**Протокол взаимодействия с USB ключом.**

Имя ключа-«Key V3.7»

Команда, отправляемая с ПК, представляет собой пакет следующего вида.

[Команда 1 байт] [Данные n байт] [Контрольная сумма crc32]

Данные возвращаемые ключом представляют собой следующую посылку:

[Идентификатор] [Данные n-байт] [Контрольная сумма crc32]

|  |  |  |
| --- | --- | --- |
| **Команды с ПК** | **Ответ Usb ключа.** | **Примечание** |
| Проверка наличия правильного устройства-0x3C | Некоторая константа из 8 байт (или более) (серийный аппаратный номер устройства)  или ответ «Не верная CRC». |  |
| Отправка серийного номера для записи во Flash память 0xA0  Данные – серийный ключ | «Команда подтверждена»  или ответ «Не верная CRC». |  |
| Отправка ключа RSA для шифрования сеансового ключа - 0xA9  Данные-ключ шифрования. | «Команда подтверждена»  или ответ «Не верная CRC». |  |
| Получить шифрованный ключом серийный номер-0x07 | Пакет с данными или  «Не верная CRC». | В ответе передается шифрованный RSA сеансовый ключ для AES и зашифрованный им серийный номер |
| Запись времени во Flash-0x15.  Данные-время. | «Команда подтверждена» или  ответ «Не верная CRC». | Используется три ячейки флэш памяти. Таким образом всегда есть статистика трех последних временных отпечатков. Время пишется только в днях. Перед записью проверить-не записано ли там уже такое точно значение.  Предусмотреть возможность проверок ячеек на случай ошибок. |
| Получить последнее актуальное время-0x17  Данные-любые. | Пакет с данными или  «Не верная CRC». |  |
| Любая команда-0xXX  Данные-любые. | Пакет с данными или  «Не верная CRC». |  |