**Этап 6 - Реализация функции шифрования-дешифрования прошивки при передаче по сети**

Ранее прошивка передавалась между программой Конфигуратор и прошиваемым устройством по локальной сети в незашифрованном виде, что позволяло легко получить доступ извне к прошивке. На данном этапе реализован функционал шифрования-дешифрования прошивки. Прошивка по сети передается в зашифрованном виде.

Применяется симметричный алгоритм AES128 - длина ключа 128 бит (16 символьный ключ) один ключ и для шифрования и для дешифрования. Теперь свой ключ шифрования прописан на каждом устройстве и не зная его, прошить устройство по сети нельзя. При запуске программы Конфигуратор для прошивки устройства по локальной сети нужно указать ключ шифрования. В соответствии с указанным ключом формируется зашифрованная прошивка, к которой в конец добавляется хеш-сумма исходной незашифрованной прошивки. Прошиваемый пульт получает зашифрованную в конфигураторе прошивку, декодирует ее в соответствии с ключом устройства и вычисляет хеш-сумму декодированной прошивки. Если вычисленная хеш-сумма совпала с полученной хеш-суммой, производится прошивка пульта и устройство автоматически перезагружается

Если в конфигураторе введен неверный ключ, то хеш-суммы не совпадут и прошивка не начнется, а включится индикация - мигающий красный светодиод. В дальнейшем планируется расширить функционал программы Конфигуратор - при передаче в Конфигуратор файла прошивки, автоматически детектируется тип прошивки (зашифрованная или нет) и если зашифрована -отключается необходимость вводить ключ - сразу начинается передача по сети (в током виде Конфигуратор можно передавать Заказчику и в дальнейшем передавать ему прошивки в зашифрованном виде)

**Этап 7 - Реализация функции шифрования-дешифрования пакетов при передаче по сети**

Ранее аудиопакеты между пультами передавались по сети в незашифрованном виде. Теперь реализовано шифрование аудиопакетов 16 символьным ключом. 128 битовый ключ один и для шифрования прошивки и для шифрования пакетов и он привязан к каждому пульту. Теперь связь возможно устанавливить только между пультами с одинаковым ключом.

Между пультами с разными ключами связь будет установлена, но в динамике будет тишина.

При фомировании каждого аудиопакета добавлен следующий функционал:

- вычисляется контрольная сумма CRC32 каждого аудиопакета и добавляется в аудиопакет

- аудиопакет шифруется с применением ключа, привязанного в пульту и передается в сеть в зашифрованном виде

- на пульте - получателе каждый аудиопакет дешифруется ключом, привязанным к пульту, затем вычисляется его контрольная сумма CRC32 и она сравнивается с CRC32, которая пришла в пакете.

- Если суммы совпали - пакет пропускается далее в звуковой тракт, иначе пакет обнуляется.

**Этап 8 - Реализация одновременной перепрошивки всех устройств системы**

Добавлен новый функционал в программу Конфигуратор. Реализована возможность одновроменной прошивки всех устройств.

В конфигураторе устанить галочку в чекбокс Send to everyone и затем нажать кнопку Upload Firmware. Успешно будут прошиты только те пульты, ключ которых совпададет с ключем, введенным в Конфигураторе. Число прошиваемых устройств не ограничено.

**Этап 9 - Реализация функции формирования уникального идентификатора устройства для архивов**

Добавлен новый функционал. У каждого устройства формируется UID - уникальный 24 симфольный идентификатор, который всегда постоянен и не зависит от адреса устройства. Релизовано добавление UID в каждый отправляемый устройством пакет, таким образом в дальнейшем, при необходимости, всегда можно идентифицировать отправителя пакета. Также это позволит добавлять новые функции, привязанные к устройствам, и не зависящие от смены адреса в конфигураторе. Чтобы увидеть формируемый UID нужна программа-сканер сетевых пакетов, например Wireshark (ранее длина каждого пакета составляла 1296 байт, новая длина каждого пакета 1321 байт и UID устройства виден при анализе сканером в каждом пакете с 43 по 67 байт)