ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 907— 2023

Квантовый Интернет вещей

ТИПОВОЙ ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, ВЫРАБОТАННЫХ СЕТЬЮ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Интерфейсы подключения

Издание официальное

Федеральное агентство по техническому регулированию и метрологии

Москва
Российский институт стандартизации
2024

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 29 декабря 2023 г. № 118-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», 2024

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

Федеральное агентство по техническому регулированию и метрологии

Введение

Типовой программно-аппаратный комплекс распределения ключей, выработанных сетью квантового распределения сетей (КРК) (ПАК РКК), обеспечивает защищенную доставку секретных ключей, выработанных сетью КРК, до объектов системы квантового Интернета вещей (КИВ), прямое подключение которых к сети КРК технически невозможно или нецелесообразно.

Настоящий стандарт определяет общие требования к интерфейсам программно-аппаратного комплекса, используемым для получения и распределения КЗК в ПАК РКК и для связи между объектами КИВ.

Федеральное агентство по техническому регулированию и метрологии

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Квантовый Интернет вещей

ТИПОВОЙ ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, ВЫРАБОТАННЫХ СЕТЬЮ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Интерфейсы подключения

Quantum Internet of Things. Typical software-hardware complex distributing keys generated by QKD network. External interfaces

Срок действия — с 2024—02—01
до 2027—02—01

1 Область применения

Настоящий стандарт устанавливает требования к интерфейсам подключения типового программно-аппаратного комплекса распределения ключей, выработанных сетью квантового распределения ключей (ПАК РКК), в части интерфейса взаимодействия с сетью квантового распределения ключей (КРК), интерфейса передачи секретных ключей на объекты квантового Интернета вещей (КИВ) и интерфейса передачи данных между объектами КИВ.

Настоящий стандарт не устанавливает требований:

- к интерфейсам взаимодействия между элементами ПАК РКК;
- организации работы сети КРК.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ПНСТ 830—2023 Квантовые коммуникации. Термины и определения

ПНСТ 832—2023 Квантовый Интернет вещей. Термины и определения

ПНСТ 906—2023 Квантовый Интернет вещей. Типовой программно-аппаратный комплекс распределения ключей, выработанных сетью квантового распределения сетей. Архитектура

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.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ПНСТ 906—2023, ПНСТ 830—2023 и ПНСТ 832—2023.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

КЗК — квантовозащищенный ключ;

КИВ — квантовый Интернет вещей;

КРК — квантовое распределение ключей;

ОКИВ — объект КИВ;

ПАК РКК — программно-аппаратный комплекс распределения ключей, выработанных сетью КРК;

СВРК — система выработки и распределения ключей;

СКЗИ — средство криптографической защиты информации;

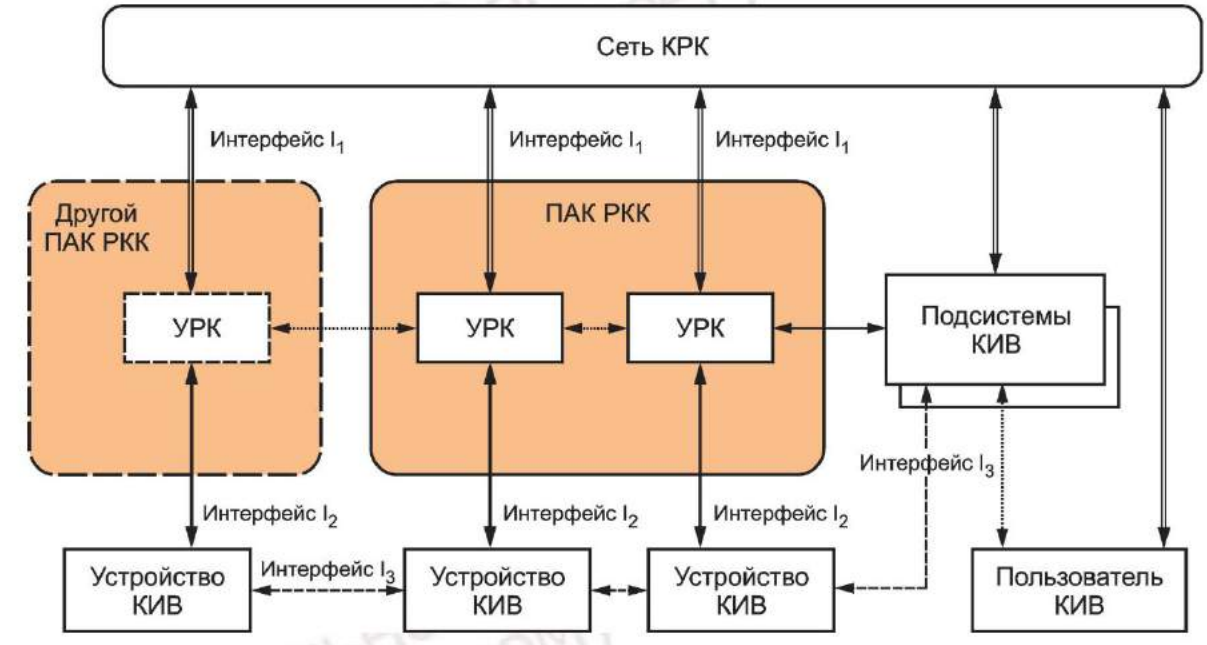
УРК — узел распределение ключей;

CRISP — неинтерактивный протокол защищенной передачи данных, разработанный для применения в индустриальных системах.

5 Интерфейсы

Архитектура ПАК РКК приведена в ПНСТ 906—2023.

Передача КЗК в ПАК РКК осуществляется по следующим интерфейсам (см. рисунок 1):



— взаимодействие с сетью КРК с использованием протокола «Протока»;

— взаимодействие с УРК с использованием протокола «Протока» или протокола, основанного на CRISP;

— взаимодействие с использованием протокола, основанного на CRISP;

— взаимодействие с использованием протокола, определенного вне настоящего стандарта.

Рисунок 1 — Интерфейсы ПАК РКК и взаимодействующих с ним элементов на прикладном уровне

- интерфейс КРК—УРК (интерфейс I_1);
- интерфейс УРК—ОКИВ (интерфейс I_2).

Передача информации между ОКИВ осуществляется по интерфейсу ОКИВ—ОКИВ (интерфейс I_3).

Взаимодействие между УРК осуществляется по интерфейсу УРК—УРК (вопросы стандартизации данного интерфейса выходят за рамки настоящего стандарта).

5.1 Интерфейс КРК—УРК

Передача сообщений между УРК и узлом сети КРК, в том числе для получения КЗК, выполняется в соответствии с протоколом «Протока», определенным в [1].

При передаче сообщений УРК выполняет функции СКЗИ-потребителя, а сеть КРК — узла СВРК (см. [1]).

Идентификатор УРК в сети КРК, идентификатор соответствующего узла сети КРК, базовые ключи (для каждого направления передачи), а также необходимая ключевая информация для формирования ключей, использующихся в алгоритме экспорта целевых ключей (см. [1]), задаются во время сопряжения УРК с сетью КРК. Регламент процедуры смены базовых ключей и необходимая периодичность повторения данной процедуры определяется в соответствии с требованиями, установленными при эксплуатации сети КРК, и находится за рамками настоящего стандарта. Порядок сопряжения УРК с сетью КРК и внутренние процедуры работы сети КРК выходят за рамки настоящего стандарта.

5.2 Интерфейс УРК—ОКИВ

Передача сообщений между УРК и ОКИВ для распределения КЗК осуществляется на основе протокола «Протока» (см. [1]). При передаче сообщений по протоколу «Протока» ОКИВ выполняет функции СКЗИ-потребителя, а УРК — узла СВРК (в терминах [1]).

Если передаваемая в системе КИВ информация не подлежит обязательной защите в соответствии с нормативно-правовыми актами Российской Федерации, передача сообщений между УРК и ОКИВ для распределения КЗК может осуществляться на основе иных протоколов, основанных на CRISP (см. [2]) и обеспечивающих требуемый уровень безопасности передачи КЗК.

5.3 Интерфейс ОКИВ—ОКИВ

Передача данных между ОКИВ с использованием КЗК должна быть осуществлена с использованием протоколов, основанных на протоколе CRISP (см. [2]).

Федеральное агентство по техническому регулированию и метрологии

Библиография

[1] МР 26.4.004—2021 Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации

[2] Р 1323565.1.029—2019 Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем

УДК 004.738:006.354 ОКС 35.110

Ключевые слова: квантовый Интернет вещей, типовой программно-аппаратный комплекс распределения ключей, сеть КРК, квантовое распределение ключей, интерфейсы подключения

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

Сдано в набор 10.01.2024. Подписано в печать 25.01.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 0,93. Уч.-изд. л. 0,70.

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

Федеральное агентство по техническому регулированию и метрологии