НИИ СОКБ
ЦЕНТР РАЗРАБОТКИ

КОМПЛЕКСНАЯ ЦИФРОВАЯ МУЛЬТИПЛАТФОРМА УПРАВЛЕНИЯ МОБИЛЬНЫМИ СРЕДСТВАМИ КОММУНИКАЦИЙ

МОБИЛЬНЫЙ КЛИЕНТ iOS

SAFEMOBILE

Москва

2023

СОДЕРЖАНИЕ

Перечень используемых терминов и сокращений

Таблица 1 – Перечень терминов и сокращений

Сокращение	Полное наименование
АРМ	Автоматизированное рабочее место
Джейлбрейк	Операция, которая открывает полный доступ к файловой системе iPhone / iPad (Jailbreak)
МСК	Мобильное средство коммуникации (смартфон, планшетный компьютер)
ОС	Операционная система
ПО	Программное обеспечение
AD	Служба каталогов корпорации Microsoft (Active Directory)
GPS	Глобальная система спутникового позиционирования (Global Positioning System)
Supervised	Режим осуществления контроля над МСК на платформе iOS. Для перевода в режим контроля требуется перепрошивка МСК при помощи ПО Apple Configurator 2 на ПК с ОС Mac OS с потерей данных пользователя
UEM	Unified Endpoint management

1 Введение

Настоящее Руководство описывает действия, выполняемые пользователем при работе с клиентским компонентом комплексной цифровой мультиплатформы управления мобильными средствами коммуникаций «UEM SafeMobile» (далее по тексту – «UEM SafeMobile»» или система), а именно: мобильным клиентом SafeMobile, работающим на устройствах iPad/iPhone на базе ОС iOS версий от 11.0 и выше.

Для МСК под управлением ОС iOS основные функции управления выполняются посредством конфигурационного профиля управления SafeMobile.

Мобильный клиент SafeMobile осуществляет мониторинг геопозиции и обнаружение взлома устройства (Джейлбрейк), а также позволяет пользователю производить установку на МСК корпоративных приложений, назначенных Администратором.

2 Регистрация МСК в системе «UEM SafeMobile»

Перед началом работы пользователю необходимо проверить корректность значений даты, времени и часового пояса на МСК.

Для того, чтобы на МСК, после подключения к системе «UEM SafeMobile», имелась возможность установки публичных приложений, сотруднику необходимо аутентифицироваться в магазине публичных приложений App Store.

В системе «UEM SafeMobile» предусмотрены два способа регистрации МСК: через приложение «EMM клиент» из App Store, либо посредством браузера.

2.1 Регистрация с помощью приложения «EMM клиент» из App Store

2.1.1 Авторизация в системе и загрузка профиля конфигурации

Для того, чтобы загрузить на МСК приложение «EMM клиент» необходимо воспользоваться учетной записью Apple ID и зайти в магазин приложений App Store, найти приложение и нажать кнопку **«Загрузить»** (рисунок 1).

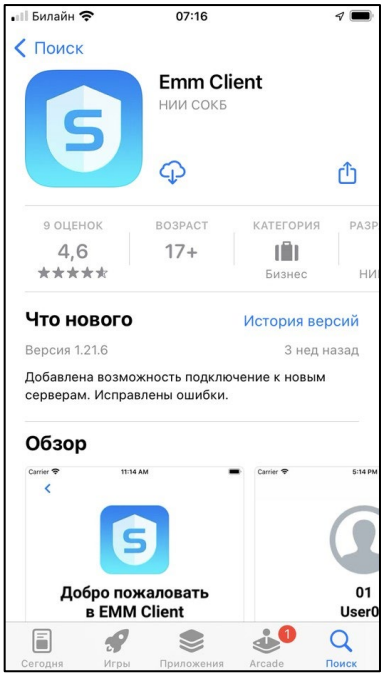

Рисунок 1 – Приложение «EMM клиент» в App Store

При подключении к системе «UEM SafeMobile» пользователю необходимо дать согласие на доступ к геопозиции и выбрать строку из вариантов (рисунок 2):

- **«Однократно»,**
- **«При использовании»,**
- **«Разрешить всегда».**

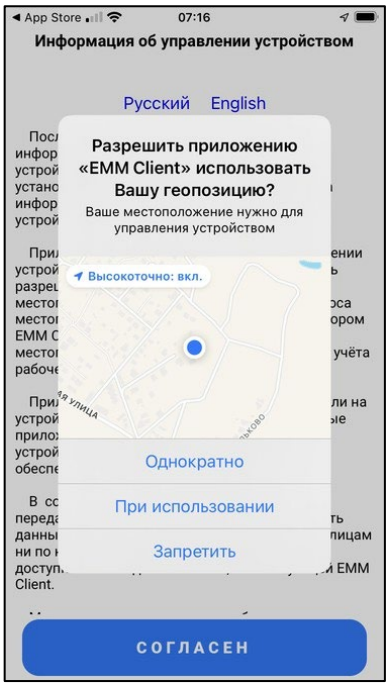

Рисунок 2 – Запрос на доступ к геопозиции

Затем дать согласие на отправку уведомлений, нажав кнопку **«Разрешить»** (рисунок 3).

Рисунок 3 – Запрос на отправку уведомлений

Далее, согласиться на сбор персональных данных и информации об устройстве. Для этого следует ознакомиться с полученным соглашением и нажать кнопку **«Согласен»** (рисунок 4).

Рисунок 4 – Пользовательское соглашение

По окончании установки в интерфейсе МСК появится иконка приложения «EMM клиент»  . Требуется открыть приложение и ввести данные, полученные от Администратора системы «UEM SafeMobile».

Если Администратор системы прислал QR-код, его необходимо просканировать, нажав кнопку «Отсканировать QR-код» и перейти к установке профиля управления (подраздел 2.1.2). В противном случае необходимо ввести адрес портала регистрации, в соответствии с рисунком 5 и нажать кнопку **«Далее»**.

Рисунок 5 – Окно ввода адреса сервера

Затем, в приветственном окне выбрать вариант авторизации в соответствии с рисунком 6.

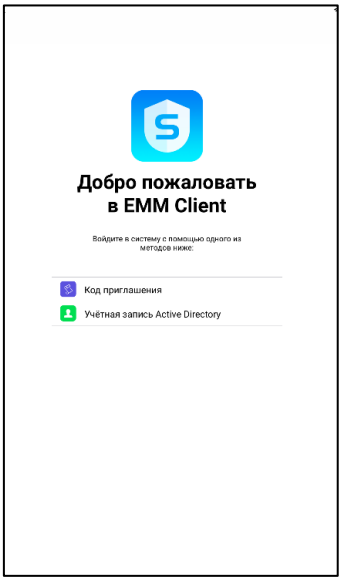

Рисунок 6 – Приветственное окно

В зависимости от конфигурации сервера при авторизации пользователю могут быть предоставлены два варианта:

1. Авторизация путем введения данных пользователя в формате «username@domain» и пароль пользователя, используя службу каталогов Microsoft Active Directory;
2. Авторизация путем введения кода приглашения, полученного у Администратора системы «UEM SafeMobile»;

В следующем окне ввести данные в зависимости от присланных Администратором системы данных (рисунки 7 а,б). Для продолжения работы нажать кнопку **«Далее»**, которая станет активна после корректного ввода данных.

а)

б)

Рисунок 7а,б – Варианты окна входа

Если при авторизации через AD логин и пароль были введены неверно, то на экране отобразится сообщение об ошибке в соответствии с рисунком 8.

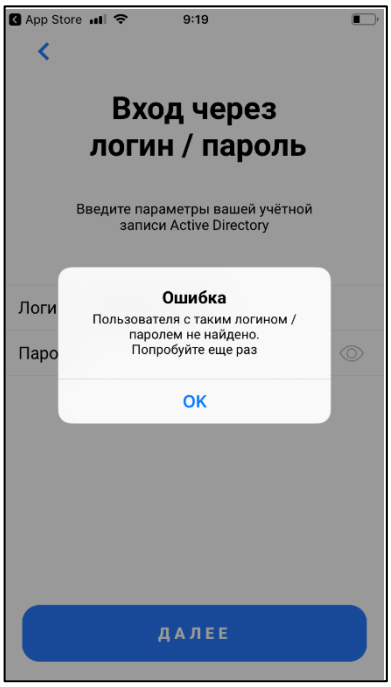

Рисунок 8 – Ошибка ввода данных через AD

Для продолжения работы необходимо подтвердить личность пользователя, нажав на кнопку **«Да, это я»** в соответствии с рисунком 9. При возникновении ошибки нажать кнопку **«Не знаю, кто это»** и осуществить авторизацию сначала.

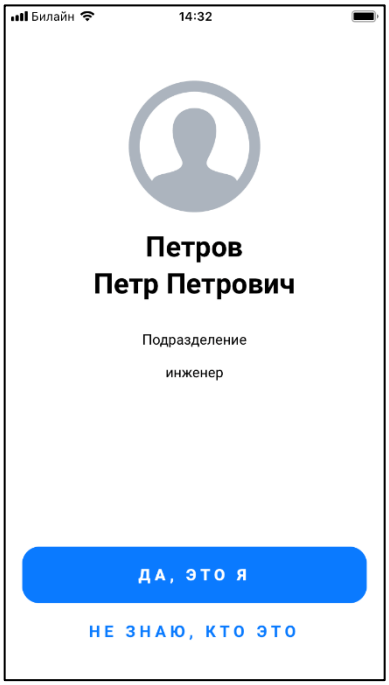

Рисунок 9 – Окно подтверждения данных

Если в АРМе Администратора задано требование о заключении с пользователем данного МСК пользовательского соглашения, то после выбора принадлежности на устройстве отобразится окно с условиями пользовательского соглашения (рисунок 10).

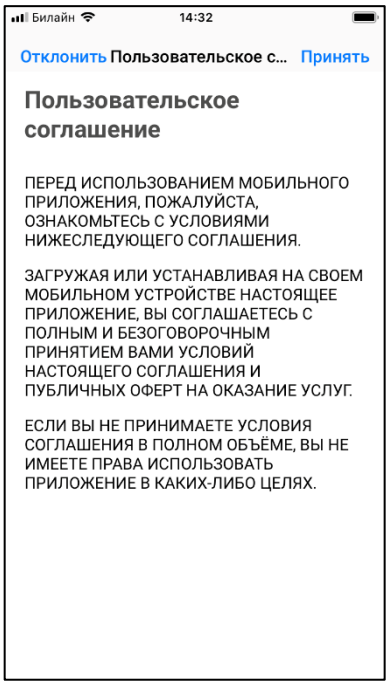

Рисунок 10 – Окно с условиями пользовательского соглашения

> ***Примечание.***
> *Текст пользовательского соглашения может отличаться от приведенного на рисунке.*

Для продолжения процедуры следует согласиться с условиями пользовательского соглашения, нажав **«Принять»** (рисунок 10). При нажатии **«Отклонить»** будет осуществлен возврат к окну ввода учетных данных, и установка профиля управления SafeMobile будет прекращена.

До установки профиля управления в приложении «EMM клиент» будет отображаться окно о передаче управления системе «UEM SafeMobile» в соответствии с рисунком 11.

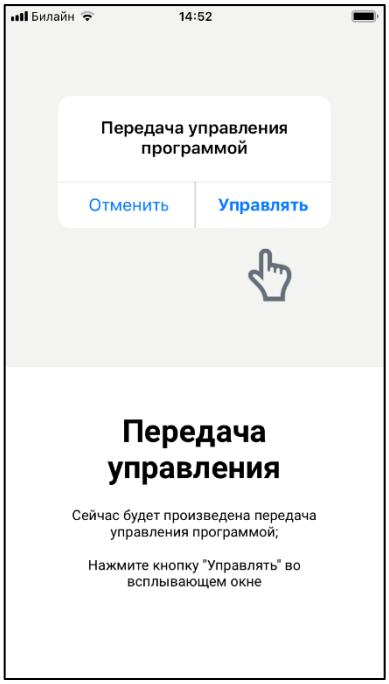

Рисунок 11 – Окно о передаче управления

2.1.2 Установка профиля управления

По окончании процедуры подключения необходимо разрешить загрузку профиля конфигурации (рисунок 12).

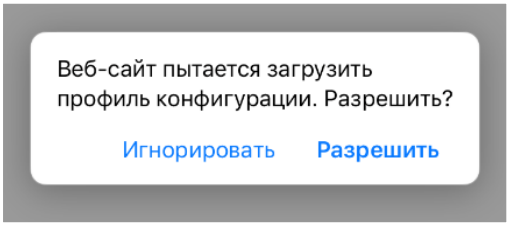

Рисунок 12 – Запрос на загрузку профиля конфигурации

Далее отобразится уведомление с указанием перейти в приложение **«Настройки»** с целью завершения установки профиля. Для продолжения работы нажать кнопку **«Закрыть»** (рисунок 13).

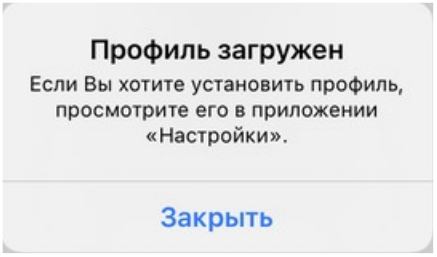

Рисунок 13 – Окно с уведомлением об окончании загрузки профиля

Для завершения установки профиля необходимо выполнить следующие действия:

1. перейти в приложение **«Настройки»;**
2. выбрать установленный профиль, после чего откроется диалоговое окно с предложением установки профиля.
3. нажать кнопку «Установить», после чего дождаться завершения процесса уставноки профиля;
4. выбрать пункт меню **«Основные» / «VPN и управление устройством»** и выбрать появившийся профиль управления. Для МСК на базе ОС iOS версий 10 и 11 переход в окно установки профиля осуществится автоматически.

В окне отобразится информация о загруженном на МСК профиле в соответствии с рисунком 14. Для продолжения работы следует нажать на кнопку **«Установить»**.

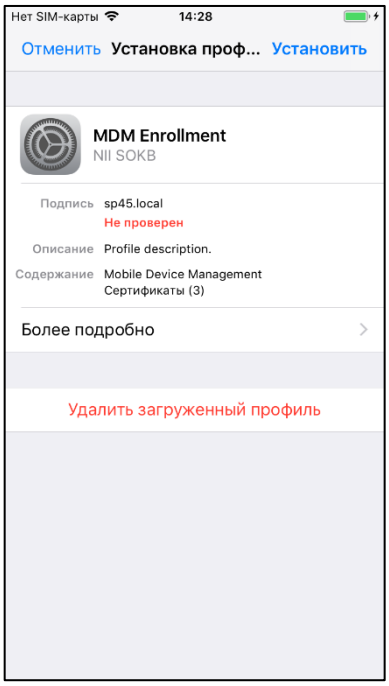

Рисунок 14 – Окно установки профиля

Примечание.
Наименование профиля управления может отличаться от приведенного на рисунке.

Далее, ознакомится с предупреждением (рисунок 15) и нажать **«Установить».**

Рисунок 15 – Предупреждение при установке профиля управления

В всплывающем окне **«Удаленное управление»** нажать **«Доверять»** (рисунок 16).

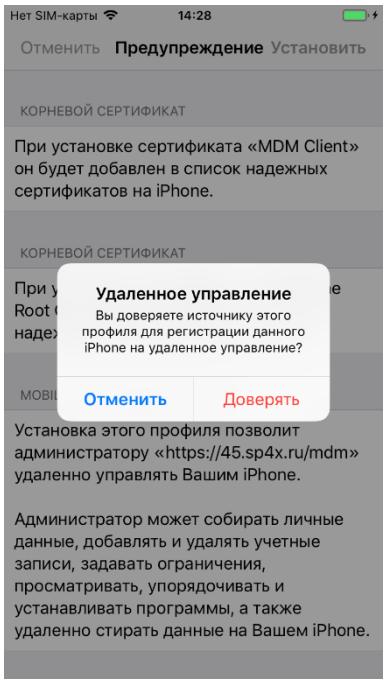

Рисунок 16 – Запрос на удаленное управление

После завершения установки в окне **«Профиль установлен»** следует нажать **«Готово»** для закрытия окна (рисунок 17).

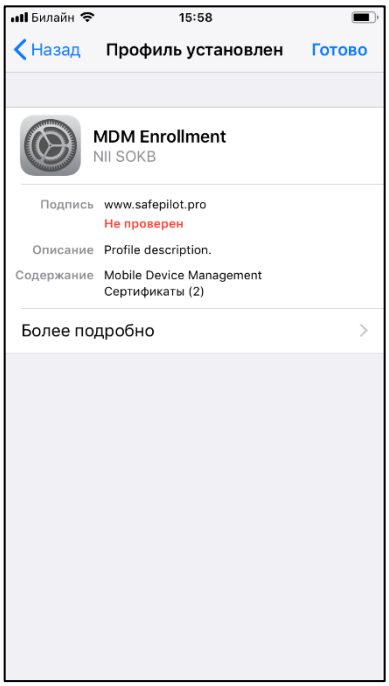

Рисунок 17 – Успешная установка профиля

Если профиль управления был установлен ***посредством приложения «EMM клиент»*** на МСК отобразится запрос на передачу управления данным приложением системе «UEM SafeMobile» в соответствии с рисунком 18, для разрешения передачи нажать на **«Управлять»**.

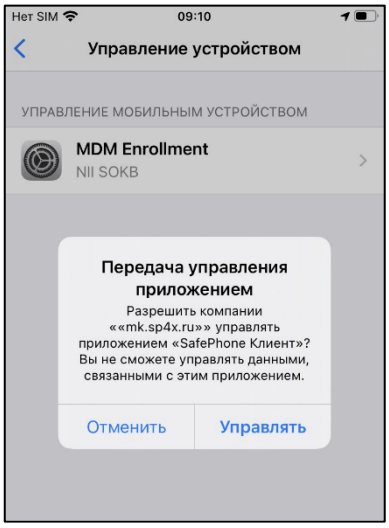

Рисунок 18 – Запрос на передачу управления приложением

Примечание.

Для администратора.

Для взятия под управление приложения монитор, необходимо в АРМ добавить и назначить ПУП на подключенное МСК (или на объект ОШС куда будет подключаться МСК). Без ПУПа передача управления не будет осуществляться

2.1.3 Управление МСК после установки профиля управления

После успешной установки профиля управления и приложения «EMM клиент» на устройство, а также регистрации в системе «UEM SafeMobile», к МСК будут применены корпоративные политики. В этом случае окно профиля управления будет отображаться в соответствии с рисунком 19.

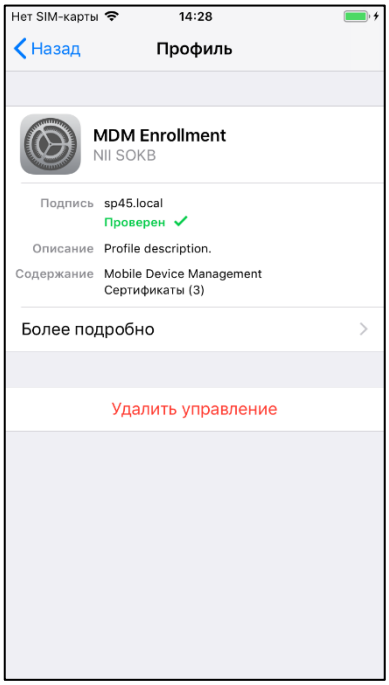

Рисунок 19 – Окно основных параметров профиля

Если в системе «UEM SafeMobile» для МСК задана настройка корпоративной электронной почты, необходимо ввести пароль учетной записи пользователя во всплывающем окне и нажать «ОК». В случае, если запрос пароля не отобразился в интерфейсе устройства (актуально для версии ОС 12.X), следует добавить пароль в окне **«Настройки» / «Пароли и учетные записи»**. При внесении администратором SafeMobile изменений в настройки корпоративной электронной почты система потребует повторного ввода пароля пользователя.

Администратор системы может осуществить перевод МСК в режим Supervised. В этом случае, после перепрошивки, на МСК в приложении **«Настройки»** отобразится сообщение об осуществлении контроля над устройством в соответствии с рисунком 20.

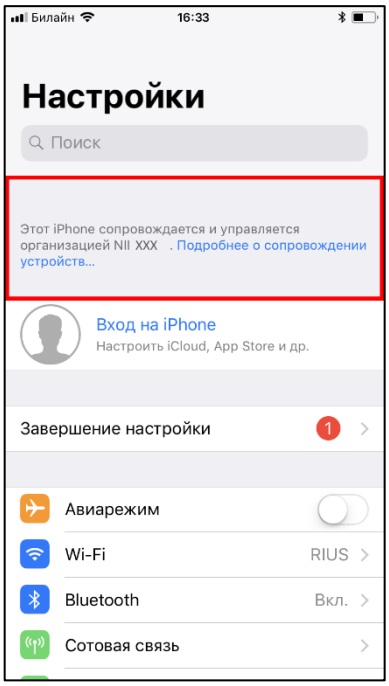

Рисунок 20 – Сообщение о контроле над устройством в приложении «Настройки»

2.2 Регистрация с помощью браузера

Открыть браузер Safari и ввести адрес портала регистрации, полученный от Администратора системы «UEM SafeMobile». В том случае, если портал недоступен, проверить наличие доступа в сеть Интернет.

Если доступ к порталу осуществляется с использованием сертификатов, выданных организацией, не входящей в состав доверенных, возможно появление следующих сообщений:

- для МСК на базе **ОС iOS версии 10** возможно появление сообщения **«Не удается проверить удостоверение сервера»** в соответствии с рисунком 21. В этом случае для продолжения работы следует нажать **«Продолжить»**.

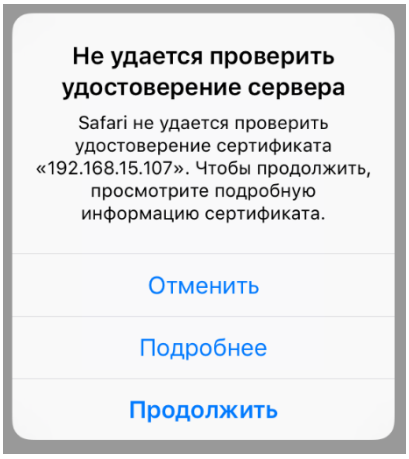

Рисунок 21 – Сообщение о невозможности проверить удостоверение сертификата сервера

Примечание.
Адрес сервера может отличаться от указанного на рисунке 21.

- для МСК на базе **ОС iOS версии 11** возможно появление сообщения: **«Это подключение не защищено»** (рисунок 22).

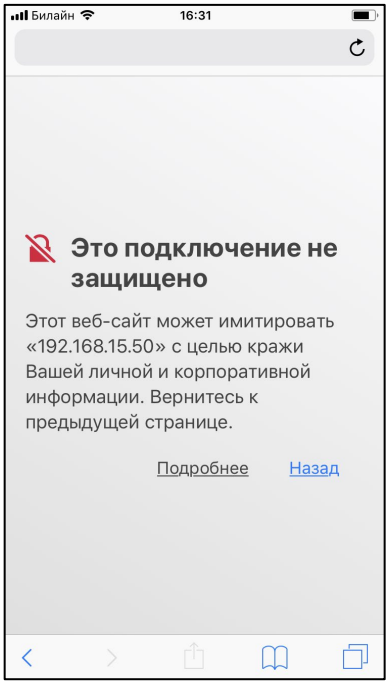

Рисунок 22 – Сообщение о незащищенном соединении

В этом случае следует нажать **«Подробнее»**, после чего отобразится окно Safari с дополнительными сведениями о сертификате в соответствии с рисунком 23.

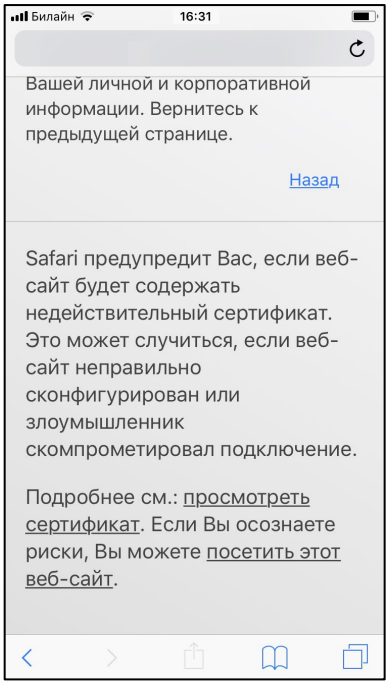

Рисунок 23 – Дополнительные сведения о сертификате

Следует нажать на ссылку **«Посетить этот веб-сайт»** в нижней части окна и подтвердить выбранное действие в соответствии с рисунком 24.

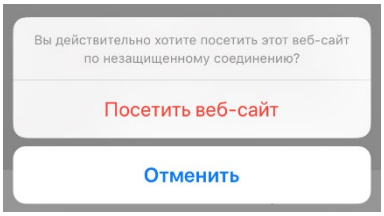

Рисунок 24 – Сообщение о необходимости подтверждения действия

Далее на экране МСК отобразится окно ввода учетных данных. В зависимости от конфигурации сервера при авторизации пользователю предоставляется два варианта:

1 Авторизация путем введения данных пользователя в формате «username@domain» и пароль пользователя, используя службу каталогов Microsoft Active Directory.
2 Авторизация путем введения кода приглашения, полученного у Администратора системы «UEM SafeMobile».

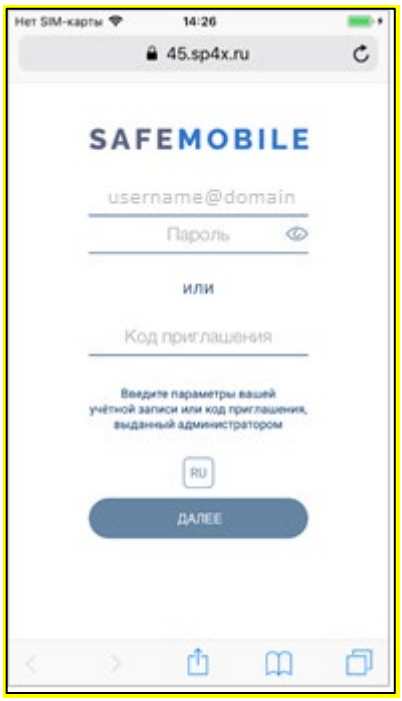

Рисунок 25 – Окно ввода учетных данных по выбору пользователя

При помощи кнопки RU осуществляется переключение языка интерфейса с русского на английский. Для обратного переключения предназначена кнопка EN.

Зарегистрировать МСК в системе «UEM SafeMobile» посредством введения учетных данных в соответствующие текстовые поля в зависимости от выбранного варианта авторизации.

Если данные были введены корректно, то для продолжения регистрации следует нажать **«ДАЛЕЕ»**.

Если данные были неверно введены три раза подряд (значение по умолчанию согласно корпоративной парольной политике), после появления сообщения о превышении допустимого числа ошибок в соответствии с рисунком 26, возможность самостоятельной регистрации пользователя будет временно заблокирована.

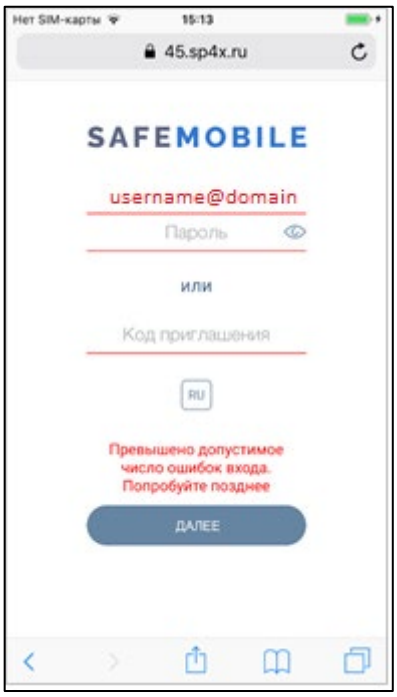

Рисунок 26 – Превышение количества попыток ввода данных

Если в АРМе Администратора задано требование о заключении с пользователем данного МСК пользовательского соглашения, то после выбора принадлежности на устройстве отобразится окно с условиями пользовательского соглашения (рисунок 27).

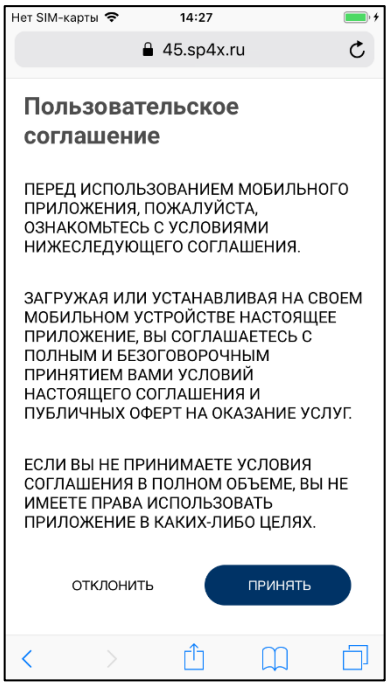

Рисунок 27 – Окно с условиями пользовательского соглашения

Примечание.
Текст пользовательского соглашения может отличаться от приведенного на рисунке.

Для продолжения процедуры следует согласиться с условиями пользовательского соглашения, нажав **«ПРИНЯТЬ»** (рисунок 27). При нажатии **«ОТКЛОНИТЬ»** будет осуществлен возврат к окну ввода учетных данных, и установка профиля управления SafeMobile будет прекращена.

Для продолжения работы следует нажать кнопку **«ДАЛЕЕ»** (рисунок 28).

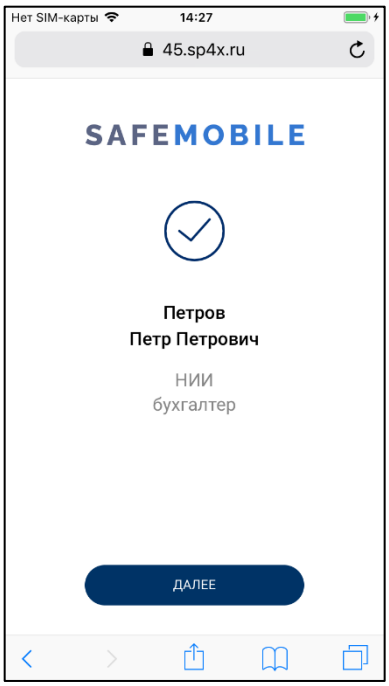

Рисунок 28 – Окно установки профиля с учетными данными пользователя

Далее, установить профиль управления в соответствии с описанием в 2.1.2. По окончании установки профиля управления на МСК отобразится запрос на установку приложения «EMM клиент» в соответствии с рисунком 29. Следует нажать **«Установить».**

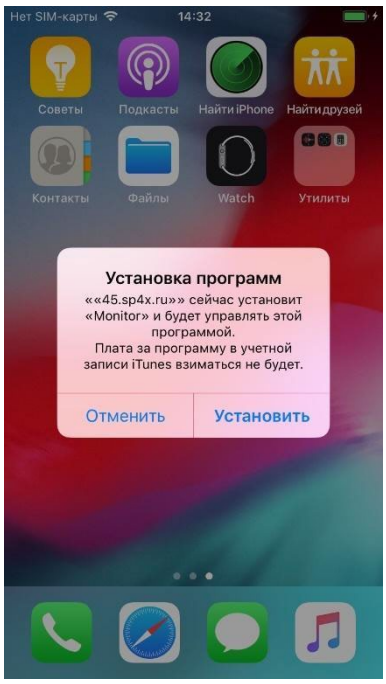

Рисунок 29 – Запрос на установку приложения

По окончании установки на экране устройства появится иконка приложения «EMM клиент» .

При успешной установке профиля управления на МСК в приложении Safari отобразится окно с учетными данными пользователя согласно рисунку 28. Для МСК на базе ОС iOS версий 10 и 11 переход в приложение Safari осуществится автоматически после нажатия на кнопку **«Готово»** в окне успешной установки профиля (рисунок 17).

3 Описание действий при работе с приложением «EMM клиент»

Приложение «EMM клиент» автоматически устанавливается на МСК после регистрации в системе «UEM SafeMobile» (или уже установлено из App Store), не рекомендуется его удалять, так как оно связано с безопасностью устройства.

3.1 Вход в приложение «EMM клиент»

При первом входе в приложение «EMM клиент» на МСК поступят следующие запросы, если разрешения не были получены ранее:

- на обновление приложения «EMM клиент»;
- на отправку уведомлений;
- на доступ к геопозиции.

Запрос на отправку пользователю уведомлений воспроизведется в соответствии с рисунком 30.

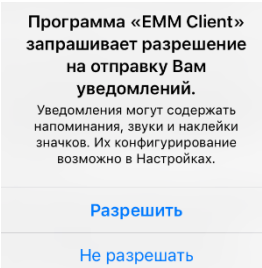

Рисунок 30 – Запрос на отправку уведомлений

Данные уведомления необходимы для получения актуальной информации о новых корпоративных приложениях, доступных для установки, а также о появлении обновлений для уже загруженных приложений. Для получения уведомлений следует нажать **«Разрешить»**. В противном случае указанная информация будет недоступна.

В случае если пользователь нажал **«Не разрешать»**, а в дальнейшей работе считает возможным получение уведомлений о приложениях, требуется открыть приложение **«Настройки»**, выбрать пункт меню **«EMM клиент»** / **«Уведомления»** / **«Допуск уведомлений»**, включить посредством переключателя уведомления и настроить их отображение (рисунок 31), исходя из индивидуальных предпочтений.

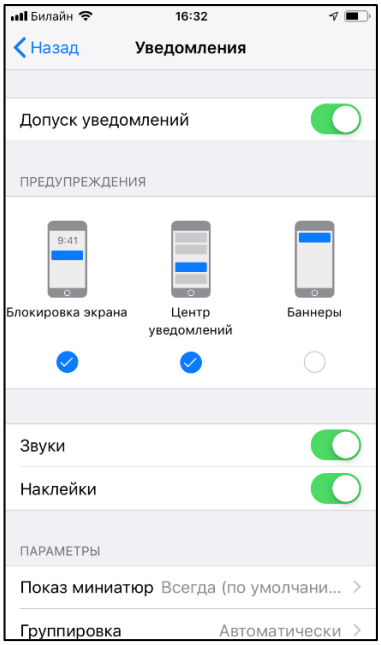

Рисунок 31 – Настройка уведомлений

Запрос о предоставлении приложению «EMM клиент» доступа к геопозиции пользователя отобразится в соответствии с рисунком 32. С целью обеспечения безошибочного функционирования МСК в системе «UEM SafeMobile» следует нажать **«Разрешать всегда»**. При нажатии на **«Только при использовании»** (программы) или **«Запретить»** функционал устройства в системе будет ограничен.

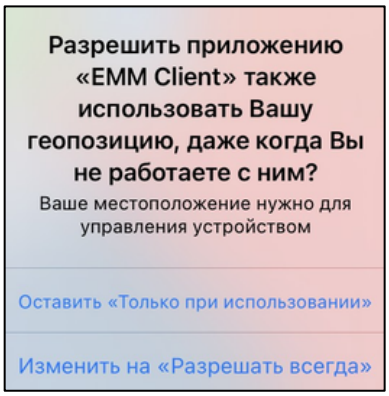

Рисунок 32 – Запрос на доступ к геопозиции пользователя

В дальнейшем, для настройки доступа, требуется открыть приложение **«Настройки»**, выбрать пункт меню **«EMM клиент»** / **«Геопозиция»** или выбрать пункт меню **«Конфиденциальность» / «Службы геолокации»** / **«EMM клиент»**, а затем выбрать строку **«Всегда»** в соответствии с рисунком 33.

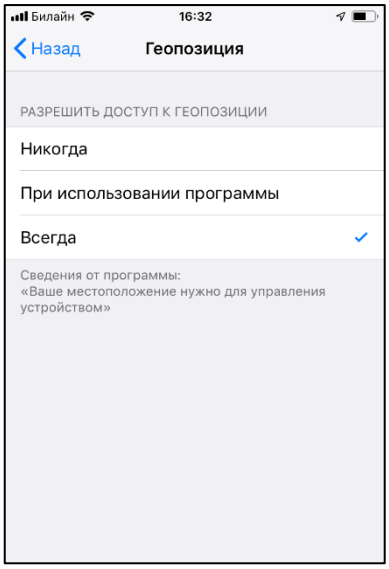

Рисунок 33 – Настройка доступа к геопозиции

При первоначальном входе в приложение, если в АРМе Администратора приложения для отображения в ПО «ЕММ клиент» не заданы, то главное окно отобразится в соответствии с рисунком 34.

Рисунок 34 – Окно приложения «ЕММ клиент» без отображаемых приложений

3.2 Информационное окно приложения «EMM клиент»

Для перехода в информационное окно следует нажать на кнопку ⓘ в левом верхнем углу главного окна приложения «EMM клиент». В информационном окне отображаются состояния МСК:

- **«Система защищена»** – признаков взлома устройства не обнаружено, доступ к уведомлениям и статус GPS зависят от разрешений пользователя (рисунок 35);
- **«Джейлбрейк»** – обнаружены признаки взлома устройства при отсутствии связи с сервером, например, в случае отсутствия соединения с Интернет (рисунок 36).

ВАЖНО!

Если обнаружены признаки взлома устройства, при наличии связи с сервером, устройство автоматически отключится от управления системой «UEM SafeMobile», корпоративные приложения и данные, включая приложение «EMM клиент», удалятся.

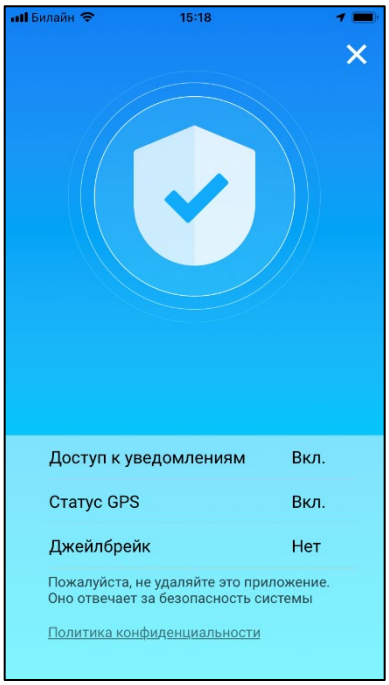

Рисунок 35 – Окно состояния «Система защищена»

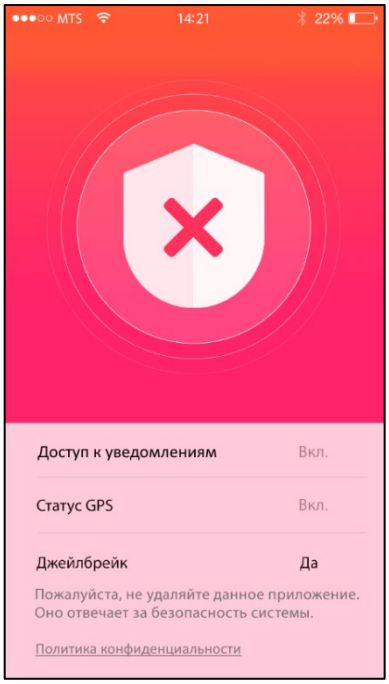

Рисунок 36 – Окно состояния «Джейлбрейк»

3.3 Главное окно приложения «EMM клиент»

При работе с приложением «EMM клиент» в интерфейсе устройства отобразится каталог приложений (рисунок 37) со списком установленных, доступных для установки корпоративных приложений, совместимых с платформой МСК.

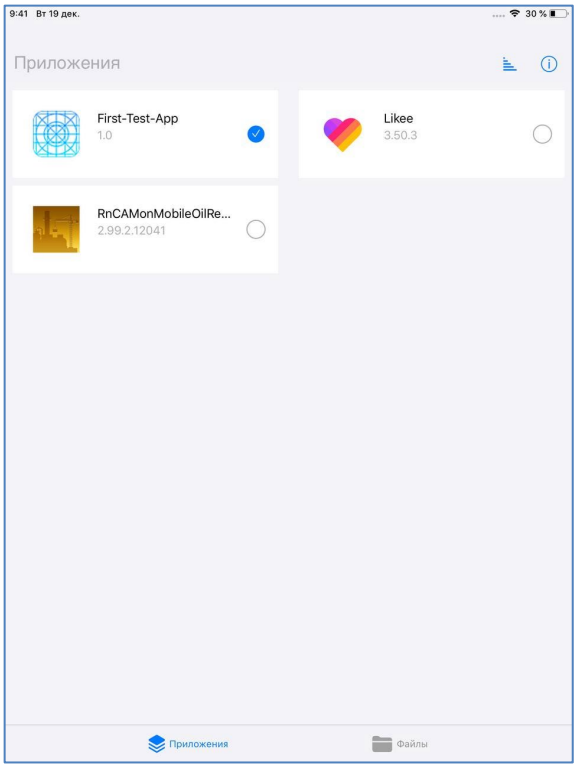

Рисунок 37 – Окно каталога приложений

Примечание.
Указанные приложения приведены условно и могут отличаться от корпоративных приложений.

В строке списка отображается иконка приложения, его название, версия и доступная для реализации процедура с выбранным приложением, а именно:

- просмотр информации о приложении;
- установка/удаление приложения на МСК.

Для получения более подробной информации о приложении необходимо выбрать требуемую строку в списке и перейти в окно в соответствии с рисунком 39. В данном окне можно ознакомиться с размером дистрибутива для скачивания.

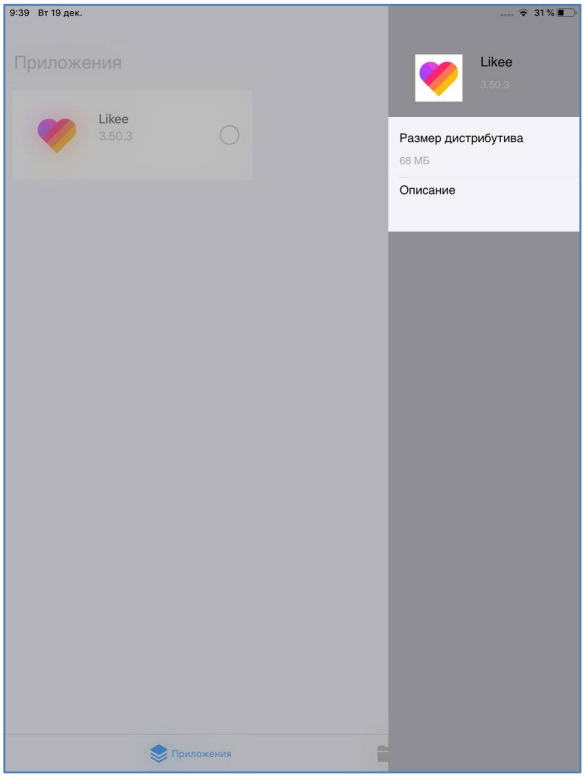

Рисунок 38 – Подробная информация о приложении

Для установки приложения на МСК следует установить галочку в строке с выбранным приложением (рисунок 40).

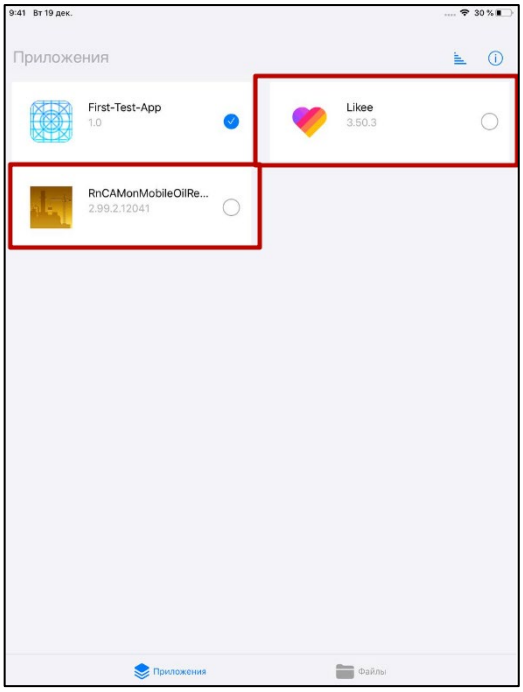

Рисунок 39 – Приложения, доступные для установки

После подтверждения процедуры пользователем в соответствии с рисунком 41, запустится процесс инсталляции.

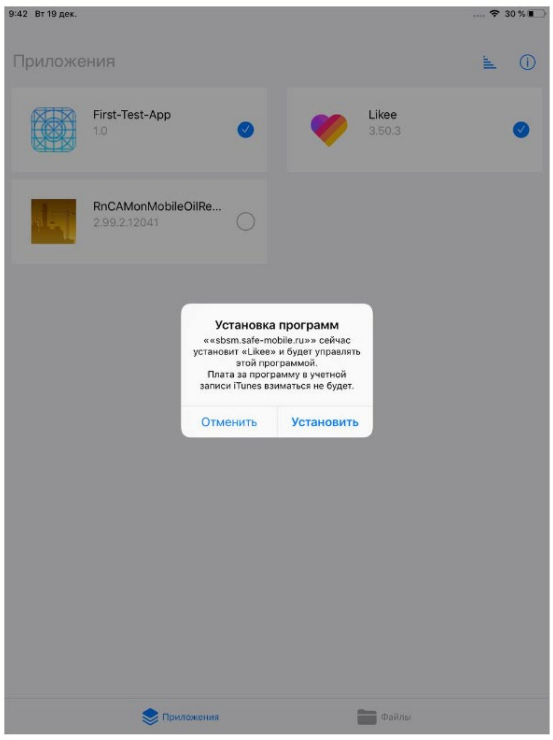

Рисунок 40 – Уведомление об установке приложения

При снятии галочки приложение будет удалено с МСК, после подтверждения правильности действия в присланном уведомлении.

Обновление версий в списке приложений осуществляется автоматически.

По окончании установки приложение отобразится со статусом: установлено (рисунок 42), а его иконка воспроизведется на рабочем столе МСК (рисунок 43).

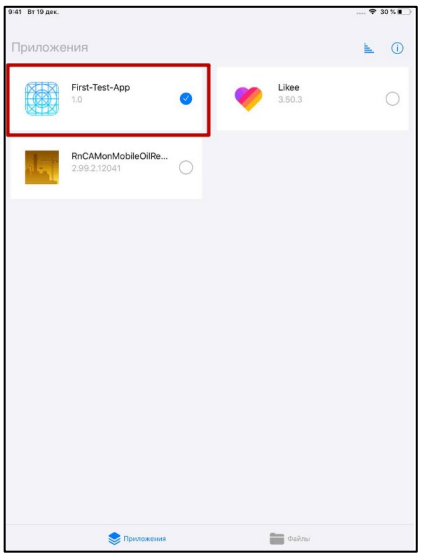

Рисунок 41 – Установленное приложение

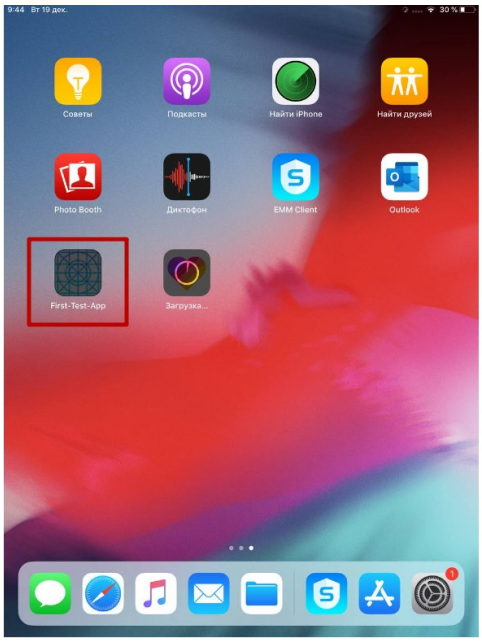

Рисунок 42 – Иконка установленного приложения на рабочем столе МСК

Если МСК какое-то время находилось вне зоны доступа сети, для получения верной информации по приложениям следует обновить текущую страницу каталога приложения движением пальца по экрану сверху-вниз (pull-to-refresh).

3.4 Получение файлов через приложение «EMM-клиент»

Пользователь МСК имеет возможность получать файлы от администратора «SafeMobile». Файлы, отправленные администратором, отображаются в приложении EMM-клиент, в папке «Файлы» (рисунок 44).

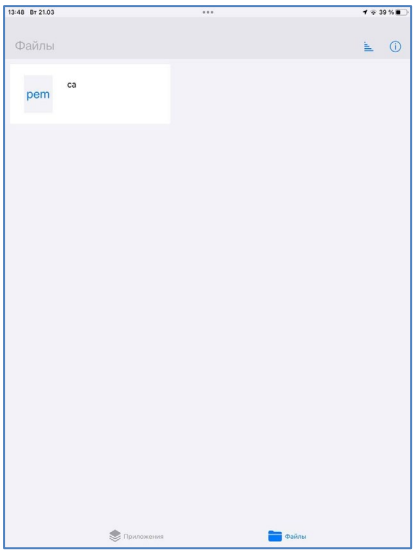

Рисунок 43 – Расположение полученных файлов

Примечание для администратора.

Для отправки файлов необходимо предварительно назначить правило управления для приложения EMM-клиент.

4 Самостоятельный выход пользователя из-под управления системы «UEM SafeMobile»

В связи с тем, что отключение пользователя от управления системой «UEM SafeMobile», как правило, осуществляется удаленно Администратором системы «UEM SafeMobile», при котором удаляются все корпоративные приложения и прекращается доступ к корпоративным данным, самостоятельный вывод мобильного устройства из-под управления следует производить только в крайних случаях.

Для осуществления самостоятельного выхода из-под управления необходимо открыть приложение **«Настройки»** и выбрать пункт меню **«Основные»** / **«Управление устройством»** и профиль управления (рисунок 19).

Затем нажать **«Удалить управление»**, при запросе пароля ввести текущий пароль устройства. В окне подтверждения удаления нажать **«Удалить управление»** (рисунок 45а) – для iPhone, нажать **«Удалить»** (рисунок 45б) – для iPad.

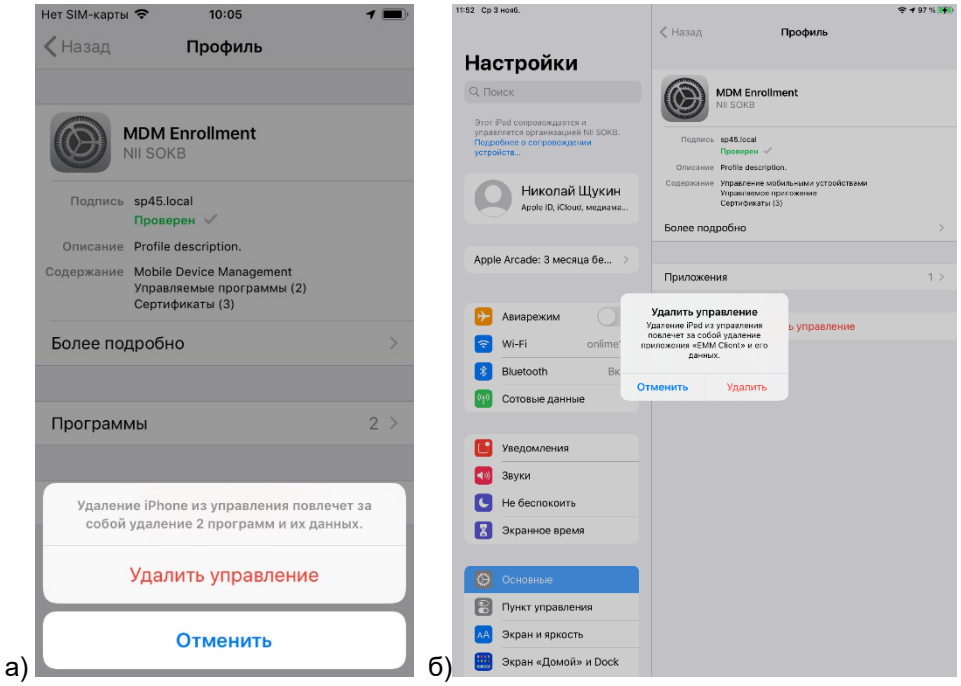

Рисунок 44 – Подтверждение удаления профиля

Приложение «EMM клиент» будет автоматически удалено после удаления профиля управления.

5 Корпоративные клиентские приложения

После установки на МСК профиля управления SafeMobile Администратор при помощи АРМ Администратора может установить на устройство корпоративные клиентские приложения.