

# РУКОВОДСТВО АДМИНИСТРАТОРА

Версия 1.0

Листов 71

## АННОТАЦИЯ

Настоящий документ является руководством администратора Операционной системы (ОС) Аврора релиз 4.0.2 update 1.

Настоящий документ содержит описание доступных администратору функциональных возможностей мобильного устройства (МУ), функционирующего под управлением ОС Аврора<sup>1</sup>.

Администратор имеет доступ к функциям и настройкам ОС Аврора, описанным как в настоящем документе, так и в документе «Руководстве пользователя».

**ПРИМЕЧАНИЕ.** Перед началом работы администратору необходимо ознакомиться с положениями настоящего документа, а также с информацией, приведенной в документе «Руководство пользователя».

Описание элементов интерфейса и особенностей работы МУ, функционирующего под управлением ОС Аврора, приведено в документе «Руководство пользователя».

**ПРИМЕЧАНИЕ.** Внешний вид интерфейса МУ может отличаться от приведенного на рисунках в настоящем документе. Снимки экрана МУ являются примером и представлены в документе для общего ознакомления с интерфейсом МУ.

---

<sup>1</sup> Описание различных способов установки ОС Аврора на МУ приведено в соответствующих документах предприятия-разработчика, которые предназначены для использования Производителями МУ и авторизованными Сервисными центрами производителя.

## СОДЕРЖАНИЕ

1. Ввод в эксплуатацию.....	5
1.1. Первое включение .....	5
1.2. Установка времени и даты .....	6
1.3. Ограничения по эксплуатации .....	8
1.4. Учетные записи ролей .....	9
1.4.1. Создание учетной записи пользователя .....	9
1.4.2. Переключение между учетными записями .....	11
1.4.3. Управление исходящими голосовыми вызовами и SMS .....	14
1.4.4. Переименование учетной записи.....	15
1.4.5. Удаление учетной записи пользователя .....	15
1.5. Настройки безопасности .....	16
1.5.1. Настройка блокировки.....	16
1.5.2. Настройки парольной политики .....	18
1.5.3. Настройки безопасности пользователя .....	23
1.6. Настройка МУ .....	31
1.6.1. Настройка USB-подключения .....	31
1.6.2. Настройка PIN-кода для SIM-карты.....	32
1.6.3. Настройки МП.....	33
2. Выполнение программы.....	35
2.1. Настройка обновлений ОС Аврора .....	35
2.2. Сброс настроек МУ.....	37
2.3. МП «Terminal» .....	39
2.3.1. Интерфейс МП «Terminal» .....	40
2.3.2. Получение прав суперпользователя.....	41
2.4. Управление сторонним ПО .....	42
2.4.1. Установка стороннего ПО .....	42
2.4.2. Подпись и проверка стороннего ПО.....	44
3. Средства разработчика.....	48
3.1. Активация режима разработчика .....	48
3.2. Инструменты разработчика.....	49
4. Описание механизмов защиты .....	51
4.1. Регистрация событий безопасности (аудит) .....	51
4.1.1. Основная информация.....	51
4.1.2. Сохранение событий безопасности во внутреннюю память.....	53
4.1.3. Просмотр сообщений аудита .....	53
4.2. Идентификация и аутентификация .....	54
4.3. Управление доступом (политики безопасности).....	55
4.4. Идентификация и аутентификация .....	59

---

4.5. Изоляция процессов .....	60
4.6. Защита памяти .....	61
4.7. Подписи RPM-пакетов .....	61
4.8. Фильтрация сетевого потока .....	62
4.9. Контроль целостности .....	62
4.10. Шифрование раздела с домашними директориями пользователей .....	63
5. Рекомендации по устранению возможных ошибок .....	65
Перечень терминов и сокращений .....	68

## 1. ВВОД В ЭКСПЛУАТАЦИЮ

**ПРИМЕЧАНИЕ.** Перед началом работы с МУ администратору необходимо ознакомиться с особенностями первоначальной настройки, подробное описание которой приведено в документе «Руководство пользователя».

### 1.1. Первое включение

**ВНИМАНИЕ!** При первом включении МУ необходимо дважды ввести код безопасности.

Код безопасности будет запрашиваться и использоваться для:

- доступа к зашифрованному домашнему каталогу пользователя (Рисунок 1);
- разблокировки МУ (Рисунок 2).

**ПРИМЕЧАНИЕ.** Шифрование раздела с домашними директориями пользователей (п. 4.10) происходит в следующих случаях:

- при первом включении МУ
- после сброса МУ до заводского состояния (п. 2.2).

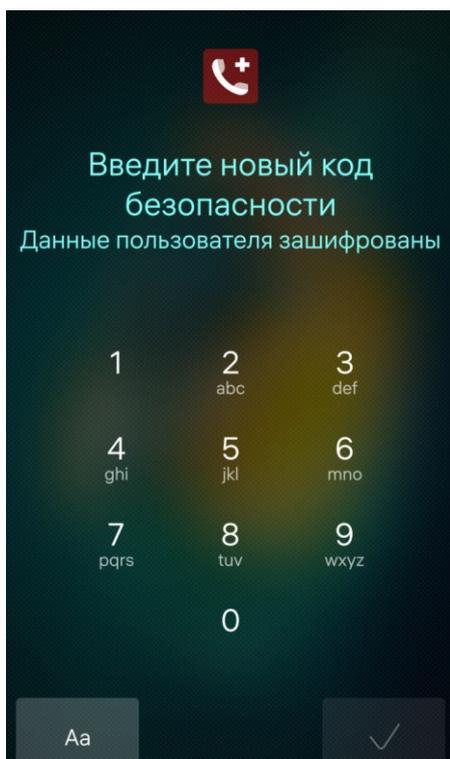


Рисунок 1

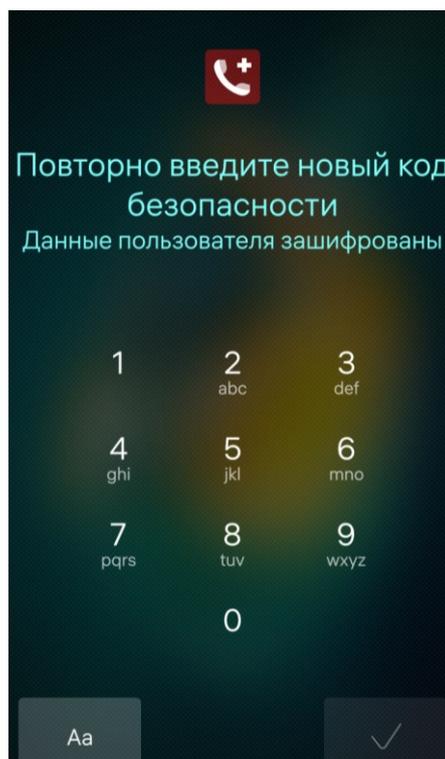


Рисунок 2

## 1.2. Установка времени и даты

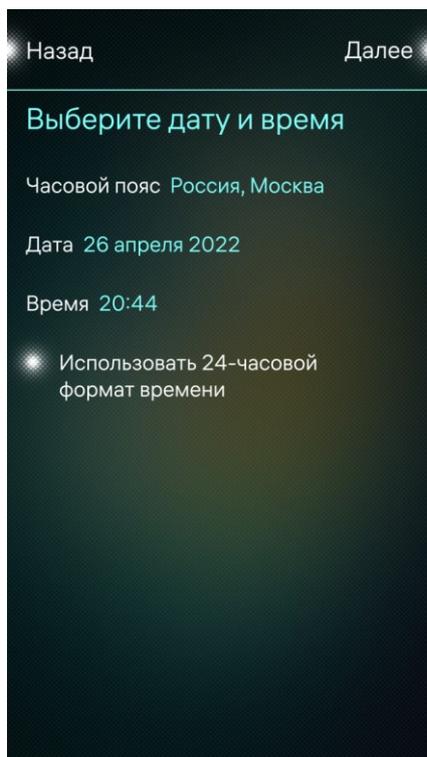


Рисунок 3

Для установки времени и даты необходимо убедиться, что все поля заполнены корректно, после чего коснуться кнопки «Далее» (Рисунок 3).

На странице выбора даты и времени доступны следующие возможности:

- изменить значения параметров «Часовой пояс», «Дата», «Время», коснувшись соответствующих полей;

- выбрать формат времени, коснувшись соответствующего переключателя.

**ПРИМЕЧАНИЕ.** Для активации переключателя достаточно коснуться поля, в котором он расположен: переключатель начнет светиться ярче, чем в состоянии по умолчанию (неактивном).

**ПРИМЕЧАНИЕ.** Изменения настроек в пункте меню «Время и дата» применяются ко всем учетным записям ролей, созданных на МУ.

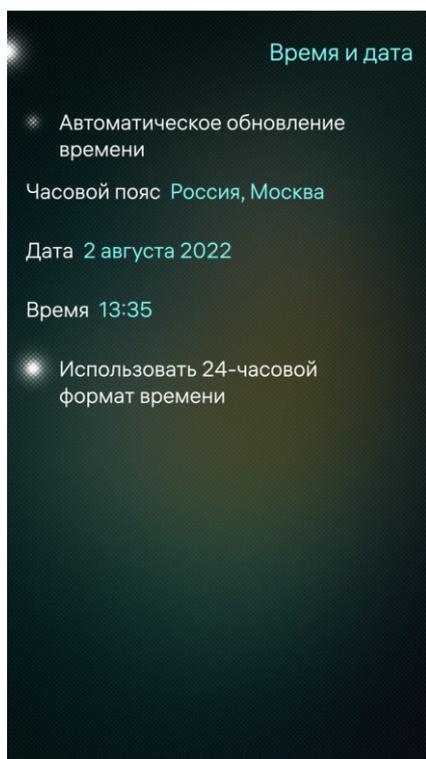


Рисунок 4

Для последующей настройки часового пояса, текущих даты и времени необходимо в меню настроек системы коснуться пункта «Время и дата» , в результате чего отобразится страница настройки даты и времени (Рисунок 5), позволяющая активировать опцию автоматического обновления даты и времени либо настроить указанные параметры вручную.

В случае необходимости задать автоматическое обновление даты и времени следует коснуться переключателя «Автоматическое обновление времени» (Рисунок 4), после чего значения полей часового пояса, даты и времени станут недоступными для редактирования, при этом в дальнейшем обновление даты и времени будет происходить автоматически.

В случае необходимости задать часовой пояс, время и дату вручную требуется выполнить следующие действия:

**ПРИМЕЧАНИЕ.** При установке часового пояса, времени и даты вручную опция автоматического обновления времени должна быть выключена.

– для установки часового пояса вручную: коснуться поля «Часовой пояс» (см. Рисунок 4) и на открывшейся странице выбрать необходимое значение (Рисунок 5). Для ускорения процесса выбора можно воспользоваться полем поиска;

– выбрать формат времени, коснувшись переключателя «Использовать 24-часовой формат» (см. Рисунок 4) для отображения времени в соответствующем формате. Если данный пункт не активирован, время будет отображаться в 12-часовом формате с уточнением «до полудня» или «после полудня»;

– для установки даты вручную: коснуться поля «Дата» (см. Рисунок 4), на открывшейся странице коснуться текущей даты и выбрать из списка текущий год, месяц и число (Рисунок 6);

– коснуться кнопки «Подтвердить» для сохранения даты либо кнопки «Отменить» для отмены операции. В случае подтверждения выбранная дата отобразится на странице настройки даты и времени, в случае отмены дата останется прежней;

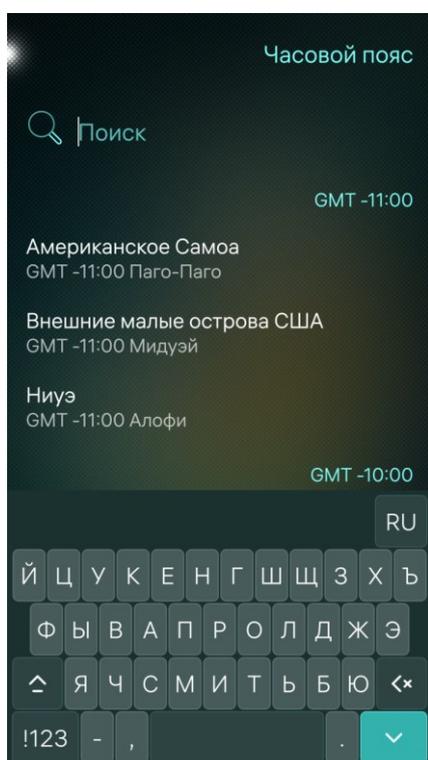


Рисунок 5



Рисунок 6

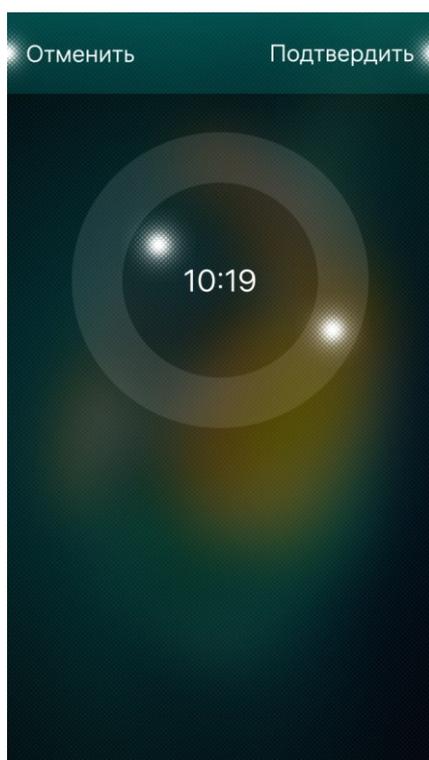


Рисунок 7

– для установки времени коснуться поля «Время» (см. Рисунок 4), в результате чего отобразится циферблат, метка во внутреннем круге которого играет роль часовой стрелки, во внешнем — минутной (Рисунок 7). Для установки необходимого значения следует поочередно коснуться каждой из меток значка и, передвигая ее по или против часовой стрелки, установить в позиции, соответствующей текущему времени;

– коснуться кнопки «Подтвердить» для сохранения установленного времени либо кнопки «Отменить» для отмены операции.

В случае подтверждения выбранная дата отобразится на странице настройки даты и времени, в случае отмены дата останется прежней.

### 1.3. Ограничения по эксплуатации

При вводе в эксплуатацию МУ, функционирующего под управлением ОС Аврора, администратор может выполнять следующие основные действия:

- соблюдать ограничения по эксплуатации (подраздел 1.3);
- создавать учетные записи пользователей и управлять ими (подраздел 1.4);
- выполнять настройку безопасности (подраздел 1.5);
- осуществлять настройку МУ (подраздел 1.6).

Администратору необходимо соблюдать следующие правила и ограничения по эксплуатации МУ, функционирующего под управлением ОС Аврора:

– не допускать установку любого ПО, поставляемого в отличном от RPM виде (самостоятельное копирование файлов, установка ПО из архивов, установка не в штатные каталоги из RPM- пакетов и т.п.);

– исключить подключение МУ, функционирующего под управлением ОС Аврора, к недоверенным точкам доступа беспроводных интерфейсов (WLAN, Bluetooth) и беспроводным МУ. Перечень доверенных точек доступа должен быть сформирован на месте эксплуатации оператором информационной системы;

– исключить передачу конфиденциальной речевой и иной информации (SMS, MMS) посредством МУ по протоколу GSM;

– предусмотреть меры, обеспечивающие отсутствие компьютерных вирусов на средствах вычислительной техники, к которым подключается МУ.

## 1.4. Учетные записи ролей

В ОС Аврора реализован многопользовательский режим работы, который позволяет использовать МУ нескольким учетным записям с различными ролями.

**ПРИМЕЧАНИЕ.** Роль – совокупность привилегий, на основе которых определяется возможность использования того или иного функционала ОС Аврора.

На МУ, функционирующем под управлением ОС Аврора, могут быть созданы одновременно до 7 учетных записей:

– учетная запись с ролью администратора, которая обладает расширенными функциональными возможностями, при этом:

- не может быть удалена с МУ;
- не обладает правами суперпользователя;
- любые изменения настроек, выполненные под учетной записью администратора, будут применимы ко всем пользователям МУ;

– до 6 учетных записей с ролью пользователя, создание которых выполняется администратором в системных настройках МУ. Пользователь имеет доступ к части собственных настроек, при этом изменения следующих настроек, выполненные под ролью пользователя, будут применимы ко всем пользователям МУ:

**ПРИМЕЧАНИЕ.** По умолчанию при первом включении МУ загружается в режиме администратора.

### 1.4.1. Создание учетной записи пользователя

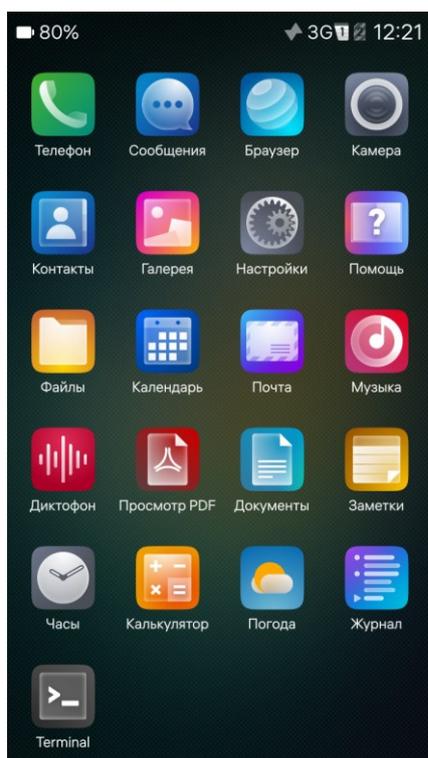


Рисунок 8

Для создания новой учетной записи пользователя администратору необходимо выполнить следующие действия:

– открыть меню настроек касанием значка  на Экране приложений (Рисунок 8);

– в меню системных настроек коснуться пункта «Пользователи» ;

– на странице «Пользователи» коснуться пункта «Добавить пользователя» (Рисунок 9);

– на отобразившейся странице ввести имя и логин новой учетной записи пользователя (Рисунок 10);

– установить количество выделяемых пользователю ГБ, перемещая соответствующий слайдер вправо для увеличения квоты либо влево для уменьшения (Рисунок 10);

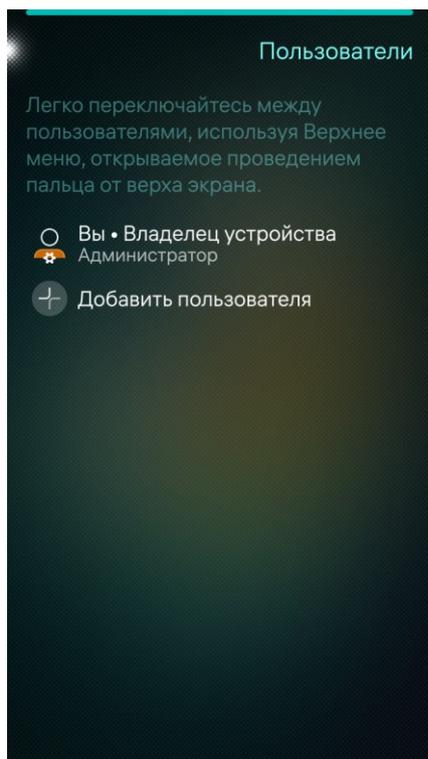


Рисунок 9

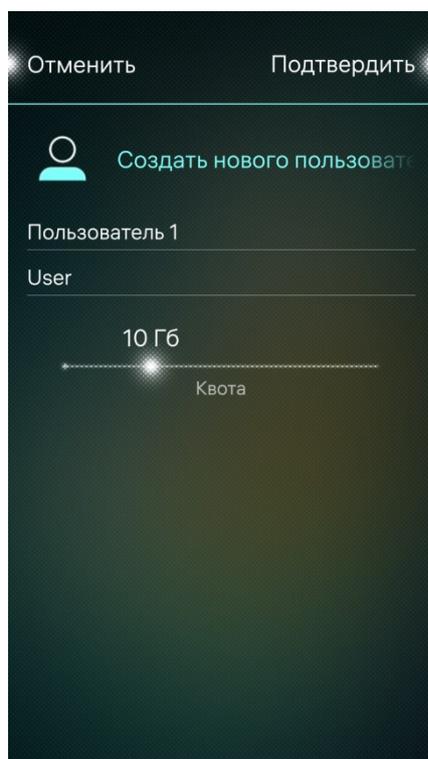


Рисунок 10

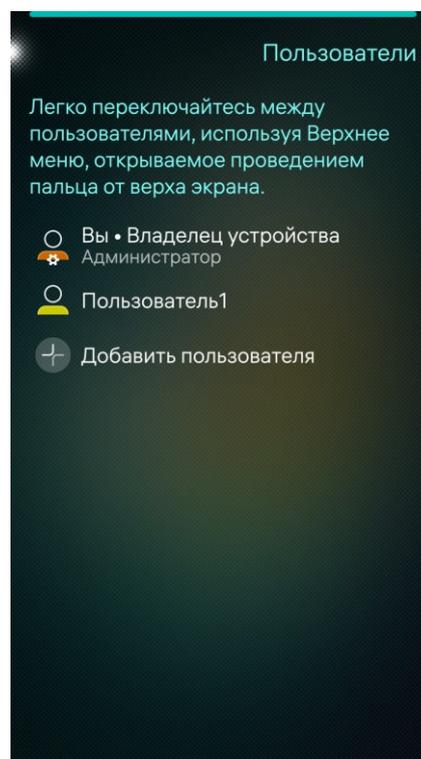


Рисунок 11

**ПРИМЕЧАНИЕ.** Минимальные и максимальные значения для задания квоты зависят от конструктивных особенностей МУ.

– коснуться кнопки «Подтвердить» для сохранения изменений либо кнопки «Отменить» для отмены операции;

– в случае необходимости сохранения изменений подтвердить действие вводом кода безопасности, в результате чего на странице «Пользователи» отобразится строка с созданным пользователем (Рисунок 11).

При первом запуске учетной записи пользователя отобразится экран, в котором необходимо задать код безопасности и коснуться значка  (см. Рисунок 25). Способ задания кода безопасности зависит от варианта исполнения ОС Аврора<sup>2</sup>.

<sup>2</sup> Описание возможных вариантов исполнения ОС Аврора приведены в таблице (Таблица 5).

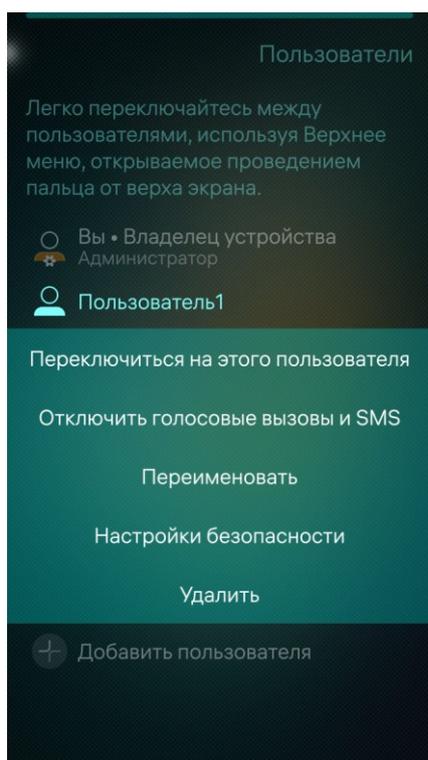


Рисунок 12

При работе с учетными записями пользователей администратору доступны следующие действия (Рисунок 12):

- переключение между учетными записями ролей (п. 1.4.2);
- управление голосовыми вызовами и SMS (п. 1.4.3);
- переименование учетной записи (п. 1.4.4);
- настройки безопасности (подраздел 1.5);
- удаление учетной записи (п. 1.4.5).

#### 1.4.2. Переключение между учетными записями

Просмотреть, под какой учетной записью загружено МУ, а также выполнить переключение между учетными записями можно как в верхнем меню, так и в системных настройках.

Для проверки активной учетной записи с помощью верхнего меню необходимо выполнить следующие действия:

- включить экран МУ;
- открыть верхнее меню, проведя с верхнего края Экрана блокировки к нижнему. В левом нижнем углу будет отображаться текущая роль: «Владелец устройства», если МУ загружено в режиме администратора, либо имя пользователя, если МУ загружено в режиме пользователя (Рисунок 13).

При нахождении в режиме пользователя с помощью верхнего меню можно осуществить переход к учетной записи администратора, выполнив следующие действия:

- включить экран МУ;
- открыть верхнее меню, проведя с верхнего края Экрана блокировки к нижнему;
- коснуться имени учетной записи пользователя;
- в раскрывающемся списке выбрать «Владелец устройства» (Рисунок 14);
- дождаться, когда ОС переключится на учетную запись администратора;

– процесс переключения займет несколько секунд. По окончании процесса переключения необходимо убедиться, что текущая роль «Владелец устройства»: слева от названия роли «Владелец устройства» должна отображаться пометка «Вы».

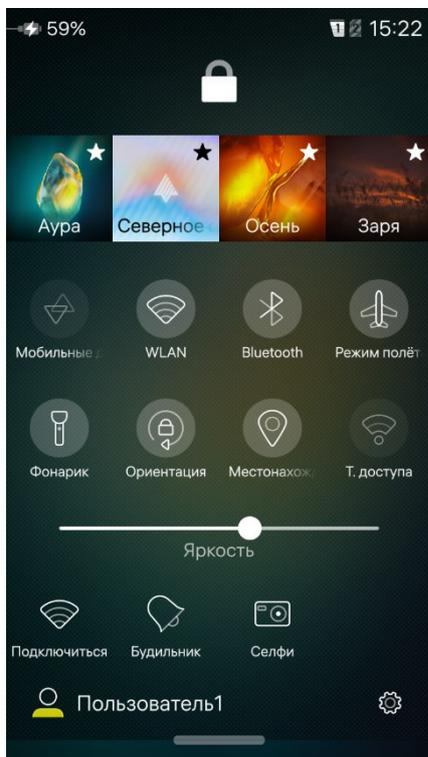


Рисунок 13

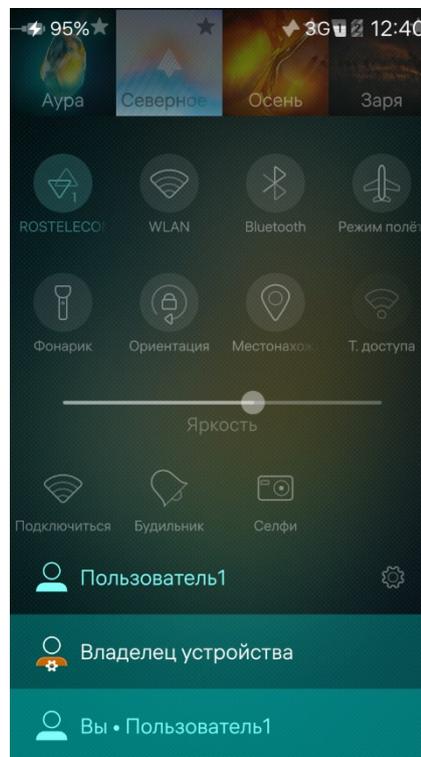


Рисунок 14

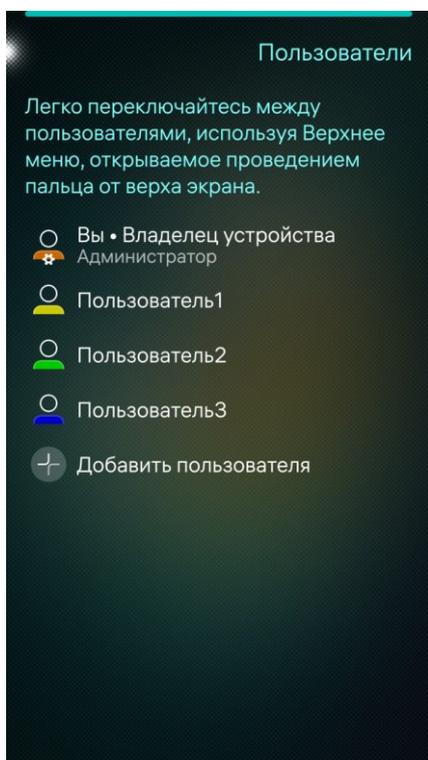


Рисунок 15

Для проверки активной учетной записи с помощью системных настроек необходимо выполнить следующие действия:

– коснуться пункта «Пользователи»  в меню системных настроек, в результате чего отобразится страница «Пользователи» со списком учетных записей пользователей, созданных на МУ (Рисунок 15);

– при работе МУ в режиме администратора в поле «Владелец устройства» отображается пометка «Вы», означающая, что текущий пользователь МУ наделен ролью администратора (Рисунок 15). Для перехода в режим пользователя необходимо выполнить следующие действия:

- коснуться строки с именем одной из учетных записей пользователей, созданных на МУ;
- в контекстном меню коснуться пункта «Переключится на этого пользователя» (см. Рисунок 12);
- процесс переключения займет несколько секунд. По окончании процесса переключения необходимо ввести код безопасности учетной записи пользователя, на которого происходит переключение;
  - при работе МУ в режиме пользователя в поле «[Имя пользователя]» отображается пометка «Вы», означающая, что выбранная учетная запись пользователя МУ является текущей (Рисунок 16). Для перехода в режим администратора необходимо выполнить следующие действия:
    - в перечне пользователей коснуться строки с пометкой «Владелец устройства»;
    - в контекстном меню коснуться пункта «Переключится на этого пользователя» (Рисунок 17);
    - процесс переключения займет несколько секунд. По окончании процесса переключения необходимо ввести код безопасности пользователя, на которого происходит переключение.

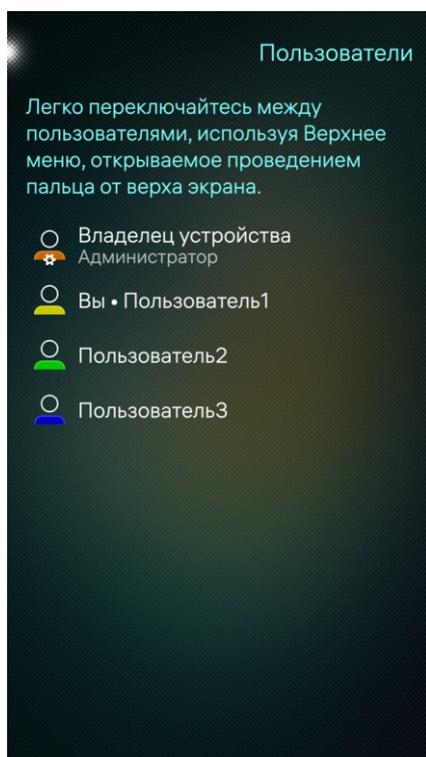


Рисунок 16

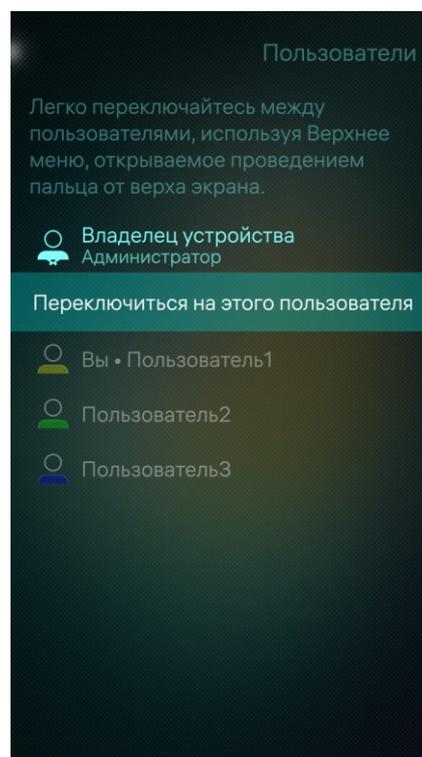


Рисунок 17

### 1.4.3. Управление исходящими голосовыми вызовами и SMS

Для отключения исходящих голосовых вызовов и SMS необходимо в контекстном меню коснуться пункта «Отключить голосовые вызовы и SMS» (см. Рисунок 12).

Далее у выбранного пользователя отобразится предупреждающий значок ✕ (Рисунок 18) и его возможности в МП «Телефон» и МП «Сообщения» будут ограничены.

Для включения исходящих голосовых вызовов и SMS администратору необходимо в контекстном меню коснуться пункта «Включить голосовые вызовы и SMS» (Рисунок 19), после чего предупреждающий значок ✕ перестанет отображаться у выбранного пользователя, и его возможности в МП «Телефон» и МП «Сообщения» будут восстановлены.

**ПРИМЕЧАНИЕ.** Подробное описание работы указанных МП приведено в документе «Руководство пользователя».

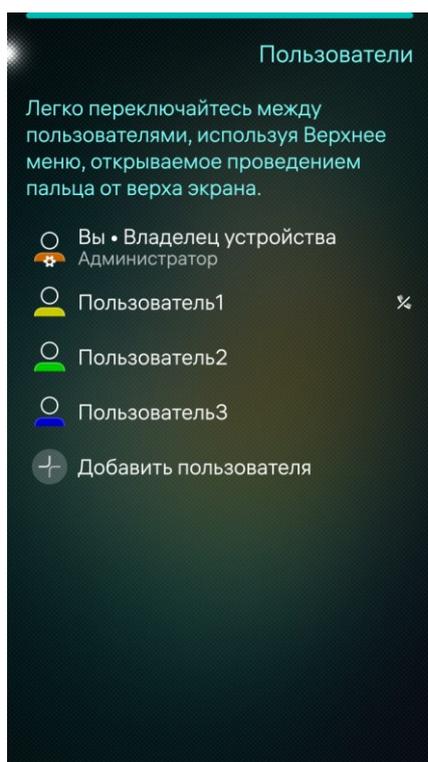


Рисунок 18

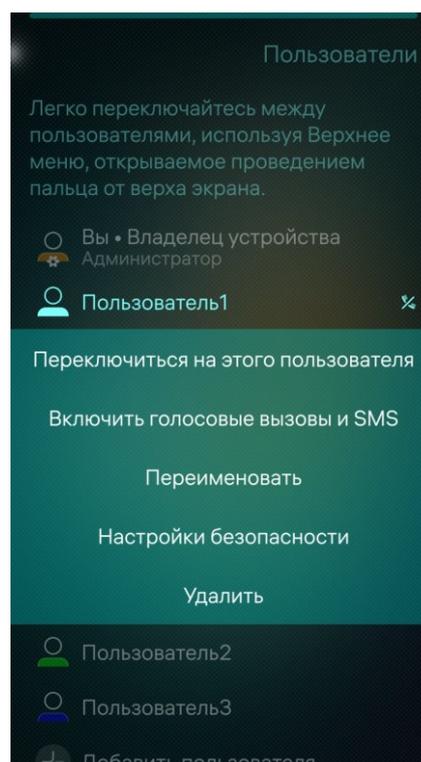


Рисунок 19

#### 1.4.4. Переименование учетной записи

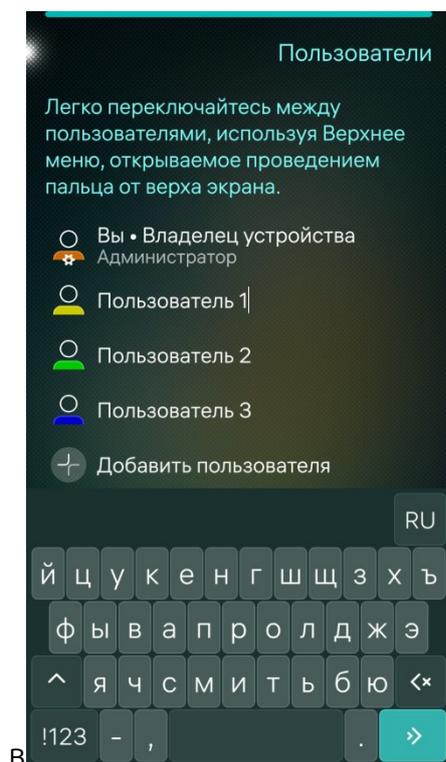


Рисунок 20

Для переименования учетной записи пользователя необходимо выполнить следующие действия:

- коснуться одной из созданных учетных записей пользователей;
- в контекстном меню коснуться пункта «Переименовать» (см. Рисунок 12);
- ввести новое имя учетной записи пользователя (Рисунок 20);
- коснуться значка  для подтверждения действия.

**ПРИМЕЧАНИЕ.** При переименовании учетной записи изменяется только ее имя, логин остается неизменным.

#### 1.4.5. Удаление учетной записи пользователя

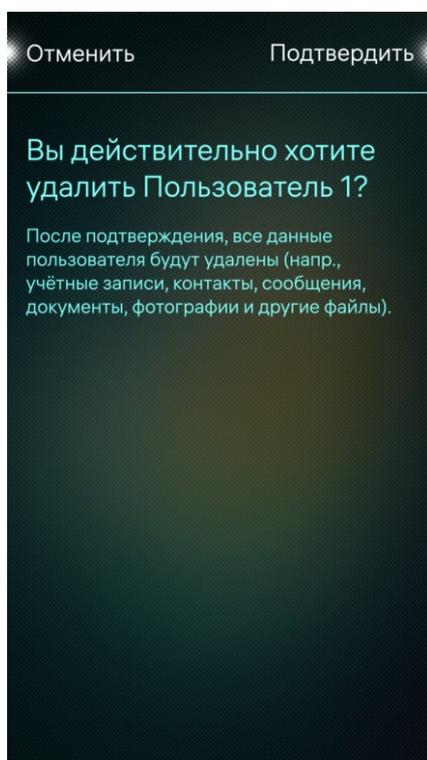


Рисунок 21

Для удаления учетной записи пользователя из списка учетных записей пользователей необходимо выполнить следующие действия:

- коснуться строки с именем учетной записи, которую необходимо удалить;
- в контекстном меню коснуться пункта «Удалить» (см. Рисунок 12);
- на отобразившейся странице коснуться кнопки «Подтвердить» для удаления учетной записи пользователя либо кнопки «Отменить» для отмены операции;
- для удаления подтвердить действие вводом кода безопасности.

В результате будет удалена учетная запись и данные пользователя.

## 1.5. Настройки безопасности

**ПРИМЕЧАНИЕ.** Подробная информация о включении и выключении МУ, а также о задании кода безопасности и первоначальных настройках приведена в документе «Руководство пользователя».

### 1.5.1. Настройка блокировки

**ПРИМЕЧАНИЕ.** Изменения настроек в пункте меню «Блокировка устройства» применяются ко всем учетным записям ролей, созданных на МУ.

Блокировка МУ позволяет обеспечить доступ к данным, хранящимся на МУ, только администратору.

#### ПРИМЕЧАНИЯ:

1. Необходимо запомнить установленный код безопасности, т.к. он потребуется для дальнейшей работы с МУ;
2. В случае утраты и/или раскрытия кода безопасности его необходимо немедленно обновить;
3. По умолчанию автоматическая блокировка МУ отключена.

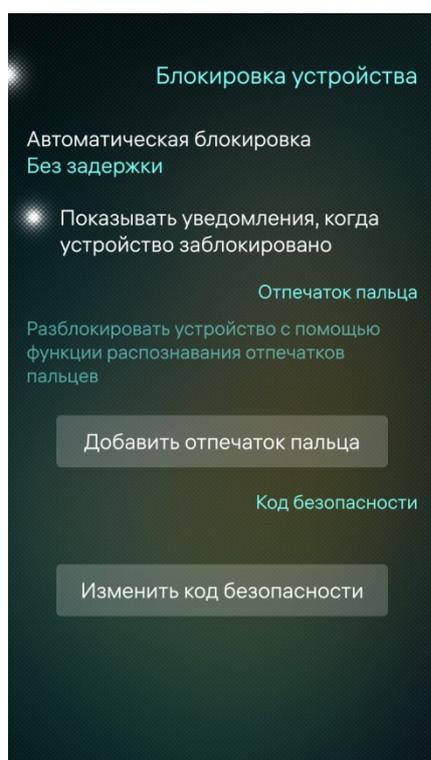


Рисунок 22

Для настройки блокировки МУ необходимо выполнить следующие действия:

- коснуться пункта «Блокировка устройства»  в меню настроек безопасности, в результате чего отобразится страница с настройками блокировки МУ (Рисунок 22);
- коснуться поля «Автоматическая блокировка» и на открывшейся странице выбрать время до автоматической блокировки МУ (Рисунок 23, Рисунок 24), коснувшись соответствующих полей;

**ВНИМАНИЕ!** Варианты значений в поле «Автоматическая блокировка» отличаются в зависимости от варианта исполнения ОС Аврора<sup>3</sup> (Рисунок 23, Рисунок 24).

<sup>3</sup> Описание возможных вариантов исполнения ОС Аврора приведены в таблице (Таблица 5).

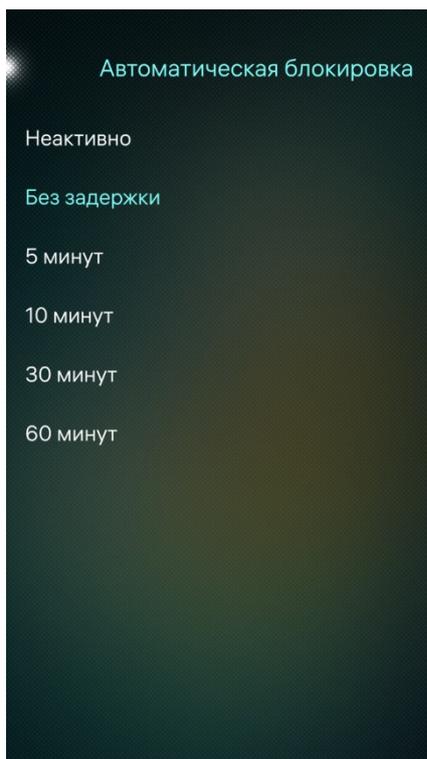


Рисунок 23

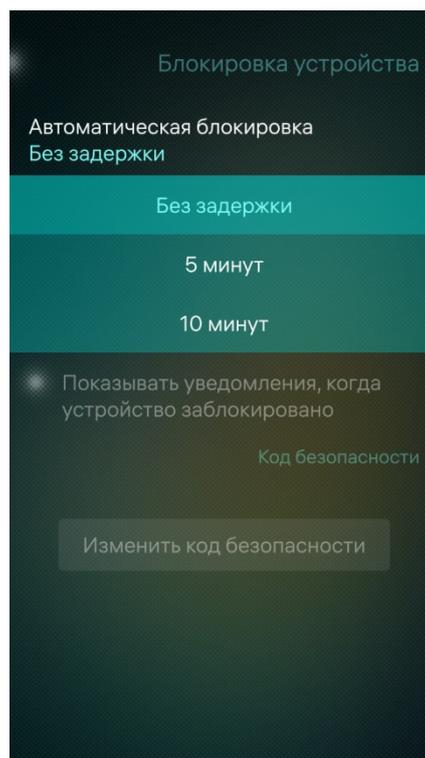


Рисунок 24

**ПРИМЕЧАНИЕ.** Если установленное время блокировки превышает время спящего режима, экран может быть неактивен, при этом МУ не будет заблокировано. Для дальнейшей работы с МУ необходимо нажать кнопку питания и продолжить работу без ввода кода безопасности.

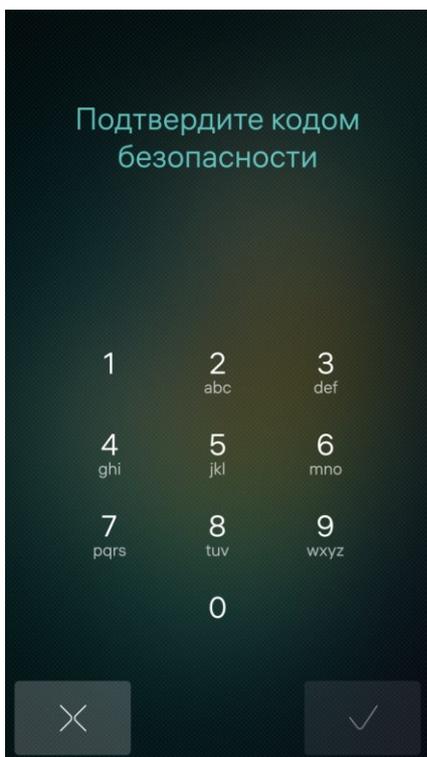


Рисунок 25

**ПРИМЕЧАНИЕ.** При превышении количества попыток ввода неверного кода безопасности МУ автоматически будет заблокировано. Время блокировки является фиксированным и составляет 15 минут.

- подтвердить действие вводом текущего кода безопасности;
- при необходимости изменить код безопасности, коснувшись кнопки с соответствующим названием (см. Рисунок 24), подтвердить действие вводом текущего кода безопасности, затем дважды ввести новый код.

На МУ предусмотрена возможность настроить блокировку с помощью функции распознавания отпечатка пальца.

**ПРИМЕЧАНИЕ.** Наличие указанной функции и расположение датчика отпечатка пальца зависит от конструктивных особенностей МУ. Подробная информация о настройке блокировки с помощью функции распознавания отпечатка пальца приведена в документе «Руководство пользователя».

### 1.5.2. Настройки парольной политики

**ПРИМЕЧАНИЕ.** Изменения настроек парольной политики будут применены ко всем учетным записям, созданным на МУ.

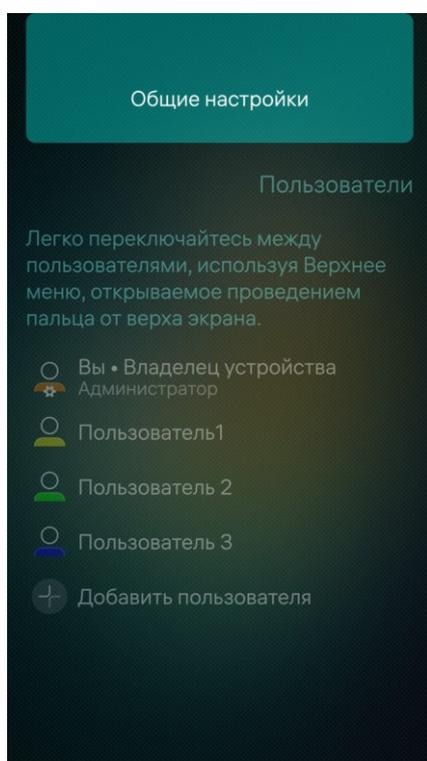


Рисунок 26

Для настройки парольной политики необходимо выполнить следующие действия:

- в меню настроек системы коснуться пункта «Пользователи» , в результате чего отобразится страница «Пользователи» с представленным списком пользователей, созданных на МУ;

- открыть меню действий;
- коснуться пункта «Общие настройки» (Рисунок 26), в результате чего отобразится страница «Общие настройки»;

- коснуться пункта «Настройка политики паролей» и на отобразившейся странице коснуться поля «Настройка политики паролей» (Рисунок 27).

**ВНИМАНИЕ!** Интерфейс страницы «Настройка паролей» может отличаться в зависимости от варианта исполнения ОС Аврора<sup>4</sup> (Рисунок 27, Рисунок 28).

<sup>4</sup> Описание возможных вариантов исполнения ОС Аврора приведены в таблице (Таблица 5).

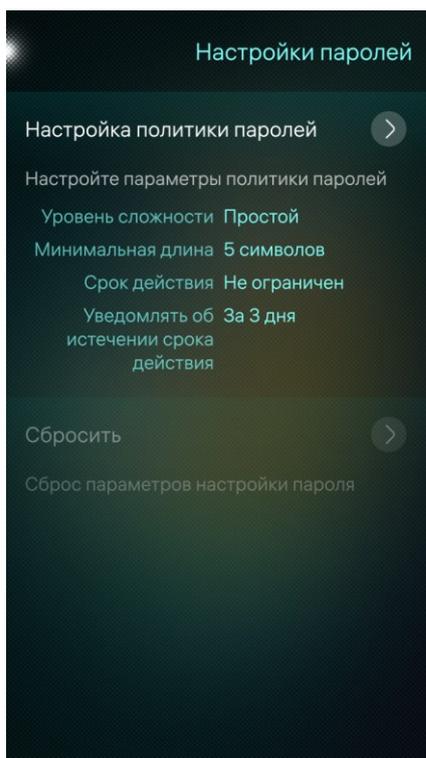


Рисунок 27

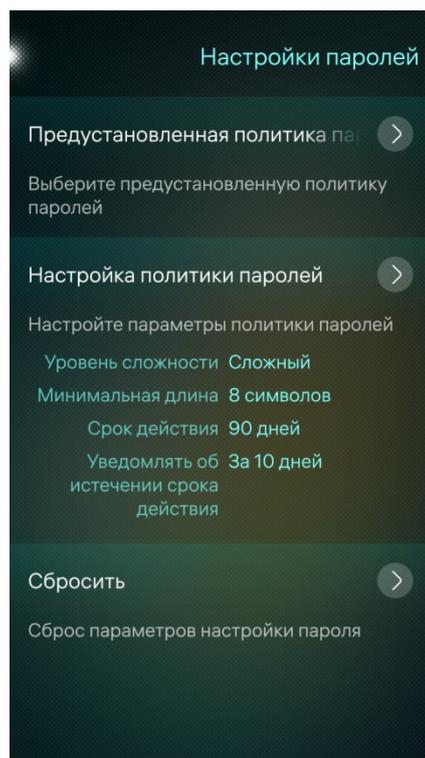


Рисунок 28

Для выбора политики паролей необходимо выполнить следующие действия:

- коснуться поля «Предустановленная политика паролей» (Рисунок 28);
- на открывшейся странице выбрать необходимую политику касанием соответствующего поля (Рисунок 29), в результате чего будет установлена необходимая политика паролей с заданными параметрами.

Для настройки политики паролей на открывшейся странице «Настройки парольной политики» задать необходимые параметры для кода безопасности (Рисунок 30):

- уровень сложности;
- длина;
- количество попыток;
- срок действия;
- уведомление об истечении срока действия.

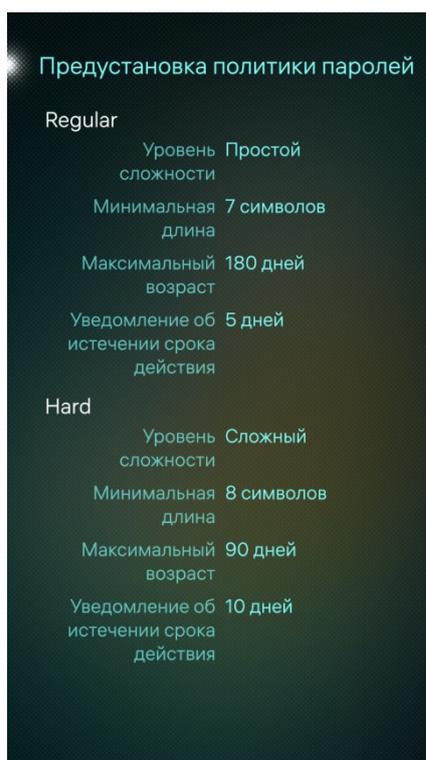


Рисунок 29

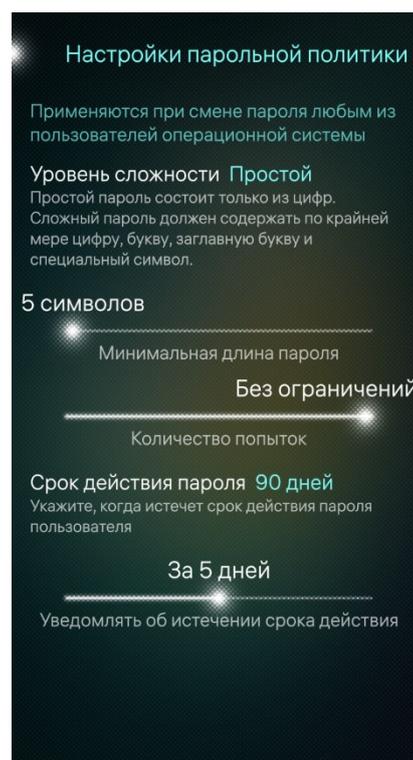


Рисунок 30

Для настройки уровня сложности кода безопасности необходимо выполнить следующие действия (Рисунок 31):

- коснуться поля «Уровень сложности» и в раскрывающемся списке выбрать значение «Простой», состоящий только из цифр, либо «Сложный», который должен содержать как минимум цифру, букву, заглавную букву и специальный символ;
- в случае выбора значения «Сложный» подтвердить действие вводом текущего кода безопасности.

Для настройки длины кода безопасности необходимо выполнить следующие действия (Рисунок 32):

- установить количество символов, перемещая слайдер «Минимальная длина пароля» влево для уменьшения количества входящих в код безопасности символов либо вправо для увеличения количества символов;
- подтвердить действие вводом текущего кода безопасности.

**ПРИМЕЧАНИЕ.** Предусмотрена возможность установить длину кода безопасности от 5 до 12 символов.

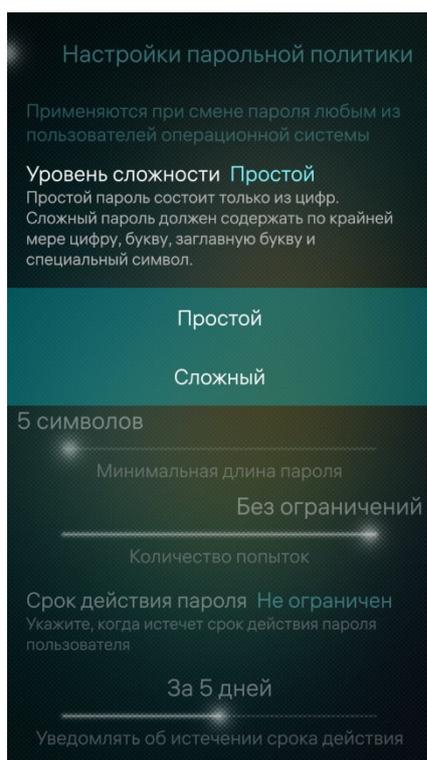


Рисунок 31



Рисунок 32

Для установки количества попыток ввода кода безопасности необходимо переместить слайдер «Количество попыток»:

- влево для уменьшения (минимальное значение: 4 попытки);
- вправо для увеличения (максимальное значение: 10 попыток либо «Без ограничений»).

**ВНИМАНИЕ!** Максимальное значение слайдера «Количество попыток» зависит от варианта исполнения ОС Аврора<sup>5</sup>.

Для задания срока действия кода безопасности необходимо выполнить следующие действия:

- коснуться поля «Срок действия пароля» (см. Рисунок 32) и на отобразившейся странице выбрать одно из значений (Рисунок 33);

**ВНИМАНИЕ!** По требованиям безопасности информационных систем, в которых планируется использование МУ, функционирующего под управлением ОС Аврора, срок действия пароля должен быть установлен в значение «180 дней».

- подтвердить действие вводом текущего кода безопасности.

Для задания времени уведомления об истечении срока действия кода безопасности необходимо выполнить следующие действия (Рисунок 34):

<sup>5</sup> Описание возможных вариантов исполнения ОС Аврора приведены в таблице (Таблица 5).

– установить, за сколько дней пользователь начнет получать уведомления об истечении срока действия кода безопасности, перемещая слайдер «Уведомлять об истечении срока действия» влево для уменьшения количества дней либо вправо для увеличения;

– подтвердить действие вводом текущего кода безопасности.

**ПРИМЕЧАНИЕ.** Предусмотрена возможность установить значение от 0 (Никогда) до 10 дней.



Рисунок 33



Рисунок 34

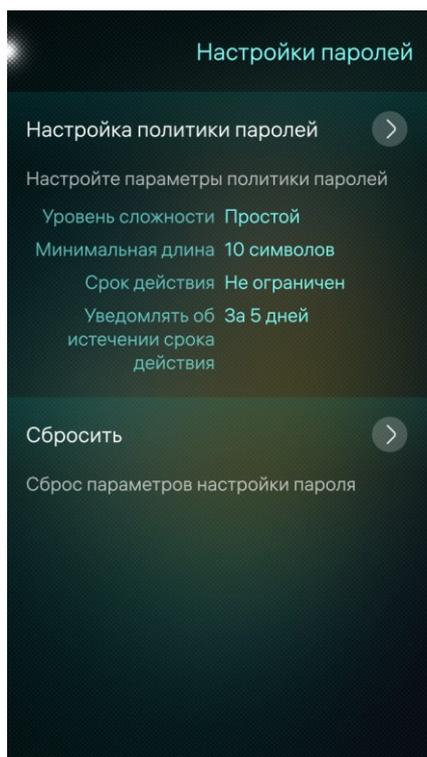


Рисунок 35

Для сброса парольной политики необходимо выполнить следующие действия:

- на странице «Настройка паролей» коснуться поля «Сбросить»;
- подтвердить действие вводом текущего кода безопасности.

### 1.5.3. Настройки безопасности пользователя

**ПРИМЕЧАНИЕ.** Изменения настроек безопасности применяются только к конкретной учетной записи пользователя.

Для настройки безопасности учетной записи пользователя необходимо выполнить следующие действия:

- коснуться одной из созданных на МУ учетных записей пользователя (Рисунок 12);
- в контекстном меню коснуться пункта «Настройки безопасности»;
- на отобразившейся странице «[Имя учетной записи пользователя]» (Рисунок 36) можно выполнить следующие действия:
  - задать для учетной записи пользователя ограничения входа в систему (п. 1.5.3.1);
  - активировать и настроить двухфакторную аутентификацию (2ФА) (п. 1.5.3.2);
  - задать одноразовый пароль (п. 1.5.3.3).

#### 1.5.3.1. Ограничения входа в систему

При необходимости установить для учетной записи пользователя ограничения входа в систему следует коснуться пункта с соответствующим названием и на открывшейся странице настроить следующие параметры (Рисунок 37):

- срок действия учетной записи пользователя;
- дни входа в систему;

- время входа в систему.

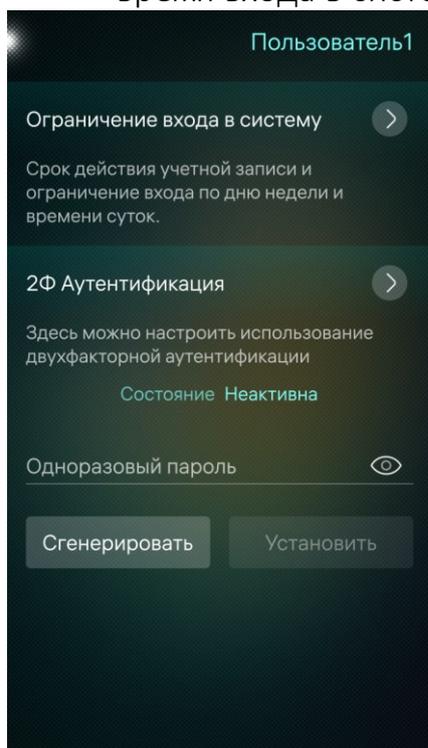


Рисунок 36



Рисунок 37

Для настройки срока действия учетной записи пользователя необходимо выполнить следующие действия:

- коснуться поля «Срок действия учетной записи пользователя» и на отобразившейся странице выбрать дату, после которой пользователь не сможет войти в систему (см. Рисунок 6);

- подтвердить действие вводом кода безопасности.

Для настройки дней, в которые пользователь сможет войти в систему, необходимо выполнить следующие действия:

- коснуться поля «Дни входа в систему» и на отобразившейся странице выбрать дни недели, в течение которых пользователь сможет войти в систему (Рисунок 38);

- подтвердить действие вводом кода безопасности.

Для настройки времени входа в систему необходимо выполнить следующие действия:

- коснуться переключателя «Круглосуточно» для его деактивации, в результате чего отобразятся поля ввода диапазона времени, в течение которого пользователь сможет войти в систему (Рисунок 39);

**ПРИМЕЧАНИЕ.** Для активации переключателя достаточно коснуться поля, в котором он расположен: переключатель начнет светиться ярче, чем в состоянии по умолчанию (неактивном).

– коснуться соответствующих полей для установки интервала времени, в течение которого пользователь сможет войти в систему. Отобразится циферблат, метка во внутреннем круге которого играет роль часовой стрелки, во внешнем — минутной. Для установки необходимого значения следует поочередно коснуться каждой из меток значка и, передвигая ее по или против часовой стрелки, установить в позиции, соответствующей требуемому времени, и коснуться кнопки «Подтвердить» для сохранения установленного времени либо кнопки «Отменить» для отмены операции (см. Рисунок 7);

– подтвердить действие вводом кода безопасности.

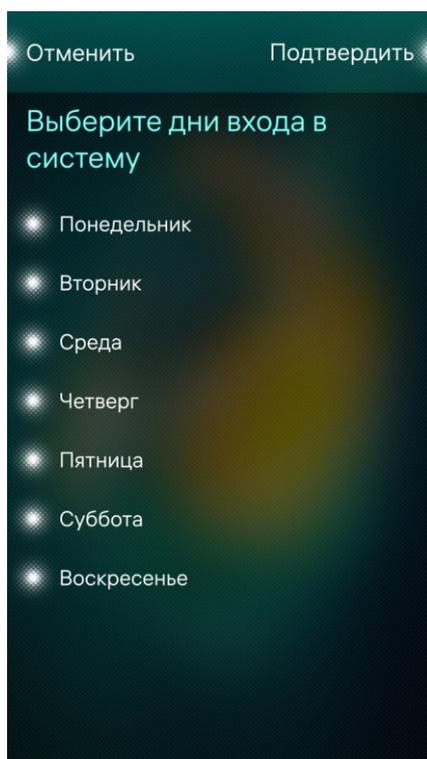


Рисунок 38

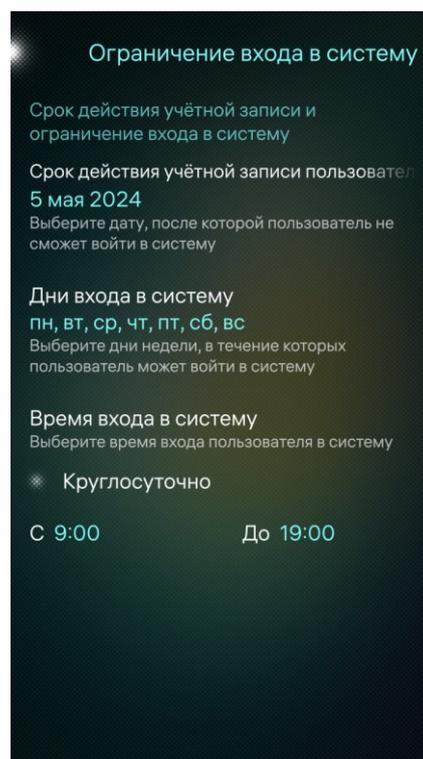


Рисунок 39

### 1.5.3.2. Настройка 2ФА

2ФА – процесс подтверждения подлинности пользователя с помощью использования нескольких различающихся факторов.

Для 2ФА в ОС Аврора применяются:

- в качестве первого фактора: пароль;
- в качестве второго фактора: токен, содержащий уникальную информацию пользователя.

#### ПРИМЕЧАНИЯ:

1. Информация о состоянии 2ФА отображается на странице «[Имя пользователя]» в пункте меню «Двухфакторная аутентификация»;

2. Для настройки и активации 2ФА администратору необходимо использовать USB смарт-карту (токен).

В ОС Аврора для 2ФА поддерживаются следующие токены:

- по предоставлению сертификата открытого ключа, расположенного на программно-аппаратном комплексе аутентификации и хранения информации «Рутокен» версии 4 (ЭЦП PKI) (сертификат ФСТЭК России №3753);
- средства аутентификации и безопасного хранения информации пользователей JaCarta (сертификат ФСТЭК России №3449).

**ВНИМАНИЕ!** Использование для 2ФА токена, отличного от указанных, не предусматривается!

#### 1.5.3.2.1. Правила настройки и использования 2ФА

Необходимо учитывать следующие основные правила настройки и использования 2ФА:

- эксплуатацию токена требуется осуществлять в соответствии с требованиями, указанными в соответствующей документации на него;
- для обеспечения подключения к МУ и последующей настройки токена требуется использовать специализированный USB-OTG переходник, который не входит в комплект поставки МУ;
- политика безопасности ОС Аврора может запрещать применение внешних USB-устройств, соответственно, необходимо дополнительно проверить установленное ограничение действующей в ОС Аврора политики безопасности (подраздел 4.3);
- при работе с токеном потребуется дополнительный пароль для доступа в защищенную область памяти токена, в которую производится назначение и сохранение аутентификационной информации пользователя;
- использование 2ФА доступно для всех учетных записей ролей (п. 1.4.1), созданных в ОС Аврора;
- проверка токена при входе пользователя происходит однократно – только при первичном входе.

#### 1.5.3.2.2. Предварительная подготовка токена

Настройка токена происходит на ЭВМ ОС Linux, на которой предварительно должен быть установлен пакет opensc.

**ПРИМЕЧАНИЕ.** Для настройки 2ФА токен должен иметь формат PKCS#15.

В случае если токен имеет другой формат, то для переинициализации токена в формат PKCS#15 на ЭВМ необходимо выполнить следующие команды:

```
pkcs15-init --erase-card -p rutoken_ecp
pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk ""
pkcs15-init --store-pin --label "User PIN" --auth-id 02 --pin
"12345678" --puk "" --so-pin "87654321" --finalize
```

**ВНИМАНИЕ!** После переинициализации токена все данные с него будут удалены!

### 1.5.3.2.3. Включение и выключение 2ФА

**ПРИМЕЧАНИЕ.** Включение 2ФА возможно только для конкретной учетной записи пользователя.

Для включения 2ФА необходимо выполнить следующие действия:

- коснуться одной из созданных учетных записей пользователя (см. Рисунок 5);
- в контекстном меню коснуться пункта «Настройки безопасности»;
- отобразится страница «[Имя учетной записи пользователя]» (см. Рисунок 30), на которой необходимо коснуться пункта «2Ф Аутентификация»;
- на отобразившейся странице коснуться кнопки «Начать настройку» для настройки 2ФА (Рисунок 40);
- подключить токен (смарт-карту). После успешного подключения на экране отобразится соответствующее сообщение (Рисунок 41);

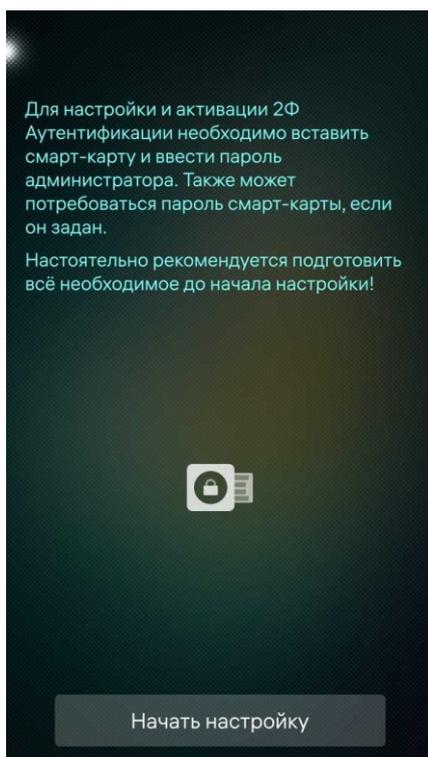


Рисунок 40

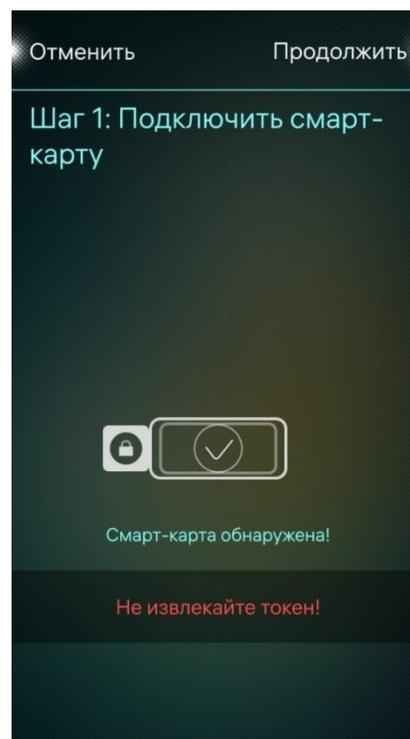


Рисунок 41

- на отобразившейся странице «Инициализация смарт-карты» коснуться кнопки «Ввести пароль» для ввода пароля от токена либо коснуться кнопки «Попробуйте другую смарт-карту» для подключения другого токена (Рисунок 42)
- в поле ввода ввести пароль от токена и коснуться значка  (Рисунок 43);

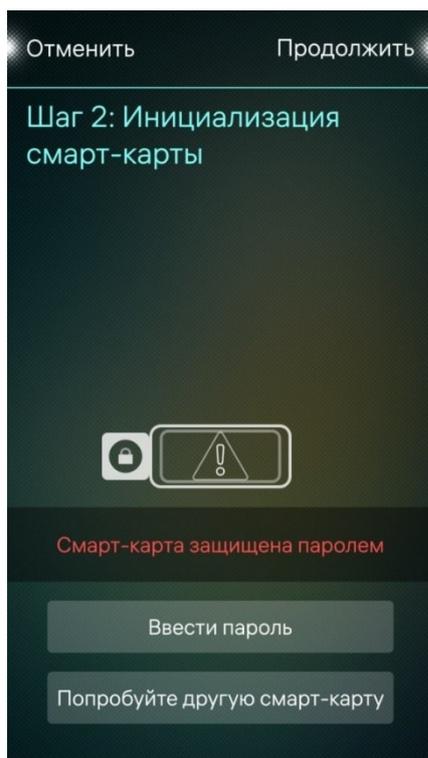


Рисунок 42

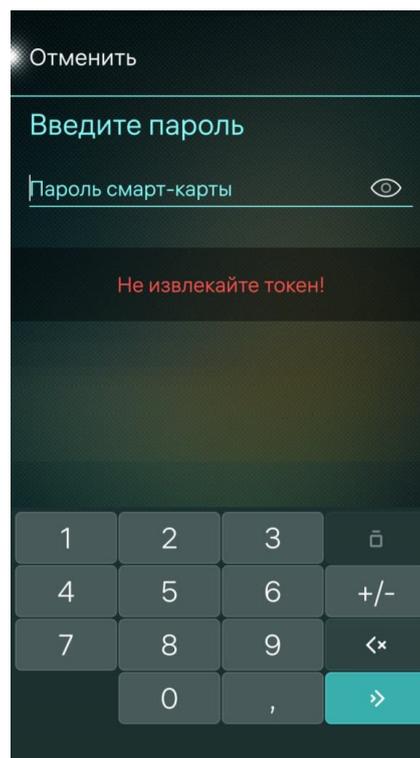


Рисунок 43

– после успешной инициализации смарт-карты на экране отобразится соответствующее сообщение;

– коснуться кнопки «Подтвердить» для подтверждения либо кнопки «Отменить» для отмены операции (Рисунок 44);

– на отобразившейся странице коснуться кнопки «Завершить» для завершения настройки 2ФА (Рисунок 45), после чего значение поля «Состояние» изменится на «Активна» (см. Рисунок 46).

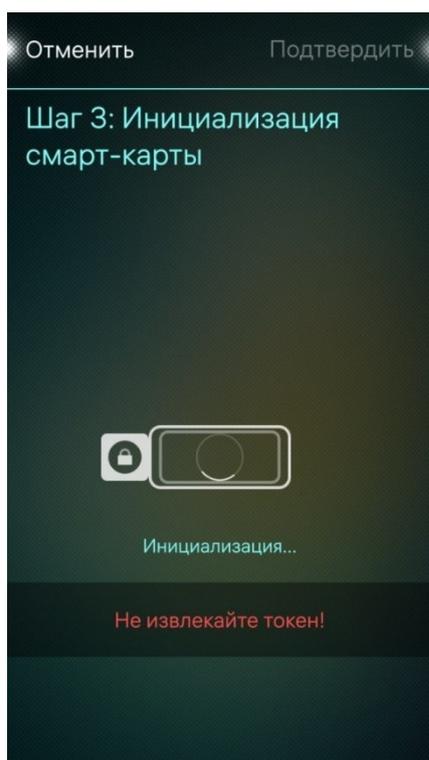


Рисунок 44

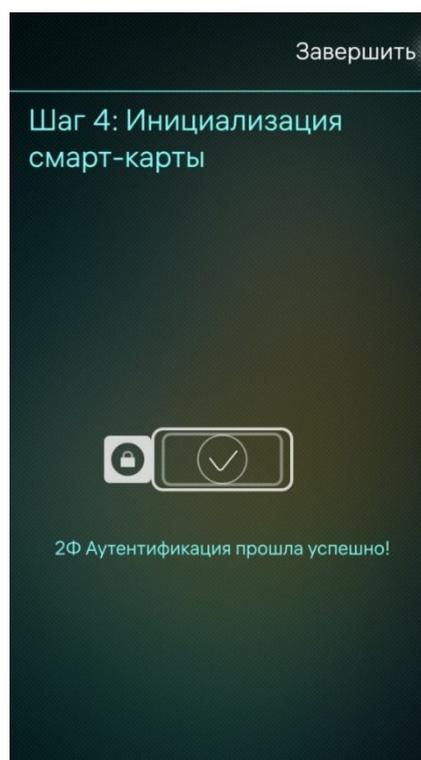


Рисунок 45

Для выключения 2ФА необходимо выполнить следующие действия:

- на странице «[Имя учетной записи пользователя]» (Рисунок 46) коснуться пункта «2Ф Аутентификация»;
- на отобразившейся странице коснуться кнопки «Отключить» для отключения токена (Рисунок 47), после чего значение поля «Состояние» изменится на «Неактивно» (см. Рисунок 36).

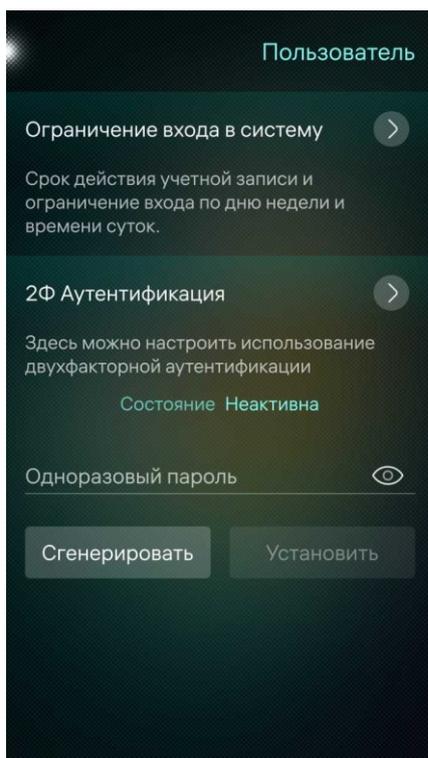


Рисунок 46

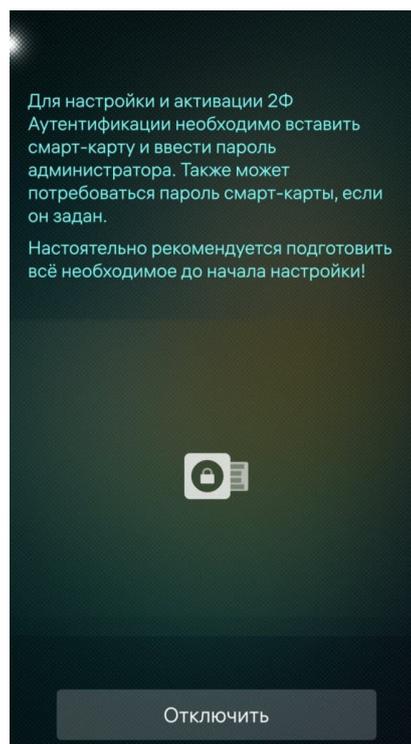


Рисунок 47

### 1.5.3.3. Задание одноразового пароля учетной записи пользователя

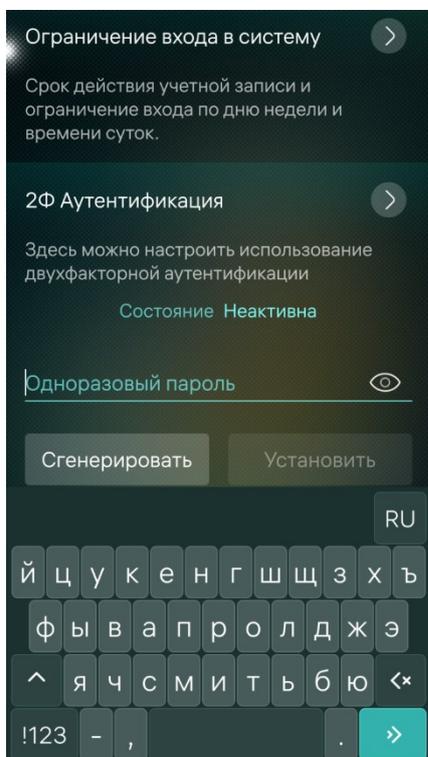


Рисунок 48

**ПРИМЕЧАНИЕ.** Одноразовый пароль требуется для выполнения входа в систему при первом включении учетной записи пользователя.

Для задания одноразового пароля учетной записи пользователя необходимо выполнить следующие действия:

- коснуться кнопки «Сгенерировать» либо установить курсор в поле «Одноразовый пароль», после чего задать пароль;
- при необходимости коснуться значка  для отображения пароля;
- коснуться кнопки «Установить» для подтверждения действия (Рисунок 48));
- подтвердить действие вводом кода безопасности.

**ПРИМЕЧАНИЕ.** Подробная информация о входе в учетную запись пользователя с помощью одноразового пароля приведена в документе «Руководство пользователя».

## 1.6. Настройка МУ

Администратору МУ доступны следующие возможности:

- настройка USB-подключения (п. 1.6.1);
- настройка PIN-кода для SIM-карты (п. 1.6.2);
- настройка МП (1.6.3).

### 1.6.1. Настройка USB-подключения

Для настройки USB-подключения необходимо выполнить следующие действия:

- коснуться пункта «USB»  в меню настроек сети;
- в открывшемся окне настроек USB-подключения (Рисунок 49) коснуться поля «Режим USB по умолчанию» и выбрать необходимое значение из раскрывающегося списка.

#### ПРИМЕЧАНИЯ:

1. В случае выбора пункта «Всегда спрашивать» при подключении МУ к ЭВМ с помощью USB-кабеля на МУ отобразится окно с выбором режима USB-подключения (Рисунок 50);

2. Значение «Режим разработчика» отображается только при активации соответствующих переключателей в разделе «Средства разработчика» системных настроек (подраздел 3.1).

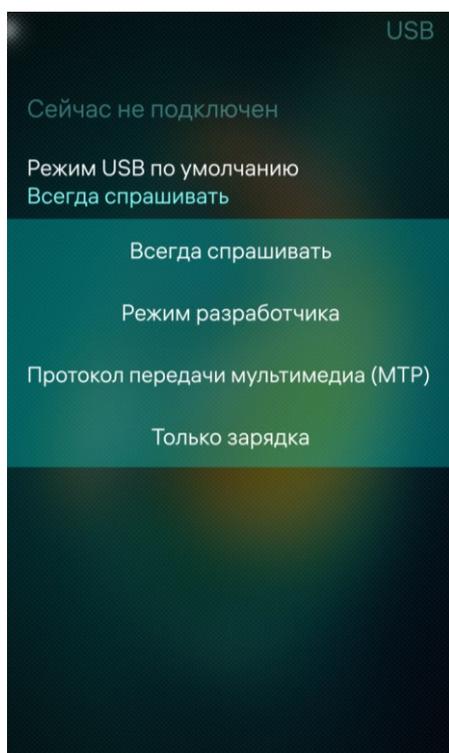


Рисунок 49

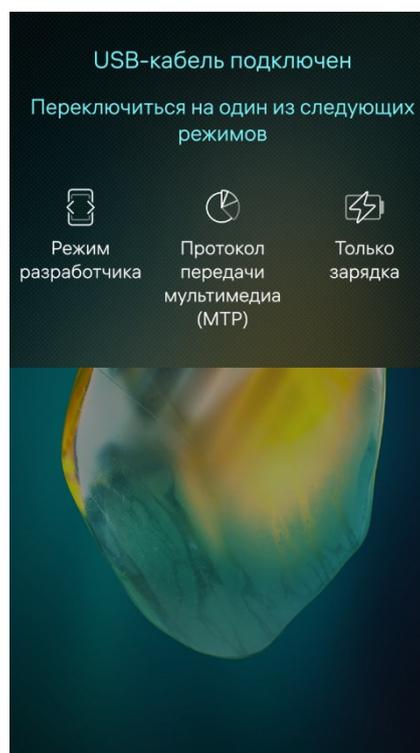


Рисунок 50

### 1.6.2. Настройка PIN-кода для SIM-карты

Защита установленной на МУ SIM-карты обеспечивается с помощью PIN-кода, который можно активировать/деактивировать отдельно для каждой из SIM-карт.

**ПРИМЕЧАНИЕ.** В зависимости от конструктивных особенностей МУ допускается установка до двух SIM-карт.

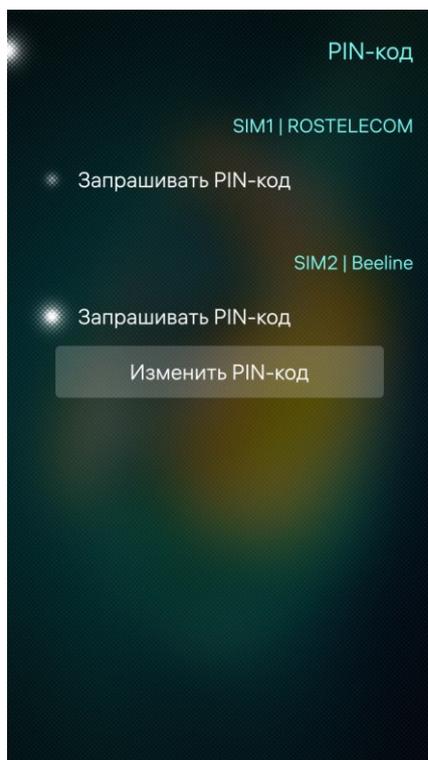


Рисунок 51

Для настройки PIN-кода необходимо выполнить следующие действия (Рисунок 51):

- коснуться пункта «PIN-код»  в меню настроек безопасности;
- коснуться переключателя «Запрашивать PIN-код» в разделах тех SIM-карт, которые необходимо защитить вводом PIN-кода/снять защиту.

После активации PIN-кода он будет запрашиваться при каждом включении МУ (Рисунок 52). В случае трехкратного ввода неверного PIN-кода SIM-карта будет заблокирована и для ее разблокировки потребуются PUK-код, для ввода которого предоставляется 10 попыток (Рисунок 53).

**ПРИМЕЧАНИЕ.** PUK-код предоставляется оператором сотовой связи.

После ввода верного PUK-кода отобразится страница для изменения PIN-кода (Рисунок 51), на которой необходимо выполнить следующие действия:

- коснуться кнопки «Изменить PIN-код»;
- внести соответствующие изменения в разделе SIM-карты, которую требуется защитить вводом PIN-кода.

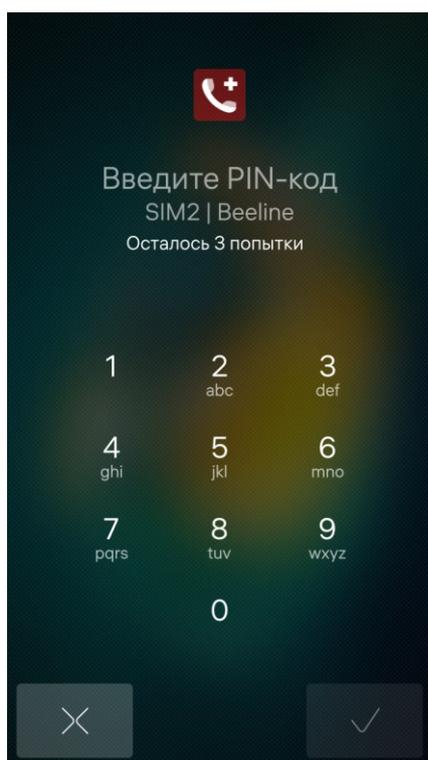


Рисунок 52



Рисунок 53

### 1.6.3. Настройки МП

**ПРИМЕЧАНИЕ.** Администратор имеет доступ к настройкам МП, описание которых приведено в документе «Руководстве пользователя», а также далее.

Для некоторых МП предусмотрена возможность дополнительной настройки. Для настройки МП необходимо выполнить следующие действия:

- открыть меню настроек касанием значка  на Экране приложений;
- коснуться раздела «Приложения» для перехода к одноименной странице;
- на странице настраиваемых МП коснуться значка соответствующего МП и задать требуемые настройки:

#### **МП «Телефон»:**

- сбросить счетчики звонков (Рисунок 54);
- при необходимости включить опцию «Запись разговора» (Рисунок 55);
- просмотреть информацию о записанных вызовах (Рисунок 56).

Для выполнения действий над записанными вызовами следует коснуться поля с количеством записанных вызовов и на отобразившейся странице в контекстном меню вызова коснуться пункта с необходимым действием.

#### **МП «Сообщения» (Рисунок 57):**

- просмотреть адрес SMS-центра;
- при необходимости включить опцию «Отчеты о доставке».



Рисунок 54

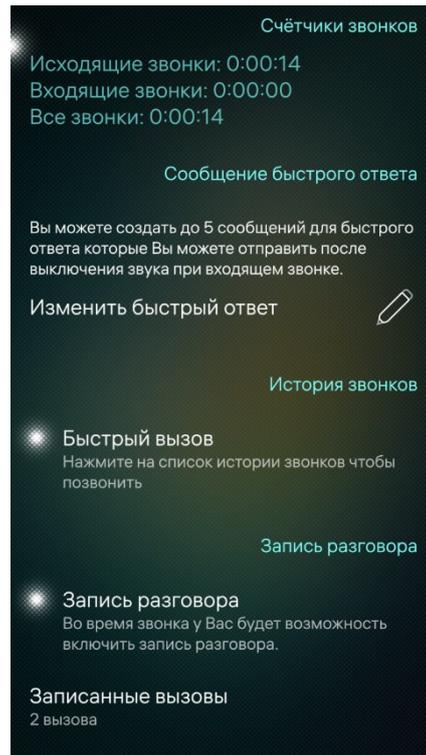


Рисунок 55

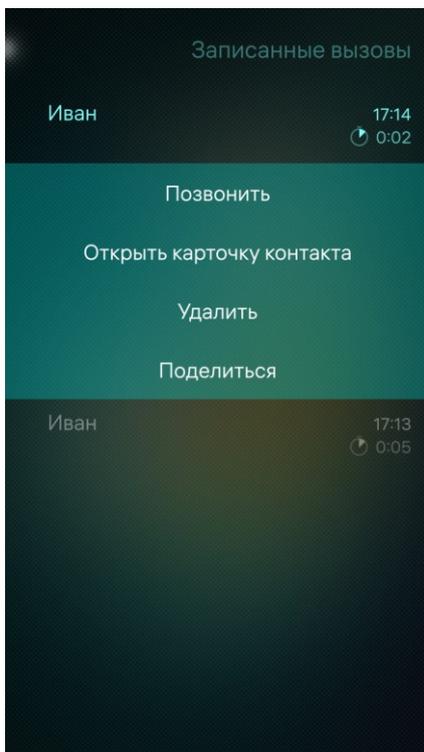


Рисунок 56

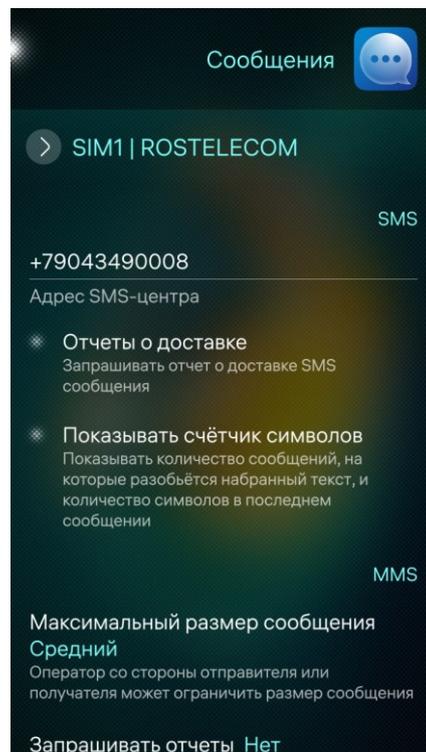


Рисунок 57

## 2. ВЫПОЛНЕНИЕ ПРОГРАММЫ

### 2.1. Настройка обновлений ОС Аврора

Обновление ОС Аврора может осуществляться администратором либо локально вручную, либо удаленно с использованием Прикладного программного обеспечения «Аврора Центр» (ППО).

**ПРИМЕЧАНИЕ.** Для получения информации по обновлению ОС Аврора посредством ППО следует обратиться к соответствующей документации на ППО, расположенной на ресурсе: <https://auroraos.ru/documentation/>.

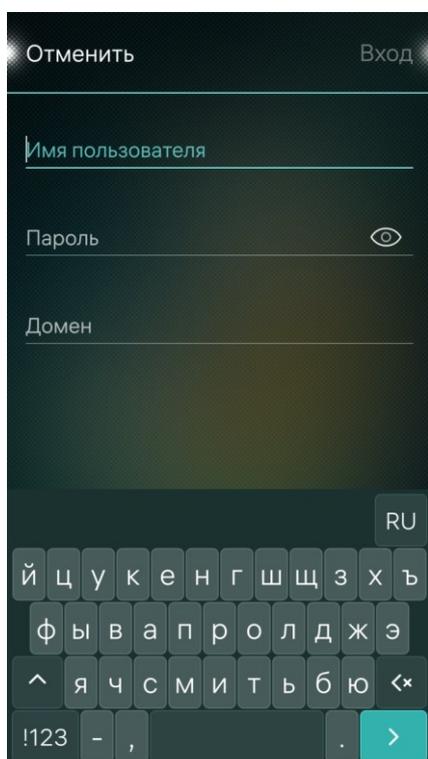


Рисунок 58

Для настройки обновлений ОС необходимо выполнить следующие действия:

- в меню системных настроек коснуться пункта «Обновления Аврора ОС» , в результате чего отобразится страница с настройками обновления;
- коснуться переключателя «Включить защищенные обновления» (см. Рисунок 59);

**ВНИМАНИЕ!** Для получения имени пользователя и пароля необходимо обратиться на [dev-support@omp.ru](mailto:dev-support@omp.ru).

- на открывшейся странице заполнить необходимые поля (Рисунок 58) для регистрации доступа к репозиториям;

- коснуться кнопки «Вход» для выполнения входа либо кнопки «Отменить» для отмены операции.

Ранее установленную версию ОС Аврора можно обновить до текущей локально через графический интерфейс, выполнив следующие действия:

- на странице с настройками обновления коснуться значка  для проверки доступных обновлений, в результате чего отобразится сообщение: «Нет доступных обновлений», а также дата и время последней проверки (Рисунок 59) либо доступное обновление (Рисунок 60);

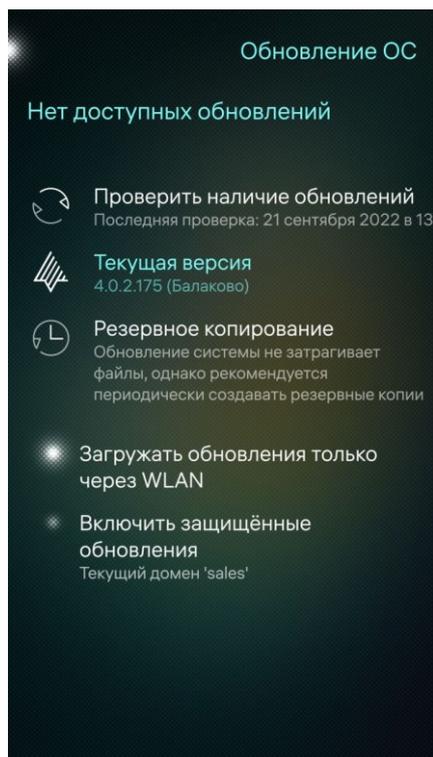


Рисунок 59

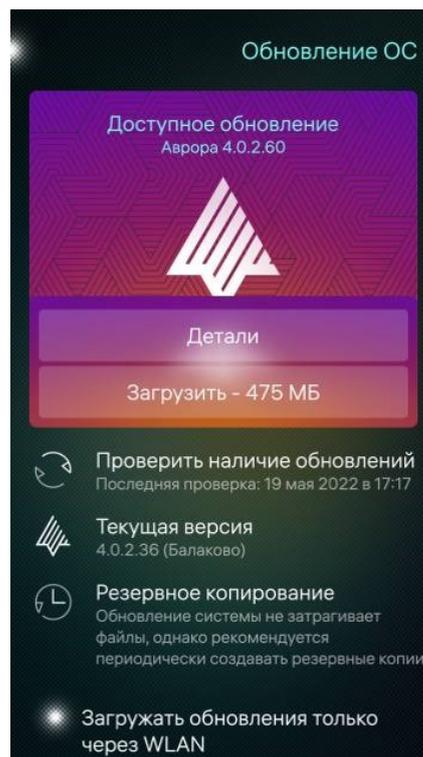


Рисунок 60

– при наличии доступного обновления коснуться кнопки «Загрузить – [Размер обновления]» для его загрузки. В случае необходимости загрузку обновления можно отменить касанием кнопки «Отменить загрузку» (Рисунок 61);

– коснуться кнопки «Детали» и на открывшейся странице ознакомится с подробной информацией об обновлении (Рисунок 62).

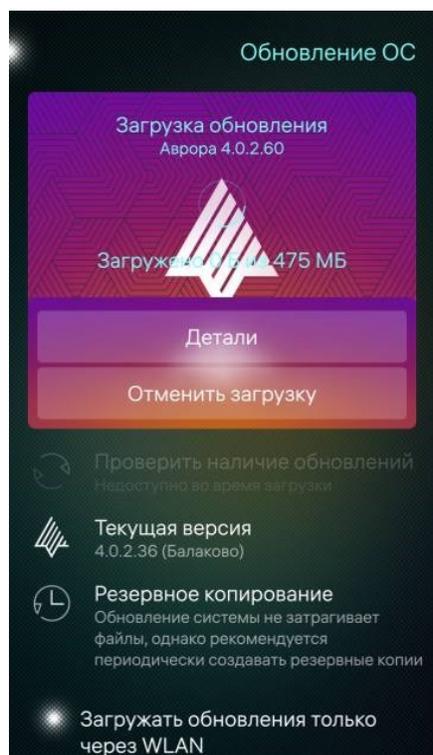


Рисунок 61

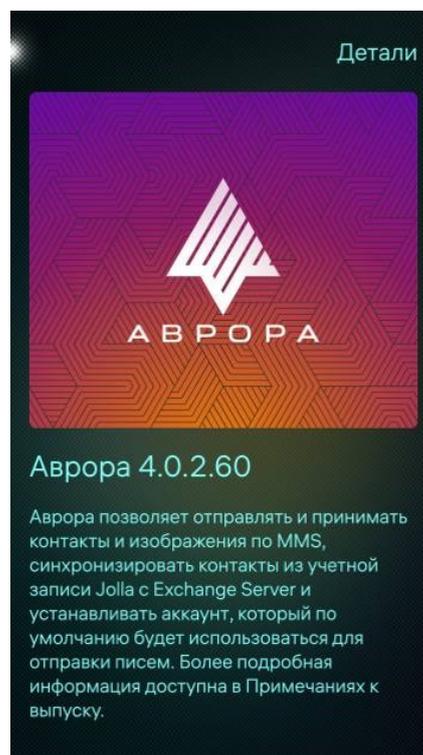


Рисунок 62

– после успешной загрузки обновления коснуться кнопки «Установить обновление» (Рисунок 63);

– на открывшейся странице коснуться кнопки «Установить» (Рисунок 64), после чего МУ автоматически будет перезагружено, либо кнопки «Отменить» для отмены операций.

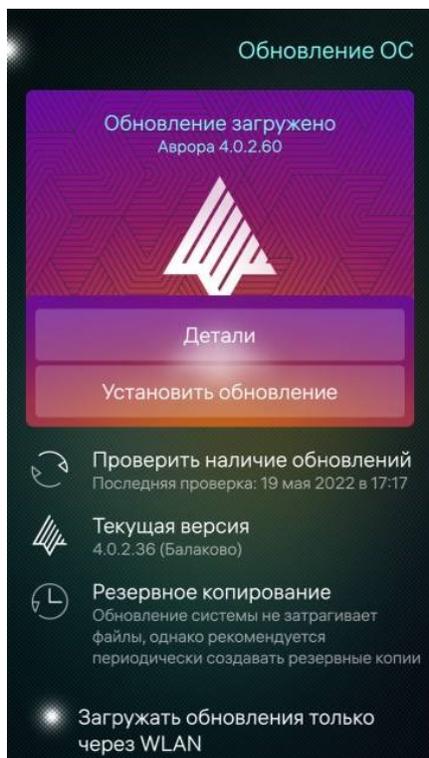


Рисунок 63

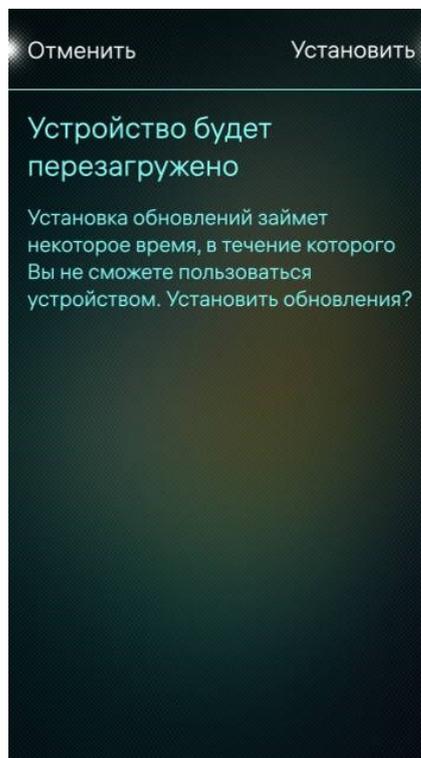


Рисунок 64

На странице «Обновление ОС» администратору также доступны следующие действия (см. Рисунок 59):

- просмотреть информацию о текущей версии ОС ;
- выполнить резервное копирование перед обновлением ОС, коснувшись значка ;

**ПРИМЕЧАНИЕ.** Подробная информация о создании резервной копии приведена в документе «Руководство пользователя».

- активировать либо деактивировать переключатель «Загружать обновления только через WLAN».

## 2.2. Сброс настроек МУ

**ПРИМЕЧАНИЕ.** Сброс настроек МУ – это процесс удаления всех данных, после которого МУ возвращается к заводскому состоянию, т.е. к версии ОС, установленной производителем МУ.

Для сброса настроек МУ до заводского состояния необходимо выполнить следующие действия:

- открыть меню настроек системы касанием значка  на Экране приложений;
- в подразделе «Информация» коснуться пункта «Сбросить устройство» ;
- коснуться кнопки «Очистить устройство» (Рисунок 65);
- коснуться кнопки «Подтвердить» для подтверждения сброса настроек МУ либо кнопки «Отменить» для отмены операции (Рисунок 66);
- при необходимости коснуться переключателя «Автоматически перезагрузить устройство после сброса» для последующей перезагрузки МУ;
- при необходимости коснуться переключателя «Стереть все данные» для удаления данных.

**ПРИМЕЧАНИЕ.** После перезагрузки МУ произойдет сброс настроек до заводского состояния с последующим запуском мастера первоначальной настройки, подробное описание работы с которым приведено в документе «Руководство пользователя».

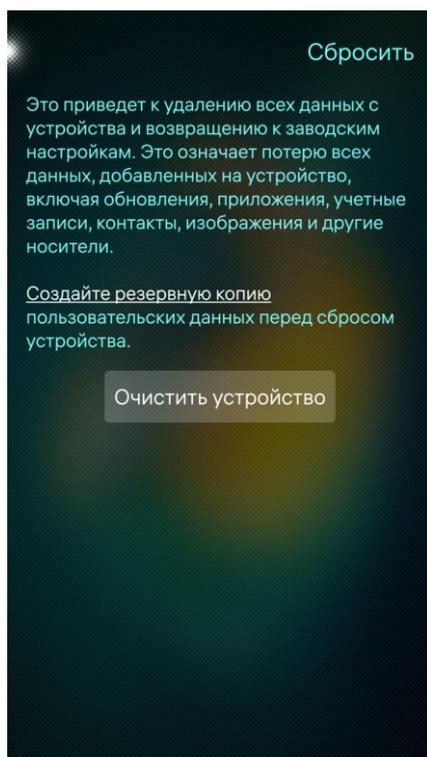


Рисунок 65

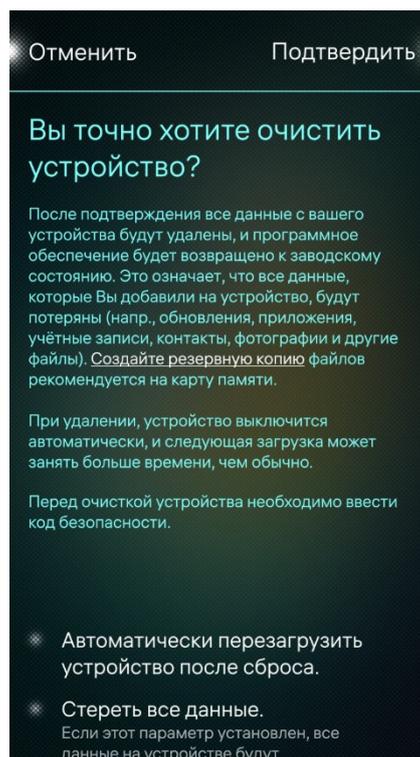


Рисунок 66

### 2.3. МП «Terminal»

**ПРИМЕЧАНИЕ.** Администратору необходимо использовать МП «Terminal» только для осуществления действий по тонкой настройке МУ в соответствии с настоящим документом. Использование МП «Terminal» для других целей запрещается.

МП «Terminal» является инструментом для выполнения команд, предоставляющим доступ к командной строке, где выводится поток данных, а также диагностические и отладочные сообщения в текстовом виде.

С помощью данного инструмента можно производить сервисные действия и более тонкую настройку МУ (в т.ч. с использованием прав суперпользователя).

По умолчанию МП «Terminal» не отображается на Экране приложений.

Для доступа к МП «Terminal» необходимо выполнить следующие действия:

- коснуться пункта «Администрирование»  в меню системных настроек;
- на открывшейся странице коснуться переключателя «Включить терминал» (Рисунок 67) для отображения МП на Экране приложений;
- коснуться поля ввода и ввести желаемый пароль либо кнопки «Сгенерировать» для получения пароля, сгенерированного случайным образом, который в дальнейшем будет использоваться для получения прав суперпользователя;

**ПРИМЕЧАНИЕ.** Необходимо запомнить заданный пароль.

– коснуться кнопки «Сохранить» (Рисунок 68), в результате чего МП «Terminal» отобразится на Экране приложений.

**ПРИМЕЧАНИЕ.** МП «Terminal» доступно только администратору.

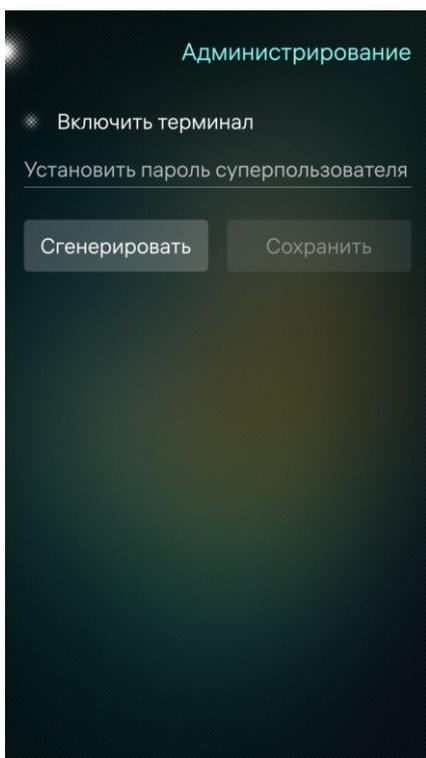


Рисунок 67

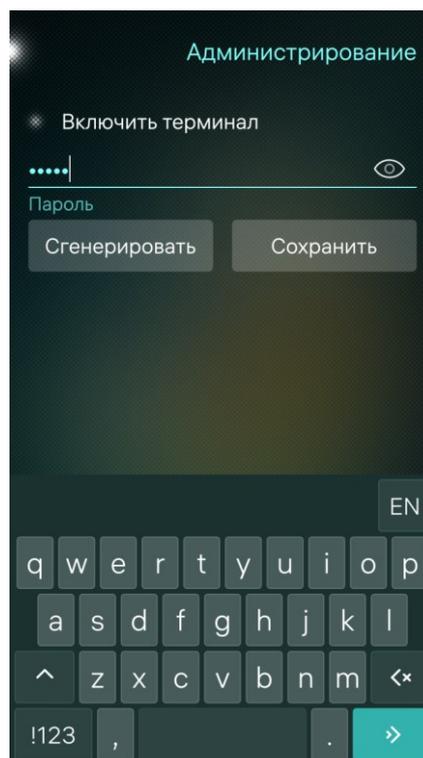


Рисунок 68

### 2.3.1. Интерфейс МП «Terminal»

Для работы с МП «Terminal» его необходимо открыть, проведя по экрану снизу вверх и на Экране приложений коснувшись значка .

В интерфейсе МП «Terminal» доступны следующие возможности:

- коснуться значка  для отображения меню с настройками интерфейса, в котором можно выполнить следующие действия (Рисунок 69):
  - коснуться кнопок «Копировать» или «Вставить» для копирования или вставки фрагмента текста;
  - коснуться кнопки «Обнаруженные URL-ссылки» для поиска URL-ссылок;

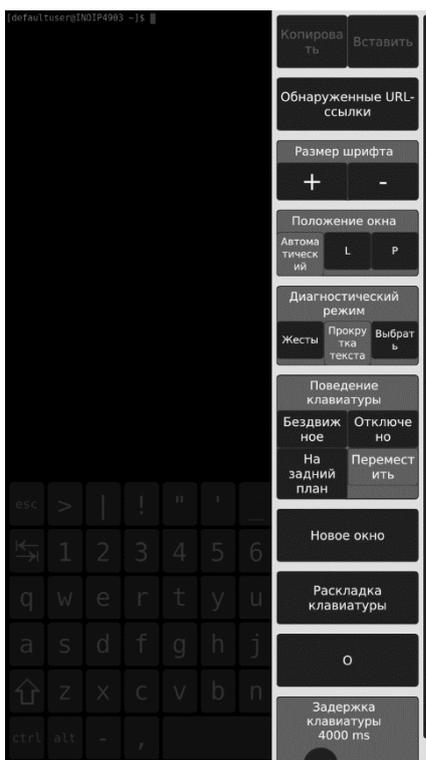


Рисунок 69

- коснуться кнопки «Новое окно» для создания нового окна;
- коснуться кнопки «Раскладка клавиатуры» для выбора языка интерфейса;
- коснуться кнопки «О приложении» для просмотра информации о МП «Terminal»;
- коснуться поля «Размер шрифта» для увеличения или уменьшения размера шрифта;
- коснуться поля «Положение окна» для выбора ориентации окна;
- коснуться поля «Проведение пальцем» для выбора действия при касании экрана;
- коснуться поля «Поведение клавиатуры» для выбора способа отображения клавиатуры;
- коснуться поля «Задержка клавиатуры» для установки времени задержки клавиатуры.

### 2.3.2. Получение прав суперпользователя

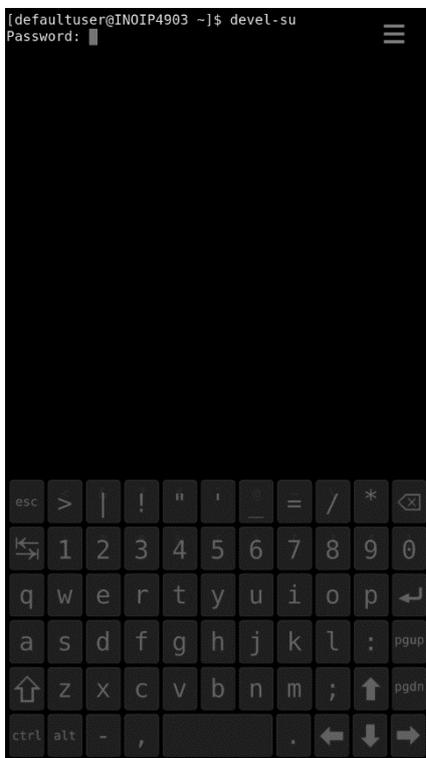


Рисунок 70

Права суперпользователя предоставляют администратору возможность работать в привилегированном режиме и выполнять любые операции в ОС Аврора.

Для получения прав суперпользователя необходимо открыть МП «Terminal» и выполнить следующие действия:

- провести по экрану снизу вверх и на Экране приложений коснуться значка .
- в МП выполнить команду: `devel-su`;
- указать заданный ранее пароль, в результате чего будет выполнен переход в режим суперпользователя.

## 2.4. Управление сторонним ПО

### 2.4.1. Установка стороннего ПО

Администратор имеет возможность устанавливать на МУ сторонние программы, не являющиеся встроенными в ОС Аврора. Сторонние разработчики могут использовать официальный набор инструментов разработки ПО для ОС Аврора, подробная информация о котором приведена на ресурсе: <https://community.omprussia.ru>

Установка и управление сторонним ПО может осуществляться администратором следующими способами:

- локально:
  - через графический интерфейс МП «Файлы» (пп. 2.4.1.1);
  - в МП «Terminal» (пп. 2.4.1.2).
- удаленно:
  - принудительная установка МП через политики;
  - установка МП с помощью ППО.

**ПРИМЕЧАНИЕ.** Подробная информация по использованию ППО приведена в соответствующей документации, расположенной на ресурсе: <https://auroraos.ru/documentation/>.

#### 2.4.1.1. Установка ПО с помощью графического интерфейса МП «Файлы»

Для установки стороннего ПО локально через графический интерфейс с использованием МП «Файлы» необходимо выполнить следующие действия:

- открыть МП «Файлы», коснувшись значка  на Экране приложений;
- коснуться установочного файла МП;
- в диалоговом окне коснуться кнопки «Установить» (Рисунок 71).

После успешной установки на экране МУ отобразится уведомление «Установка успешна» (Рисунок 72), а значок установленного МП будет отображаться на Экране приложений.

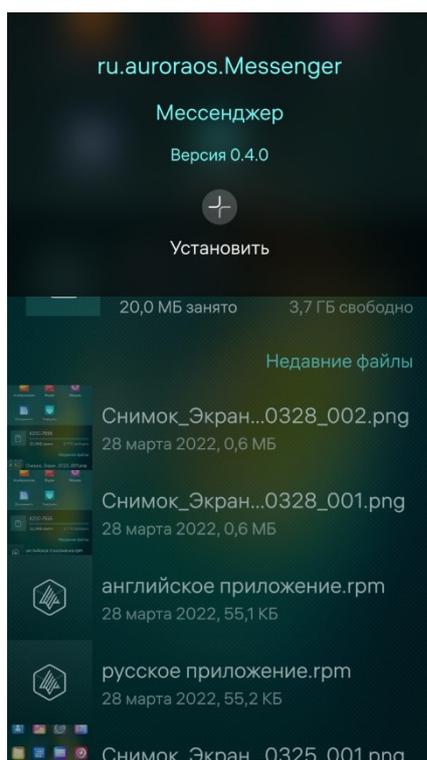


Рисунок 71



Рисунок 72

#### 2.4.1.2. Установка ПО с помощью МП «Terminal»

Для управления МП локально с использованием интерфейса необходимо получить права суперпользователя (п. 2.3.2).

Управление МП осуществляется в МП «Terminal» с помощью менеджера RPM-пакетов посредством выполнения следующих команд:

– для установки скачанного RPM-пакета:

```
#rpm -ihv имя_пакета
```

– для удаления RPM-пакета:

```
#rpm -e имя_пакета
```

– для просмотра перечня установленных RPM-пакетов:

```
#rpm -qa
```

Подробнее с возможностями менеджера RPM-пакетов можно ознакомиться, выполнив команду:

```
#rpm -help
```

**ПРИМЕЧАНИЕ.** Для получения информации о возникающих ошибках и нестандартных ситуациях в процессе управления МП необходимо настроить МП «Журнал» и ознакомиться с представленной в нем информацией. Подробное описание работы МП приведено в документе «Руководство пользователя».

## 2.4.2. Подпись и проверка стороннего ПО

Администратор имеет возможность устанавливать на МУ сторонние программы, не являющиеся встроенными в ОС Аврора. Сторонние разработчики могут использовать официальный набор инструментов разработки ПО для ОС Аврора, подробная информация о котором приведена на ресурсе: <https://community.omprussia.ru>

Для функционирования дополнительных сторонних программ и МП, не являющихся встроенными в ОС Аврора, администратору МУ необходимо выполнить следующие действия:

- добавление корневого сертификата УЦ в доверенные (пп. 2.4.2.22.4.2.1);
- проверка сертификатов (пп. 2.4.2.3);
- подпись МП (пп. 2.4.2.4);
- проверка подписи МП (пп. 2.4.2.5);
- проверка подписи RPM-пакета (пп. 2.4.2.6);
- запуск МП (2.4.2.7).

### 2.4.2.1. Общая информация

Для подписи МП требуется две ключевые подписанные пары и два сертификата (Таблица 1).

Таблица 1

Назначение	Алгоритм	Имя файла закрытого ключа по умолчанию	Имя файла запроса на сертификат по умолчанию	Имя файла сертификата по умолчанию
Подпись бинарных файлов и библиотек внутри RPM-пакета	RSA 2048	binaries-key.pem	binaries-csr.pem	binaries-cert.pem
Подпись RPM-пакетов	ГОСТ Р 34.10-2012 (256 бит)	packages-key.pem	packages-csr.pem	packages-cert.pem

**ПРИМЕЧАНИЕ.** Генерацию ключевых пар и запросы на сертификаты необходимо запускать внутри build-engine, подробная информация о котором приведена на ресурсе: <https://community.omprussia.ru/>.

Пример команды для генерации ключевых пар и запросов на сертификаты:

```
customer-gen-csrs \ --common-name "developer company name" \ --binaries-key binaries-key.pem \ --packages-key packages-key.pem
```

В процессе выполнения команды будут запрошены пароли для шифрования файлов с закрытыми ключами и в рабочей директории скрипта будут созданы файлы запросов `binaries-csr.pem` и `packages-csr.pem`.

Файлы запросов (не файлы ключей) необходимо передать представителю предприятия-разработчика, а взамен получить подписанные файлы сертификатов.

**ПРИМЕЧАНИЕ.** При проведении финального тестирования созданных МП потребуется сертификат сторонней организации на подпись RPM-пакета.

Сертификат сторонней организации необходимо дополнительно запросить у представителя предприятия-разработчика. Создавать дополнительные ключи и запросы на сертификат не требуется. В дальнейшем именем по умолчанию для файла сертификата сторонней организации будет считаться `packages-client-cert.pem`.

#### 2.4.2.2. Добавление корневого сертификата УЦ

Для добавления корневого сертификата УЦ в доверенные необходимо выполнить следующие действия:

- подключить МУ к ЭВМ с помощью USB-кабеля и, выбрав режим «Протокол передачи данных (МТР)», перенести на МУ сертификат УЦ;
- открыть МП «Terminal» и выполнить следующие команды:

```
devel-su
cp <путь к файлу> /etc/pki/ca-trust/source/anchors/
update-ca-trust
```

Загрузить корневой сертификат УЦ на МУ также возможно из сети Интернет, выполнив в МП «Terminal» следующие команды:

```
devel-su
curl -o /etc/pki/ca-trust/source/anchors/root_ca.crt "https://url_сертификата/root_ca.crt"
update-ca-trust
```

#### 2.4.2.3. Проверка сертификатов

Для проверки сертификатов необходимо выполнить следующие действия:

- загрузить корневые сертификаты с помощью следующих команд:
  - `curl -L http://community.omprussia.ru/files/doc/rootcacert-omp.pem -o rootcacert-omp.pem`
  - `curl -L http://community.omprussia.ru/files/doc/ima-root-ca.x509.pem -o ima-root-ca.x509.pem`
- проверить сертификат подписи бинарных файлов с помощью команды:

```
echo "test" > testfile openssl smime -sign \      -in testfile \
-signer binaries-cert.pem \      -inkey binaries-key.pem \      -out
testfile.sig openssl smime -verify \      -in testfile.sig \      -signer
binaries-cert.pem \      -CAfile ima-root-ca.x509.pem
```
- проверить сертификат подписи пакетов с помощью команды:

```
echo "test" > testfile openssl smime -sign \      -in testfile \
-signer packages-cert.pem \      -inkey packages-key.pem \      -out
testfile.sig.gost openssl smime -verify \      -in testfile.sig.gost \
-signer packages-cert.pem \      -CAfile rootcacart-omp.pem
```

При необходимости проверки сертификата сторонней организации требуется выполнить команду:

```
echo "test" > testfile-client openssl smime -sign \      -in
testfile-client \      -signer packages-client-cert.pem \      -inkey
packages-key.pem \      -out testfile-client.sig.gost openssl smime -
verify \      -in testfile-client.sig.gost \      -signer packages-client-
cert.pem \      -CAfile rootcacart-omp.pem
```

#### 2.4.2.4. Подпись МП

Для подписи МП его разработчику необходимо выполнить следующую команду:

```
customer-sign \      --binaries-key binaries-key.pem \      --
packages-key packages-key.pem \      --packages-cert packages-cert.pem \
sampleapp.rpm
```

где:

- sampleapp.rpm - пакет, содержащий ПО;
- binaries-key.pem - закрытый ключ подписи бинарных файлов;
- packages-key.pem - закрытый ключ подписи пакетов;
- packages-cert.pem - сертификат подписи пакетов.

В процессе подписи будут запрошены пароли от файлов с закрытыми ключами для подписи бинарных файлов и пакетов.

Если требуется подпись от сторонней организации, необходимо выполнить следующую команду:

```
ompcert-cli sign sampleapp.rpm packages-key.pem packages-client-
cert.pem
```

где:

- sampleapp.rpm - пакет, содержащий ПО;
- packages-key.pem - закрытый ключ подписи пакетов;
- packages-client-cert.pem - сертификат подписи пакетов от имени компании-клиента.

#### 2.4.2.5. Проверка подписи бинарных файлов МП

Для проверки подписи бинарных файлов МП необходимо выполнить следующую команду:

```
rpm -q --qf "[%{FILENAMES}]\n%{FILESIGNATURES}\n]" package.rpm |
grep -A1 /usr/bin/ | tail -n 1 | cut -c 7-14
```

где:

- package.rpm - имя файла подписанного пакета.

Результатом работы программы будет 4 байта, например: de39e183.

Такая же последовательность цифр должна присутствовать в выводе команды `cat /proc/keys`, если сертификат подписи бинарных файлов был добавлен в папку `/etc/keys/ima`.

**ПРИМЕЧАНИЕ.** При проверке подписи МП может потребоваться перезагрузка МУ.

#### 2.4.2.6. Проверка подписи RPM-пакета

Для проверки подписи пакета необходимо выполнить команду:

```
ompcert-cli verify someapplication.rpm -r rootcacert-omp.pem
```

Для просмотра важных атрибутов подписи (имени субъекта, метки и ID ключа) необходимо выполнить команду:

```
ompcert-cli dump someapplication.rpm
```

#### 2.4.2.7. Запуск МП

Перед запуском МП необходимо убедиться, что необходимый сертификат присутствует в папке `/etc/keys/ima` в формате `.der` и присутствует в выводе `cat /proc/keys`.

**ПРИМЕЧАНИЕ.** При запуске МП может потребоваться перезагрузка МУ.

Перед тем, как МП будет установлено на ОС Аврора, оно должно пройти валидацию непосредственно на МУ.

**ПРИМЕЧАНИЕ.** В случае неуспешной валидации на МУ МП не будет установлено.

Во избежание ошибок при установке следует пройти валидацию заранее с помощью утилиты `rpmvalidation`, выполнив команду:

```
rpmvalidation -t target_name package_name
```

,где:

`target_name` - цель проверки.

Отобразить список имеющихся целей для проверки можно, выполнив команду:

```
rpmvalidation -l
```

### 3. СРЕДСТВА РАЗРАБОТЧИКА

Режим разработчика предоставляет администратору доступ к расширенному функционалу настроек.

**ВНИМАНИЕ!** Запрещается активация режима разработчика на МУ, функционирующем под управлением ОС Аврора в сертифицированном варианте исполнения, и предназначенном для использования в информационных системах, аттестованных по требованиям обеспечения безопасности в соответствии с законодательством Российской Федерации!

**ПРИМЕЧАНИЕ.** Режим разработчика невозможно отключить после активации!

#### 3.1. Активация режима разработчика

**ПРИМЕЧАНИЕ.** Перед активацией режима разработчика необходимо убедиться в наличии на МУ доступа к сети Интернет.

Для активации режима разработчика необходимо выполнить следующие действия:

- коснуться пункта «Средства разработчика»  в меню системных настроек, в результате чего откроется страница «Инструменты разработчика»;
- коснуться переключателя «Режим разработчика» (Рисунок 73) и подтвердить действие вводом кода безопасности;
- на открывшейся странице ознакомится с условиями разработчика и коснуться кнопки «Подтвердить» для подтверждения активации режима разработчика либо кнопки «Отменить» для отмены операции (Рисунок 74).

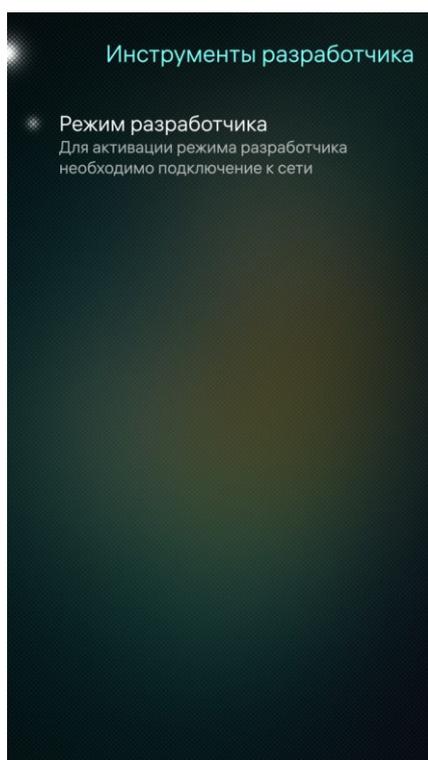


Рисунок 73

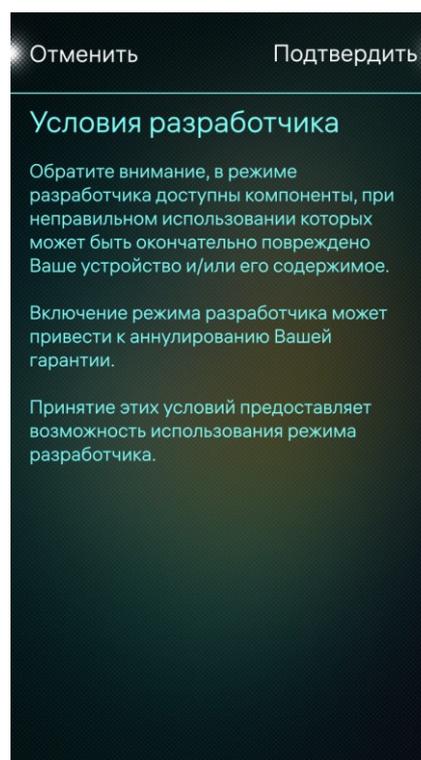


Рисунок 74

### 3.2. Инструменты разработчика

Для работы с инструментами разработчика необходимо выполнить следующие действия:

- активировать режим разработчика (п. 3.1);
- разрешить вход по SSH-паролю, коснувшись переключателя «Удаленное соединение» (Рисунок 75) и подтвердив действие вводом кода безопасности;
- задать либо сгенерировать пароль, коснувшись поля «Установить пароль для SSH и доступа», после чего коснуться кнопки «Сохранить» и подтвердить действие вводом кода безопасности (Рисунок 75);

#### ПРИМЕЧАНИЯ:

1. Поле «Установить пароль для SSH и доступа» отображается после активации переключателя «Удаленное соединение»;

2. SSH-пароль используется для получения прав суперпользователя.

– настроить отображение частоты кадров запущенных МП, коснувшись поля «Изображение частоты кадров» в подразделе «Инструменты», и на отобразившейся странице коснуться пункта «Простое» или «Подробное» либо коснуться поля «Отключено» для отключения диагностики (Рисунок 76);

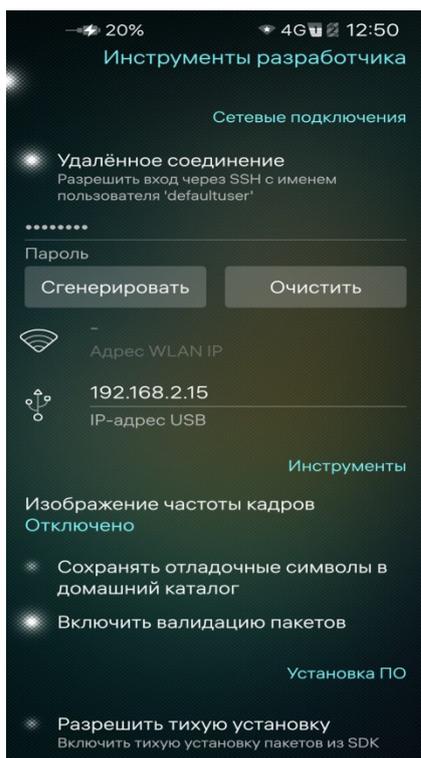


Рисунок 75

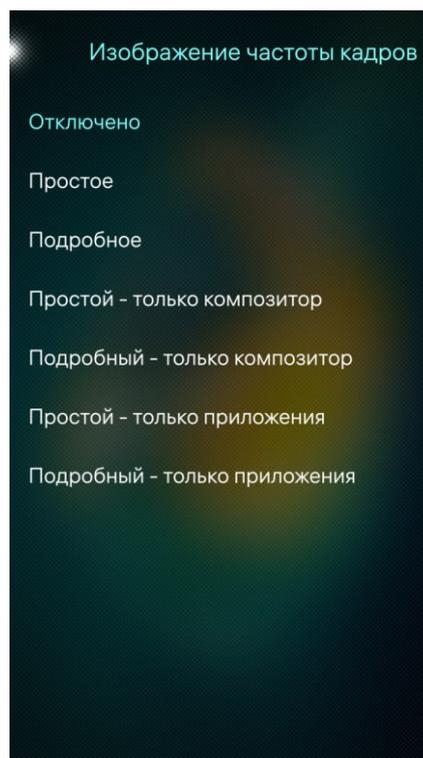


Рисунок 76

- разрешить либо запретить сохранение отладочных символов в домашнем каталоге, коснувшись переключателя «Сохранять отладочные символы в домашний каталог» в подразделе «Инструменты» (см. Рисунок 75);
- включить либо отключить валидацию пакетов, коснувшись переключателя «Включить валидацию пакетов» в подразделе «Инструменты» (см. Рисунок 75);
- разрешить либо запретить тихую установку пакетов из SDK, коснувшись переключателя «Разрешить тихую установку» в подразделе «Установка ПО» (см. Рисунок 75) и подтвердить действие вводом кода безопасности.

## 4. ОПИСАНИЕ МЕХАНИЗМОВ ЗАЩИТЫ

### 4.1. Регистрация событий безопасности (аудит)

#### 4.1.1. Основная информация

**ПРИМЕЧАНИЕ.** Аудит – описание использования функций регистрации событий безопасности, а также правил их настройки.

ОС Аврора осуществляет регистрацию и хранение:

- сообщений из системного журнала (syslog), ядра (kernel log);
- сообщений, которые процессы служб выводят на стандартные потоки вывода (stdout);
- ошибок (stderr).

Полученная информация индексируется и хранится в системном журнале, при этом основной системный журнал находится во временном каталоге и после перезагрузки не сохраняется.

Для надежного хранения определенного набора сообщений, относящихся к системе защиты информации, используется демон `sdjd`, который анализирует системный журнал и сохраняет отдельные сообщения в файл `/var/log/sdjd-v2.log`.

Файл `/var/log/sdjd-v2.log` имеет размер 50 МБ и организован по принципу кольцевого буфера, при его заполнении до максимального размера старые сообщения перезаписываются новыми.

В ОС Аврора программным компонентом `sdjd` регистрируются и долговременно хранятся следующие типы событий:

- результат попытки входа в систему;
- блокирование интерактивного сеанса как по запросу пользователя, так и по истечении установленного периода неактивности пользователя;
- блокировка доступа после установленного количества неуспешных попыток ввода аутентификационной информации;
- истечение срока действия пароля;
- смена пароля;
- запуск процедуры и результат проверки контроля целостности;
- обнаружение нарушения целостности;
- постоянная блокировка МУ;
- результат попытки установки, удаления или обновления пакетов;
- подключение и отключение внешних носителей информации;
- переполнение журнала событий безопасности;
- старт, перезагрузка и выключение ОС;
- добавление правил сетевого фильтра;
- запуск, завершение и изменение конфигурации службы аудита;

- изменение системного времени;
- нештатное завершение программы;
- попытки доступа к файлам, которые находятся под аудитом;
- сбой в механизме изоляции процессов;
- ошибки валидации пакетов;
- создание, переключение и удаление пользователя;
- инициализация и результат прохождения 2ФА;
- события антивируса;
- события Доверенной среды исполнения Аврора;
- запуск МП «Журнал»;
- обнаружение нарушения целостности сторонних файлов;
- изменение парольной и пользовательской политик;
- включение режима разработчика;
- включение и выключение удаленного доступа;
- разрешение и запрет доступа к терминалу.

Каждое событие содержит в себе следующую информацию:

- уникальный идентификатор события;
- тип события;
- время события в микросекундах с 01.01.1970 г.;
- уровень важности сообщения;
- опциональный текст сообщения (или пустая строка);
- PID процесса-отправителя;
- PID родительского процесса для процесса-отправителя;
- UID процесса-отправителя;
- Effective UID процесса-отправителя;
- Saved UID процесса-отправителя;
- File system UID процесса-отправителя;
- Real GID процесса-отправителя;
- Effective GID процесса-отправителя;
- Saved GID процесса-отправителя;
- File system GID процесса-отправителя;
- Supplementary groups процесса-отправителя;
- эффективные привилегии процесса-отправителя;
- полный путь к исполняемому файлу процесса-отправителя;
- контекст безопасности процесса-отправителя (текущая роль или метка SELinux);
- текстовое представление идентификатора события для удобства отладки.

Администратор может определить список объектов файловой системы (ФС), попытки доступа к которым будут регистрироваться в файле `/usr/share/security-audit/security-audit-rules.conf`, добавив правило аудита для наблюдаемого объекта отдельной строкой в файл `/usr/share/security-audit/security-audit-rules.conf`.

Все регистрируемые события безопасности отображаются в журнале событий с указанием времени и цветовой индикацией и доступны для просмотра в МП «Журнал». Пользователь имеет возможность сохранить журнал событий безопасности в постоянную внутреннюю память МУ в зашифрованном виде.

#### 4.1.2. Сохранение событий безопасности во внутреннюю память

Для сохранения событий безопасности в постоянную внутреннюю память МУ необходимо выполнить следующие действия:

- открыть МП «Terminal» и выполнить команду:

```
vi /etc/systemd/journald.conf;
```

- установить параметры в следующие значения:

```
Storage=persistent;  
SystemMaxUse=500M;  
RuntimeMaxUse=1M;
```

- перезагрузить МУ, чтобы изменения вступили в силу.

Для выгрузки файла журнала необходимо выполнить команду: `journalctl -a > j.log`, при этом потребуется создать файл лога, который будет иметь название: `j.log` (при необходимости название файла можно изменить) и содержать все события (`-a = all`).

#### 4.1.3. Просмотр сообщений аудита

Для просмотра сообщений аудита и доступа к ним необходимо использовать следующие инструменты:

- программу `journalctl`, имеющую интерфейс командной строки;
- программу `dmesg`, имеющую интерфейс командной строки;
- конфигурационный файл `/etc/omp/sdjd.conf`;

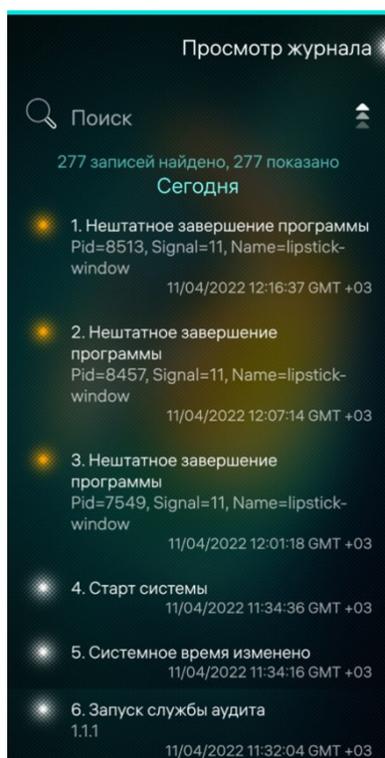


Рисунок 77

– МП «Журнал» (`/usr/bin/log-viewer`), в графическом интерфейсе которого отображаются записи о следующих событиях аудита:

- запуск выполнения службы аудита;
- старт проверки контроля целостности;
- модификация аутентификационной информации (смена пароля);
- успешный вход в систему и т.п.

**ПРИМЕЧАНИЕ.** В МП «Журнал» отображается как информация о событиях аудита, так и различная системная информация (Рисунок 77). Подробное описание работы МП приведено в документе «Руководство пользователя».

## 4.2. Идентификация и аутентификация

Для выполнения функций администрирования используются общие интерфейсы, при этом интерфейсы функциональных возможностей безопасности ОС представляют собой конфигурационные файлы либо команды оболочки.

Для работы с объектами системы администратору присваиваются следующие идентификаторы:

- символьный: `defaultuser`;
- числовой: `100000`.

Для усиления защиты МУ рекомендуется установить и периодически изменять код безопасности, который:

- в случае шифрования раздела с домашними каталогами пользователей будет храниться в LUKS-слоте, соответствующем идентификатору пользователя;
- в иных случаях будет храниться в виде свертки, полученной с помощью алгоритма криптографического преобразования `sha1`.

Для задания кода безопасности при первичной загрузке МУ:

- в корпоративном варианте исполнения<sup>6</sup> пользователю будет необходимо установить код безопасности для доступа к МУ;

<sup>6</sup> Описание возможных вариантов исполнения ОС Аврора приведены в таблице (Таблица 5Таблица 5).

– в сертифицированном варианте исполнения пользователю будет предложен пароль, сгенерированный случайным образом на основе датчика случайных чисел.

**ПРИМЕЧАНИЯ:**

1. Необходимо запомнить установленный код безопасности, т.к. он потребуется для дальнейшей работы с МУ;

2. В случае утраты и/или раскрытия кода безопасности его необходимо немедленно обновить.

В целях предотвращения несанкционированного доступа к МУ, функционирующего под управлением ОС Аврора, код безопасности потребуется для подтверждения выполнения следующих действий:

- создания учетных записей ролей;
- настройки парольной политики;
- задания ограничений входа в систему;
- включения и настройки 2ФА;
- задания одноразового пароля;
- изменения настроек блокировки;
- разрешения установки стороннего ПО;
- установки SSH-пароля;
- активации и настройки режима разработчика;
- просмотра данных учетных записей;
- сброса настроек МУ.

**ПРИМЕЧАНИЯ:**

1. При превышении количества попыток ввода неверного кода безопасности МУ автоматически будет заблокировано;

2. Время блокировки является фиксированным и составляет 15 минут.

### 4.3. Управление доступом (политики безопасности)

Для определения полномочий пользователя по использованию ресурсов и функциональных возможностей ОС Аврора применяется ролевая модель, на общесистемном уровне позволяющая всем пользователям МУ задать ограничения на использование функционала ОС посредством политик безопасности.

**ПРИМЕЧАНИЕ.** Настройка управления доступом, а также изменение данной настройки доступны только администратору либо через MDM систему.

Для перехода к настройкам политик безопасности необходимо выполнить следующие действия:

- открыть меню настроек касанием значка  на Экране приложений;

– в подразделе «Безопасность» системных настроек коснуться пункта «Политики безопасности» , в результате чего отобразится страница «Политики безопасности» (Рисунок 78).

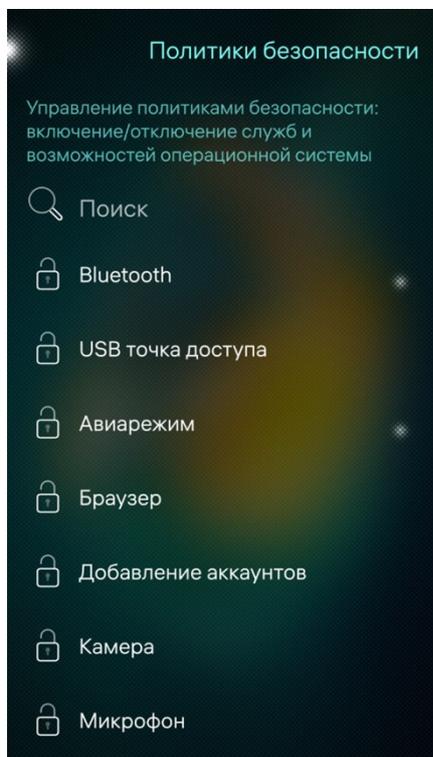


Рисунок 78

На странице «Политики безопасности» доступны следующие настройки:

– быстрый поиск политики безопасности с помощью ввода первых букв ее названия в поле «Поиск»;

– блокировка и разблокировка политики безопасности касанием соответствующего значка слева от выбранной политики либо касанием поля, в котором расположена выбранная политика.

**ПРИМЕЧАНИЕ.** Значок  указывает на то, что политика разблокирована (доступна), значок  указывает на то, что политика заблокирована (недоступна).

**ПРИМЕЧАНИЕ.** При работе с политиками безопасности необходимо коснуться непосредственно переключателя для его активации или деактивации: при активации переключатель начнет светиться ярче, чем в состоянии по умолчанию (неактивном).

Наименование и описание управляемых политик безопасности приведено в таблице (Таблица 2).

Таблица 2

№	Название политики	Описание политики	Атрибут безопасности	Политика по умолчанию	Управления политикой
1.	Камера	Использование камеры	CameraEnabled	Разблокирована	GUI
2.	Bluetooth	Использование интерфейса Bluetooth®	BluetoothToggleEnabled	Заблокирована	GUI
3.	Сброс к заводским настройкам	Выполнение сброса ОС к заводским настройкам	DeviceResetEnabled	Разблокирована	GUI
4.	Настройки WLAN	Использование сети WLAN	WlanToggleEnabled	Разблокирована	GUI

№	Название политики	Описание политики	Атрибут безопасности	Политика по умолчанию	Управления политикой
5.	Настройки точки доступа Wi-Fi	Использование МУ в качестве беспроводной точки доступа	InternetSharingEnabled	Разблокирована	GUI
6.	Снимки экрана	Создание снимков экрана	ScreenshotEnabled	Разблокирована	GUI
7.	Настройки мобильной сети	Настройки мобильной сети	MobileNetworkSettingsEnabled	Разблокирована	GUI
8.	Передача файлов на ПК (MTP)	Передача файлов по протоколу MTP	UsbMtpEnabled	Заблокирована	GUI
9.	USB точка доступа	Использование МУ в качестве USB-модема	UsbConnectionSharingEnabled	Разблокирована	GUI
10.	Настройки геолокации	Использование служб местоположения	LocationSettingsEnabled	Разблокирована	GUI
11.	Настройка даты и времени	Изменение настроек времени и даты	DateTimeSettingsEnabled	Разблокирована	GUI
12.	Авиарежим	Использование режима полета	FlightModeToggleEnabled	Разблокирована	GUI
13.	Микрофон	Использование микрофона	MicrophoneEnabled	Разблокирована	GUI
14.	Браузер	Работа пользователя с браузером	BrowserEnabled	Разблокирована	GUI
15.	Добавление аккаунтов	Добавление данных учетных записей	AccountCreationEnabled	Разблокирована	GUI
16.	Настройка VPN	Управление VPN-соединениями	VpnConnectionSettingsEnabled	Разблокирована	GUI
17.	Настройка VPN-соединения	Настройка/редактирование VPN-соединений	VpnConfigurationSettingsEnabled	Разблокирована	GUI
18.	Настройки прокси	Настройка прокси-сервера	NetworkProxySettingsEnabled	Заблокирована	GUI

№	Название политики	Описание политики	Атрибут безопасности	Политика по умолчанию	Управления политикой
19.	Установка приложений	Установка МП	ApplicationInstallationEnabled	Разблокирована	GUI
20.	-	Использование Android Debug Bridge	UsbAdbEnabled	Разблокирована	policy.conf
21.	-	Настройка мобильных точек доступа	MobileDataAccessPointSettingsEnabled	Разблокирована	policy.conf
22.	-	Работа с обновлением ОС	OsUpdatesEnabled	Разблокирована	policy.conf
23.	-	Принятие решений о загрузке сторонних пакетов	SideLoadingSettingsEnabled	Разблокирована	policy.conf
24.	-	Активация режима разработчика	DeveloperModeSettingsEnabled	Разблокирована	policy.conf
25.	-	Использование режима USB Mass Storage	UsbMassStorageEnabled	Разблокирована	policy.conf
26.	-	Работа со статистикой интернет-данных	NetworkDataCounterSettingsEnabled	Разблокирована	policy.conf
27.	-	Работа со статистикой звонков	CallStatisticsSettingsEnabled	Разблокирована	policy.conf
28.	-	Изменение типа технологии мобильной передачи данных	CellularTechnologySettingsEnabled	Разблокирована	policy.conf
29.	-	Режим разработчика	UsbDeveloperModeEnabled	Разблокирована	policy.conf
30.	-	Режим сетевого адаптера	UsbHostEnabled	Разблокирована	policy.conf
31.	-	Режим отладки	UsbDiagnosticModeEnabled	Разблокирована	policy.conf

#### 4.4. Идентификация и аутентификация

В ОС Аврора для исполняемых файлов используется формат, позволяющий установить режим доступа к сегментам в адресном пространстве процесса.

С помощью `seccomp-bpf` можно запретить некоторые системные вызовы, например: `mount/umount`, `ptrace`, `keexec` и др.

**ПРИМЕЧАНИЕ.** Максимальные квоты пользовательских процессов на аппаратные ресурсы задаются администратором в конфигурационном файле `/etc/security/limits.conf`.

Разрешения по доступу к ресурсам определяются элементами, представленными в таблице (Таблица 3).

Таблица 3

№	Элемент	Описание
1	Accounts	Просмотр, модификация и синхронизация учетных записей
2	Ambience	Установка и редактирование тем
3	AppLaunch	Запуск и остановка сервисов <code>systemd</code>
4	ApplicationInstallation	Установка и удаление МП
5	Audio	Воспроизведение и запись аудио, изменение конфигурации
6	Bluetooth	Подключение и использование устройств по Bluetooth®
7	Calendar	Просмотр и модификация событий календаря
8	CallRecordings	Доступ к записанным вызовам
9	Camera	Доступ к камере, съемка фото и видео
10	CommunicationHistory	Доступ к истории вызовов и сообщений
11	Contacts	Просмотр и модификация данных контактов
12	Documents	Доступ к каталогу «Documents»
13	Downloads	Доступ к каталогу «Downloads»
14	E-mail	Чтение и отправка электронной почты, доступ к вложениям
15	Internet	Использование сети Интернет
16	Location	Использование геопозиционирования
17	MediaIndexing	Доступ к перечню файлов на МУ
18	Messages	Доступ к чтению и отправке SMS
19	Microphone	Запись аудио с помощью микрофона
20	Music	Доступ к каталогу "Music", плейлистам и обложкам
21	NFC	Подключение и использование устройств NFC

№	Элемент	Описание
22	Phone	Осуществление вызовов напрямую или через пользовательский интерфейс
23	Pictures	Доступ к каталогу «Pictures»
24	PublicDir	Доступ к каталогу «Public»
25	RemovableMedia	Использование карт памяти и USB
26	Synchronization	Доступ к каркасу синхронизации
27	UserDirs	Доступ к каталогам «Documents», «Downloads», «Music», «Pictures», «Public» и «Video»
28	Videos	Доступ к каталогу «Videos»
29	WebView	Для использования Gecko WebView
30	AccessSecurityLog	Доступ к регистрационному журналу
31	DeviceInfo	Извлечение данных об устройстве
32	LogSecurityEvents	Запись в регистрационный журнал
33	PushNotifications	Чтение push-уведомлений
34	Reports	Генерирование архива с системными отчетами
35	SecureStorage	Хранение зашифрованных файлов
36	UserStatus	Извлечение списка пользователей системы

#### 4.5. Изоляция процессов

Решение задачи изоляции адресных пространств процессов основано на архитектуре ядра ОС Аврора, которое обеспечивает собственное изолированное адресное пространство для каждого процесса в системе. Данный механизм изоляции основан на страничном механизме защиты памяти, а также механизме трансляции виртуального адреса в физический, поддерживаемый модулем управления памятью. Одни и те же виртуальные адреса (с которыми работает процессор) преобразуются в разные физические адреса для разных адресных пространств. Процесс не может несанкционированным образом получить доступ к пространству другого процесса, т.к. непривилегированный пользовательский процесс лишен возможности работать с физической памятью напрямую.

**ПРИМЕЧАНИЕ.** Механизм разделяемой памяти является санкционированным способом, позволяющим нескольким процессам получить доступ к одному и тому же участку памяти и находится под контролем дискреционной политики управления доступом.

Адресное пространство ядра защищено от прямого воздействия пользовательских процессов с использованием механизма страничной защиты. Страницы пространства ядра являются привилегированными и доступ к ним из непривилегированного кода вызывает исключение процессора, который обрабатывается корректным образом ядром ОС.

Единственным санкционированным способом доступа к ядру ОС из пользовательской программы является механизм системных вызовов, который гарантирует возможность выполнения пользователем только санкционированных действий.

Дополнительные механизмы изоляции процессов не только друг от друга, но и от внешних ресурсов (внешних ресурсов от процессов) обеспечиваются применяемыми технологиями контейнеризации.

Программные средства, реализующие данную технологию, поддерживают широкий спектр «разрешений», согласно которому процессу разрешен только определенный перечень действий, выполняемых по отношению к другим процессам и периферийным устройствам, включая постоянное запоминающее устройство. Такой перечень определяется при установке пакета, содержащего исполняемый файл.

#### 4.6. Защита памяти

Решение задачи очистки оперативной памяти основано на архитектуре ядра ОС Аврора, которое гарантирует, что обычный непривилегированный процесс не получит данные чужого процесса, если это явно не разрешено правилами разграничения доступа (ПРД). Средства взаимодействия между процессами контролируются с помощью ПРД и процесс не может получить неочищенную память (как оперативную, так и дисковую).

Каждому процессу ядро выделяет виртуальное адресное пространство, которое транслируется в физические адреса памяти с поддержкой рандомизации.

Доступные для пользовательского процесса функции выделения и распределения памяти осуществляют выполнение режима инициализации, при котором происходит обнуление ячеек памяти. Таким образом, ядро и системная библиотека `libc` гарантируют получение процессом только очищенных страниц памяти без остаточной информации.

Решение задачи очистки памяти на внешних носителях (eMMC) основано на реализации механизма `scdcl`, который очищает на носителе неиспользуемые блоки ФС непосредственно при их освобождении с помощью перезаписи их маскирующей последовательностью.

#### 4.7. Подписи RPM-пакетов

В ОС Аврора используется механизм подписи RPM-пакетов и его содержимого, при этом:

- для пакетов отключены и не используются GPG подписи;
- подпись разработчика подписывает пакет целиком;
- клиентская подпись подписывает область подписи разработчика;

– каждая последующая подпись добавляется в конец и подписывает предыдущую.

Используется единый сертификат для проверки подписи пакета и подписи файлов IMA, т.е. для подписи как пакета, так и содержимого используется одна подпись.

Механизм безопасности IMA отвечает за отсутствие возможности запуска на МУ для неподписанных исполняемых файлов пакета, а также для исполняемых файлов пакета, подписанных неверной подписью либо подписью, которая верна, но отличается от текущего корневого сертификата.

Поддерживаются следующие алгоритмы для: IMASHA256, RSA2048 и GOST 34.10 2012.

Для отзыва скомпрометированных ключей происходит отзыв именно ключа, а не сертификата.

Для разделения зоны и глубины интеграции сторонних пакетов имеются дополнительные подгруппы для подписей: Regular, Extended, MDM, Antivirus, которые различаются набором правил и разрешений по расположению и взаимодействию файлов в ОС, а также использованием взаимосвязанных компонентов.

Для упрощения процесса разработки у разработчика остается возможность отключения процесса валидации пакетов, но при этом основные критические для системы проверки останутся активными.

#### 4.8. Фильтрация сетевого потока

Фильтрация сетевых потоков в ОС Аврора осуществляется с помощью встроенного в ядро ОС фильтра сетевых пакетов `netfilter` и монитора обращений, контролирующего сетевой стек IPv4.

Администратор при помощи утилиты `iptables` может задавать модулю ядра `netfilter` правила (или цепочки) фильтрации в соответствии с атрибутами отправителя и получателя сетевых пакетов, а также атрибутами передаваемой информации в IP-заголовках пакетов.

#### 4.9. Контроль целостности

Подсистема контроля целостности ОС обеспечивает проверку неизменности среды исполнения и предоставляет сторонним разработчикам API для верификации целостности ключевых файлов пакетов. Компоненты `integrityd` и `securityd` в связке блокируют доступ к ОС при обнаружении нарушения целостности системных файлов.

**ПРИМЕЧАНИЕ.** Начиная с релиза 4.0, программный компонент `integrityd` заменил AIDE и начал осуществлять подсчет контрольных сумм, который ранее выполнялся компонентами: `securityd` и `libpartitioninfo`.

Основная задача `integrityd` - верификация целостности объектов: обычных файлов, ELF-файлов и разделов, которые могут объединяться в группы. В отличие от других инструментов, `integrityd` использует электронную подпись (IMA и `secureboot`) как источник доверия.

**ПРИМЕЧАНИЕ.** Информация о старте и/или завершении процедуры контроля целостности, а также о результатах ее выполнения записывается в системный журнал.

#### 4.10. Шифрование раздела с домашними директориями пользователей

В ОС Аврора раздел с домашними директориями шифруется с помощью алгоритма `aes-xts-plain64` 512-битным мастер-ключом, для хранения которого используется LUKS-заголовок, состоящий из следующих 8 слотов:

- 1 слот используется администратором;
- 6 слотов доступны создаваемым учетным записям пользователя;
- 1 слот резервируется для смены паролей.

Идентификатор пользователя однозначно определяет номер используемого слота, при этом в каждом из слотов хранится мастер-ключ, шифрованный паролем соответствующего пользователя с помощью алгоритма PBKDF. Количество итераций алгоритма подбирается таким образом, чтобы проверка одной комбинации выполнялась примерно 1 секунду.

Выполнение следующих действий потребует введение корректного кода безопасности из слота LUKS-заголовка, соответствующего идентификатору конкретного пользователя:

- разблокировка домашней директории при загрузке МУ;
- разблокировка UI `Lipstick`.

#### ПРИМЕЧАНИЯ:

1. Старт пользовательской сессии невозможен без ввода корректного кода безопасности, при превышении количества попыток неверного ввода которого МУ автоматически будет заблокировано;

2. Время блокировки является фиксированным и составляет 15 минут.

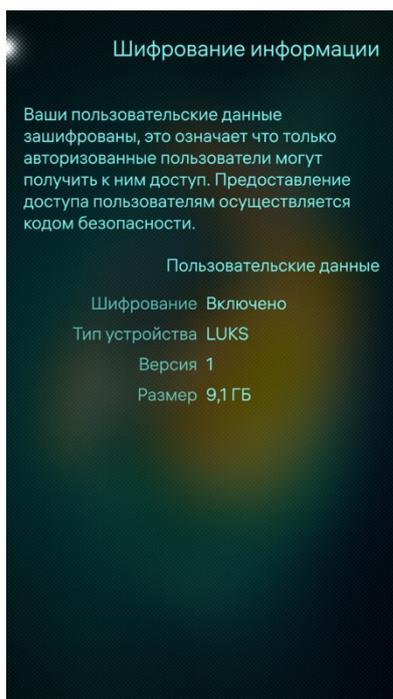


Рисунок 79

Для просмотра информации о шифровании (Рисунок 79) необходимо выполнить следующие действия:

- открыть меню настроек системы касанием значка  на Экране приложений;
- в подразделе «Безопасность» коснуться пункта меню «Шифрование» , в результате чего отобразится страница «Шифрование информации» с пользовательскими данными.

## 5. РЕКОМЕНДАЦИИ ПО УСТРАНЕНИЮ ВОЗМОЖНЫХ ОШИБОК

Действия по устранению возможных ошибок приведены в таблице (Таблица 4).

Таблица 4

№	Ошибка	Причина/рекомендации по устранению
1.	Невозможно выполнить обновления, т.к. не работает кнопка «Загрузить»	Для получения обновления ОС Аврора требуется доступ к определенным ресурсам компании-разработчика. Такой доступ предоставляется клиентам, оформившим техническую поддержку, включающую услугу обновления ОС. Более подробная информация доступна по электронной почте support@omp.ru.
2.	Не получается установить МП	Установка МП на МУ, функционирующее под управлением ОС Аврора, возможна следующими способами: <ul style="list-style-type: none"> <li>– с использованием ППО «Аврора Центр», развернутой для компании-клиента: внутри периметра организации или у внешнего поставщика (ИТ-интегратора);</li> <li>– непосредственно на МУ в режиме разработчика. Для переключения МУ в данный режим необходимо выполнить операции, описанные в документе «Руководство пользователя ОС Аврора» (актуальная версия документации доступна по ссылке: <a href="https://auroraos.ru/documentation">https://auroraos.ru/documentation</a>);</li> <li>– из графического интерфейса ОС Аврора;</li> <li>– с использованием МП «Terminal»</li> </ul>
3.	Ошибка сертификата	Один из доверенных сертификатов, входящих в третье поколение ОС, устарел, в результате чего была утрачена доверенность ресурсов, подписанных такими сертификатами.
4.	При получении обновлений с ППО «Аврора Центр» отображается сообщение «Appmanager is busy»	Проблемы с сетевым доступом МУ к ППО «Аврора Центр». Если при скачивании МП происходит сетевой разрыв, то последующие МП становятся в очередь и их установка не происходит

№	Ошибка	Причина/рекомендации по устранению
5.	Отображается сообщение «Управление обновлением ОС запрещено»	Установленный на МУ mdm-клиент (например, клиент ППО «Аврора Центр») запрещает обновления через интерфейс МУ
6.	МУ заблокировано, требуется код доступа	Необходимо обратиться к администратору МУ либо оператору ППО «Аврора Центр» для сброса пароля МУ, подключенного к сети Интернет
7.	При установке RPM на МУ возникает ошибка	Несовместимость ключей в ОС и ключей, которыми подписано МП. Необходимо переподписать МП либо использовать ОС с ключами, соответствующими МП
8.	Пользователь забыл код безопасности МУ	Необходимо обратиться к администратору для сброса пароля МУ
9.	Администратор забыл код безопасности МУ	Необходимо последовательно выполнить следующие действия: – ввести МУ в Recovery Mode (выключить МУ одновременным нажатием кнопки уменьшения громкости и кнопки включения МУ), в результате чего на экране отобразится строка «Recovery: Connect USB cable and open telnet to address 10.42.66.66»; – подключить МУ к ЭВМ через USB-кабель; – открыть терминал и ввести команду: <code>telnet 10.12.66.66</code> ; – выбрать пункт «Reset device to factory state»; нажать «Enter» 5 раз, после чего ожидать «Wipe Device»
10.	После загрузки обновлений МП на МУ оно не обновилось	Убедившись, что МУ имеет доступ к сети Интернет и заряд аккумулятора МУ составляет не менее 50%, необходимо осуществить принудительное обновление, выполнив следующие действия: – открыть Экран приложений, проведя по Домашнему экрану снизу вверх; – перейти в пункт меню системных настроек «Обновления ОС Аврора», после чего выбрать пункт «Проверить наличие обновлений». Если после выполнения описанных действий МП не было установлено либо обновлено, необходимо провести анализ системных сообщений

№	Ошибка	Причина/рекомендации по устранению
11.	Невозможно сбросить МУ к заводским настройкам	Данная функция отключена с помощью политики безопасности, необходимо отключить данную политику в меню безопасности
12.	Недоступны настройки даты и времени	Данная функция отключена с помощью политики безопасности, необходимо отключить данную политику в меню безопасности

## ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

В настоящем документе приняты следующие термины и сокращения (Таблица 5).

Таблица 5

Термин/ Сокращение	Расшифровка
Администратор	Пользователь, обладающий правами на выполнение операций, связанных с администрированием системы
Атмосфера (тема МУ)	Совокупность визуального оформления всех экранов и цветового оформления интерфейса
Варианты исполнения ОС Аврора	<ol style="list-style-type: none"> <li>1. Корпоративный вариант исполнения – релиз, предназначенный для использования компаниями, у которых есть потребность в использовании доверенных мобильных рабочих мест, на которых не происходит обработка конфиденциальной информации;</li> <li>2. Сертифицированный вариант исполнения – набор готовых к сертификации и серийному производству артефактов сертифицированного изделия, имеющих сертификат, находящихся на сертификационных испытаниях или подготовленных к проведению сертификационных испытаний. Сертифицированный релиз может поставляться по Лицензионному договору в период прохождения сертификации в согласованной комплектации. После получения сертификата соответствия поставки релиза не осуществляются, а поставляется Сертифицированное изделие</li> </ol>
2ФА	Двухфакторная аутентификация
Квота	Объем дискового пространства, выделяемого администратором для записи данных учетных записей пользователей
Криптоконтейнер	Криптографический контейнер
МП	Мобильное приложение
МУ	Мобильное устройство
ОС	Операционная система
Переключатель	Элемент интерфейса ОС Аврора, представляющий собой светящуюся точку, расположенную в поле, и позволяющий выбрать одно из состояний, чаще всего включение или выключение. При активации переключателя точка начинает светиться ярче, чем в неактивном состоянии

Термин/ Сокращение	Расшифровка
Пользователь	Лицо, использующее систему для выполнения заложенных в ней функций
Предприятие-разработчик	Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа»)
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение «Аврора Центр»
ПРД	Правила разграничения доступа
СКЗИ СледопытSSL	Программное средство криптографической защиты информации СледопытSSL
Суперпользователь	Пользователь, обладающий правами на выполнение всех без исключения операций в системе (в системе имеет логин «root»)
Токен	Аутентификационные данные, которые выдаются пользователю после успешной авторизации и являются ключом для доступа к службам
ФС	Файловая система
ЭВМ	Электронно-вычислительная машина
GUI	Graphical User Interface - разновидность пользовательского интерфейса, в котором элементы интерфейса (меню, кнопки, значки, списки), представленные пользователю на дисплее, исполнены в виде графических изображений
MTP	Media Transfer Protocol – основанный на RTP аппаратно-независимый протокол, разработанный компанией Microsoft для подключения цифровых плееров к компьютеру
NFC	Near field communication - технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров
PIN-код	Personal Identification Number - персональный код, состоящий из 4 цифр, предназначенный для получения доступа к SIM-карте и предотвращающий ее несанкционированное использование
PUK-код	Personal Unlock Key - дополнительный код, состоящий из 8 цифр и применяемый для разблокировки SIM-карты после неудачного ввода значения PIN-кода 3 раза подряд

Термин/ Сокращение	Расшифровка
RPM	Red Hat Package Manager – менеджер пакетов Red Hat обозначает две сущности: формат пакетов ПО (RPM-пакет) и программа, созданная для управления этими пакетами. Программа позволяет устанавливать, удалять и обновлять ПО
RPM-пакет	Файл формата RPM, позволяющий устанавливать, удалять и обновлять приложение на МУ
RBAC	Role Based Access Control - развитие политики избирательного управления доступом, при этом права доступа субъектов системы на объекты группируются с учетом специфики их применения, образуя роли
SIM	Subscriber Identification Module – модуль идентификации абонента
SSU	SourceSafe для Unix – утилита, обеспечивающая доступ из командной строки к локальным и удаленным репозиториям Source Safe/VSS через TCP
SSH	Secure SHell – сетевой протокол прикладного уровня, позволяющий производить удаленное управление ОС и туннелирование TCP-соединений (например, для передачи файлов)
USB	Universal Serial Bus – универсальная последовательная шина
VPN	Virtual Private Network – виртуальная частная сеть, обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, сети Интернет)
WLAN	Wireless Local Area Network – беспроводная локальная сеть

