**Интерфейс и протокол обмена**

Для обмена данными между сервером QKD и внешними устройствами предлагается использовать Ethernet по протоколу UDP (User Datagram Protocol) c полезной нагрузкой не более 1432 байт.

## Общее для всех пакетов

* Посылаемые из управляющего устройства на сервер QKD команды и запросы данных отправляются в порт 5551.
* Ответы, подтверждающие прием команды или содержащие запрашиваемые данные отправляются в порт 5552.
* IP адрес ответа равен IP адресу отправителя последней принятой команды.
* Нумерация всех сущностей начинается с 0.
* В случае, если данные занимают меньше, чем размер сетевого пакета, пакет отправляется как есть, без заполнения.
* На каждый запрос должен быть отправлен соответствующий ответ, содержащий код ошибки, или результат выполнения.
* Порядок следования байт - big-endian.

**Таблица 1.** Порты для передачи данных

|  |  |  |
| --- | --- | --- |
| Номер порта | Назначение | Примечания |
| **5551** | Отправка всех команд и запросов на сервер QKD. | Исходящий порт - любой.  Структура пакета - ***REQUEST***. |
| **5552** | Отправка ответов на запросы и команды c сервера QKD. | Исходящий порт - любой.  Структура пакета - ***REPLY***. |

**Таблица 2.** Общий формат *заголовка* команд и запросов данных (из внешнего устройства на сервер QKD) - ***REQUEST***.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Размер, байт | Название | Примечание |
| 0 | 4 | общесистемная метка пакетов | Константа, ACEAACEBh |
| 1 | 2 | идентификатор запроса | Должен быть возвращен в ответе на запрос. Для каждого запроса отправляется свой уникальный идентификатор. Например, можно использовать автоинкремент. |
| 2 | 2 | код команды |  |
| 3 | 8 | зарезервировано |  |
| 4 | до 1416 | данные | Зависит от кода команды |

**Таблица 3.** Общий формат *заголовка* ответов (из прибора на ПК) - ***REPLY***.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Размер, байт | Название | Примечание |
| 0 | 4 | общесистемная метка пакетов | Константа, ACEAACEBh |
| 1 | 2 | идентификатор запроса | переданный в соответствующем запросе |
| 2 | 2 | код результата | >= 0 – успех, < 0 - неудача |
| 3 | 8 | зарезервировано |  |
| 4 | до 1416 | данные | зависит от кода команды |

**Таблица 4.** Коды команд (поле *код команды* структуры ***REQUEST***).

|  |  |  |
| --- | --- | --- |
| Код команды | Описание команды | Примечание |
| 1 | Запрос ключа по длине | В поле *данные* структуры ***REQUEST***  передается структура ***KEY\_BY******\_LENGTH\_REQUEST***  В поле *данные* структуры ***REPLY*** возвращается структура ***KEY\_BY\_LENGTH\_REPLY*** или структура ***ERROR\_DESCRIPTION*** |
| 2 | Запрос ключа по квиду | В поле *данные* структуры ***REQUEST***  передается структура ***KEY\_BY\_ID\_REQUEST***  В поле *данные* структуры ***REPLY*** возвращается структура ***KEY\_BY\_ID\_REPLY*** или структура***ERROR\_******DESCRIPTION*** |

**Таблица 5.** Коды ошибок (поле *код результата* структуры ***REPLY***).

|  |  |  |
| --- | --- | --- |
| Код результата | Описание кода результата | Примечание |
| 0 | Успешный ответ, никаких ошибок не возникло. |  |
| -1 | Сервер занят или перегружен, необходимо повторить запрос позднее. | ERROR\_BUSY |
| -2 | Недостаточно накопленного ключа на сервере, необходимо повторить запрос позднее. | ERROR\_KEY\_EXHAUSTED |
| -99 | Внутренняя ошибка сервера | ERROR\_INTERNAL |
| -101 | Указан неверный идентификатор ключа (несуществующий, использованный или истёкший) | ERROR\_KEY\_UNKNOWN |
| -102 | Указано недопустимое значение параметра. | ERROR\_INVALID\_ARGUMENT |
| -201 | Потеряно соединение с устройством квантовой криптографии |  |

**Таблица 6.** Формат данных для запроса ключа по длине (передается в поле *данные* структуры ***REQUEST***  с кодом команды 1) - ***KEY\_BY\_LENGTH\_REQUEST***.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Размер, байт | Название | Примечание |
| 0 | 4 | Запрашиваемая длина ключа в байтах | Из-за ограничений на длину пакета может быть не более 1384 байт |

**Таблица 7.** Формат данных ответа на запрос ключа по длине (передается в поле *данные* структуры ***REPLY***) - ***KEY\_BY\_LENGTH\_REPLY***.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Размер, байт | Название | Примечание |
| 0 | 16 | Квид - идентификатор ключа | Используется для последующего получения этого ключа на другой стороне. |
| 1 | 8 | Время действия ключа | Представлено как UNIX timestamp в миллисекундах в зоне UTC+0 |
| 2 | 8 | Зарезервировано |  |
| 3 | до 1384 | Квантовый ключ |  |

**Таблица 8.** Формат данных для запроса ключа по длине (передается в поле *данные* структуры ***REQUEST***  с кодом команды 2) - ***KEY\_BY\_ID\_REQUEST***

|  |  |  |  |
| --- | --- | --- | --- |
| № | Размер, байт | Название | Примечание |
| 0 | 16 | Квид - идентификатор ключа |  |

**Таблица 9.** Формат данных ответа на запрос ключа по длине (передается в поле *данные* структуры ***REPLY***) - ***KEY\_BY\_ID\_REPLY***.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Размер, байт | Название | Примечание |
| 0 | до 1384 | Квантовый ключ |  |

**Таблица 10.** Формат данных ответа на запрос при возникновении ошибки (передается в поле *данные* структуры ***REPLY***) - ***ERROR\_DESCRIPTION***.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Размер, байт | Название | Примечание |
| 0 | 8 | Время в секундах, через которое можно повторить запрос | Имеет тип double. Может иметь ненулевое значение при кодах ошибки от -1 до -99.  На данный момент всегда 0. |
| 1 | 8 | Зарезервировано |  |
| 2 | до 1392 | Текстовое описание ошибки |  |