ПРОБЛЕМЫ ЗАЩИТЫ БАЗ ДАННЫХ КОНТАКТОВ И СООБЩЕНИЙ НА МОБИЛЬНЫХ УСТРОЙСТВАХ И ИХ РЕШЕНИЕ

Подготовил: студент 5-го курса 6-ой группы

Петринич Алексей

Научный руководитель : к. т. н., доцент кафедры телекоммуникаций и компьютерных технологий

Анищенко Владимир Викторович

Цель

Разработать приложение для защиты базы данных контактов и сообщений на мобильных устройствах от фирмы Apple, которое будет служить дополнительной защитой клиентских БД

Задачи

1. Изучить стандартные способы защиты платформы iOS, возможности разработки дополнительных средств защиты.

2. Разработать приложение для защиты БД контактов и сообщений для iOS.

3. Проанализировать работу, разработанного приложения

Минусы защиты iOS

Синхронизация мобильного устройства с компьютером злоумышленника

- ПК + iTunes + устройство + утилита для чтения

Подключение по ssh с произвольной записью root:alpine и получить неограниченные возможности в управлении

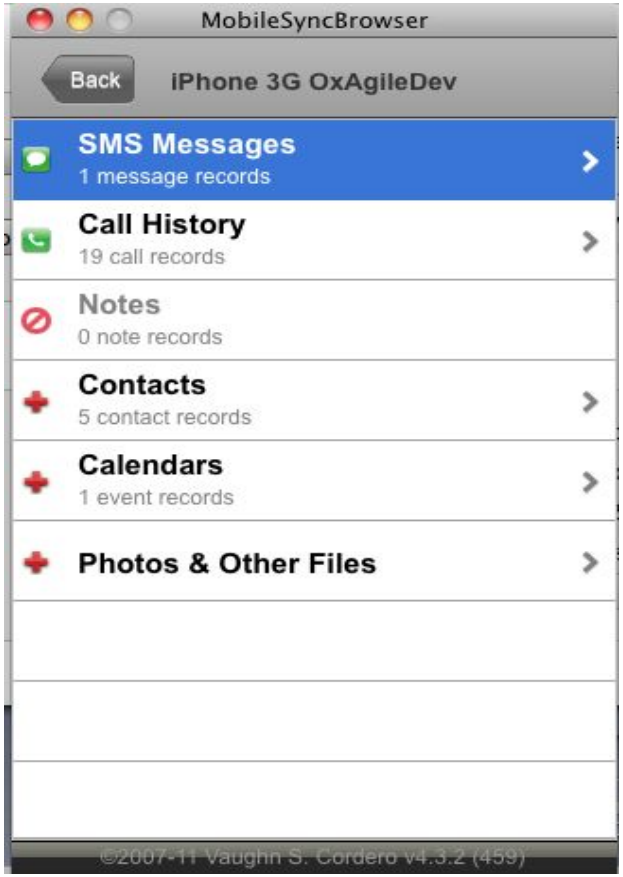
- Только на взломанных iPhone (СНГ)

Моделирование ситуации кражи данных с мобильного аппарата

Средства исследования:

1. **мобильный телефон на платформе iOS iPhone 3GS с четвертой версией прошивки**
2. **персональный компьютер на платформе Mac OS**
3. **утилита для чтения данных резервных копий данных iPhone MobileSyncBrowser.**

Моделирование ситуации кражи данных с мобильного аппарата



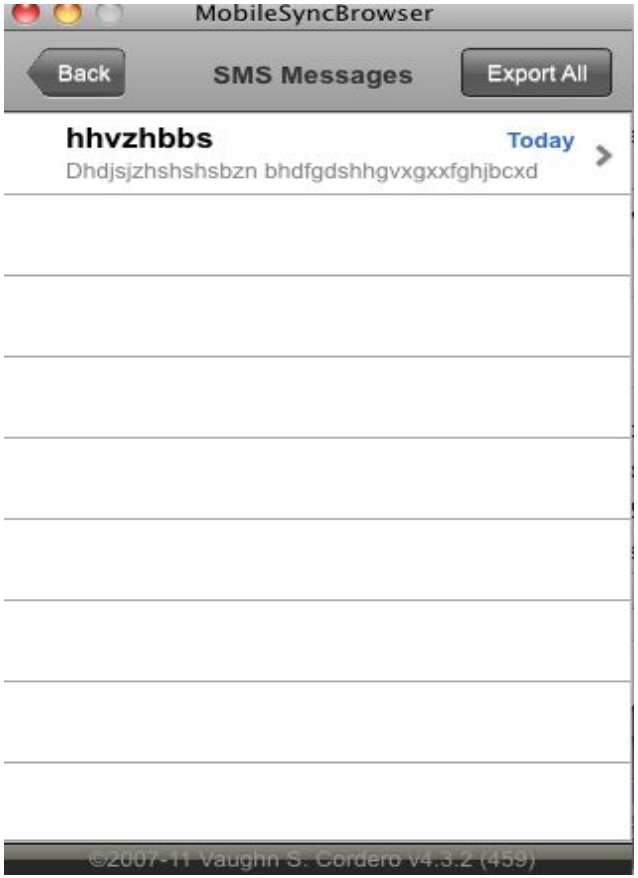
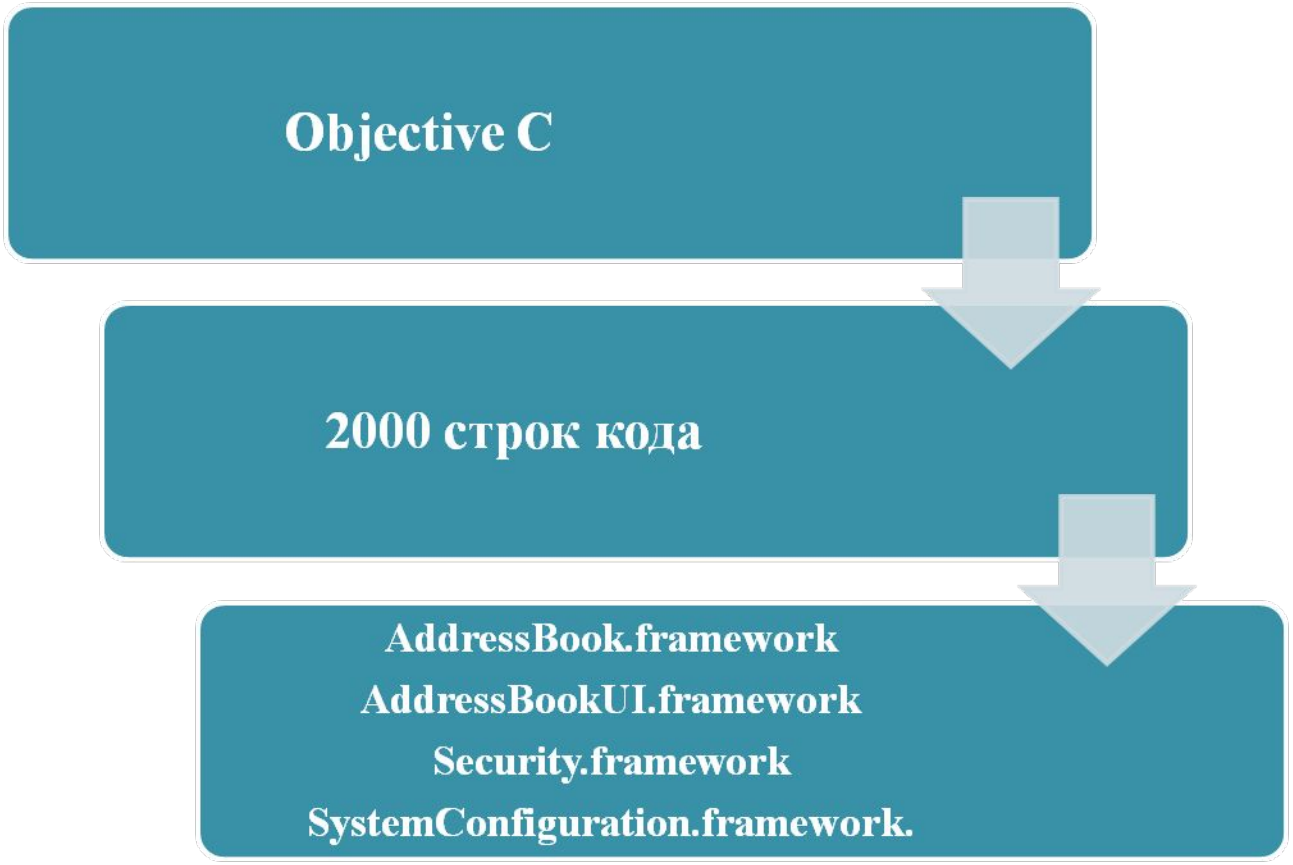


Рис.3.Просмотр файлов резервной копии с помощью MobileSyncBrowser.

Приложение



БД защищается путем ее шифрования блочным AES-алгоритмом с размером блока 128 бит
KBDiplomViewController – класс контроллера представления

Приложение

Рис.4. Запрос пароля при старте приложения.

Рис. 5. Интерфейс приложения

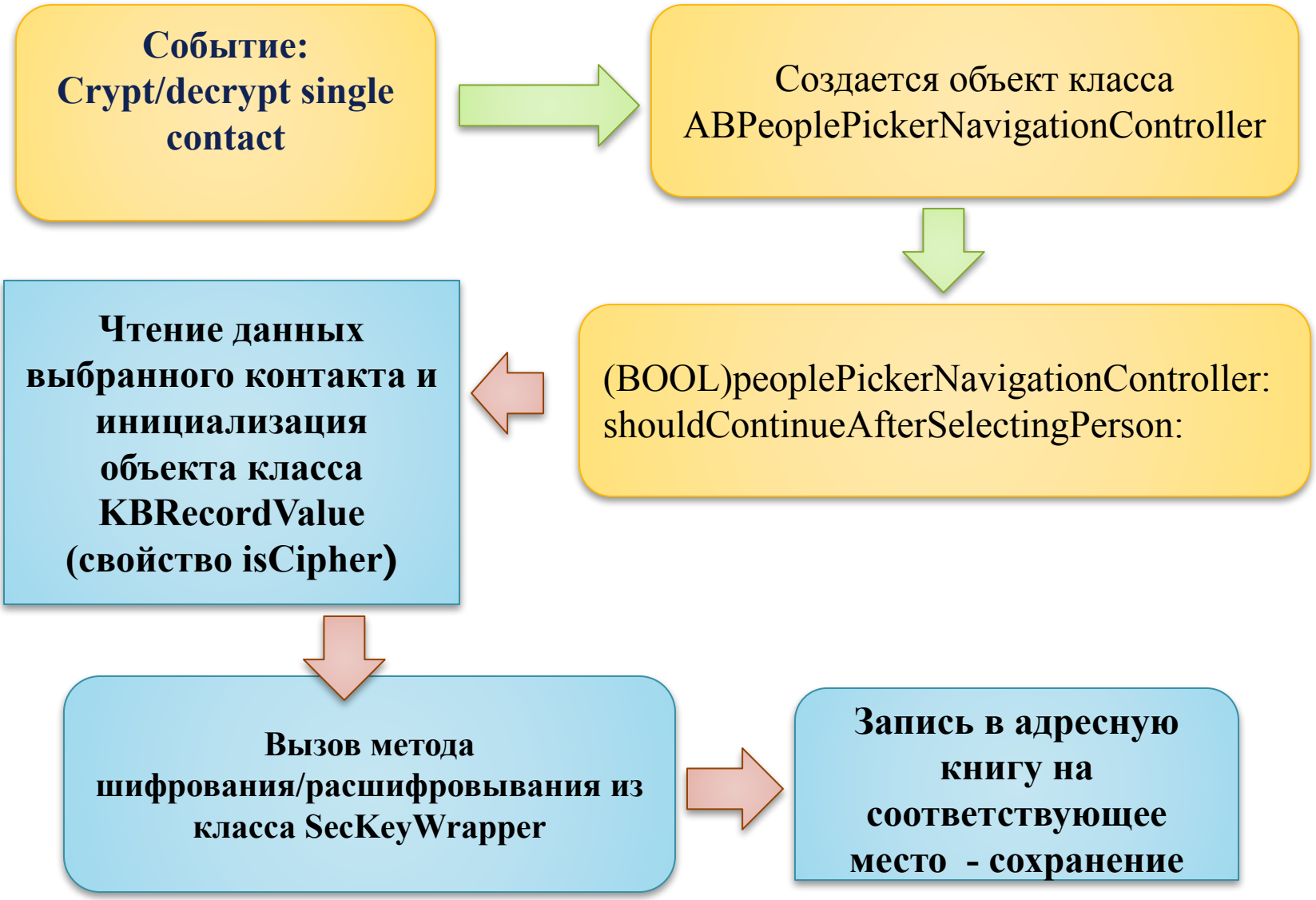
Приложение

Событие шифрования/расшифровывания БД контактов.

Приложение

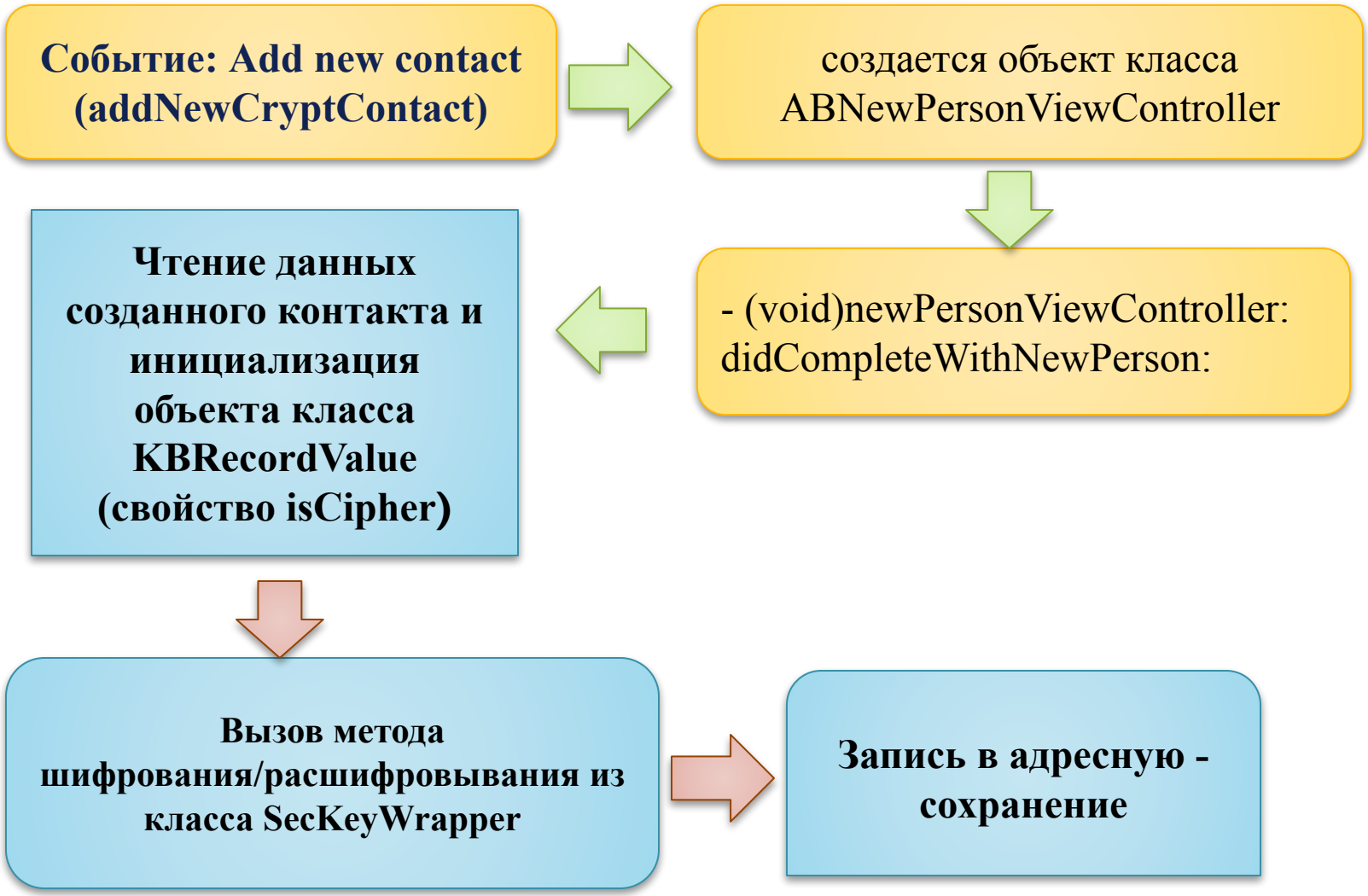
Рис. 6. Вид адресной книги после и до шифрования.

Приложение



Событие шифрования/расшифровывания одиночного контакта

Приложение



Событие добавления нового контакта в зашифрованном виде

Приложение

Событие:Change password (changePassword)

Создается объект класса UIAlertView

-(void)alertView: clickedButtonAtIndex:

Замена пароля новым, генерация нового ключа шифрования

Событие замены пароля

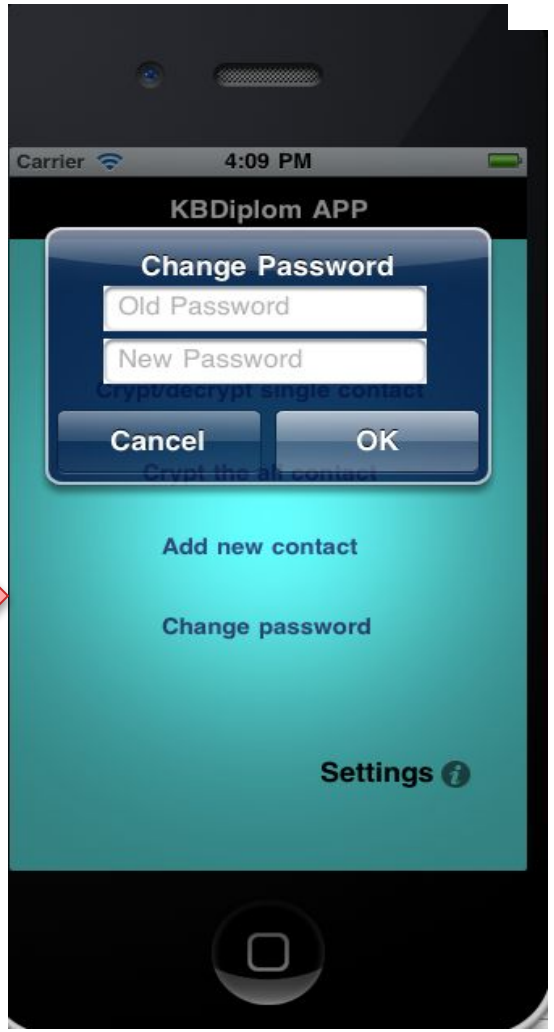
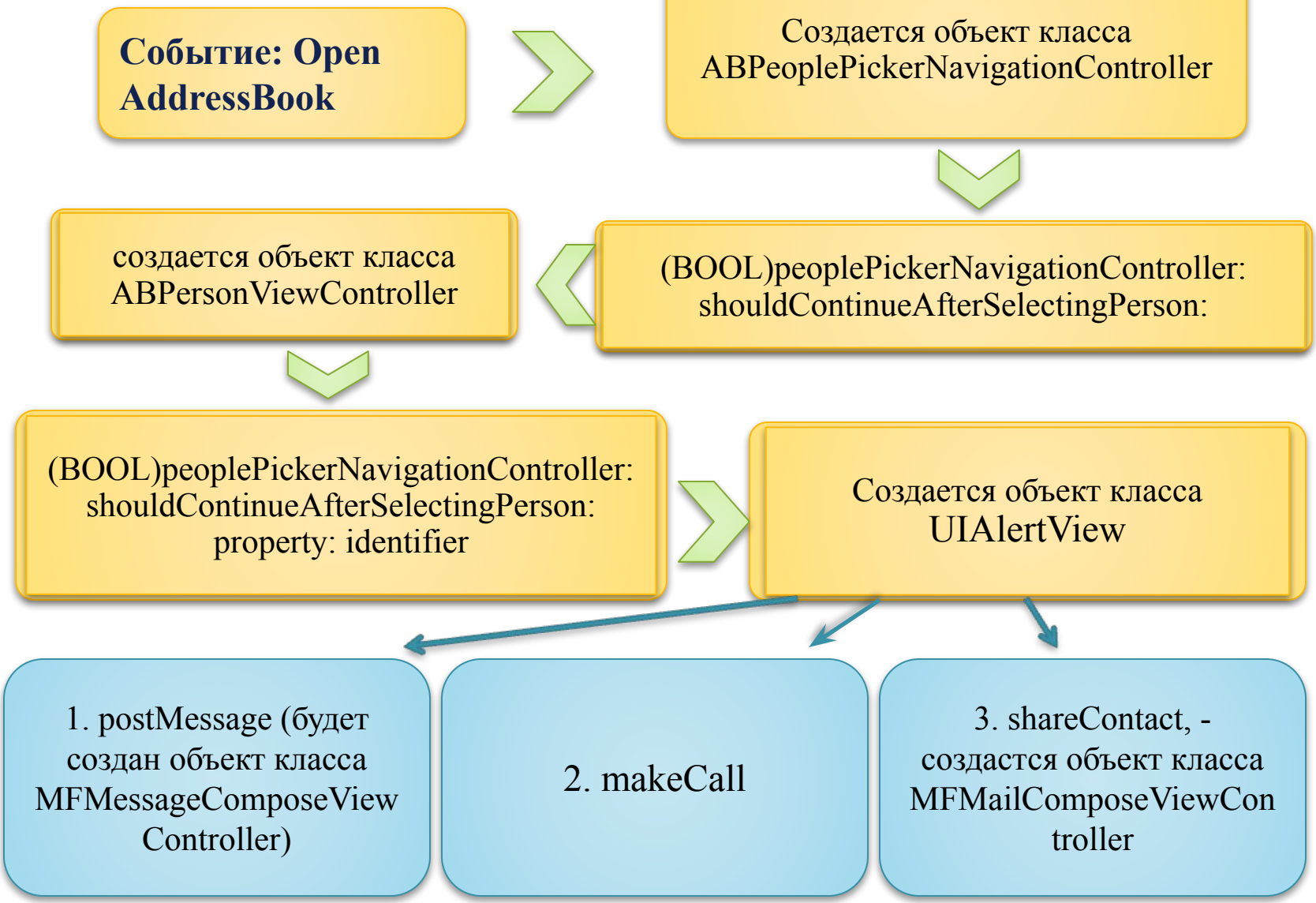


Рис. 7. Замена пароля.

Приложение


Событие: Open AddressBook
Создается объект класса ABPeoplePickerNavigationController
(BOOL)peoplePickerNavigationController: shouldContinueAfterSelectingPerson:
создается объект класса ABPersonViewController
(BOOL)peoplePickerNavigationController: shouldContinueAfterSelectingPerson: property: identifier
Создается объект класса UIAlertView
1. postMessage (будет создан объект класса MFMessageComposeView Controller)
2. makeCall
3. shareContact, - создастся объект класса MFMailComposeViewCon troller

Проблемы БД сообщений

Закрытость платформы iOS

Отсутствие API для работы с БД сообщений изнутри стороннего приложения. Только отправка СМС

Отсутствие возможности шифровать БД сообщений

Если бы данная возможность имелась

Поля сообщения: наименования контакта либо номер телефона и текст сообщения, - представляют собой объекты типов UITextField и UITextView соответственно.

Они имеют свойство text, которое содержит их текущее значение типа NSString

Преобразование в NSData

Шифрование методом класса SecKeyWrapper – doCipher: key: context: padding:

Обратное преобразование в NSString и запись значений в соответствующие поля

Заключение

1.Разработанное приложение успешно выполняет свои функции, предоставляя дополнительный уровень защиты БД контактов, защищая их от злоумышленника.

2. Разработанное приложение раскрывает новые способности последних версий платформы iOS.

3. Из-за закрытости платформы iOS нет возможности шифровать БД сообщений. Поэтому пока Apple не предоставит возможности работать с базой сообщений, их неприкасаемость находиться под угрозой.

4. Функционал приложения может быть расширен за счет дополнений, которые позволяют хранить в зашифрованном виде не только одну базу контактов, но и базу паролей к электронной почте, социальным сетям, корпоративным сетям.

Спасибо за внимание!