ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

УТВЕРЖДЕН

АДМГ.20134-01 90 01-1-ЛУ

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Руководство пользователя. Часть 5

Мобильное приложение «Аврора Центр»

АДМГ.20134-01 90 01-5

Листов 32

Подп. и дата	
Инв. №дубл.	
Взам. инв. №	
Подп. и дата	
Инв. №подл.	

2021

АННОТАЦИЯ

Настоящий документ является пятой частью руководства пользователя прикладного программного обеспечения «Аврора Центр» АДМГ.20134-01 релиз 2.5.1 (далее – ППО).

Руководство пользователя состоит из пяти частей:

– «Руководство пользователя. Часть 1. Подсистема безопасности» АДМГ.20134-01 90 01-1;

– «Руководство пользователя. Часть 2. Подсистема «Маркет» АДМГ.20134-01 90 01-2;

– «Руководство пользователя. Часть 3. Подсистема Платформа управления» АДМГ.20134-01 90 01-3;

– «Руководство пользователя. Часть 4. Мобильное приложение «Аврора Маркет» АДМГ.20134-01 90 01-4;

– «Руководство пользователя. Часть 5. Мобильное приложение «Аврора Центр» АДМГ.20134-01 90 01-5.

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

СОДЕРЖАНИЕ

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1. Основная информация

ППО предназначено для управления мобильными устройствами (МУ), функционирующими под управлением операционной системы (ОС) Аврора, имеющей действительный сертификат соответствия ФСТЭК России, управления жизненным циклом МП и обновлением ОС, 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.

ПРИМЕЧАНИЕ. Под обновлением ОС понимается инициализация в ОС процессов получения пакетов с изменениями ОС (образа ОС) из доверенного хранилища и их установки. Получение пакетов с изменениями ОС и их установка осуществляется штатными средствами ОС. ППО не гарантирует успех получения пакетов с изменениями ОС и их установки.

ППО является прикладным программным обеспечением с встроенными механизмами защиты информации от несанкционированного доступа. ППО может быть использовано, но не ограничиваться, в следующих системах и объектах:

– 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;

– на значимых объектах критической информационной инфраструктуры до 1 категории включительно в соответствии с документом «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденным приказом ФСТЭК России от 25 декабря 2017 г. № 239.

В документе АДМГ.20134-01 90 01-3 приведена следующая основная информация:

– информация о назначении и составе ППО;

– перечень субъектов доступа и права на доступ к интерфейсам ППО;

– назначение и состав Подсистемы Платформа управления (ПУ);

– описание принципов безопасной работы.

Требования к условиям выполнения ППО приведены в документе «Руководство администратора» АДМГ.20134-01 91 01.

1.2. Мобильное приложение «Аврора Центр»

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

– активация МУ;

– передача сообщений компонентам ОС Аврора и компонентам ПУ сведений о настройках и состоянии МУ;

– получение сообщений от ПУ о результатах выполнения операций.

МП «Аврора Центр» выполняется на МУ под управлением ОС Аврора, служит для получения управляющих сообщений от Сервера приложений ПУ и передачи их компонентам ОС Аврора, а также передачи на Сервер приложений ПУ сведений о настройках и конфигурации ОС Аврора. В зависимости от управляющего сообщения или офлайн-сценария, полученного от Сервера приложений ПУ, МП «Аврора Центр» посредством вызова интерфейсных функций ОС Аврора имеет возможность:

– включать и выключать доступ к камере на МУ;

– включать и выключать доступ к браузеру на МУ;

– обновлять версию ОС на МУ;

– блокировать и разблокировать МУ;

– очищать данные (восстанавливать заводские настройки) МУ;

– устанавливать и удалять приложения на МУ;

– получать данные о состоянии МУ и событиях безопасности МУ;

– получать логи с МУ;

– устанавливать расписание обмена данными с МУ;

– включать и выключать доступ к управлению WLAN настройками;

– включать и выключать доступ к WLAN на МУ;

– включать и выключать доступ к точке доступа WLAN на МУ;

– ограничивать и предоставлять доступ к MTP;

– ограничивать и предоставлять доступ к Bluetooth (функционал доступен для версии ОС Аврора 4.0.1 и выше);

– изменять пароль учетной записи пользователя в ОС Аврора;

– блокировать МУ при смене SIM-карты (офлайн-сценарий);

– блокировать МУ при отсутствии связи с сервером (офлайн-сценарий);

– блокировать МУ при входе в зону действия WLAN (офлайн-сценарий);

– блокировать и разблокировать МУ при нахождении вне зоны действия WLAN (офлайн-сценарий).

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»;

– при получении Push-уведомления о наличии операции (в случае если имеется интеграция с Сервисом уведомлений Аврора (СУА)).

2. РАБОТА С МОБИЛЬНЫМ ПРИЛОЖЕНИЕМ «АВРОРА ЦЕНТР»

ПРИМЕЧАНИЕ. Приведенные снимки экрана МУ (смартфон) на основе атмосферы «Северное сияние» являются примером. При использовании другого МУ и другой атмосферы размер экрана и внешний вид интерфейса МУ могут отличаться.

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

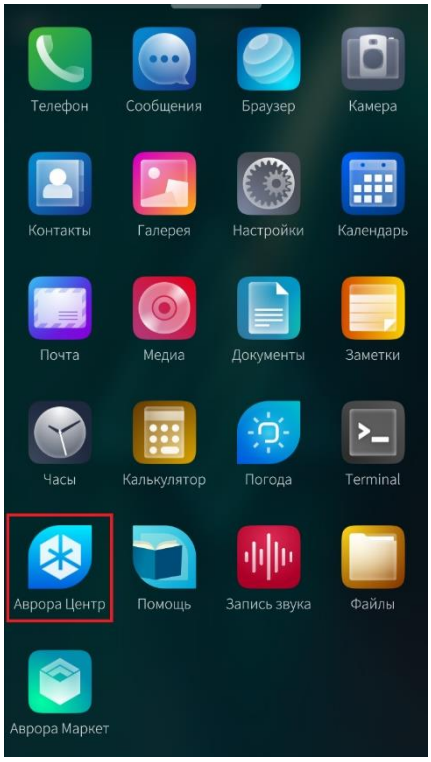

Рисунок 1

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

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

ПРИМЕЧАНИЕ. Состав приложений может меняться в зависимости от варианта исполнения ОС Аврора.

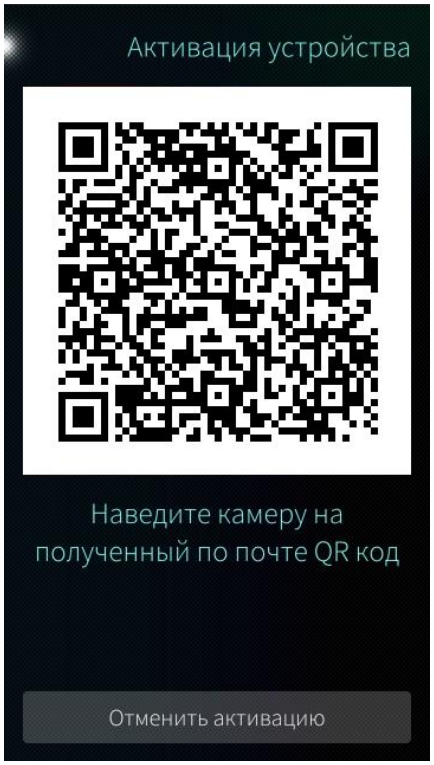

Рисунок 2

– навести камеру МУ на QR-код на странице «Активация устройства» (Рисунок 2). Подробное описание генерации QR-кода в ПУ приведено в документе «Руководство пользователя. Часть 3. Подсистема Платформа управления»;

ПРИМЕЧАНИЕ. Изображение QR-кода должно поместиться в рамку, которая отображается на экране МУ.

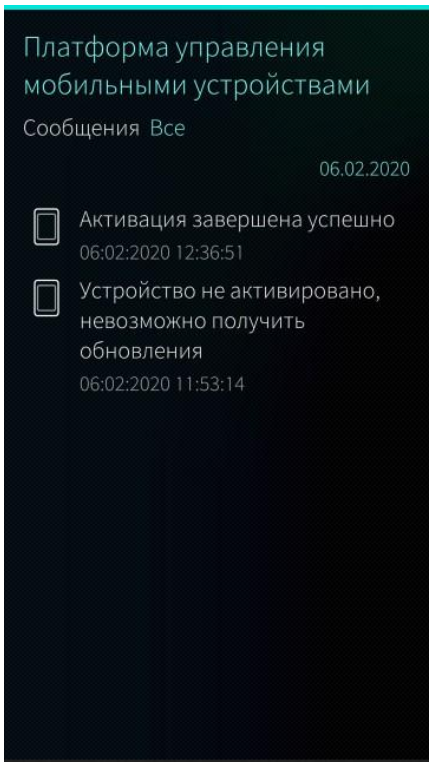

Рисунок 3

– когда МУ будет активировано в ПУ, 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).

ПРИМЕЧАНИЯ:

1. В случае если будет трижды отсканирован неверный QR-код, отобразится сообщение об ошибке: «Активация завершена с ошибкой: Учетная запись временно заблокирована. Обратитесь к администратору». Аккаунт на сервере авторизации будет заблокирован на 15 минут.

2. В случае если срок действия QR-кода истек, отобразится сообщение об ошибке: «Активация завершена с ошибкой: Срок действия кода истек».

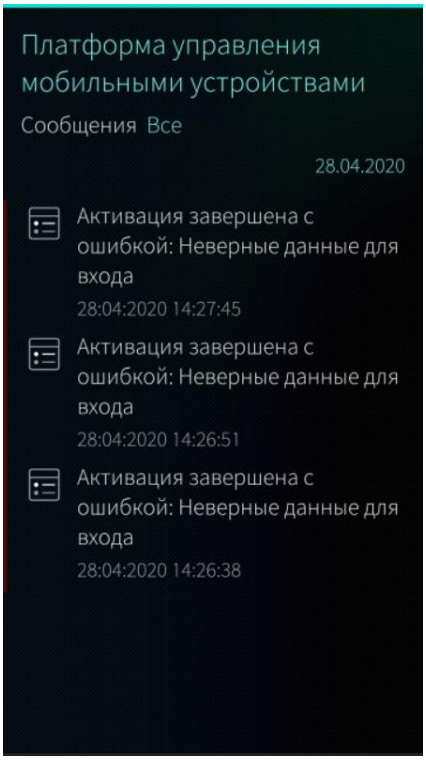

Рисунок 4

Рисунок 5

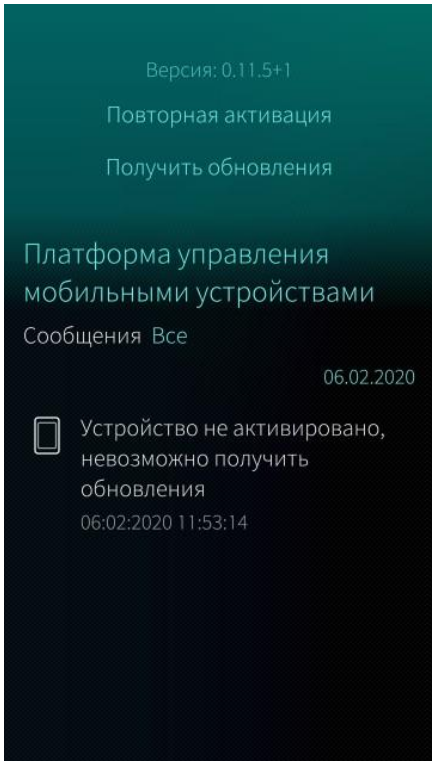

Рисунок 6

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);

ПРИМЕЧАНИЕ. 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).

ПРИМЕЧАНИЕ. 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).

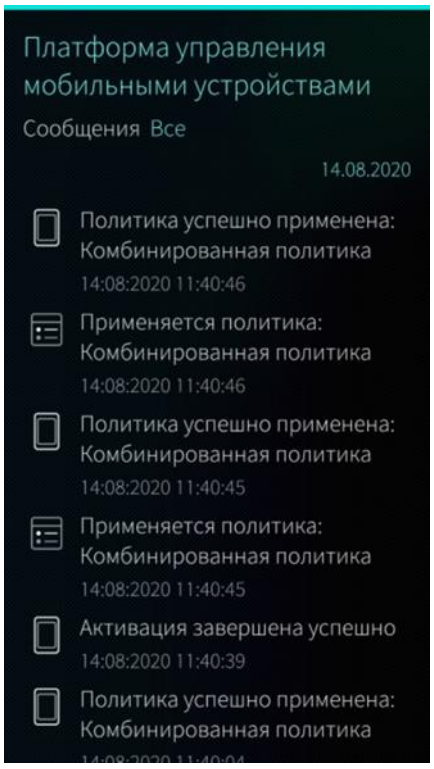

Рисунок 7

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 сертифицированной 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 АДМГ.20134-01 90 01-3;

– 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 АДМГ.20134-01 90 01-3.

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

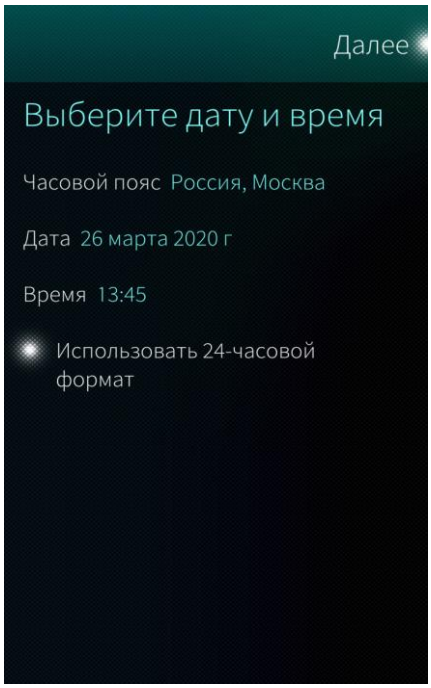

Рисунок 8

Для упрощенной активации МУ необходимо выполнить следующие действия:

– включить МУ;

– принять условия «Лицензионного соглашения» для конечного пользователя МУ;

– 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);

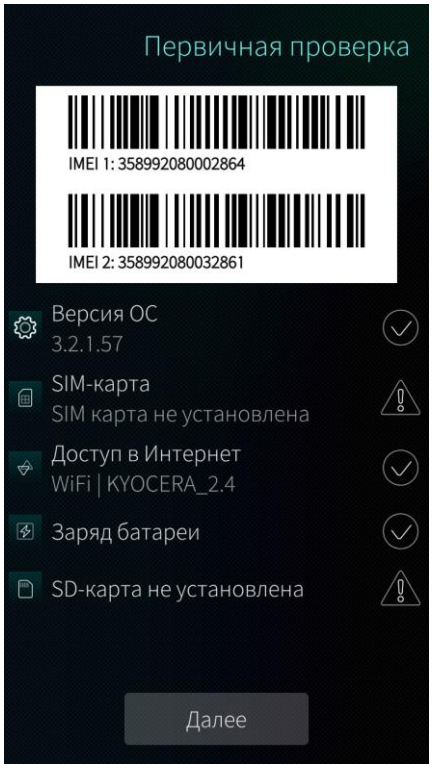

Рисунок 9

– дождаться выполнения первичной проверки и коснуться кнопки «Далее» (Рисунок 9);

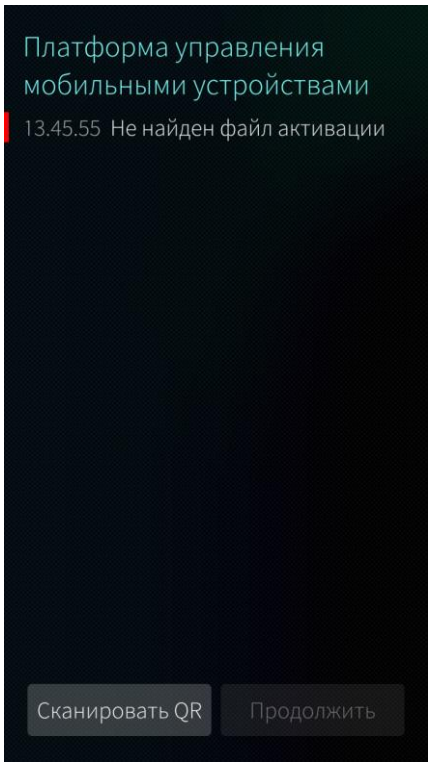

Рисунок 10

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

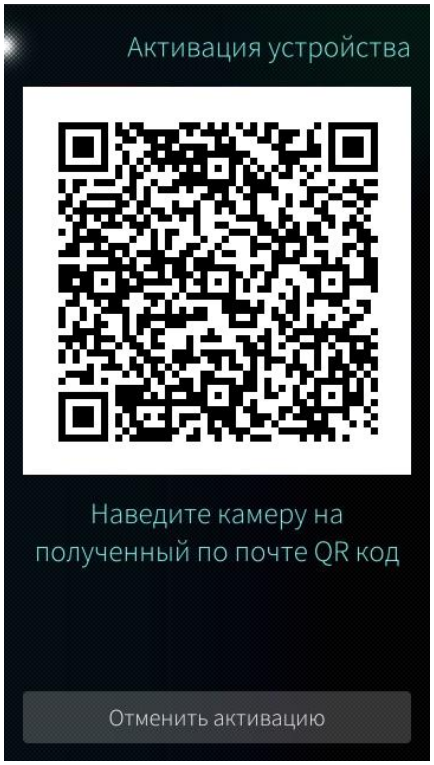

Рисунок 11

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

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

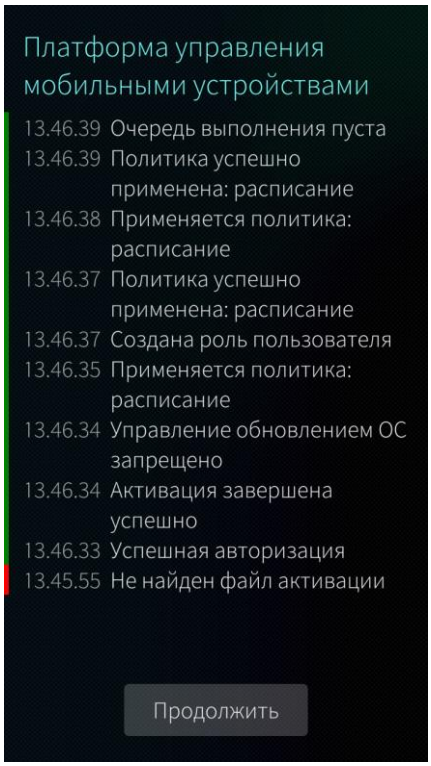

Рисунок 12

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

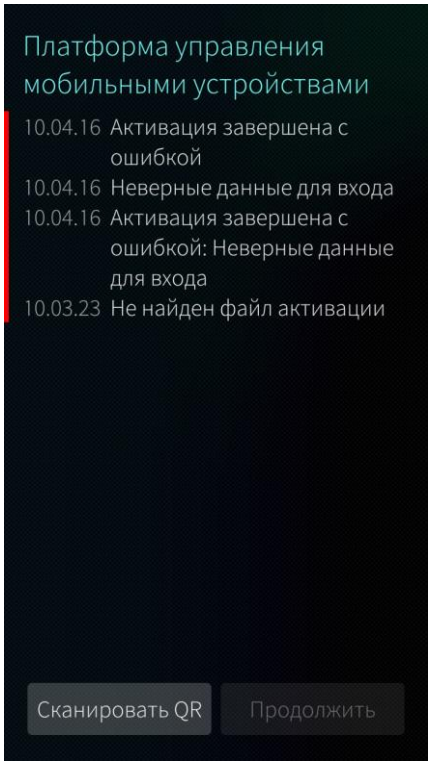

Рисунок 13

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 коснуться кнопки «Сканировать QR».

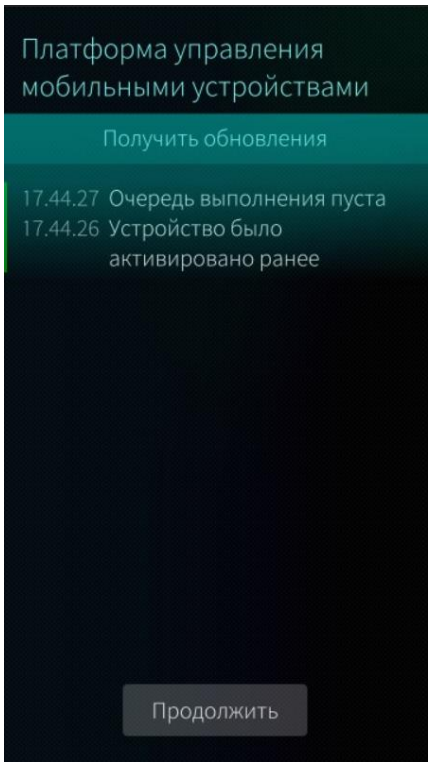

Рисунок 14

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 (получении обновлений) 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.

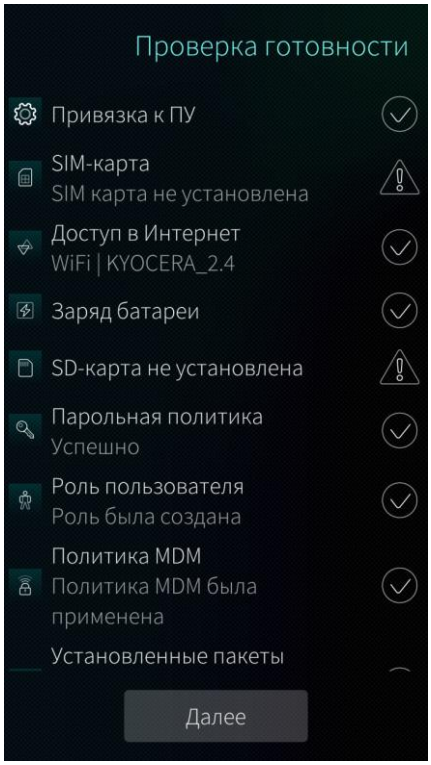

Рисунок 15

Для завершения подготовки МУ к работе следует коснуться кнопки «Продолжить» (Рисунок 14) и выполнить следующие действия:

– дождаться завершения проверки готовности МУ и коснуться кнопки «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 которую включено МУ, затем перезагрузить МУ и пройти упрощенную активацию повторно;

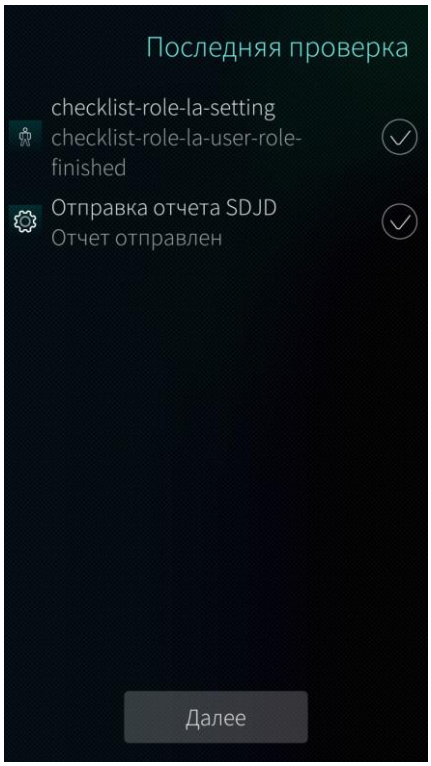

Рисунок 16

– после прохождения проверки готовности необходимо дождаться завершения последней проверки и коснуться кнопки «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

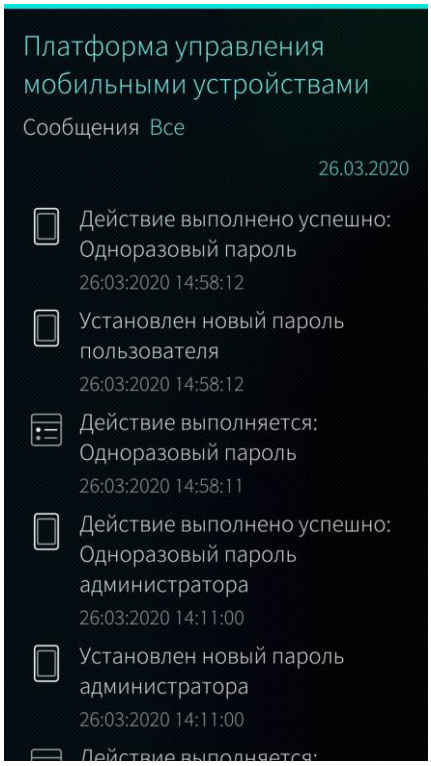

Рисунок 17

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» (функционал доступен только для сертифицированной версии ОС Аврора) и «Задать одноразовый пароль администратора» соответственно.

Подробное описание оперативных команд приведено в документе АДМГ.20134-01 90 01-3.

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

Рисунок 18

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 АДМГ.10034-02 91 01;

– ввести одноразовый пароль, который был выдан Администратором Платформы Управления (Рисунок 18);

Рисунок 19

– использовать предложенный пароль МУ, коснувшись кнопки «Использовать», или сгенерировать новый, коснувшись кнопки «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

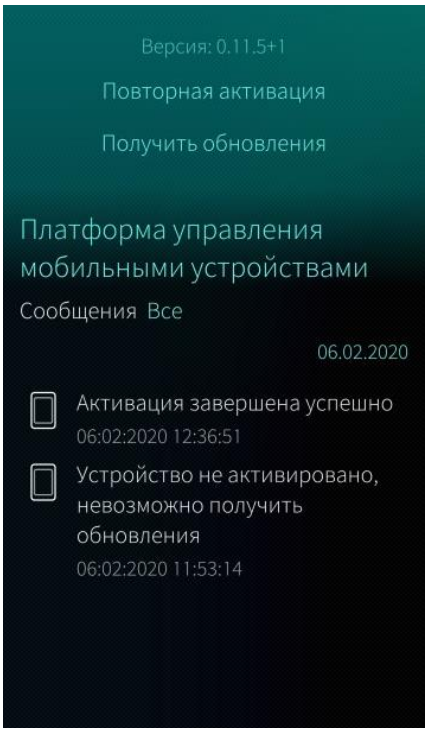

Рисунок 20

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

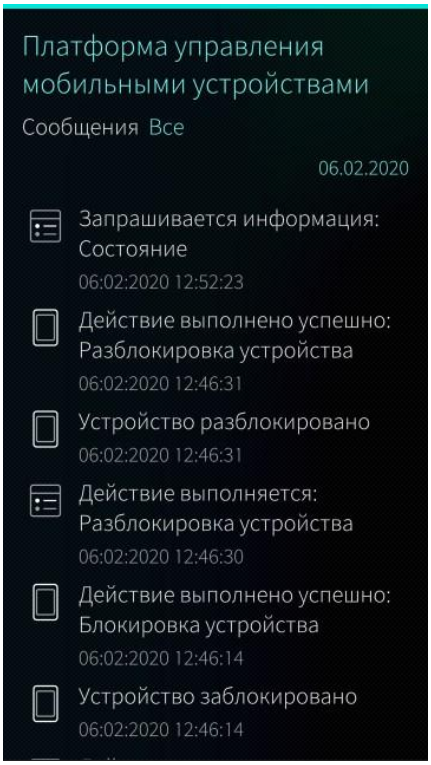

Рисунок 21

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

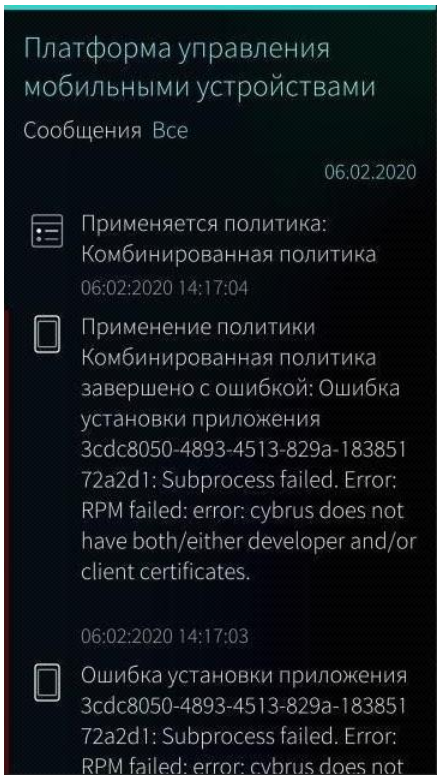

Рисунок 22

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

2.5. Обновление состояния

Если Администратор Платформы Управления запросил состояние с помощью оперативных команд, на МУ отобразится информационное сообщение (см. Рисунок 21).

Данное сообщение означает, что текущее состояние МУ отправлено Администратору Платформы Управления.

2.6. Блокировка мобильного устройства

Рисунок 23

При блокировке МУ через ПУ (описание приведено в документе АДМГ.20134-01 90 01-3) на экране блокировки отображается сообщение «Заблокировано при помощи Aurora Device Manager» (Рисунок 23).

Использование МУ до разблокировки невозможно, кроме совершения экстренного вызова.

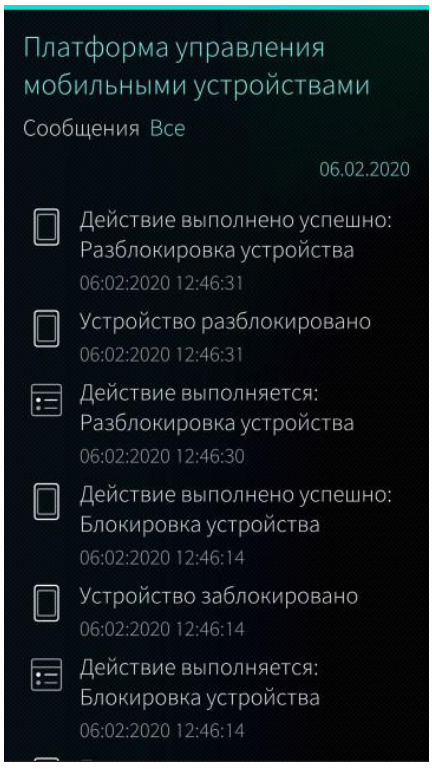

Рисунок 24

По истечении времени блокировки МУ, заданного Администратором Платформы Управления, выполнится разблокировка. В МП «Аврора Центр» отобразится информационное сообщение о разблокировке МУ (Рисунок 24).

2.7. Просмотр информации об операциях по категориям

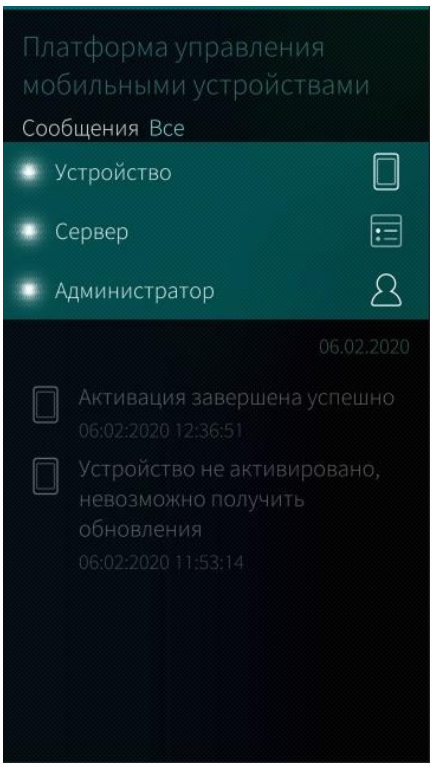

Рисунок 25

В МП «Аврора Центр» можно просмотреть информацию по операциям из следующих категорий (Рисунок 25):

– «Устройство» — сообщения, формируемые МУ;

– «Сервер» — сообщения, которые отправляются с Консоли администратора ПУ;

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

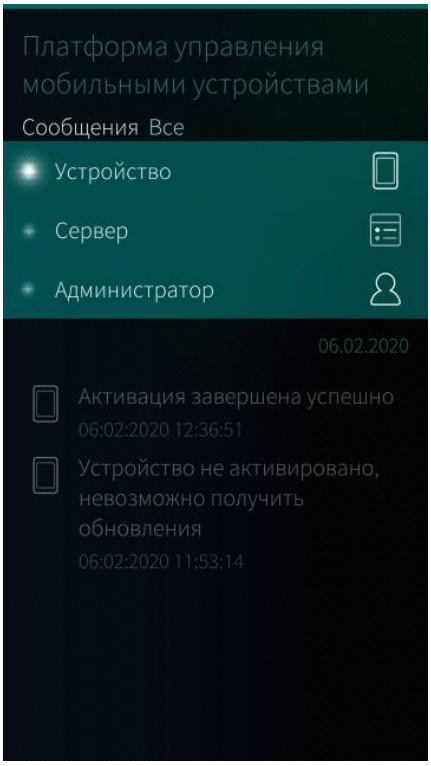

Рисунок 26

Для просмотра информации в поле «Сообщения» в раскрывающемся списке выбрать необходимые категории (Рисунок 26).

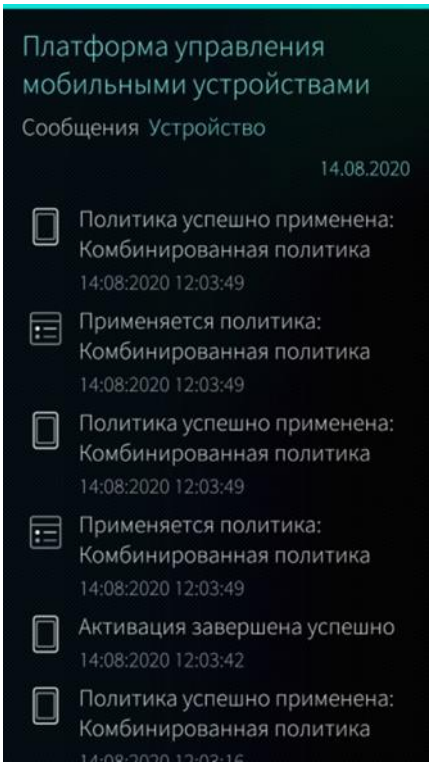

Рисунок 27

В результате отобразится подробная информация по операциям выбранной категории (Рисунок 27).

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

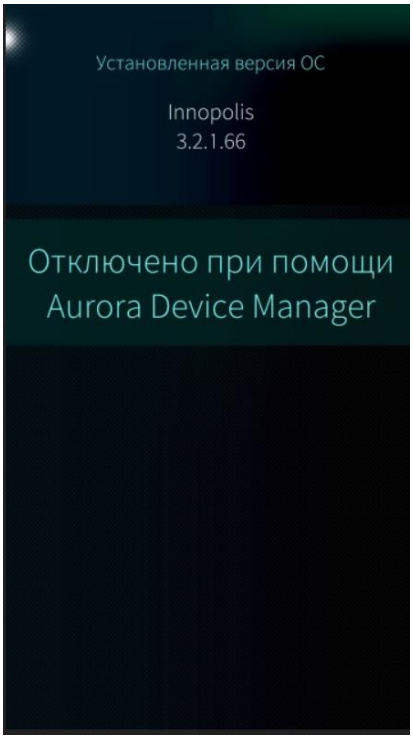

Рисунок 28

Если МУ активировано в ПУ, обновить ОС Аврора через интерфейс нельзя.

При попытке обновить ОС Аврора через интерфейс ОС появится сообщение «Отключено при помощи Aurora Device Manager» (Рисунок 28).

Обновить ОС Аврора на МУ можно с помощью правила политики «Система / Назначить версию ОС». Подробное описание правил политик приведено в документе АДМГ.20134-01 90 01-3.

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

Если на МУ текущая версия ОС Аврора, ниже заданной в политике, отобразится сообщение «Доступно обновление системы [номер версии ОС Аврора]. После скачивания установка будет запланирована на нерабочие часы (чч:мм-чч:мм)» в журнале МП «Аврора Центр» (Рисунок 29) и в уведомлениях на экране событий ОС Аврора (Рисунок 30).

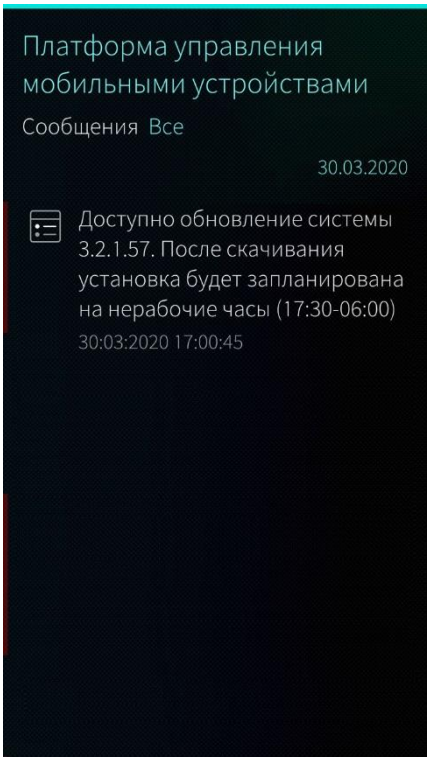

Рисунок 29

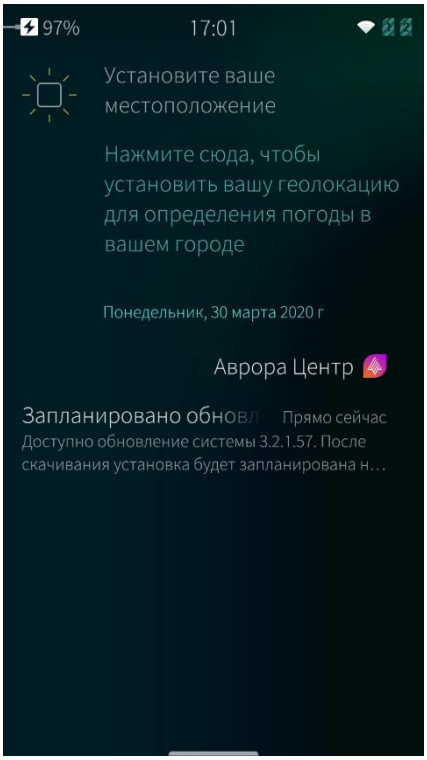

Рисунок 30

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

В результате начнется процесс скачивания загрузочного модуля версии ОС Аврора. Будет отображено сообщение «Загрузка обновления [номер версии ОС Аврора]» в журнале МП «Аврора Центр» (Рисунок 31) и «Обновление системы [номер версии ОС Аврора] загружается» в уведомлениях на экране событий ОС Аврора (Рисунок 32).

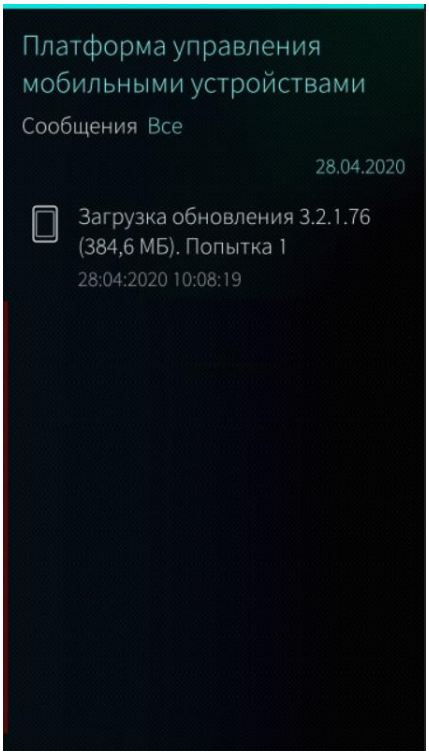

Рисунок 31

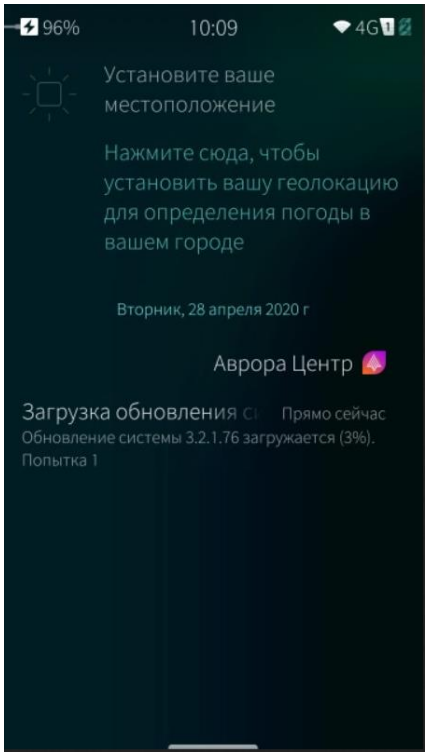

Рисунок 32

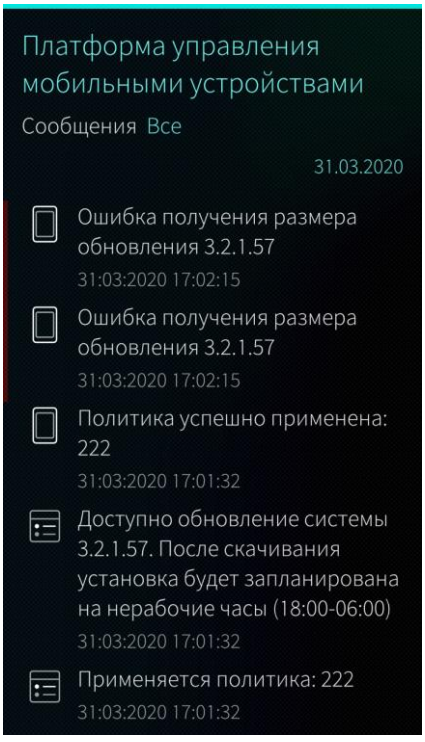

Рисунок 33

Если репозиторий с обновлением недоступен (подробная информация приведена в документе АДМГ.20134-01 91 01), или на МУ недостаточно свободного места для скачивания обновления, отобразится сообщение «Ошибка получения размера обновления [номер версии ОС Аврора]» в журнале МП «Аврора Центр» (Рисунок 33).

После завершения скачивания в журнале МП «Аврора Центр» отобразится сообщение «Установка обновления [номер версии ОС Аврора] будет произведена в чч:мм» (Рисунок 34) и в уведомлениях на экране событий ОС Аврора (Рисунок 35). Во временной интервал между завершением скачивания обновления и его установкой можно продолжать управлять МУ через ПУ.

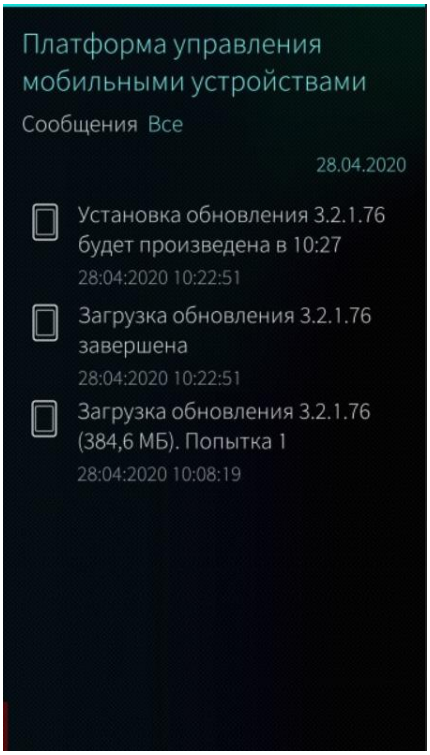

Рисунок 34

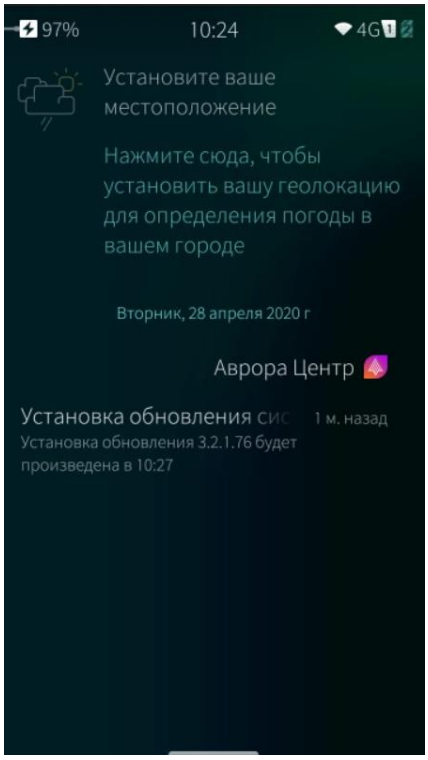

Рисунок 35

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

ПРИМЕЧАНИЕ. Нельзя перезагружать или выключать МУ во время установки обновления ОС Аврора.

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

2.9. Офлайн-сценарии

В подразделе «Сценарии» Консоли администратора ПУ Администратор Платформы Управления может создавать сценарии команд по событию для офлайн применения на МУ группы МУ или группы пользователей МУ.

Сценарии действуют на МУ в течение неограниченного времени, т.е. могут срабатывать несколько раз, в случае если события будут повторяться, например, пользователь будет несколько раз входить в зону WLAN.

Подробное описание работы со сценариями приведено в документе АДМГ.20134-01 90 01-3.

С помощью офлайн-сценариев Администратор Платформы Управления имеет возможность:

– заблокировать МУ группы МУ или группы пользователей МУ;
– разблокировать МУ;
– очистить МУ;
– задать одноразовый пароль;
– задать одноразовый пароль администратора;
– задать период отправки сообщений SDJD;
– сбросить период отправки сообщений SDJD.

Если Администратор Платформы Управления назначил на группу МУ сценарий по событию «Отсутствие связи с сервером» с реакцией «Блокировать устройство» и задал определенный период времени, в течение которого МУ может не выходить на связь с Консолью администратора ПУ, то МУ получает данный сценарий и создает триггер.

На МУ при этом отображаются следующие информационные сообщения (Рисунок 36, Рисунок 37):

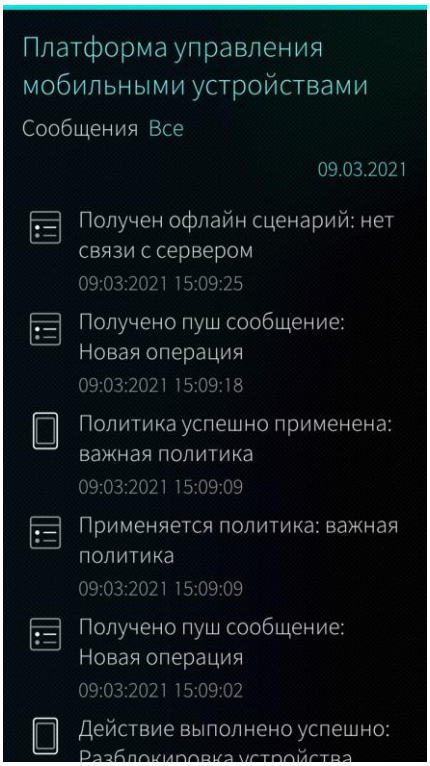

Рисунок 36

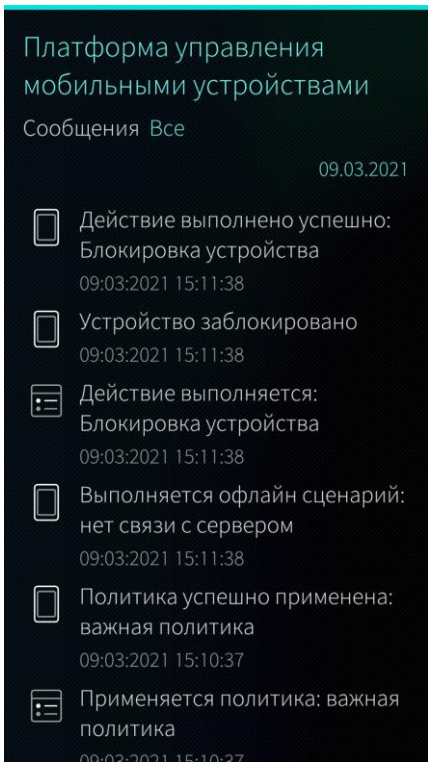

Рисунок 37

Если связь МУ с сервером отсутствует в течение заданного периода (например, на МУ нет интернета), то МУ блокируется. На экране блокировки отображается сообщение «Заблокировано при помощи Aurora Device Manager» (см. Рисунок 23). Отменить действие сценария возможно через оперативное управление ПУ. В случае если на МУ придет команда разблокировки через оперативное управление, устройство разблокируется.

Если Администратор Платформы Управления назначил на группу МУ сценарий по событию «Смена SIM-карты» с реакцией «Блокировать устройство», то МУ получает данный сценарий, сохраняет тот список SIM-карт, которые в него вставлены на данный момент, и создает триггер. Когда пользователь меняет SIM-карту или просто вытаскивает ее, срабатывает триггер и МУ блокируется.

Если Администратор Платформы Управления назначил на группу МУ сценарий по событию «Вход в зону WLAN» с реакцией «Блокировать устройство» и ввел BSSID точки доступа WLAN, то МУ получает данный сценарий и блокируется, если в зоне видимости появляется указанная выше точка доступа WLAN.

ПРИМЕЧАНИЕ. Данный сценарий возможен только при включенном WLAN на МУ.

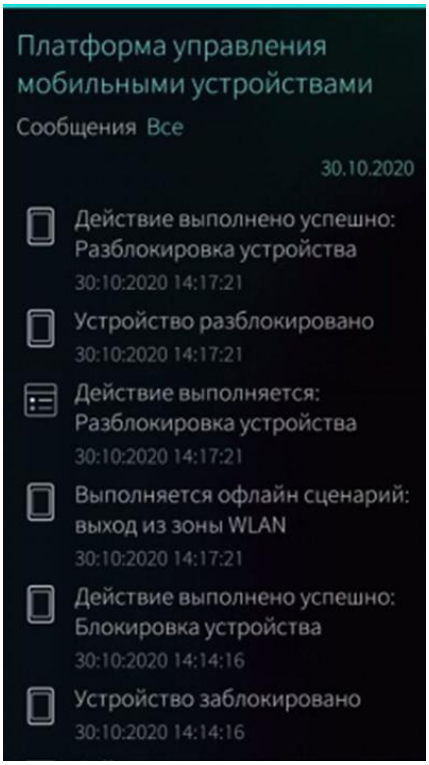

Рисунок 38

Если Администратор Платформы Управления назначил на группу МУ сценарий по событию «Вне зоны действия WLAN» с реакцией «Разблокировать устройство», то МУ, получив данный сценарий, будет разблокировано при выходе из зоны доступа WLAN (около 3 мин) (Рисунок 38).

ПРИМЕЧАНИЕ. При наличии двух сценариев с триггерами-антагонистами на МУ, реакции на такие триггеры будут отменять друг друга. В описанном выше примере: вход в зону WLAN — блокировка устройства, выход из зоны — разблокировка.

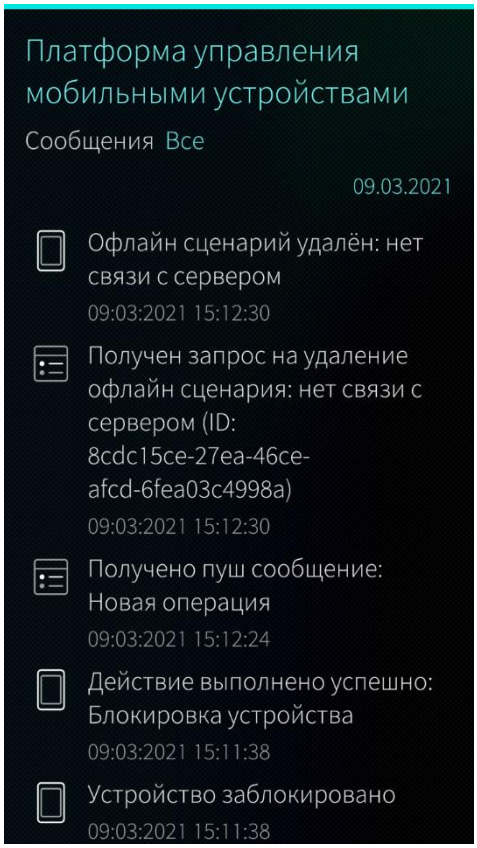

Рисунок 39

Если Администратор Платформы Управления назначил операцию на удаление офлайн-сценария с МУ (Рисунок 39), то при получении операции на МУ в случае, если событие уже наступило, действие на МУ будет сохранено. Например, если МУ было заблокировано из-за смены SIM-карты, то при удалении сценария по событию «Смена SIM-карты» с реакцией «Блокировать устройство», МУ останется заблокировано.

Но в случае, если событие еще не наступило, сценарий удалится.

2.10. Push-уведомления

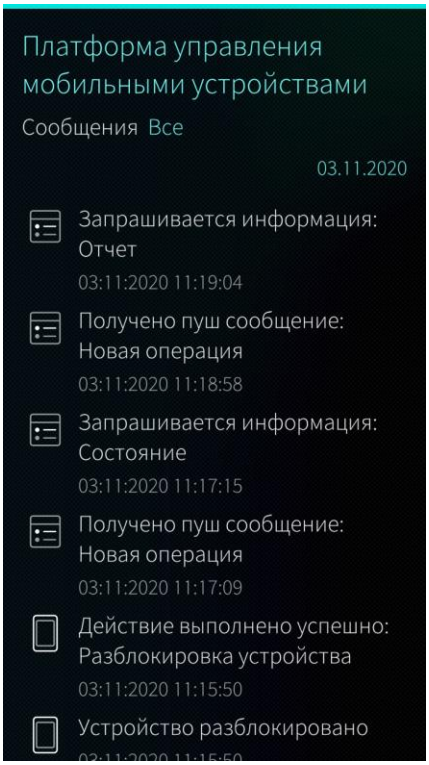

Рисунок 40

С помощью СУА на МУ осуществляется оперативная доставка информации (текстовые сообщения и команды) в виде текстовых Push-уведомлений (Рисунок 40). При интеграции МУ с СУА все операции на МУ приходят в реальном времени, т.е. в реальном времени приходят и применяются на МУ оперативные команды, политики, сценарии.

После отправки команды с Консоли администратора ПУ на МУ оно немедленно получает уведомление от СУА и выполняет операцию.

В случае отправки Push-уведомления в момент недоступности МУ, МП получит Push-уведомления после подключения к сети, обеспечивающей доступ к СУА.

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 QR код 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
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

№	Текст ошибки в интерфейсе	Действия для устранения ошибок
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
9.	Активация завершена с ошибкой: Учетная запись временно заблокирована. Обратитесь к администратору	Было совершено более 3 попыток активации неверным QR кодом (или json файлом активации). Длительность блокировки 15 минут

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 2).

Таблица 2

Термин/ Сокращение	**Расшифровка**
МП	Мобильное приложение
МУ	Мобильное устройство
ОС	Операционная система
Офлайн-сценарий	Набор значений опций и/или команд, который отправляется с указанием события срабатывания на МУ, и должен «мгновенно» примениться по этому событию
ППО	Прикладное программное обеспечение «Аврора Центр»
ПУ	Подсистема Платформа управления
СУА	Сервис уведомлений Аврора
Push-уведомления	(англ. push букв. «проталкивание») — текстовые сообщения, предназначенные для оперативной (мгновенной) доставки на МУ пользователей
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
JSON	JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript
MTP	Media Transfer Protocol — основанный на PTP[en] аппаратно-независимый протокол, разработанный компанией Microsoft для подключения цифровых плееров к компьютеру
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

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					