленные настоящим стандартом, рекомендуется использовать во всех видах документации, научной, учебной и справочной литературе по квантовым коммуникациям.

2 Термины и определения

Общие понятия

1 **квантовая информация:** Информация, представленная в виде состояний квантовой системы. quantum information

2

кубит; квантовый бит: Единица представления квантовой информации, реализуемая двумя состояниями квантовой системы, находящейся в одном из состояний или в суперпозиции обоих состояний. qubit, quantum bit
[Адаптировано из ГОСТ Р 57257—2016, статья 2.12]

Примечание — Кубит описывается вектором в комплексном двухмерном гильбертовом пространстве.

3 **кудит:** Единица представления квантовой информации, реализуемая несколькими состояниями квантовой системы (d -состояний), находящейся в одном из d -состояний или в их суперпозиции. qudit, quantum d-git

Примечание — d — целое число больше 1. При $d = 2$ кудит является кубитом. Кудит описывается вектором в комплексном d -мерном гильбертовом пространстве.

4 **квантовая система:** Физическая система, представляющая собой объект или ансамбль объектов, описывающихся в терминах квантовой механики и подчиняющихся ее постулатам. quantum system

5 **квантовое состояние:** Состояние квантовой системы. quantum state

6

квантовая запутанность; сцепленность: Квантовое явление, при котором квантовые состояния двух или более частиц являются взаимозависимыми. quantum entanglement

Примечание — Квантовую запутанность описывают состоянием квантовой системы в целом, а не квантовым состоянием отдельных входящих в нее частиц.

[Адаптировано из ГОСТ Р 57257—2016, статья 2.6]

7 распределение квантовой запутанности: Распределение квантовых состояний, находящихся в состоянии квантовой запутанности, между различными точками пространства. entanglement distribution

8 квантовая телепортация: Формирование квантового состояния, идентичного квантовому состоянию, измеряемому в удаленной точке пространства, на основе распределения между данными точками пространства квантовой запутанности и передачи между ними измерений исходного квантового состояния по классическому каналу связи. quantum teleportation

9 квантовое сверхплотное кодирование: Протокол квантовой передачи двух битов информации посредством передачи одного кубита, при котором передаваемый кубит находится в состоянии запутанности с кубитом, используемым при его измерении. superdense coding

10

квантовые коды коррекции ошибок: Процедуры кодирования квантовых состояний для защиты от ошибок, возникающих при передаче или хранении квантовых состояний. quantum error correction codes

[Адаптировано из [1], статья 3.1]

11

квантовый сигнал: Сигнал, описываемый квантовым состоянием [[2], статья 5.4.1.16] quantum signal

12

квантовые коммуникации: Передача информации посредством прямой передачи квантовых состояний или посредством квантовой запутанности. quantum communication

[Адаптировано из [2], статья 5.3.1.6]

13

квантовый канал: Канал связи для передачи квантовых сигналов. [[2], статья 5.4.1.9] quantum channel

14

классический канал: Канал связи, используемый для обмена информацией, закодированной в форме, позволяющей прочитать и воспроизвести ее обратимым неразрушающим образом. classical channel

[Адаптировано из [1], статья 3.1]

15 квантовая оптика: Раздел оптики, связанный с изучением явлений, в которых проявляются квантовые свойства света. quantum optics

16 темное волокно: Волокно, которое не используется для передачи классических сигналов (например, резервное в кабеле). dark fiber

Примечание — Квантовые сигналы, как правило, передаются по темным волокнам.

17 квантовая подпись: Квантовая информация, связанная с другой информацией в электронной форме (подписываемой информацией) и используемая для определения лица, подписывающего информацию. quantum signature

Примечание — Выработка и проверка квантовой подписи реализуется с помощью протокола квантовой передачи и квантовых методов обработки информации.

18 квантовое разделение секрета: Процедура разделения секрета, реализуемая с помощью протокола квантовой передачи. quantum secret sharing

19

квантовая тактовая синхронизация: Синхронизация источников времени с помощью квантовых систем и явления квантовой запутанности. [Адаптировано из [2], статья 5.1.2.4] quantum clock synchronization

Квантовое оборудование

20 квантовое оборудование: Вид оборудования, ключевые функциональные процессы которого основаны на использовании квантовых законов и явлений. quantum device

21 (коммуникационное) квантово-оптическое оборудование: Квантовое оборудование, использующее квантовые свойства света для обработки, хранения и передачи информации. optical quantum (communication) device

Примечание — Кубиты в квантово-оптическом оборудовании реализуются с помощью фотонов.

22 квантовый передатчик (Алиса): Программно-аппаратный комплекс, обеспечивающий приготовление и передачу квантовых сигналов. quantum transmitter (Alice)

23 квантовый приемник (Боб): Программно-аппаратный комплекс, обеспечивающий прием и обработку квантовых сигналов. quantum receiver (Bob)

24 канал синхронизации (квантово-оптического оборудования): Классический канал, используемый для передачи сигнала синхронизации между квантовыми передатчиком и приемником. synchronization channel

25 служебный канал (квантово-оптического оборудования): Классический канал, используемый для передачи служебной информации между квантовыми передатчиком и приемником, необходимой для реализации протокола квантовой передачи. classical public channel

26 квантово-оптический тракт: Совокупность квантово-оптических компонентов квантового приемника, квантового передатчика и квантового канала. quantum optical path

27

источник одиночных фотонов: Источник фотонов, испускающий в среднем не более одного фотона в импульсе. [Адаптировано из [2], статья 5.3.2.42] single-photon source

28 квантово-оптические компоненты: Компоненты квантового приемника и квантового передатчика, реализующие формирование или преобразование квантовых сигналов (например: источник одиночных фотонов, светоделители, фазовый модулятор, детектор фотонов и др.). quantum optical components

29 протокол квантовой передачи; ПКП: Протокол физического уровня, обеспечивающий подготовку, передачу, прием и измерение квантовых сигналов между квантовыми передатчиком и приемником по квантовому каналу связи.

quantum communication protocol

Примечание — Физический уровень определен в соответствии с сетевой моделью OSI.

30 система квантовой коммуникации: Система передачи квантовой информации, состоящая из квантового передатчика и квантового приемника, соединенных квантовыми каналом, каналом синхронизации и служебным каналом.

quantum communication system

31 квантовый повторитель: Комплекс устройств, расположенных в одном или нескольких узлах квантовой сети, обеспечивающий ретрансляцию квантового сигнала посредством распределения квантовой запутанности и квантовой телепортации.

quantum repeater

Примечание — Квантовый повторитель, имеющий более одного входа и/или выхода и обеспечивающий возможность маршрутизации, называется квантовым роутером.

32

квантовый генератор случайных чисел; КГСЧ: Устройство, использующее квантово-механические эффекты для выработки случайных чисел. [[2], статья 5.2.2.23]

quantum random number generator

Примечание — Термины «квантовый генератор случайных чисел» и «квантовый датчик случайных чисел» являются синонимами.

33

протокол квантовой тактовой синхронизации: ПКП, используемый для квантовой тактовой синхронизации. [Адаптировано из [2], статья 5.1.2.5]

quantum clock synchronization protocol

Квантовое распределение ключей

34 квантовое распределение ключей; КРК: Процедура выработки и распределения секретных ключей, реализуемая с помощью квантовых криптографических протоколов и квантовых каналов связи.

quantum key distribution, QKD

Примечание — Термин «секретный ключ» определен в ПНСТ 799—2022.

35 квантовый криптографический протокол выработки и распределения ключей; ККП ВРК: Распределенный алгоритм, выполняющийся в аппаратно-программных средствах ККС ВРК с целью распределения секретных ключей для сопряженных средств криптографической защиты информации; включает в себя ПКП и ККПО.

QKD protocol

Примечания

1 Термин «секретный ключ» определен в ПНСТ 799—2022.

2 Термины «квантовый криптографический протокол выработки и распределения ключей» и «протокол КРК» являются синонимами.

3 Как правило, протокол КРК на дискретных переменных включает стадии генерации (формирования) сырого ключа, формирования просеянного ключа (просеивания), измерения QBER, исправления ошибок и усиления стойкости ключа. Протокол КРК на непрерывных переменных, как правило, включает стадии просеивания, оценки параметров квантового канала, исправления ошибок, подтверждения (сравнения хеш-значений после согласования) и усиления стойкости ключа.

36 квантовый криптографический протокол обработки; ККПО: quantum cryptographic processing protocol
Протокол обработки результатов ПКП, в результате выполнения которого формируется квантовый ключ.

Примечание — Включает в себя протокол просеивания, протокол коррекции ошибок, протокол верификации, протокол усиления секретности.

37 протокол просеивания ключа: Составная часть ККПО, в процессе которой из квантовой ключевой последовательности сырой выбираются значимые биты для дальнейшего формирования квантового ключа. sifting protocol

38 протокол коррекции ошибок: Составная часть ККПО, в процессе которой из квантовой ключевой последовательности просеянной получают идентичные с заданной вероятностью битовые последовательности, называемые очищенными квантовыми ключевыми последовательностями. reconciliation protocol, error correction protocol

39 протокол верификации: Составная часть ККПО, в процессе которой производится верификация того, что очищенные квантовые ключевые последовательности являются идентичными с заданной вероятностью. verification protocol

40 протокол усиления секретности: Составная часть ККПО, в процессе которой очищенные квантовые ключевые последовательности, прошедшие верификацию, ужимаются в короткие битовые строки (квантовые ключи) с целью уменьшения информации, полученной злоумышленником из открытых каналов в процессе выполнения ККП ВРК. privacy amplification protocol

41 квантовый ключ; КК: Секретный ключ, полученный в результате выполнения ККП ВРК. quantum key, secure (quantum) key

Примечание — Термины «квантовый ключ» и «квантовая ключевая последовательность» тождественны.

42 квантовозащищенный ключ; КЗК: Секретный ключ, защита которого при передаче или хранении осуществляется с использованием квантового ключа (ключей). quantum encrypted key

43 сырая квантовая ключевая последовательность: Битовая последовательность, полученная в результате ПКП. raw key

44 просеянная квантовая ключевая последовательность: Битовая последовательность, полученная в процессе ККПО в результате протокола просеивания из сырой квантовой ключевой последовательности. sifted key

45 очищенная квантовая ключевая последовательность: Битовая последовательность, полученная в процессе ККПО в результате протокола коррекции ошибок из квантовой ключевой последовательности просеянной. reconciliated quantum key sequence

46 верифицированная квантовая ключевая последовательность: Битовая последовательность, полученная в процессе ККПО в результате протокола верификации из очищенной квантовой ключевой последовательности. verified quantum key sequence

47 скорость генерации ключа: Количество бит ключа, выработанных в единицу времени. key rate

48 коэффициент квантовых ошибок на бит: Относительный показатель количества ошибок в квантовой ключевой последовательности просеянной. quantum bit error rate, QBER

Примечание — В ряде случаев используют англоязычный термин «QBER» — Quantum Bit Error Rate.

49 квантовая криптографическая система выработки и распределения ключей; ККС ВРК: Квантовая криптографическая система, предназначенная для выработки квантовых ключей и их распределения в сопряженные средства криптографической защиты информации. QKD system

Примечание — Термины «квантовая криптографическая система выработки и распределения ключей» и «система квантового распределения ключей (система КРК)» являются синонимами.

50 ККС ВРК на дискретных переменных: ККС ВРК, кодирующая квантовую информацию в виде дискретных переменных конечной размерности и использующая для регистрации квантовых состояний однофотонные детекторы в режиме счета фотонов. discrete variable QKD, DV-QKD

51 ККС ВРК на непрерывных переменных: ККС ВРК, кодирующая информацию в непрерывном гильбертовом пространстве с использованием квадратур электромагнитного поля и использующая когерентное детектирование для регистрации квантовых состояний. continuous variable QKD, CV-QKD

52 модуль ККС ВРК: Квантовый приемник (передатчик), реализующий протокол квантового распределения ключей. QKD module

Примечание — Связанные два и более модуля ККС ВРК образуют ККС ВРК.

53 служебный канал ККС ВРК: Классический канал связи с имитозащитой, предназначенный для обмена сообщениями в ходе реализации ККПО. QKD classical public channel

Примечание — Термин «имитозащита» определен в [3].

54 сеанс КРК: Процесс однократной последовательной реализации всех этапов ККП ВРК для получения квантового ключа (ключей). QKD session

55 атака на протокол КРК: Комплекс действий нарушителя, направленный на получение информации, используя уязвимости протокола КРК. attack on QKD protocol

56 атака на техническую реализацию ККС ВРК: Комплекс действий нарушителя, направленный на получение криптографически опасной информации, используя уязвимости квантово-оптического оборудования ККС ВРК, в том числе с возможностью самостоятельного создания уязвимостей путем активного воздействия на квантово-оптическое оборудование ККС ВРК. quantum hacking

57 состояния-ловушки: Специальные квантовые состояния, предусмотренные протоколом КРК, которыми легитимные пользователи намеренно и случайным образом подменяют квантовые сигналы, в целях обнаружения атак на протокол КРК. decoy states

Квантовые сети

58 квантовая (коммуникационная) сеть: Технологическая система, включающая средства и линии связи, предназначенные для передачи квантовой информации. quantum network

59 узел квантовой сети: Узел, который может передавать, принимать, повторять (ретранслировать), коммутировать или маршрутизировать квантовые сигналы в квантовой сети. quantum network node

60 сегмент квантовой сети: Участок квантовой сети, ограниченный смежными узлами квантовой сети. quantum network segment

61 магистральный сегмент квантовой передачи: Два или более последовательно соединенных квантовых повторителя в составе квантовой сети.

quantum backbone link

62

квантовый интернет: Глобальная информационная квантовая сеть, в узлах которой формируется, обрабатывается и хранится квантовая информация и узлы которой соединены квантовыми каналами.
[Адаптировано из [2], статья 5.4.2.4]

quantum internet

63 сеть КРК: Технологическая система (квантовая сеть), включающая в себя аппаратуру ККС ВРК и линии связи и предназначенная для выработки КК (при помощи ККП ВРК) и КЗК.

QKD network, QKDN

64 система управления ключами; СУК: Распределенный программно-технический комплекс, обеспечивающий синхронизацию, выработку, идентификацию и распределение ключевой информации в сети КРК.

key manager

Примечание — Устанавливаемые в отдельных узлах сети КРК программно-аппаратные комплексы, входящие в состав СУК, называются модулями управления ключами (МУК).

65 система управления и мониторинга сетью КРК; СУМ сетью КРК: Распределенный программно-аппаратный комплекс, осуществляющий централизованное автоматизированное управление и мониторинг элементами сети КРК.

QKD network manager

66 квантовозащищенная сеть связи; КЗСС: Сеть связи, предназначенная для защищенной передачи данных с использованием квантовых ключей и/или квантовозащищенных ключей.

quantum encrypted communication network, QECN

67 система управления и мониторинга квантовозащищенной сетью связи; СУМ КЗСС: Распределенный программно-технический комплекс, осуществляющий централизованное автоматизированное управление и мониторинг элементами КЗСС.

QECN network manager

Услуги в области квантовых коммуникаций

68 услуга с использованием КЗСС: Услуга, заключающаяся в приеме, обработке, хранении, передаче, доставке информации по КЗСС.

QECN service

69 услуга с использованием сети КРК: Услуга, заключающаяся в выдаче квантовых и/или квантовозащищенных ключей, формируемых сетью КРК.

QKDN service

70 пользователь услуг с использованием сети КРК [КЗСС]: Физическое или юридическое лицо, заказывающее и/или использующее услуги с использованием сети КРК [КЗСС].

QKDN (QECN) user

71 потребитель услуг с использованием сети КРК [КЗСС]: Физическое или юридическое лицо, получающее, заказывающее или имеющее намерение получить или заказать услугу с использованием сети КРК [КЗСС] для собственных нужд.

QKDN (QECN) service consumer

72 абонент сети КРК [КЗСС]: Пользователь, с которым заключен договор об оказании услуг с использованием сети КРК [КЗСС] при выделении для этих целей абонентского номера или уникального кода идентификации.

QKDN (QECN) subscriber

73 оператор сети КРК [КЗСС]: Юридическое лицо или индивидуальный предприниматель, оказывающие услуги с использованием сети КРК [КЗСС] на основании соответствующей лицензии. QKDN (QECN) operator

74 оказание услуг с использованием сети КРК [КЗСС]: Деятельность оператора сети КРК [КЗСС] по обеспечению услуг с использованием сети КРК [КЗСС]. QKDN (QECN) service provision

75 качество услуг с использованием сети КРК [КЗСС]: Степень соответствия показателей, характеризующих реализуемые на базе сети КРК [КЗСС] услуги, требованиям, предъявляемым к показателям функционирования сети КРК [КЗСС], и требованиям, закрепленным договором об оказании услуг связи и/или соглашением между оператором сети КРК [КЗСС] и абонентом сети. QKDN (QECN) QoS

Алфавитный указатель терминов на русском языке

абонент КЗСС	72
абонент сети КРК	72
атака на протокол КРК	55
атака на техническую реализацию ККС ВРК	56
<i>бит квантовый</i>	2
волокно темное	16
генератор случайных чисел квантовый	32
запутанность квантовая	6
интернет квантовый	62
информация квантовая	1
источник одиночных фотонов	27
канал квантово-оптического оборудования служебный	25
канал квантовый	13
канал ККС ВРК служебный	53
канал классический	14
канал синхронизации	24
канал служебный	25
канал синхронизации квантово-оптического оборудования	24
качество услуг с использованием КЗСС	75
качество услуг с использованием сети КРК	75
КГСЧ	32
КЗК	42
КЗСС	66
ККП ВРК	35
ККПО	36
ККС ВРК	49
ККС ВРК на дискретных переменных	50
ККС ВРК на непрерывных переменных	51
ключ квантовозащищенный	42
ключ квантовый	41
кодирование сверхплотное квантовое	9
коды коррекции ошибок квантовые	10
коммуникации квантовые	12
компоненты квантово-оптические	28
коэффициент квантовых ошибок на бит	48
КРК	34
кубит	2
кудит	3
модуль ККС ВРК	52
оборудование коммуникационное квантово-оптическое	21
оборудование квантовое	20
оборудование квантово-оптическое	21
оказание услуг с использованием КЗСС	74
оказание услуг с использованием сети КРК	74

оператор КЗСС	73
оператор сети КРК	73
оптика квантовая	15
передатчик квантовый	22
передатчик квантовый Алиса	22
ПКП	33
повторитель квантовый	31
подпись квантовая	17
пользователь услуг с использованием КЗСС	70
пользователь услуг с использованием сети КРК	70
последовательность ключевая квантовая верифицированная	46
последовательность ключевая квантовая очищенная	45
последовательность ключевая квантовая просеянная	44
последовательность ключевая квантовая сырая	43
потребитель услуг с использованием КЗСС	71
потребитель услуг с использованием сети КРК	71
приемник квантовый	23
приемник квантовый Боб	23
протокол верификации	39
протокол выработки и распределения ключей квантовый криптографический	35
протокол квантовой передачи	29
протокол коррекции ошибок	38
протокол обработки квантовый криптографический	36
протокол просеивания ключа	37
протокол тактовой квантовой синхронизации	33
протокол усиления секретности	40
разделение секрета квантовое	18
распределение квантовой запутанности	7
распределение ключей квантовое	34
сеанс КРК	54
сегмент квантовой передачи магистральный	61
сегмент квантовой сети	60
сеть квантовая	58
сеть коммуникационная квантовая	58
сеть КРК	63
сеть связи квантовозащищенная	66
сигнал квантовый	11
синхронизация тактовая квантовая	19
система выработки и распределения ключей квантовая криптографическая	49
система квантовая	4
система квантовой коммуникации	30
система управления и мониторинга квантовозащищенной сетью связи	67
система управления и мониторинга сетью КРК	65
система управления ключами	64
скорость генерации ключа	47

состояние квантовое	5
состояния-ловушки	57
СУК	64
СУМ КЗСС	67
СУМ сетью КРК	65
<i>сцепленность</i>	6
телепортация квантовая	8
тракт квантово-оптический	26
узел квантовой сети	59
услуга с использованием КЗСС	68
услуга с использованием сети КРК	69

Алфавитный указатель эквивалентов терминов на английском языке

attack on QKD protocol	55
classical channel	14
classical public channel (of QKD system)	25
continuous variable QKD	51
CV-QKD	51
dark fiber	16
decoy states	57
discrete variable QKD	50
DV-QKD	50
entanglement distribution	7
error correction protocol	38
key manager	64
key rate	47
optical quantum (communication) device	21
privacy amplification protocol	40
QBER	48
QECN	66
QECN network manager	67
QECN operator	73
QECN QoS	75
QECN service	68
QECN service consumer	71
QECN service provision	74
QECN subscriber	72
QECN user	70
QKD classical public channel	53
QKD module	52
QKD network	63
QKD network manager	65
QKD protocol	35
QKD session	54
QKD system	49
QKDN	63
QKDN operator	73
QKDN QoS	75
QKDN service	69
QKDN service consumer	71
QKDN service provision	74
QKDN subscriber	72
QKDN user	70
quantum backbone link	61
quantum bit	2
quantum bit error rate	48
quantum channel	13
quantum clock synchronization	19

quantum clock synchronization protocol	33
quantum communication	12
quantum communication protocol	29
quantum communication system	30
quantum cryptographic processing protocol	36
quantum device	20
quantum d-git	3
quantum encrypted communication network	66
quantum encrypted key	42
quantum entanglement	6
quantum error correction codes	10
quantum hacking	56
quantum information	1
quantum internet	62
quantum key	41
quantum key distribution	34
quantum network	58
quantum network node	59
quantum network segment	60
quantum optical components	28
quantum optical path	26
quantum optics	15
quantum photon source	27
quantum random number generator	32
quantum receiver (Bob)	23
quantum repeater	31
quantum secret sharing	18
quantum signal	11
quantum signature	17
quantum state	5
quantum system	4
quantum teleportation	8
quantum transmitter (Alice)	22
qubit	2
qudit	3
raw key	43
reconciliated quantum key sequence	45
reconciliation protocol	38
secure (quantum) key	41
sifted key	44
sifting protocol	37
superdense coding	9
synchronization channel	24
verification protocol	39
verified quantum key sequence	46

Приложение А
(справочное)

Термины, применяемые в классических и квантовых коммуникациях

А.1 Термины, применяемые в классических и квантовых коммуникациях

А.1.1 атмосферная оптическая линия связи: Реализованная возможность передачи данных между двумя объектами посредством распространяющегося в атмосфере излучения видимого и ИК диапазонов.

А.1.2 базис: Упорядоченный (конечный или бесконечный) набор векторов в векторном пространстве, такой, что любой вектор этого пространства может быть единственным образом представлен в виде линейной комбинации векторов из этого набора. Векторы базиса называются базисными векторами.

А.1.3 волоконно-оптическая линия связи: Реализованная возможность передачи данных между двумя объектами посредством распространяющегося по кабелю излучения видимого и ИК диапазонов.

А.1.4

оптический кабель; ОК: Кабельное изделие, содержащее одно или несколько оптических волокон, объединенных в единую конструкцию, обеспечивающую их работоспособность в заданных условиях эксплуатации.

Примечание — При необходимости оптический кабель может содержать также токопроводящие жилы.

[ГОСТ Р 57139—2016, статья 1]

А.1.5

канал передачи (сети электросвязи): Комплекс технических средств и среды распространения, который обеспечивает передачу сигнала электросвязи в нормированной полосе частот или с нормированной скоростью передачи.

[ГОСТ Р 53801—2010, статья 30]

А.1.6

канал связи: Совокупность технических средств, обеспечивающих передачу информации от источника к получателю. В совокупность технических средств могут входить, в частности, передатчик, линия связи, носитель информации, приемник, аппаратные и/или программные средства.

Примечание — Примерами каналов связи могут служить: проводные и беспроводные каналы, радио-каналы, а также каналы, реализуемые с использованием отчуждаемых (съемных) носителей информации.

[[3], статья 3.1.16]

А.1.7

сеть связи: Технологическая система, включающая в себя средства связи и линии связи и предназначенная для электросвязи или почтовой связи.

[ГОСТ Р 53801—2010, статья 39]

А.1.8

система электросвязи, система связи: Совокупность технических средств, образующих вторичную сеть на базе типовых физических цепей, типовых каналов передачи и сетевых трактов первичной сети, и подсистем нумерации, сигнализации, тарификации, технического обслуживания и управления, обеспечивающая электросвязь определенного вида.

[ГОСТ 22348—86, статья 1]

А.1.9

когерентное детектирование: Принцип детектирования оптических сигналов, заключающийся в том, что оптический сигнал смешивается с опорным излучением (ОИ) и суммарное излучение поступает на несколько фотодиодов, преобразующих его в электрический сигнал биений.

Примечание — Для получения полной информации об оптическом сигнале необходимо использовать четыре канала: по два канала для каждой из двух ортогональных поляризаций.

[ГОСТ Р 58568—2019, статья 2.3.7.10]

Приложение Б
(справочное)

Терминосистема в области квантовых коммуникаций

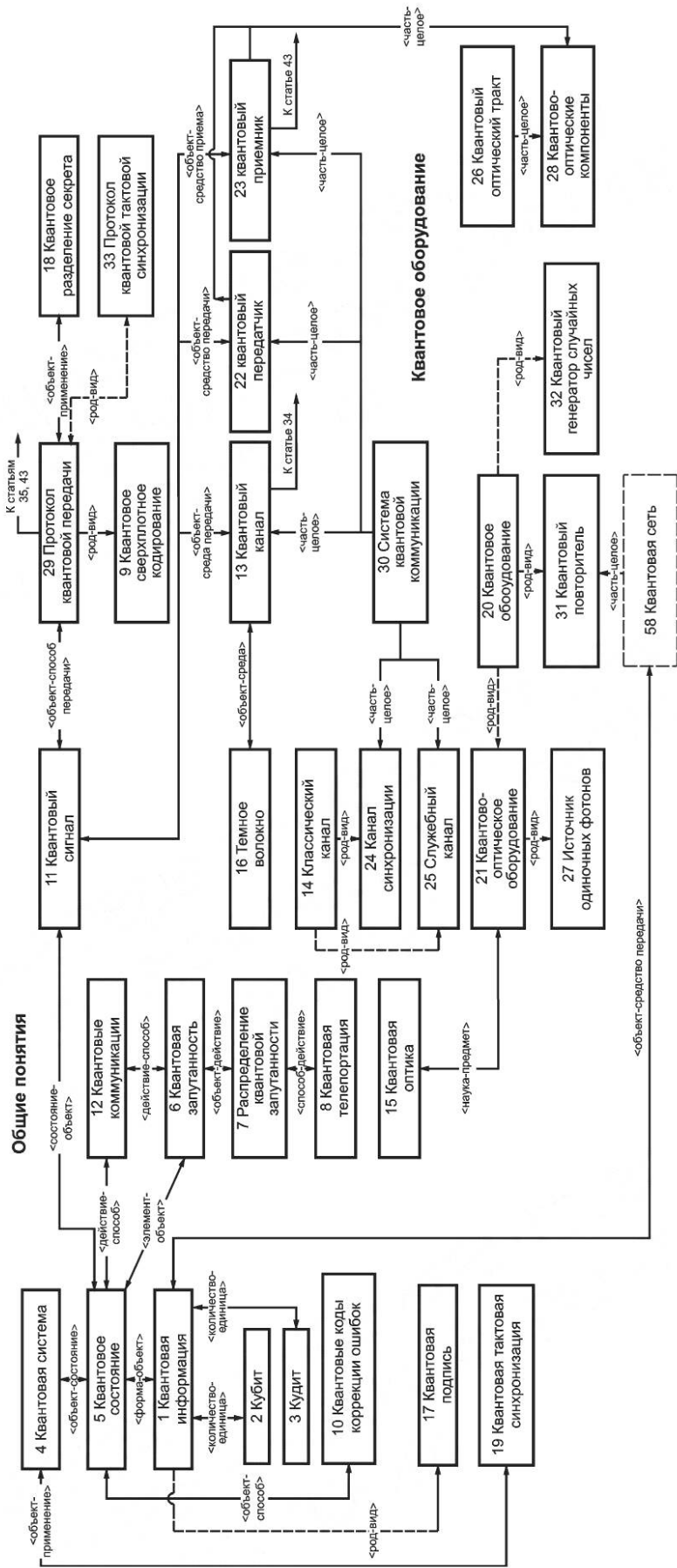


Рисунок Б.1, лист 1

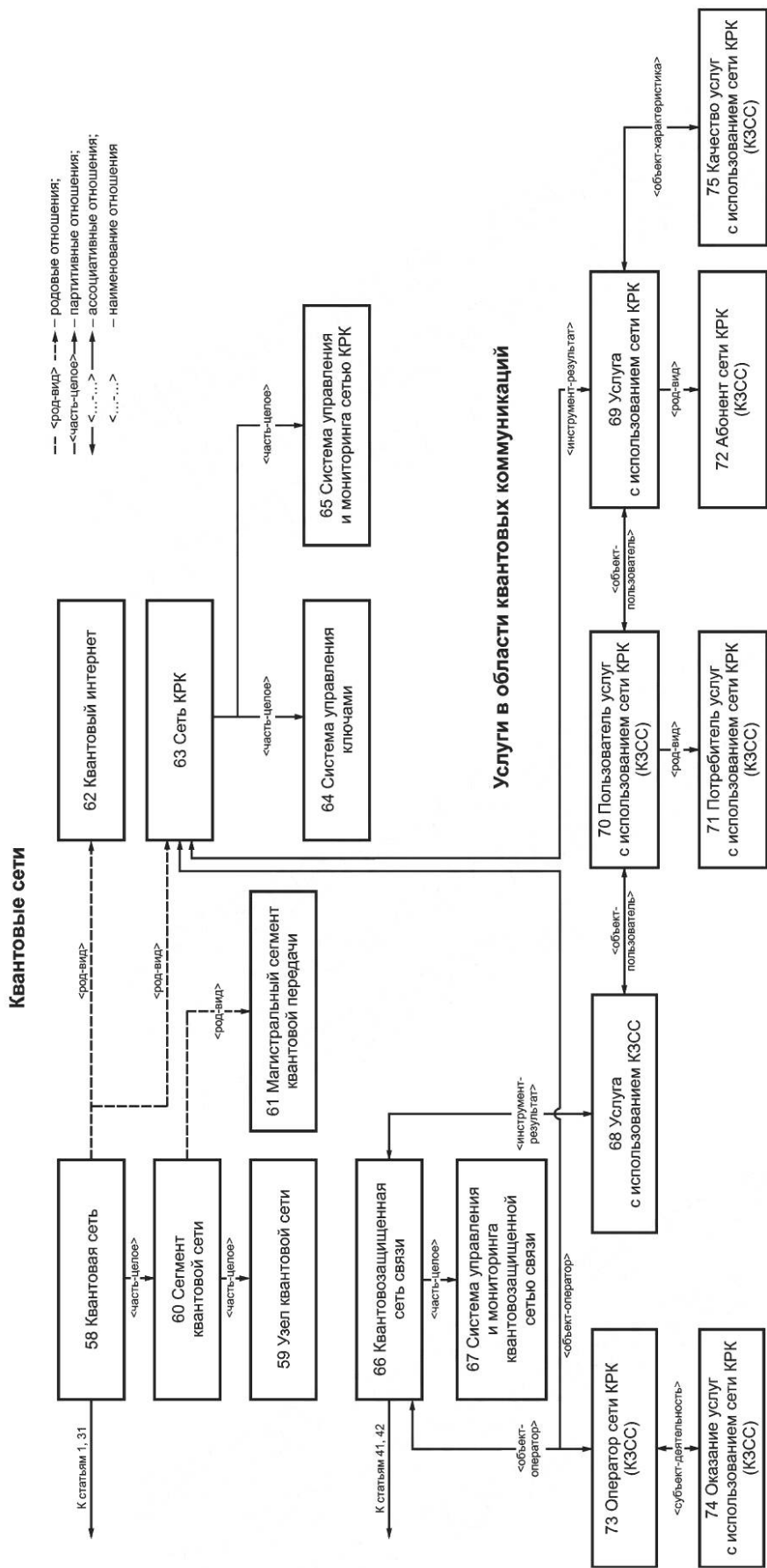


Рисунок Б.1, лист 3

Библиография

- [1] Отчет группы ETSI GR QKD 007 V1.1.1 (2018-12) Квантовое распределение ключей. Словарь (Quantum Key Distribution (QKD). Vocabulary)
- [2] Технический отчет МСЭ-T FG QIT4N D1.1 (ITU-T Technical Report. FG QIT4N D1.1) Квантовые информационные технологии для сетевых технологий: Сетевые аспекты для квантовых информационных технологий (Quantum information technology for networks terminology: Network aspects of quantum information technologies)
- [3] Рекомендация Р 1323565.1.012—2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

УДК 004.738:006.354

ОКС 35.110

Ключевые слова: квантовые коммуникации, термины и определения, квантовое состояние, квантовая информация, квантовый канал, квантовая телепортация

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И.Першина*
Компьютерная верстка *И.Ю. Литовкиной*

Сдано в набор 12.07.2023. Подписано в печать 19.07.2023. Формат 60×84 $\frac{1}{8}$. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч-изд. л. 2,37.

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