

1. Функционал в микроконтроллере (4.10) [Все функции для мк]
 - Идентификация пользователя по username/password
 - Генерация неизвлекаемого мастер ключа с помощью ФДСЧ
 - Его обработка с помощью хэш-функции HMAC-SHA512 по протоколу BIP 32
 - Генерация дочерних иерархически детерминированных ключевых пар согласно протоколу BIP32
 - Генерация дочерних иерархически детерминированных ключевых пар согласно протоколу BIP 43
 - Генерация дочерних иерархически детерминированных ключевых пар согласно протоколу BIP44
 - Хэширование ключа по алгоритмам SHA-256 и Ethash
 - Подпись хэш сумм криптовалютных транзакций по алгоритму ECDSA
 - Получение списка дочерних ключей проверки подписи
 - Удаление неизвлекаемого мастер ключа из Flash
 - Удаление неизвлекаемого дочернего ключа из Flash
 - Просмотр / редактирование списка разрешенных пользователей
2. Работа с журналом(11.10) [Файл в пк]
 - Генерация записей журнала
 - Просмотр журнала
 - Удаление журнала
 - Запрет выполнения операций, в случае переполнения журнала
3. Работа с приложением(27.09) [Сначала будет написано приложение с пустыми функциями, затем подключено к мк через serial]
 - Идентификация пользователя по username/password
 - Просмотр / редактирование списка разрешенных пользователей
 - Прием хэш-сумм для вызова функций вычисления электронной подписи
 - Генерации ключей подписи
 - Вызов функций удаления ключей подписи из Flash
4. Работа с flash памятью в микроконтроллере(11.10) [Добиться того, чтобы в журнале мк можно было хранить много записей]
 - Создание внутреннего журнала в микроконтроллере
 - Синхронизация журнала в мк с журналом на пк
 - Установка бита секретности