ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 906— 2023

Квантовый Интернет вещей

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

Архитектура

Издание официальное

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. № 117-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)

Введение

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения 2
5 Задачи ПАК РКК 3
6 Архитектура и основные функции компонентов ПАК РКК 3
Приложение А (справочное) Пример реализации типового ПАК РКК с централизованным управлением и с записью КЗК на ОНКИ 4

Введение

Использование Интернета вещей требует наличия защищенной связи. К таким областям в первую очередь относится применение Интернета вещей на критически важной инфраструктуре (например, в нефтегазовом комплексе, в жилищно-коммунальном хозяйстве и в финансовом секторе), а также использование в автоматизированных комплексах и в системах с участием беспилотных средств (беспилотных автомобилей, беспилотных летальных аппаратов и др.).

Квантовые коммуникации обладают уникальными возможностями в сфере защиты линий связи и передаваемой по ним информации. Одним из способов такой защиты является использование квантовых или квантовозащищенных ключей для криптографической защиты информации, передаваемой по классическим сетям.

Настоящий стандарт определяет архитектуру типового программно-аппаратного комплекса (ПАК), обеспечивающего распределение между сущностями (элементами) системы квантового Интернета вещей (КИВ) (см. ПНСТ 831—2023 и ПНСТ 832—2023) ключей, выработанных сетью квантового распределения ключей (КРК) (см. ПНСТ 829—2023 и ПНСТ 830—2023).

Данный ПАК позволяет обеспечить защищенную доставку квантовозащищенных ключей до различных типов устройств КИВ, в том числе расположенных в удаленных и труднодоступных местах, до подвижных устройств КИВ, а также до устройств КИВ, не имеющих двусторонней связи с инфраструктурой системы КИВ.

Описание в стандарте архитектуры типового ПАК представлено на высоком уровне с целью стандартизации общего состава необходимого оборудования и его основных функций.

Сети КРК являются внешними системами по отношению к представленному типовому ПАК, поэтому вопросы, связанные с их внутренним функционированием, в том числе алгоритмы выработки ключей квантовыми методами, в настоящем стандарте не рассматриваются.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Квантовый Интернет вещей

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

Архитектура

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

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

1 Область применения

Настоящий стандарт устанавливает архитектуру типового программно-аппаратного комплекса распределения ключей, выработанных сетью квантового распределения ключей (ПАК РКК), распределяющего ключи до различных сущностей системы квантового Интернета вещей (КИВ) (например, устройств КИВ, подсистем КИВ и др.), прямое подключение которых к сетям квантового распределения сетей (КРК) технически невозможно или нецелесообразно.

Архитектура программно-аппаратного комплекса позволяет обеспечить распределение ключей в системе КИВ следующими способами:

- с использованием проводных и беспроводных сетей передачи данных;
- использованием отчуждаемого носителя ключевой информации.

Одним из примеров возможного применения ПАК РКК является система КИВ, состоящая из большого количества устройств КИВ, имеющих двустороннюю связь с несколькими базовыми станциями (БС) сети КИВ. В данном случае использование ПАК РКК на БС сети КИВ позволит обеспечить получение секретных ключей в узлах сети КРК, наиболее близко расположенных к БС сети КИВ, и распределение полученных ключей через БС сети КИВ.

Другим примером является система КИВ, устройства которой имеют только обратный канал связи (т. е. канал от устройств КИВ к сети КИВ). В данном случае распределение секретных ключей, выработанных сетью КРК, на устройства КИВ может обеспечиваться путем их записи в ПАК РКК на отчуждаемые носители ключевой информации (ОНКИ) и доставки ОНКИ до устройств КИВ.

Настоящий стандарт не устанавливает требований к построению сетей КРК.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ПНСТ 829—2023 Квантовые коммуникации. Общие положения

ПНСТ 830—2023 Квантовые коммуникации. Термины и определения

ПНСТ 832—2023 Квантовый Интернет вещей. 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

Издание официальное

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 и ПНСТ 832—2023, а также следующие термины с соответствующими определениями:

3.1 **объект квантового Интернета вещей;** (ОКИВ): Любая сущность системы КИВ (например, устройство КИВ или подсистема КИВ), подключенная к программно-аппаратному комплексу распределения ключей, выработанных сетью квантового распределения ключей, для получения квантовозащищенного ключа.

3.2 **узел распределения ключей;** УРК: Элемент программно-аппаратного комплекса распределения ключей, выработанных сетью квантового распределения ключей, обеспечивающий получение квантовозащищенного ключа из сети квантового распределения ключей и распределение квантовозащищенного ключа между ОКИВ.

3.3 **узел связи с объектами;** УСО: Элемент программно-аппаратного комплекса распределения ключей, выработанных сетью квантового распределения ключей, обеспечивающий коммуникационное взаимодействие УРК с ОКИВ.

3.4

контролируемая зона: Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств.

[ГОСТ Р 56115—2014, статья 3.1.2]

3.5 **ключ доставки;** КД: Ключ, используемый для защищенной передачи квантовозащищенного ключа от УРК в ОКИВ.

3.6 **парные ОКИВ:** Два ОКИВ, получающие общие квантовозащищенные ключи.

3.7 **квантовозащищенный ключ;** (КЗК): Секретный ключ, защита которого при передаче или хранении осуществляется с использованием квантового(ых) ключа(ей).

Примечание — см. ПНСТ 830—2023.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ДПУ — доверенный промежуточный узел;
КИВ — квантовый Интернет вещей;
ККС ВРК — квантовая криптографическая система выработки и распределения ключей;
КРК — квантовое распределение ключей;
ОНКИ — отчуждаемый носитель ключевой информации;
ПАК — программно-аппаратный комплекс;
ПАК РКК — ПАК распределения ключей, выработанных сетью КРК;
ПАТ РКСО — программно-аппаратный терминал распределения ключей и связи с объектами;
ПРС — подвижная радиосвязь;
СВРК — система выработки и распределения ключей;
СКЗИ — средство криптографической защиты информации.

5 Задачи ПАК РКК

Основными задачами ПАК РКК являются:
- подключение, регистрация и аутентификация ОКИВ;
- сопряжение с узлами сети КРК;
- обработка запросов от ОКИВ на выдачу КЗК;
- получение КЗК из узлов сети КРК;
- распределение и доставка КЗК до ОКИВ.

6 Архитектура и основные функции компонентов ПАК РКК

6.1 ПАК РКК включает:

а) УРК, обеспечивающий сопряжение с сетью КРК, а также распределение и доведение КЗК до объектов КИВ;

б) УСО, обеспечивающий коммуникационное взаимодействие УРК с объектами КИВ.

6.2 УРК должен обеспечивать:

а) подключение по защищенному протоколу к ДПУ сети КРК в качестве СКЗИ-потребителя и получение от них КЗК как для собственного использования, так и для последующего распределения ОКИВ (в том числе устройствам КИВ и подсистемам КИВ) для обеспечения их взаимодействия на КЗК;

б) получение и загрузку первичной ключевой информации (порядок получения и загрузки выходит за рамки настоящего стандарта);

в) распределение по защищенному протоколу КЗК для связи между ОКИВ. ОКИВ, подключаемые к УРК, должны быть СКЗИ-потребителями;

г) распределение по защищенному протоколу КЗК для связи между ОКИВ, подключенными как к одному УРК, так и к различным УРК;

д) взаимодействие с другими УРК по защищенному протоколу;

е) при необходимости, перешифрование КЗК и изменение формата контейнеров КЗК.

6.3 УРК, создаваемые различными производителями, могут объединяться в единую сервисную платформу. Допустимо централизованное и децентрализованное управление различными УРК.

УРК должны обеспечивать возможность распределения и доведения КЗК до ОКИВ в том случае, если они подключены к различным, но сопряженным сетям КРК.

Допустимо подключение УРК непосредственно к отдельным ККС ВРК. В этом случае подключение производится к модулю КРК (см. ПНСТ 829—2023).

УРК может обеспечивать запись КЗК на ОНКИ в доверенной зоне для доставки КЗК на ОКИВ посредством ОНКИ. УСО должно обеспечивать коммуникационное взаимодействие ОКИВ с УРК с использованием Интернет или другой сети передачи данных, например: через сети проводной связи, сети подвижной радиосвязи 3G—5G, сети WiFi, ZigBee, Bluetooth, Bluetooth Low Energy, NFC и др. УСО должно реализовывать физический, канальный и сетевой уровни взаимодействия с ОКИВ, а также — при необходимости — транспортный уровень.

ОКИВ должны иметь в своем составе СКЗИ [программный или аппаратный модуль (далее — СКЗИ-модуль)] для операций с КЗК и для криптографической защиты информации, передаваемой через коммуникационную сеть КИВ.

Количество УРК и УСО в составе ПАК РКК определяется в зависимости от количества и территориального расположения ОКИВ, которым необходимо обеспечить доставку КЗК.

Архитектура типового ПАК РКК показана на рисунке 1.

Пример реализации ПАК РКК с централизованным управлением УРК приведен в приложении А.

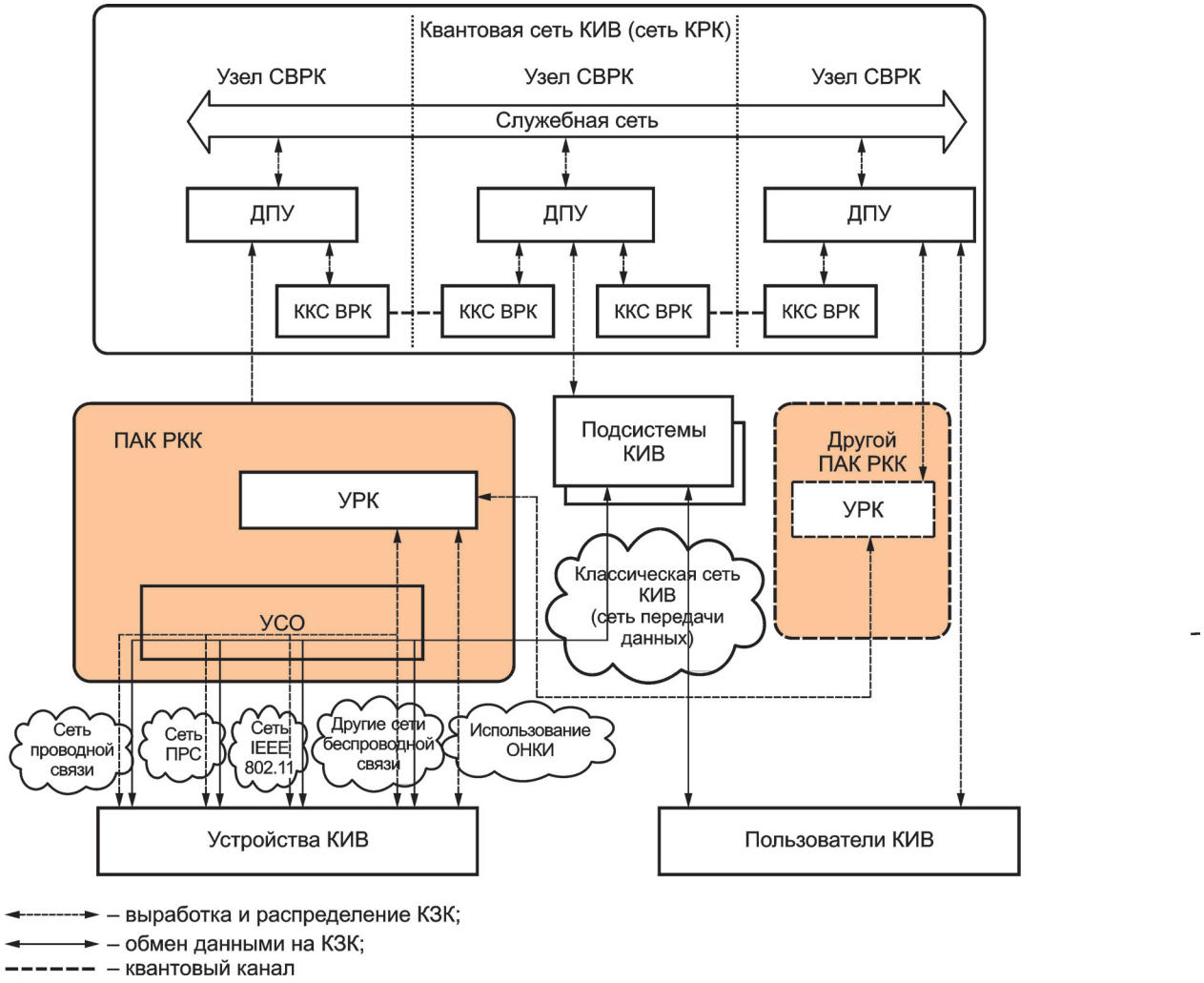

Рисунок 1 — Архитектура ПАК РКК и взаимодействующие с ПАК РКК элементы системы КИВ

Приложение А
(справочное)

Пример реализации типового ПАК РКК с централизованным управлением и с записью КЗК на ОНКИ

А.1 ПАК РКК с централизованным управлением включает:

- один или несколько программно-аппаратных терминалов распределения ключей и связи с объектами (ПАТ РКСО), состоящих из УРК и УСО;
- сервер ПАК.

Доставка КЗК от ПАК РКК в ОКИВ осуществляется:

- через транспортную (проводную/беспроводную) сеть;
- путем прямой записи КЗК на ОНКИ ОКИВ в доверенной зоне ПАТ.

А.2 Сервер ПАК обеспечивает мониторинг и управление работой ПАТ, включая хранение информации о структуре ПАК, идентификаторах, входящих в ПАК ПАТ и зарегистрированных ОКИВ, в том числе:

- хранение базы данных ОКИВ, зарегистрированных в ПАК;

- синхронизацию запросов парных ПАТ к узлам сети КРК;
- управление жизненным циклом КЗК в ПАТ;
- определение и выдачу идентификатора парного ПАТ[1)] по идентификатору парного ОКИВ;
- обеспечение доступа для администрирования ПАК РКК.

Сервер ПАК может быть отдельным устройством или входить в состав одного из ПАТ (центрального ПАТ).

Пример архитектуры ПАК РКК с централизованным управлением приведен на рисунке А.1.

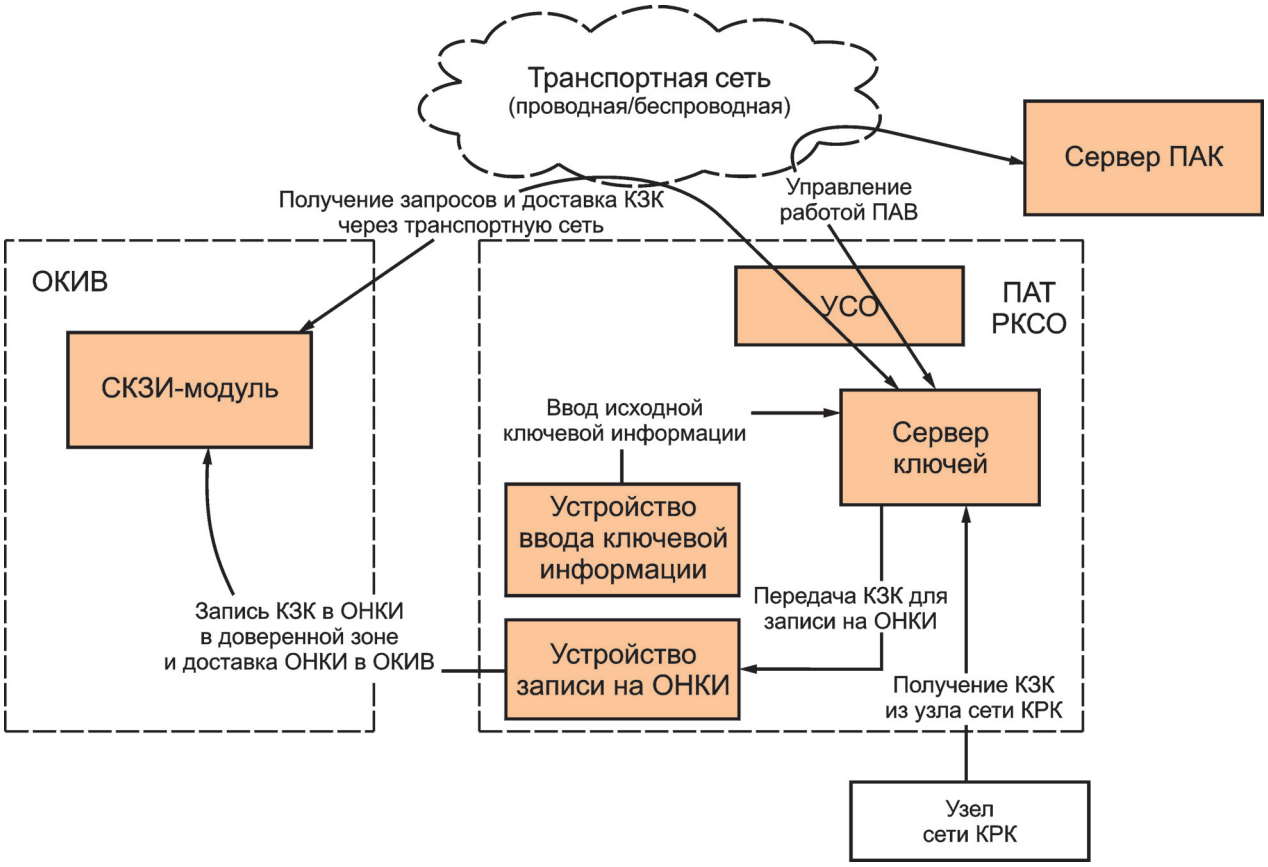

Рисунок А.1 — Пример архитектуры ПАК РКК с централизованным управлением

А.3 Основными функциями ПАТ являются:

а) регистрация и первичная идентификация ОКИВ в ПАК РКК;

б) проведение взаимной аутентификации с ОКИВ, сервером ПАК и с узлом сети КРК;

в) сопряжение с узлом сети КРК и получение КЗК;

г) запись КЗК в ОНКИ ОКИВ в доверенной зоне с использованием устройства записи;

д) получение запроса от подключенных ОКИВ на выдачу КЗК через транспортную сеть;

е) доставка в защищенном виде КЗК в ОКИВ (через транспортную сеть или посредством ОНКИ).

А.4 УРК включает: сервер ключей, устройство ввода ключевой информации и устройство записи на ОНКИ.

Сервер ключей обеспечивает выполнение основных функций УРК, в том числе сопряжение с сетью КРК и получение КЗК, регистрацию ОКИВ, обработку запросов ОКИВ на выдачу КЗК и их защищенную передачу через транспортную сеть, а также запись КЗК на ОНКИ ОКИВ в доверенной зоне.

Устройство ввода ключевой информации ПАТ используют для ввода исходной ключевой информации, необходимой для обеспечения взаимной аутентификации с другими компонентами ПАК РКК и узлами сети КРК, а также для защиты передаваемых сообщений.

Для ОКИВ, имеющих связь с ПАТ посредством УСО (подключенные ОКИВ), первичная запись на ОНКИ ключей аутентификации, ключей доставки и, при необходимости, ключей для обеспечения защищенной связи между ОКИВ осуществляется в доверенной зоне ПАТ при регистрации ОКИВ. Далее получение КЗК для обеспечения защищенной связи между ОКИВ и, при необходимости, обновление ключей аутентификации и ключей доставки осуществляется посредством направления соответствующего запроса в ПАТ через транспортную сеть. ПАТ при получении данного запроса формирует КЗК и передает их в ОКИВ в защищенном виде.

[1)] Парные ПАТ — ПАТ, обеспечивающие передачу КЗК парным ОКИВ.

Для ОКИВ, не имеющих связь с ПАТ посредством УСО (автономные ОКИВ), запись и обновление ключей аутентификации, ключей доставки и ключей для обеспечения защищенной связи между ОКИВ осуществляется в доверенной зоне ПАТ с использованием ОНКИ. Набор записываемых КЗК выбирается исходя из перечня парных ОКИВ, для которых планируется установление защищенных соединений в системе КИВ, а также с учетом планируемой частоты смены КЗК.

А.5 Функционирование ПАК РКК включает следующий порядок действий:

а) осуществляется сопряжение ПАТ с сервером ПАК и регистрация ПАТ в ПАК РКК. При регистрации для ПАТ формируется уникальный идентификатор $ID_{ПАТ}$ и иные атрибуты аутентификации (при необходимости), которые хранятся в ПАТ и на сервере ПАК. Сервер ПАК хранит уникальные идентификаторы $ID_{ПАТ}$ и иные атрибуты аутентификации (при необходимости) всех зарегистрированных в комплексе ПАТ;

б) осуществляется сопряжение ПАТ с узлом сети КРК;

в) ПАТ опционально запрашивает в сети КРК и формирует набор КЗК до получения запросов на выдачу КЗК со стороны ОКИВ (далее — буфер КЗК). Порядок формирования буфера КЗК в ПАТ и синхронизация запросов между парными ПАТ осуществляется сервером ПАК:

1) ПАТ получает КЗК из сети КРК,

2) ПАТ для каждого КЗК сохраняет уникальный идентификатор $ID_{КЗК\_ПАТ}$ (внутренний идентификатор), который использовался при взаимодействии с сетью КРК. Одинаковые КЗК должны иметь одинаковый идентификатор $ID_{КЗК\_ПАТ}$ на парных ПАТ;

г) осуществляется первичная регистрация ОКИВ в ПАТ. При первичной регистрации ОКИВ в ПАТ:

1) формируется уникальный идентификатор $ID_{ОКИВ}$ и иные атрибуты аутентификации (при необходимости). Данная информация хранится в ОКИВ и ПАТ, а также передается на сервер ПАК,

2) формируются уникальные для каждого ОКИВ ключи:

- ключ аутентификации доступа к ПАТ,
- ключи доставки.

Для формирования данных ключей могут быть использованы КЗК из буфера КЗК или новые КЗК, полученные на основе запросов к сети КРК [с учетом перечисления в) 2)],

3) для автономного ОКИВ (опционально для подключенного ОКИВ) формируется матрица связей (на основе идентификаторов ОКИВ) между регистрируемым ОКИВ и другими (парными) ОКИВ, с которыми планируется установка защищенного соединения, и по ней формируется набор соответствующих ключей и идентификаторов $ID_{КЗК\_ПАТ}$ [с учетом перечисления в) 2)].

Для формирования данных ключей используются КЗК из буфера КЗК или новые КЗК, полученные на основе запросов к сети КРК [с учетом перечисления в) 2)],

4) для ключей, указанных в перечислении г) 2) и 3), формируются идентификаторы $ID_{КЗК\_ОКИВ}$ (внешние идентификаторы) и таблица соответствия между соответствующими внутренними и внешними идентификаторами ($ID_{КЗК\_ПАТ}$, $ID_{КЗК\_ОКИВ}$) таким образом, что КЗК($ID_{КЗК\_ПАТ}$) = КЗК($ID_{КЗК\_ОКИВ}$),

5) для КЗК, предназначенных для ОКИВ, зарегистрированных в разных ПАТ, ПАТ направляет таблицу соответствия ($ID_{КЗК\_ПАТ}$, $ID_{КЗК\_ОКИВ}$) другому парному ПАТ. Парный ПАТ проверяет наличие КЗК с идентификаторами $ID_{КЗК\_ПАТ}$ в буфере КЗК, при их отсутствии запрашивает выдачу КЗК из сети КРК и включает данные КЗК в буфер КЗК. Затем парный ПАТ присваивает $ID_{КЗК\_ОКИВ}$ соответствующим ключам согласно таблице соответствия ($ID_{КЗК\_ПАТ}$, $ID_{КЗК\_ОКИВ}$),

6) проводится защищенная запись КЗК, сформированных в перечислении г) 2) и 3), а также их идентификаторов $ID_{КЗК\_ОКИВ}$ в ОНКИ,

7) ОНКИ с ключами [см. перечисление г) 6)] доставляется до ОКИВ и осуществляется запись ключей в хранилище ключей СКЗИ-модуля (хранилище ключей ОКИВ);

д) автономные ОКИВ осуществляют защищенную связь с использованием КЗК, записанных в хранилище ключей ОКИВ;

е) подключенные ОКИВ осуществляют защищенную связь с использованием КЗК, записанных в хранилище ключей ОКИВ, или с применением КЗК, которые получают через транспортную сеть следующим способом:

1) ОКИВ, инициирующий защищенную передачу данных ($ОКИВ_1$) направляет авторизованный запрос на выдачу КЗК в ПАТ ($ПАТ_1$), в котором он зарегистрирован с предоставлением собственного $ID_{ОКИВ1}$, необходимых атрибутов аутентификации и идентификатора парного ОКИВ $ID_{ОКИВ2}$. В рамках одной сессии запроса и получения КЗК ОКИВ может осуществляться запрос нескольких КЗК,

2) $ПАТ_1$ проверяет регистрацию парного ОКИВ ($ОКИВ_2$),

3) если парный $ОКИВ_2$ зарегистрирован на другом ПАТ, то $ПАТ_1$ направляет запрос на сервер ПАК на выдачу идентификатора парного ПАТ ($ID_{ПАТ2}$) по идентификатору парного ОКИВ ($ID_{ОКИВ2}$),

4) $ПАТ_1$ выбирает КЗК из буфера КЗК [см. перечисление в)] или запрашивает новый КЗК в сети КРК. Для КЗК, полученного из сети КРК, формируется $ID_{КЗК\_ПАТ}$ согласно перечислению в) 2). Затем для КЗК определяется $ID_{КЗК\_ОКИВ}$ согласно перечислению г) 4). В случае запроса нескольких КЗК каждый КЗК должен иметь уникальный $ID_{КЗК\_ОКИВ}$. Если $ОКИВ_1$ и $ОКИВ_2$ зарегистрированы в разных ПАТ, то выполняется действие по перечислению г) 5),

5) $ПАТ_1$ защищенным способом передает идентификатор $ID_{КЗК\_ОКИВ}$ и КЗК ($ID_{КЗК\_ОКИВ}$) на $ОКИВ_1$ с использованием ключа доставки,

6) $ОКИВ_1$ согласует по информационному каналу $ID_{КЗК\_ОКИВ}$ с $ОКИВ_2$,

7) парный $ОКИВ_2$ по $ID_{КЗК\_ОКИВ}$ осуществляет аутентифицированный запрос на получение КЗК ($ID_{КЗК\_ОКИВ}$) у $ПАТ_2$, к которому он подключен, с предоставлением собственного $ID_{ОКИВ2}$ и прочих атрибутов аутентификации (при необходимости), а также $ID_{КЗК\_ОКИВ}$,

8) $ПАТ_2$, используя таблицу соответствия между $ID_{КЗК\_ПАК}$, $ID_{КЗК\_ОКИВ}$, полученную согласно перечислению г) 5), осуществляет выдачу КЗК ($ID_{КЗК\_ОКИВ}$) из буфера КЗК,

9) $ОКИВ_1$ и $ОКИВ_2$ осуществляют защищенную передачу сообщений с использованием КЗК ($ID_{КЗК\_ОКИВ}$).

Пример ПАК РКК, состоящего из двух ПАТ, с двумя ОКИВ, подключенными к разным ПАТ, приведен на рисунке А.2. На рисунке А.2 также указаны функциональные связи между ОКИВ и элементами ПАК РКК согласно приведенной выше нумерации.

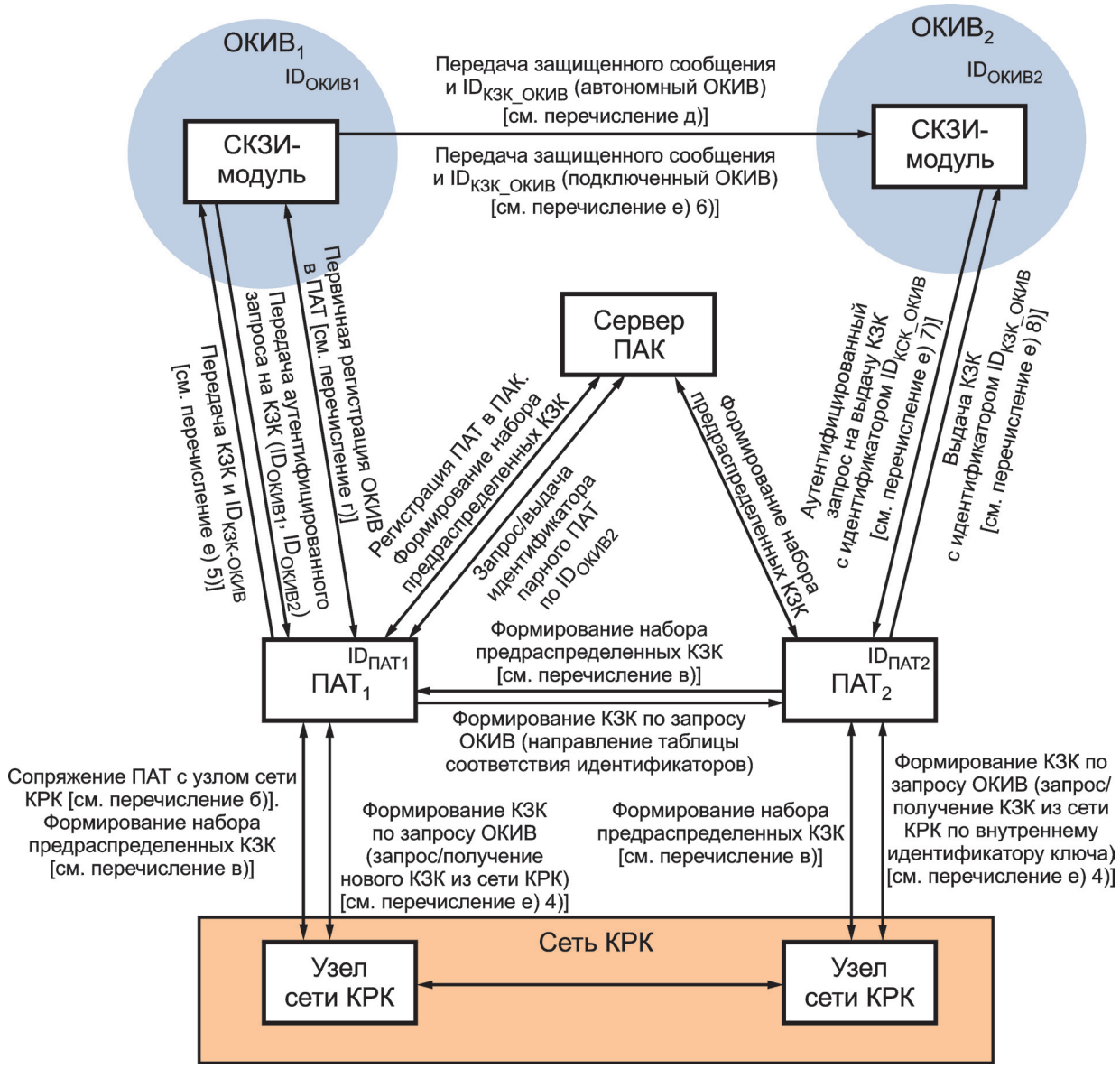

Рисунок А.2 — Пример функциональных связей ПАК РКК с централизованным управлением

УДК 004.738:006.354 ОКС 35.110

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

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

Сдано в набор 10.01.2024. Подписано в печать 29.01.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,26.

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