

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Руководство пользователя. Часть 4
Мобильное приложение «Аврора Центр»

Версия документа 1.0

Листов 28

АННОТАЦИЯ

Настоящий документ является четвертой частью руководства пользователя прикладного программного обеспечения «Аврора Центр» релиз 2.2.2 (далее – ППО).

Руководство пользователя состоит из четырех частей:

- «Руководство пользователя. Часть 1. Подсистема «Маркет»;
- «Руководство пользователя. Часть 2. Подсистема Платформа управления»;
- «Руководство пользователя. Часть 3. Мобильное приложение «Аврора Маркет»;
- «Руководство пользователя. Часть 4. Мобильное приложение «Аврора Центр».

Настоящий документ содержит общую информацию о ППО, а также описание работы в Мобильном приложении (МП) «Аврора Центр».

СОДЕРЖАНИЕ

1. Общая информация	4
1.1.Основная информация	4
1.2.Мобильное приложение «Аврора Центр».....	5
1.2.1. Назначение	5
1.2.2. Функции.....	6
2. Работа с Мобильным приложением «Аврора Центр»	7
2.1.Активация мобильного устройства на сервере при помощи QR-кода	7
2.2.Упрощенная активация мобильного устройства	10
2.3.Сброс пароля пользователя или администратора мобильного устройства при помощи оперативной команды	15
2.4.Получение обновлений	16
2.5.Обновление состояния	18
2.6.Блокировка мобильного устройства	18
2.7.Просмотр информации об операциях по категориям	19
2.8.Обновление операционной системы с помощью политики	21
3. Сообщения об ошибках.....	25
Перечень терминов и сокращений.....	27

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1. Основная информация

ППО предназначено для управления мобильными устройствами (МУ) под управлением защищенной мобильной операционной системы общего назначения на базе Sailfish Mobile OS RUS, имеющей действительный сертификат соответствия ФСТЭК России, и/или операционной системы (ОС) Аврора, имеющей действительный сертификат соответствия ФСТЭК России (ЗМОС), и управления жизненным циклом приложений, а также для автоматизированной обработки следующих видов информации:

- общедоступная информация;
- информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну, подлежащая защите в соответствии с требованиями действующего законодательства Российской Федерации в области информационной безопасности.

ППО является прикладным программным обеспечением с встроенными механизмами защиты информации от несанкционированного доступа. ППО предназначено для использования:

- в государственных информационных системах, не содержащих информации, составляющей государственной тайны, до 1 класса защищенности включительно в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17;

– в информационных системах персональных данных до 1 уровня защищенности включительно в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18 февраля 2013 г. № 21;

– в автоматизированных системах управления до 1 класса защищенности включительно в соответствии с документом «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», утвержденным приказом ФСТЭК России от 14 августа 2014 г. № 31.

В документе «Руководство пользователя. Часть 2. Подсистема Платформа управления» приведена следующая основная информация:

- общая информация о назначении и составе ППО;
- перечень субъектов доступа и права на доступ к интерфейсам ППО;
- назначение и состав ПУ;
- описание принципов безопасной работы.

Требования к условиям выполнения ППО приведены в документе «Руководство администратора. Часть 1. Подсистема безопасности».

1.2. Мобильное приложение «Аврора Центр»

1.2.1. Назначение

МП «Аврора Центр» предназначено для получения сообщений от ПУ, передачи сообщений компонентам ЗМОС и компонентам ПУ сведений о настройках и состоянии МУ.

1.2.2. Функции

С помощью МП «Аврора Центр» возможно выполнение следующих функций:

- активация МУ;
- получение сообщений от ПУ о результатах выполнения операций.

МП «Аврора Центр» позволяет пользователю МУ применить политики и команды оперативного управления, отправленные Администратором Платформы Управления:

- установку и удаление приложений;
- обновление версии приложения;
- обновление версии ОС;
- ограничение и предоставление доступа к камере на МУ;
- ограничение и предоставление доступа к браузеру;
- ограничение и предоставление доступа к WLAN и его настройкам;
- ограничение и предоставление доступа к точке доступа WLAN;
- установку одноразового пароля пользователя и администратора МУ;
- получение данных о состоянии МУ;
- получение логов с МУ и сообщений о событиях безопасности МУ;
- блокировка и разблокировка МУ;
- очистка (восстановление заводских настроек) МУ.

МУ обращаются к ПУ с целью проверки обновления при следующих условиях:

- в соответствии с заданным Администратором Платформы Управления временным интервалом;
- принудительно, когда пользователь МУ в МП «Аврора Центр» выбирает в меню действий пункт «Проверить обновления».

2. РАБОТА С МОБИЛЬНЫМ ПРИЛОЖЕНИЕМ «АВРОРА ЦЕНТР»

2.1. Активация мобильного устройства на сервере при помощи QR-кода

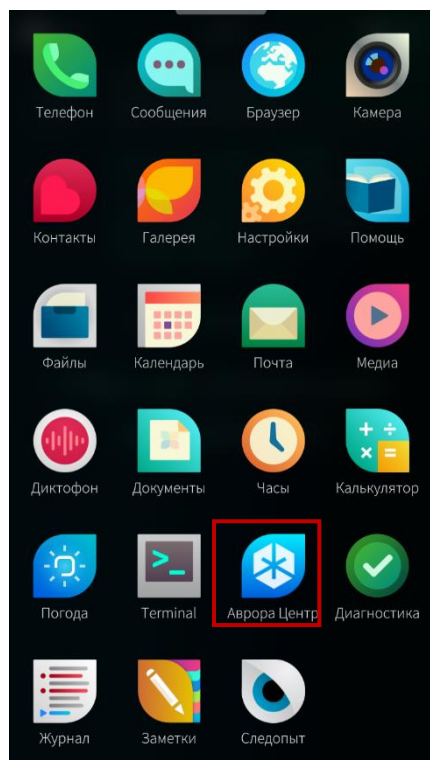


Рисунок 1

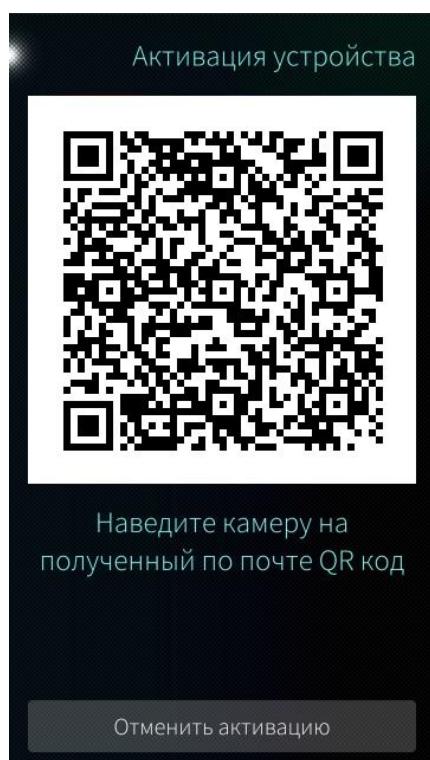


Рисунок 2

Для активации МУ необходимо отсканировать QR-код. Для этого нужно выполнить следующие действия:

– запустить МП «Аврора Центр», коснувшись значка  на экране приложений (Рисунок 1);

Состав приложений может меняться в зависимости от варианта исполнения ЗМОС

– привести камеру МУ на QR-код на странице «Активация устройства» (Рисунок 2);

Изображение кода должно поместиться в рамку, которая отображается на экране МУ

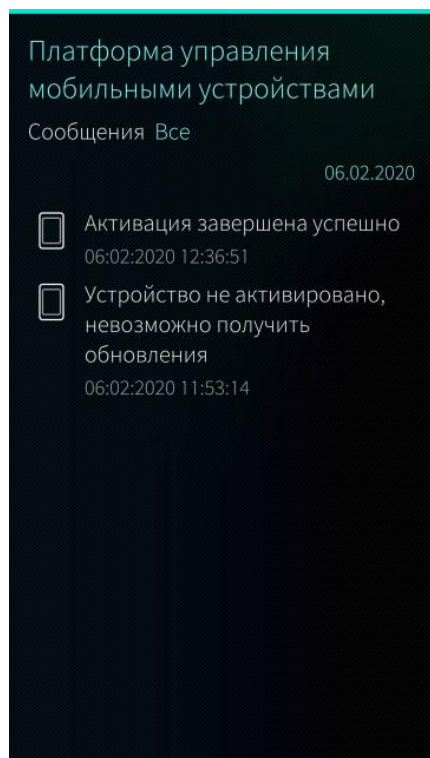


Рисунок 3

– если QR-код успешно отсканирован, отобразится сообщение «Активация завершена успешно» (Рисунок 3).

Если не удалось активировать МУ с помощью QR-кода, то на главной странице МП «Аврора Центр» отобразится сообщение «Активация завершена с ошибкой» (Рисунок 4). Также будет отображено уведомление МП «Аврора Центр» (Рисунок 5).

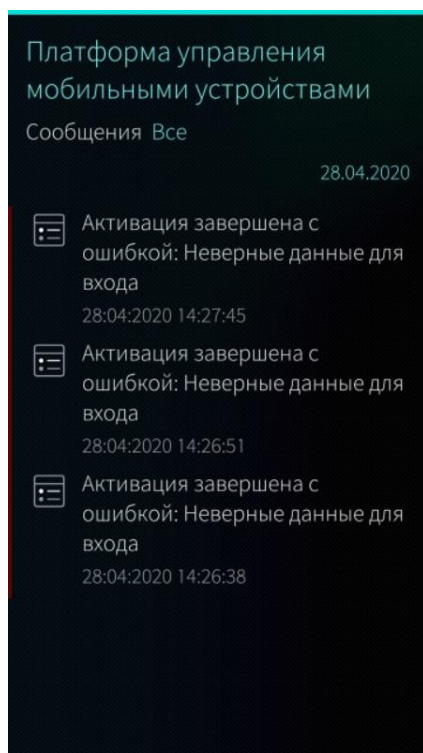


Рисунок 4

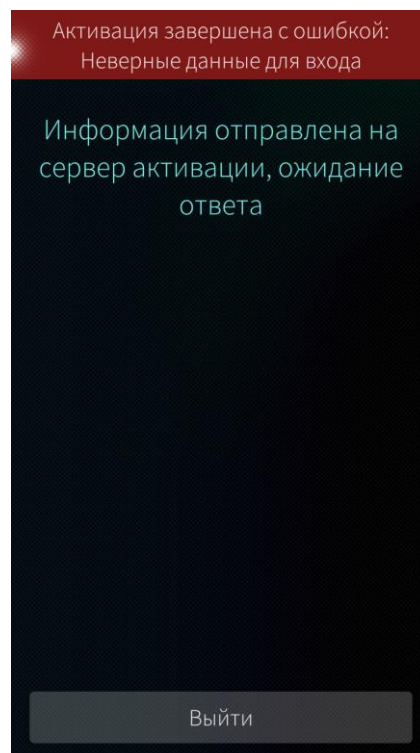


Рисунок 5

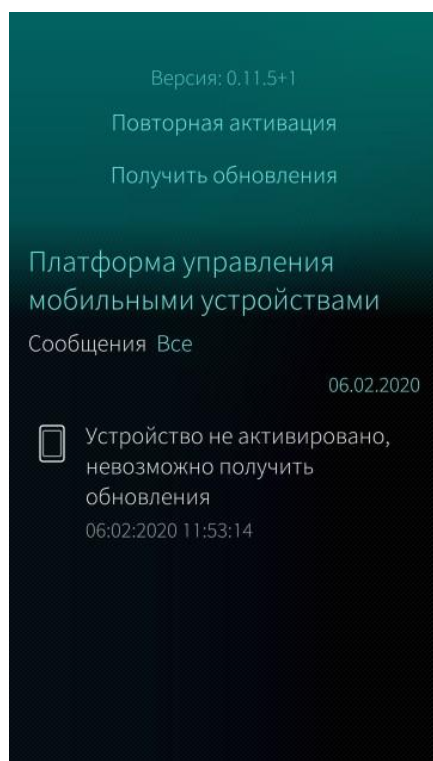


Рисунок 6

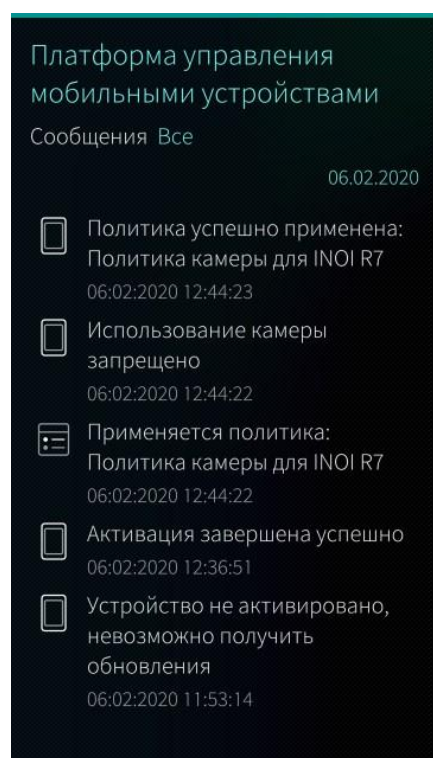


Рисунок 7

Для повторной попытки активации МУ необходимо выполнить следующие действия:

- проверить наличие подключения МУ к сети Интернет;
- в меню действий выбрать пункт «Повторная активация» (Рисунок 6);

Пункт «Повторная активация» недоступен, если на МУ назначена политика с правилом «Использование камеры запрещено»

- навести камеру МУ на QR-код на странице «Активация устройства» (см. Рисунок 2).

Если МУ уже было активировано на сервере, в режиме пользователя его нельзя повторно активировать на другом сервере

После успешной активации МУ подключится к ПУ, на МУ будут применены все назначенные Администратором Платформы Управления политики и команды оперативного управления (Рисунок 7).

2.2. Упрощенная активация мобильного устройства

Упрощенная активация позволяет активировать МУ при его первом включении.

Для упрощенной активации МУ необходимо выполнение следующих условий:

- ОС Аврора версии 3.2.1 и выше;
- JSON-файл для активации группы устройств создан и импортирован в ПУ.

Подробное описание создания и импорта приведено в документе «Руководство пользователя. Часть 2. Подсистема Платформа управления»;

– на МУ назначена политика с правилами «Создание пользователя» и «Требования к паролю». Эти правила обязательны для завершения упрощенной активации. При этом можно назначить на МУ политики с другими правилами. Они будут применены при завершении активации. Подробное описание правил политик приведено в документе «Руководство пользователя. Часть 2. Подсистема Платформа управления».

Команды оперативного управления «Задать одноразовый пароль пользователя» и «Задать одноразовый пароль администратора» не будут выполнены при упрощенной активации

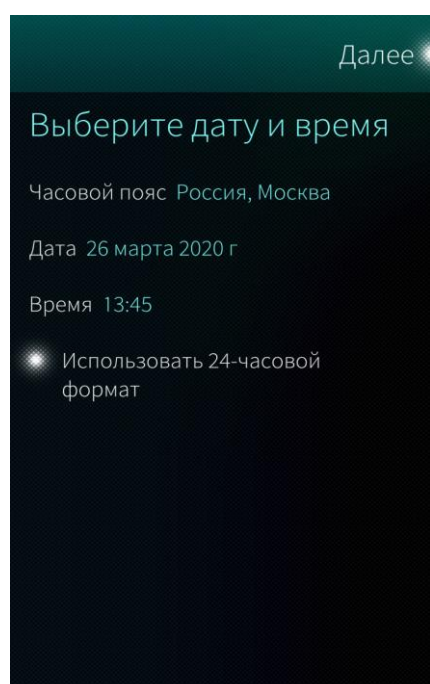


Рисунок 8

Для упрощенной активации МУ необходимо выполнить следующие действия:

- включить МУ;
- принять условия Лицензионного соглашения для конечного пользователя;
- ознакомиться с сообщением о том, что на МУ установлены сервисы Mobile Device Management;
- дождаться запуска ОС Аврора;
- включить WLAN и подключиться к сети WLAN;
- выбрать часовой пояс, дату, время, формат времени и нажать кнопку «Далее» (Рисунок 8);

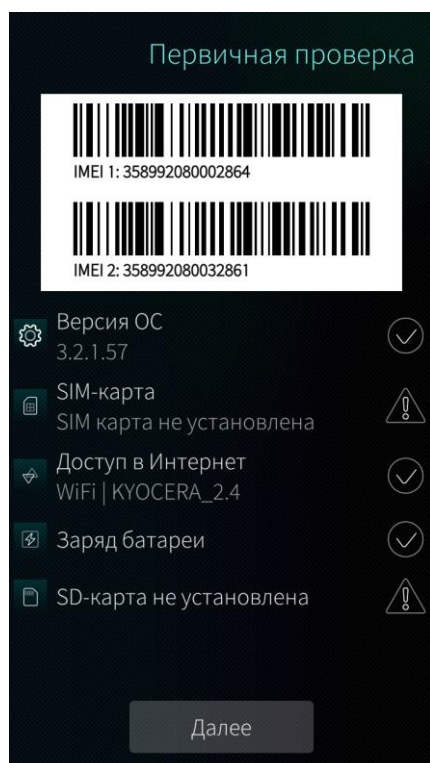


Рисунок 9

– дождаться выполнения первичной проверки и нажать кнопку «Далее» (Рисунок 9);

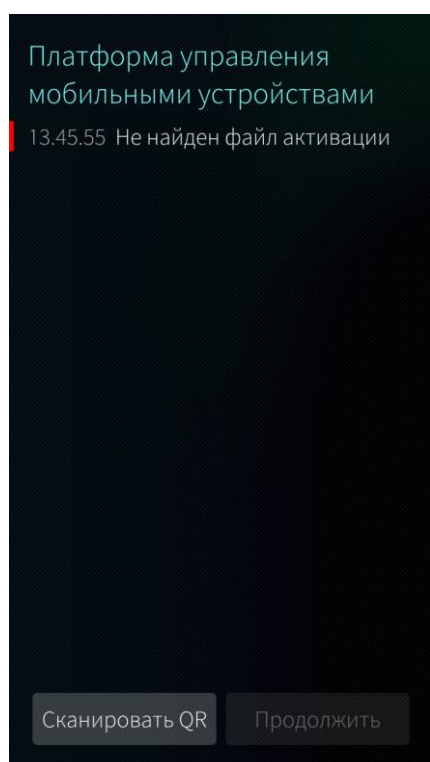


Рисунок 10

– дождаться результата поиска файла активации на МУ. Если нужный файл будет найден, МУ будет активировано. Если файл не найден, для продолжения активации следует нажать кнопку «Сканировать QR» (Рисунок 10);

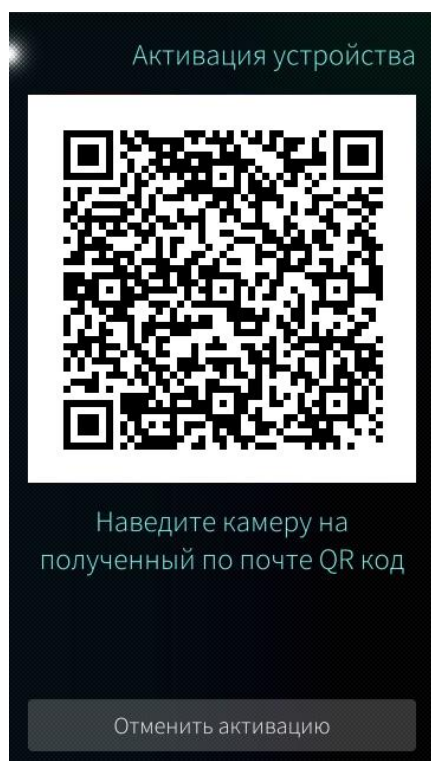


Рисунок 11

– навести камеру МУ на QR-код на странице «Активация устройства» (Рисунок 11);

Изображение кода должно поместиться в рамку, которая отображается на экране МУ

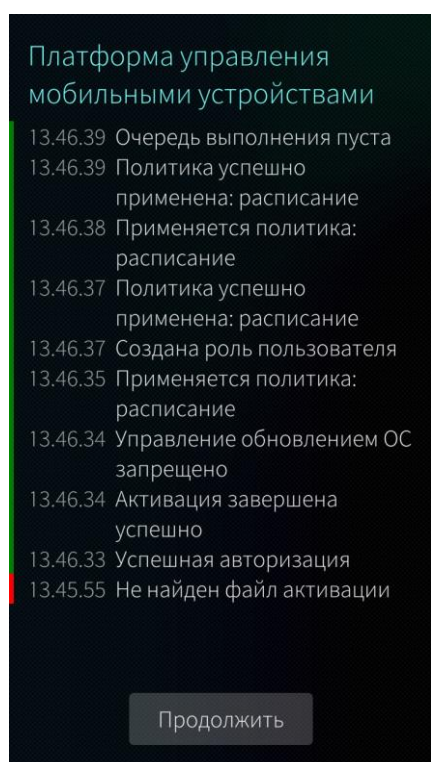


Рисунок 12

– если QR-код успешно отсканирован, в журнале МУ отобразится запись «Активация успешно завершена» и на МУ будут назначены политики (Рисунок 12).

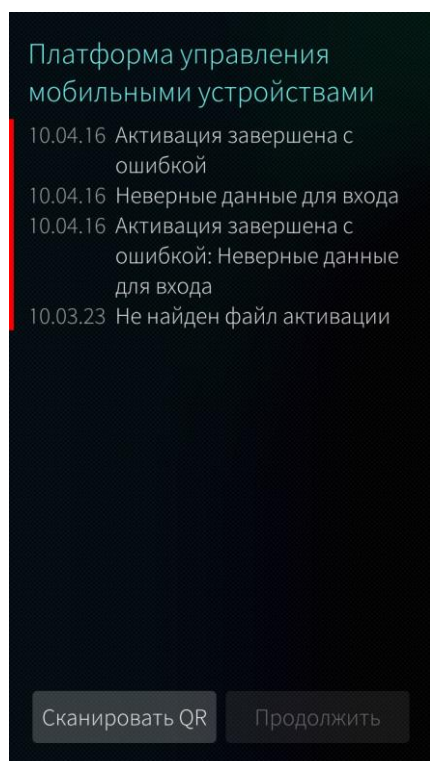


Рисунок 13

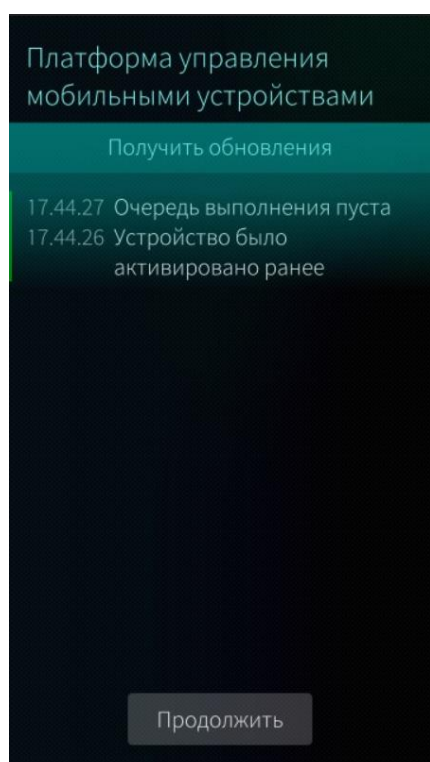


Рисунок 14

Если не удалось активировать МУ с помощью QR-кода, то на главной странице МП «Аврора Центр» отобразится сообщение «Активация завершена с ошибкой» (Рисунок 13). Для повторного сканирования QR-кода следует нажать кнопку «Сканировать QR».

Если на МУ не были получены все политики, следует открыть меню действий, проведя по экрану МУ сверху вниз, и выбрать пункт «Получить обновления» (Рисунок 14).

Если при получении политик доступ в интернет был потерян, следует открыть меню действий, проведя по экрану МУ сверху вниз, выбрать пункт «Подключиться к сети» и подключиться к сети WLAN. Затем необходимо пройти все шаги повторно, начиная с первичной проверки.

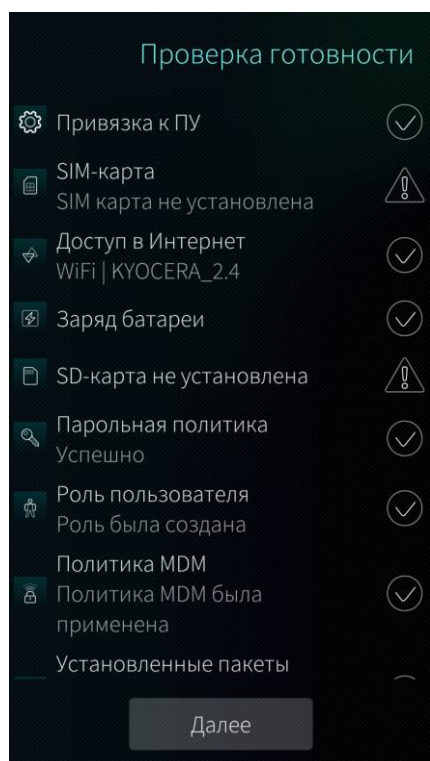


Рисунок 15

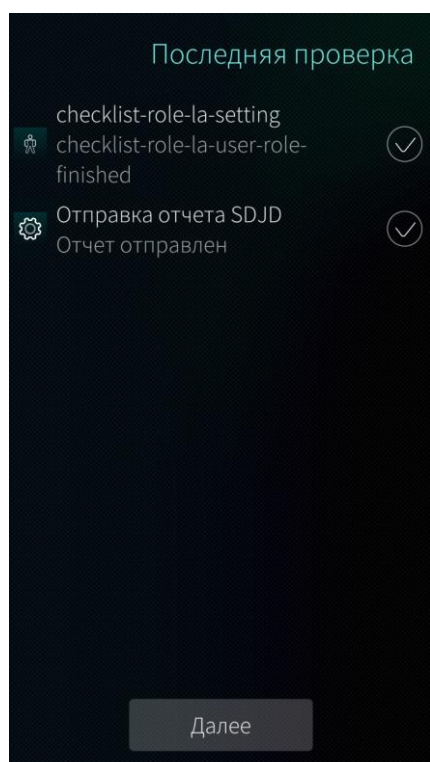


Рисунок 16

Для завершения подготовки МУ к работе следует нажать кнопку «Продолжить» и выполнить следующие действия:

- дождаться завершения проверки готовности МУ и нажать кнопку «Далее» (Рисунок 15);

- если проверка готовности МУ не пройдена (политики с правилами «Создание пользователя» и «Требования к паролю» не установлены или не применились), необходимо убедиться, что требуемые политики назначены на группу, в которое включено МУ, затем перезагрузить устройство и пройти на МУ упрощенную активацию повторно;

- после прохождения проверки готовности необходимо дождаться завершения последней проверки и нажать кнопку «Далее» (Рисунок 16).

После этого МУ будет перезагружено и готово к работе. Если при последней проверке отправка отчета SDJD не была осуществлена, это означает, что необходимые события безопасности не были отправлены в ПУ. Это не будет препятствовать завершению упрощенной активации.

Подробное описание событий безопасности, отправляемых с МУ, приведено в документе «Операционная система Аврора. Руководство администратора» АДМГ.10034-02 91 01.

2.3. Сброс пароля пользователя или администратора мобильного устройства при помощи оперативной команды

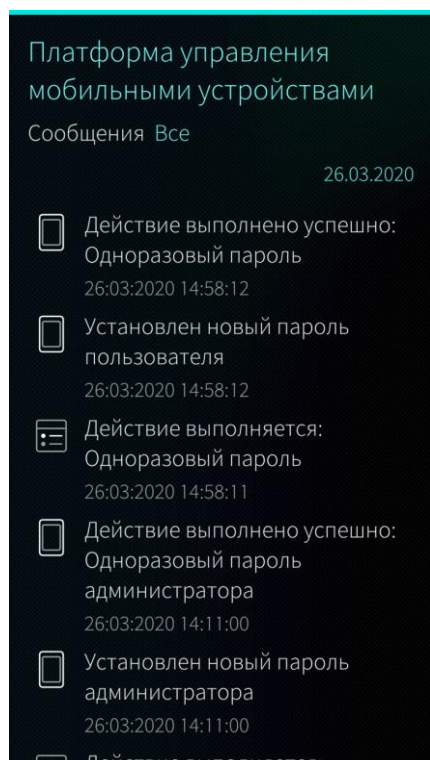


Рисунок 17

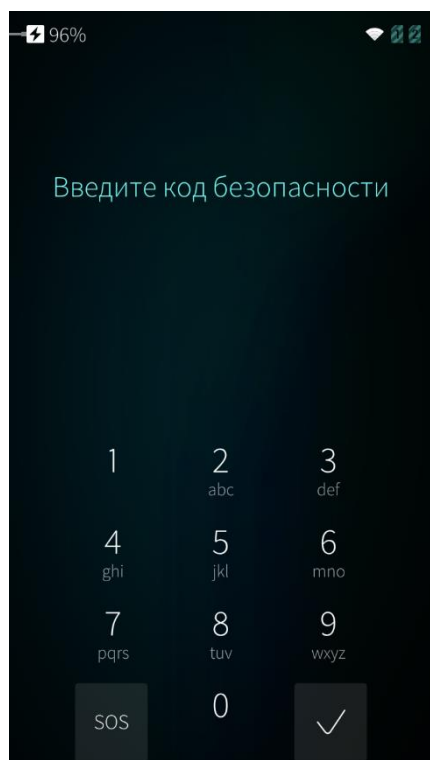


Рисунок 18

Если пользователь или администратор МУ потерял, забыл или не знает пароль для разблокирования МУ, пароль можно сбросить при помощи команды оперативного управления МУ «Задать одноразовый пароль пользователя» и «Задать одноразовый пароль администратора» соответственно.

Подробное описание оперативных команд приведено в документе «Руководство пользователя. Часть 2. Подсистема Платформа управления».

После выполнения оперативной команды в журнале отобразится запись «Установлен новый пароль пользователя» (Рисунок 17).

Затем необходимо выполнить следующие действия на МУ:

- загрузить МУ в режиме пользователя или администратора. Подробное описание перехода в режим пользователя или администратора приведено в документе «Операционная система Аврора. Руководство администратора» АДМГ.10034-02 91 01;

- ввести одноразовый пароль, который был выдан Администратором ПУ (Рисунок 18);

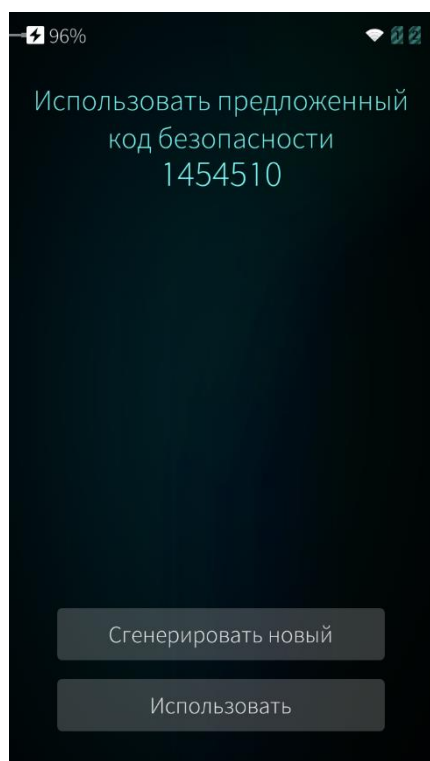


Рисунок 19

– использовать предложенный пароль МУ, нажав кнопку «Использовать», или сгенерировать новый, нажав кнопку «Сгенерировать новый», и затем принять пароль (Рисунок 19);

– ввести дважды новый пароль.

После этого пароль пользователя или администратора МУ будет переустановлен.

2.4. Получение обновлений

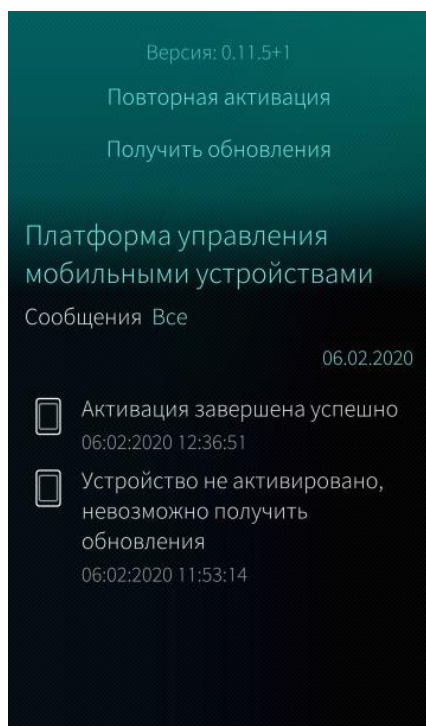


Рисунок 20

Для проверки обновлений необходимо в меню действий выбрать пункт «Получить обновления» (Рисунок 20).

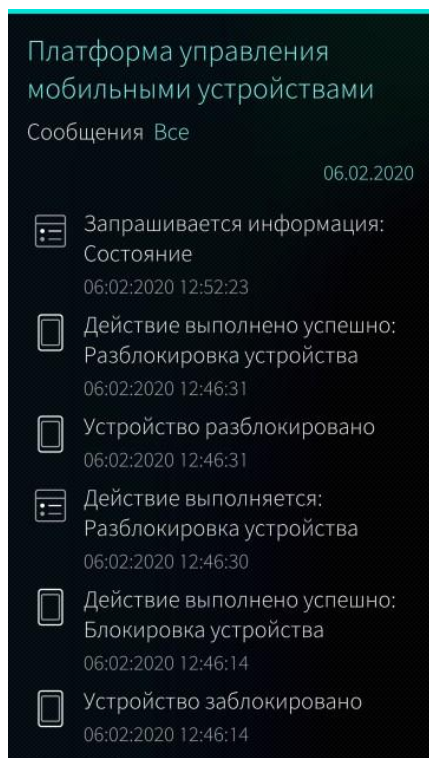


Рисунок 21

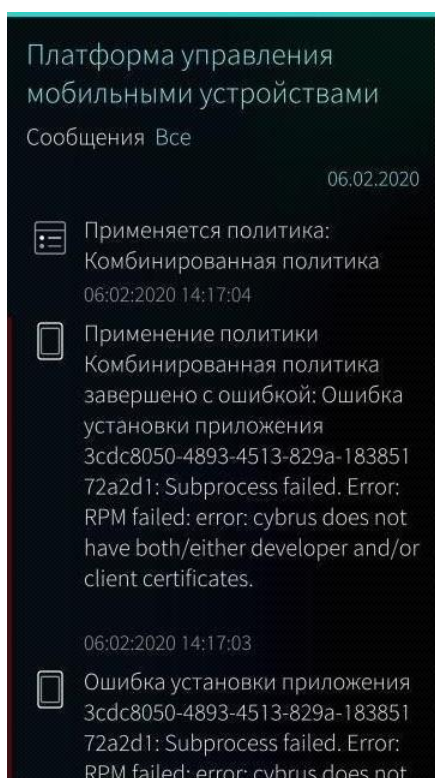


Рисунок 22

По окончании процесса обновления отобразится результат завершения операции (Рисунок 21).

При ошибке применения политики отобразится подробная информация по выбранной политике (Рисунок 22).

2.5. Обновление состояния

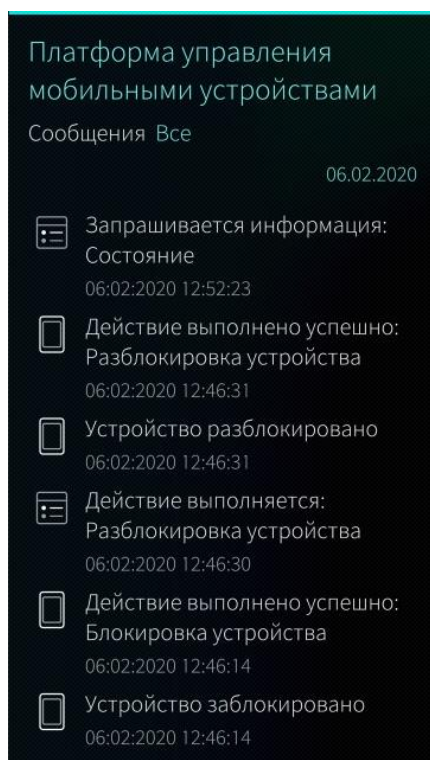


Рисунок 23

Если Администратор Платформы Управления запросил состояние с помощью оперативных команд, на МУ отобразится информационное сообщение (Рисунок 23).

Сообщение означает, что текущее состояние МУ отправлено Администратору Платформы Управления.

2.6. Блокировка мобильного устройства



Рисунок 24

При блокировке МУ на экране блокировки отображается сообщение «Заблокировано при помощи Aurora Device Manager / Sailfish Mobile OS RUS» (Рисунок 24).

Использование МУ до разблокировки невозможно, кроме совершения экстренного вызова.

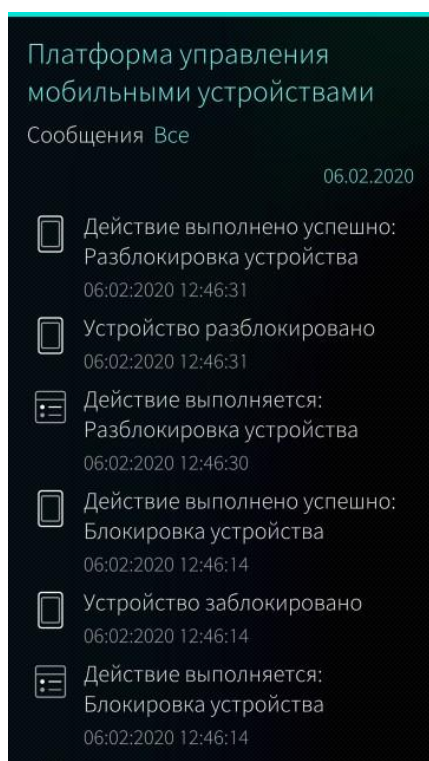


Рисунок 25

По истечении времени блокировки МУ, заданного Администратором Платформы Управления, выполнится разблокировка. В МП «Аврора Центр» отобразится информационное сообщение о разблокировке МУ (Рисунок 25).

2.7. Просмотр информации об операциях по категориям

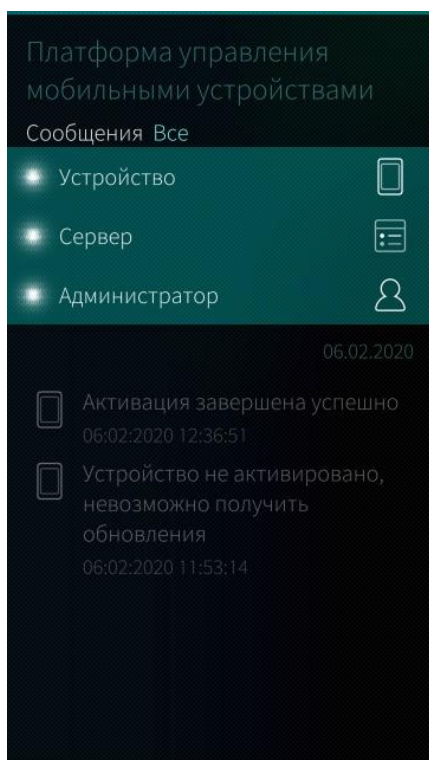


Рисунок 26

В МП «Аврора Центр» можно просмотреть информацию по операциям и следующим категориям (Рисунок 26):

- «Устройство» — сообщения, формируемые МУ;

- «Сервер» — сообщения, которые отправляются с сервера ПУ;

- «Администратор» — сообщения, формируемые Администратором Платформы Управления.

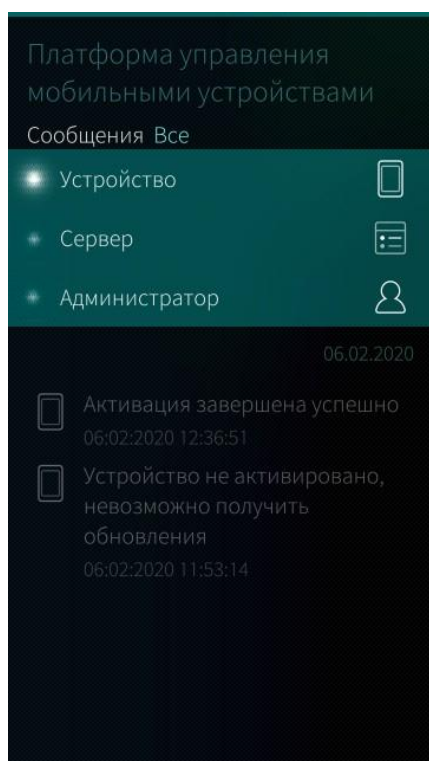


Рисунок 27

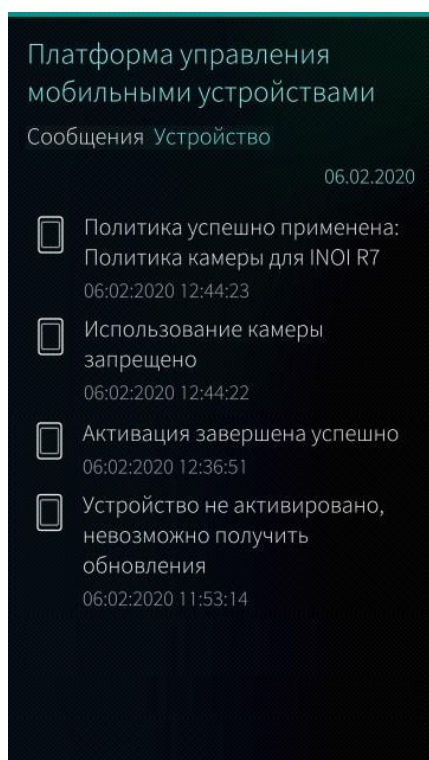


Рисунок 28

Для просмотра в поле «Сообщения» в раскрывающемся списке выбрать необходимые категории (Рисунок 27).

После этого отобразится подробная информация по выбранной категории (Рисунок 28).

Для быстрого перемещения по странице вверх или вниз можно воспользоваться кнопками  и  соответственно. Кнопки располагаются с правой стороны экрана МУ и появляются при быстром пролистывании.

2.8. Обновление операционной системы с помощью политики

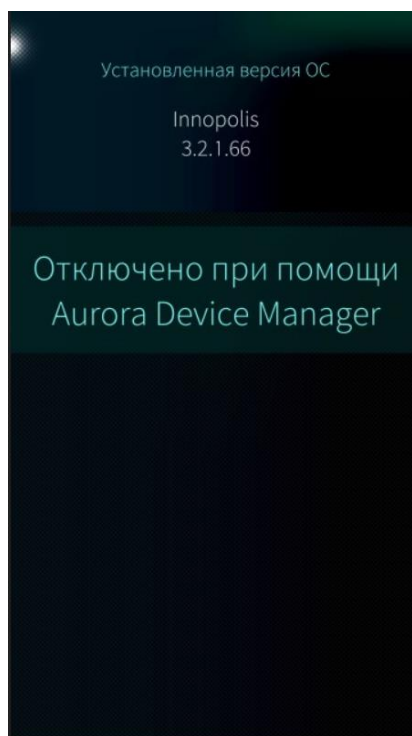


Рисунок 29

Если МУ активировано в ПУ, обновить ЗМОС через интерфейс нельзя.

При попытке обновить ЗМОС через интерфейс ОС появится сообщение «Отключено при помощи Aurora Device Manager / Sailfish Mobile OS RUS» (Рисунок 29).

Обновить ЗМОС на МУ можно с помощью правила политики «Система / Назначить версию ОС». Подробное описание правил политик приведено в документе «Руководство пользователя. Часть 2. Подсистема Платформа управления».

Если на МУ текущая версия ЗМОС равна или выше заданной в политике, обновление установлено не будет.

Если на МУ текущая версия ЗМОС, ниже заданной в политике, отобразится сообщение «Доступно обновление системы [номер версии ЗМОС]. После скачивания установка будет запланирована на нерабочие часы (чч:мм-чч:мм)» в журнале МП «Аврора Центр» (Рисунок 30) и в уведомлениях ЗМОС (Рисунок 31).

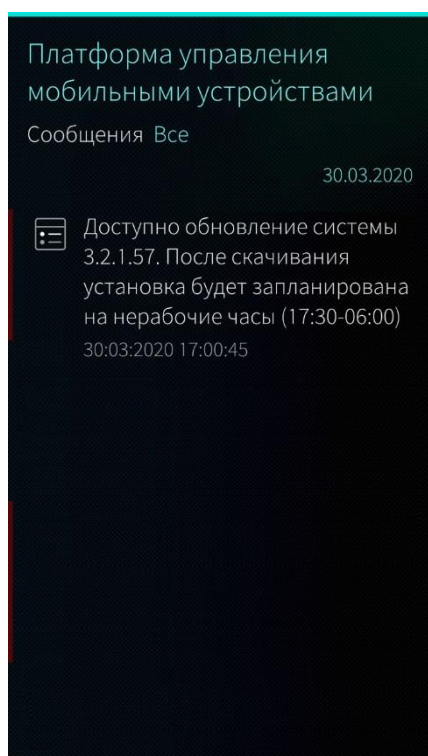


Рисунок 30

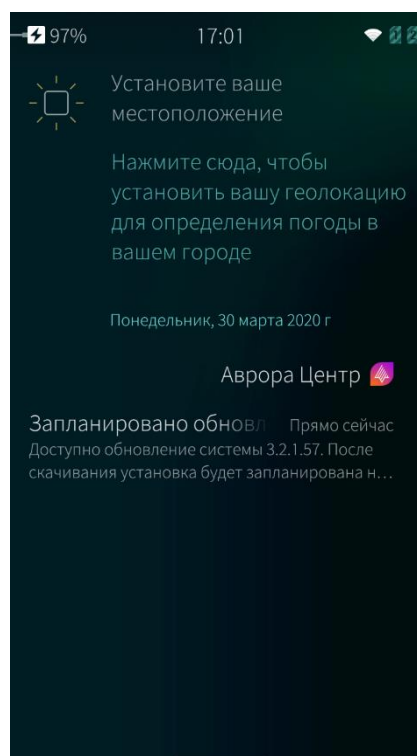


Рисунок 31

Если между текущей версии ЗМОС и версией, установленной в политике, есть промежуточная версия, будет отображено сообщение «Обнаружена обязательная промежуточная версия [номер версии ЗМОС]». В этом случае сначала будет установлена промежуточная версия ЗМОС.

После этого начнется процесс скачивания загрузочного модуля версии ЗМОС. Будет отображено сообщение «Загрузка обновления [номер версии ЗМОС]» в журнале МП «Аврора Центр» (Рисунок 32) и «Обновление системы [номер версии ЗМОС] загружается» в уведомлениях ЗМОС (Рисунок 33).

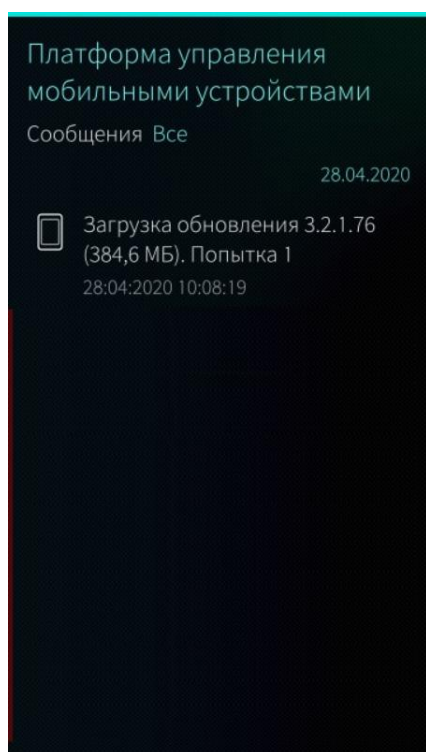


Рисунок 32

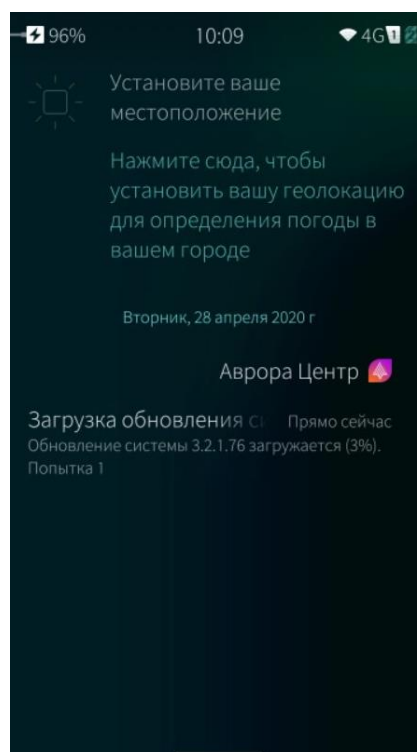


Рисунок 33

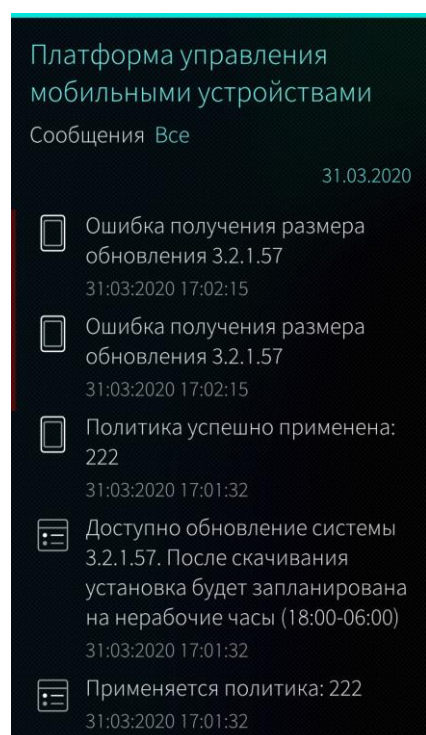


Рисунок 34

Если репозиторий с обновлением недоступен, или на МУ недостаточно свободного места для скачивания обновления, отобразится сообщение «Ошибка получения размера обновления [номер версии ЗМОС]» в журнале МП «Аврора Центр» (Рисунок 34).

После завершения скачивания отобразится сообщение «Установка обновления [номер версии ЗМОС] будет произведена в чч:мм» в журнале МП «Аврора Центр» (Рисунок 35) и в уведомлениях ЗМОС (Рисунок 36). Во временной интервал между завершением скачивания обновления и его установкой можно продолжать управлять МУ через ПУ.

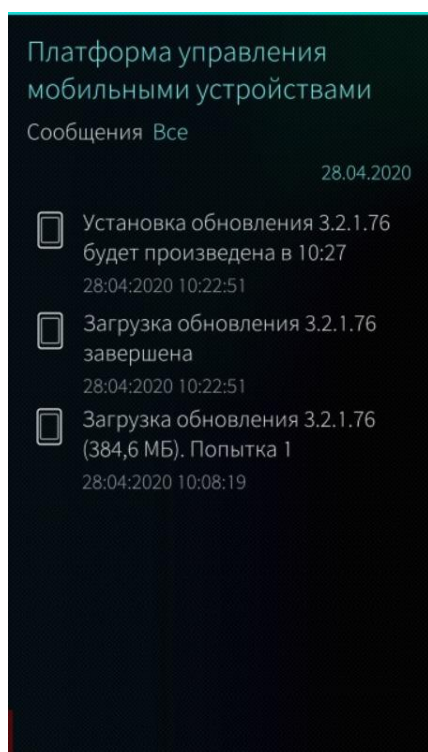


Рисунок 35

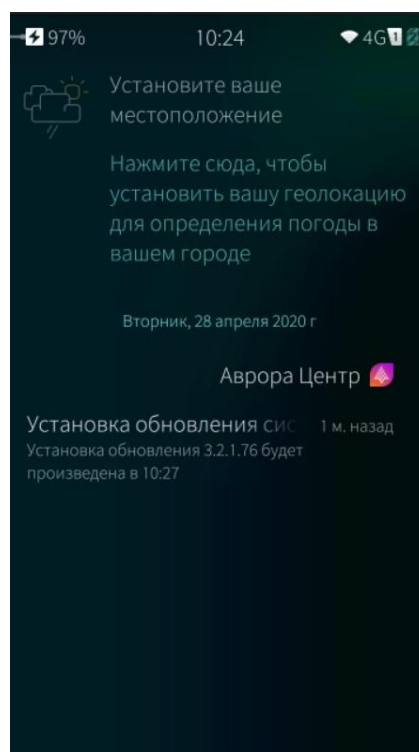


Рисунок 36

Для установки обновления заряд МУ должен быть не менее 50%. В назначенное время начнется установка обновления.

Нельзя перезагружать или выключать МУ во время установки обновления ЗМОС

После установки обновления МУ будет перезагружено. Если обновление ЗМОС прошло успешно, отобразится сообщение «ОС успешно обновлена до версии [номер версии ЗМОС]».

3. СООБЩЕНИЯ ОБ ОШИБКАХ

В ходе работы с МП «Аврора Центр» пользователям могут выдаваться сообщения об ошибках, приведенные в таблице (Таблица 1).

Таблица 1

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
1.	Активация устройства завершена с ошибкой. QR код был использован ранее	Был отсканирован ранее использованный QR код либо МУ уже было активировано на сервере. Необходимо ознакомиться с информацией в 2.1
2.	Сеть недоступна	Проверить подключение к сети на МУ
3.	Вы пытаетесь произвести повторную активацию на сервере ПУ с помощью QR кода, который содержит неверный адрес сервера. QR код для повторной активации обязательно должен содержать url сервера, на котором производилась первичная активация МУ	Повторная активация на другом сервере возможна только в режиме администратора. Необходимо перевести МУ в режим администратора и повторно активировать МУ
4.	Активация завершена с ошибкой: QR код не валиден	Попытка активации МУ через с невалидной информацией. Необходимо повторно сгенерировать QR код для активации
5.	Активация завершена с ошибкой: Неправильный адрес сервера	Попытка активации МУ через QR код или json с невалидной информацией. Необходимо повторно сгенерировать QR код для активации

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
6.	Активация завершена с ошибкой: Срок действия кода истек	Попытка активации МУ через QR код или JSON с просроченной датой активации. Необходимо повторно сгенерировать QR код для активации
7.	Активация завершена с ошибкой: Неверные данные для входа	Попытка активации МУ с использованием QR кода другого МУ. Необходимо повторно сгенерировать QR код для активации. Либо произошла ошибка авторизации учетной записи МУ. Необходимо обратиться к системному администратору
8.	Активация завершена с ошибкой: Учетная запись заблокирована	Ошибка авторизации учетной записи МУ. Необходимо обратиться к системному администратору

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 1).

Таблица 1

Термин/ Сокращение	Расшифровка
ЗМОС	Защищенная мобильная операционная система общего назначения на базе Sailfish Mobile OS RUS, имеющая действительный сертификат соответствия ФСТЭК России, и/или операционная система Аврора, имеющая действительный сертификат соответствия ФСТЭК России
МП	Мобильное приложение
МУ	Мобильное устройство
ОС	Операционная система
ППО	Прикладное программное обеспечение «Аврора Центр»
ПУ	Подсистема Платформа управления
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
JSON	JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript
QR-код	Quick response code – код быстрого реагирования, матричный код (двумерный штрихкод)
WLAN	Wireless Local Area Network — локальная сеть, построенная на основе беспроводных технологий

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]