

РУКОВОДСТВО АДМИНИСТРАТОРА

Версия 1.0

Листов 35

АННОТАЦИЯ

Настоящий документ является руководством администратора Операционной системы (ОС) Аврора релиз 4.0.1 update 1.

ОС Аврора представляет собой защищенную мобильную многозадачную ОС для мобильных применений под аппаратные платформы на базе процессоров ARM.

ОС Аврора – современная мобильная ОС, позволяющая выполнить широкий спектр задач независимо от местонахождения пользователя.

ОС Аврора предоставляет оригинальный и интуитивно понятный интерфейс, позволяющий управлять мобильными устройствами (МУ) одной рукой с помощью жестов. Мобильные приложения (МП) для ОС Аврора отличает единый лаконичный дизайн, который может быть адаптирован под необходимую цветовую и графическую схему. Аудиовизуальный профиль ОС изменяется в несколько касаний, подстраивая ее окружение под выбранный пользователем стиль.

В ОС Аврора предусмотрена поддержка следующих форматов файлов:

- видеокодеки: H.264, MPEG-4, VP8;
- форматы видео: 3GP, AVI, MKV, MP4, WebM;
- аудиокодеки: AAC, MP3, MP4, Vorbis;
- форматы аудио: FLAC, MP3, OGG, WAV;
- документы: .doc, .docx, .txt, .rtf, .xlsx, .xls, .pptx, .ppt, .rdf.

Кроме того, в ОС Аврора реализовано большое количество механизмов безопасности, направленных на сохранение конфиденциальности обрабатываемой информации и данных пользователя.

В ОС Аврора предусмотрена возможность создания до семи ролей и переключения между режимами (подраздел 2.1).

Настоящий документ содержит описания работы пользователя с ролью Администратор. Описание функциональных возможностей роли Пользователя приведено в документе «Руководство пользователя»

Настоящий документ содержит общую информацию о порядке работы и основных действиях Администратора, выполняемых в ходе работы с МУ, функционирующими под управлением ОС Аврора.

СОДЕРЖАНИЕ

1. Подготовка к работе	4
1.1. Общие требования.....	4
1.2. Настройка мобильного устройства.....	6
1.3. Установка часового пояса, текущей даты и времени.....	6
1.4. Управление SIM-картами	9
1.5. Настройка режима разработчика	9
1.6. Обновление ОС Аврора	11
2. Выполнение программы.....	13
2.1. Управление ролями	13
2.1.1. Получение привилегий Администратора	14
2.1.2. Создание и удаление Пользователя	15
2.1.3. Переключение между режимами (ролями)	18
2.2. Настройки парольных политик	21
2.3. Настройки безопасности	22
2.3.1. Политики безопасности	22
2.3.2. Аудит	24
2.3.3. Шифрование.....	26
2.3.4. Недоверенные программы	26
2.4. Управление мобильными приложениями.....	28
Перечень терминов и сокращений.....	29
Приложение 1.....	31

1. ПОДГОТОВКА К РАБОТЕ

Приведенные в настоящем документе снимки экрана на основе атмосферы «Северное сияние» являются примером. При использовании другой атмосферы внешний вид интерфейса МУ может отличаться

1.1. Общие требования

К администратору ОС Аврора предъявляются следующие требования:

- знание принципов построения и функционирования современных вычислительных систем, механизмов защиты информации;
- навыки работы с ОС семейства Linux;
- навыки администрирования общесистемного и прикладного программного обеспечения (ПО);
- навыки настройки средств защиты, используемых в составе ОС Аврора.

К среде функционирования ОС Аврора предъявляются следующие требования:

- обеспечение установки любого ПО (загрузочных модулей, библиотек, файлов конфигурации и т.п.) в ОС Аврора исключительно в формате пакетного менеджера RPM;

Не допускается установка любого ПО, поставляемого в отличном от RPM виде (самостоятельное копирование файлов, установка ПО из архивов, установка не в штатные каталоги из пакетов RPM и т.п.)

- совместимость ОС Аврора с МУ, на котором она функционирует;
- обеспечение установки, конфигурирования и управления ОС Аврора;
- обеспечение защиты от осуществления действий, направленных на нарушение физической целостности МУ, на котором функционирует ОС Аврора;
- обеспечение ограничения на установку ПО и его компонентов, не задействованных в технологическом процессе обработки информации;
- обеспечение доверенного маршрута между ОС Аврора и пользователями ОС Аврора (администраторами, пользователями);

- обеспечение доверенного канала передачи данных между ОС Аврора и средствами вычислительной техники, с которых осуществляется администрирование ОС;
- обеспечение невозможности отключения (обхода) компонентов ОС Аврора;
- реализация мер, препятствующих несанкционированному копированию содержащейся в ОС Аврора информации на съемные машинные носители информации (или за пределы МУ). В том числе должен осуществляться контроль вноса (выноса) в (из) контролируемую зону (контролируемой зоны) съемных машинных носителей информации;
- осуществление проверки целостности внешних модулей уровня ядра, получаемых от заявителя (разработчика, производителя), перед их установкой в ОС Аврора;
- обеспечение выделения вычислительных ресурсов для процессов в соответствии с их приоритетами;
- лица, ответственные за функционирование ОС Аврора, должны обеспечивать данное функционирование;
- лица, ответственные за эксплуатацию ОС Аврора, должны обеспечивать сохранность аутентификационной информации пользователей ОС Аврора. Информация подобного рода должна содержаться в тайне и быть недоступна лицам, не уполномоченным ее использовать;
- при работе ОС Аврора на МУ необходимо не допустить возможность воспроизведения любых мультимедийных файлов, полученных из недоверенных источников.

1.2. Настройка мобильного устройства

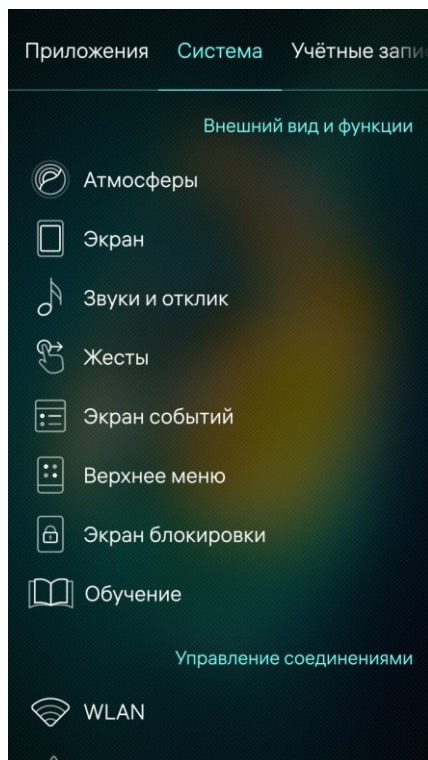



Рисунок 1


Для настройки общих функций необходимо выполнить следующие действия:

- открыть меню настроек системы касанием значка  на Экране приложений (Рисунок 1);
- выбрать один из пунктов меню раздела;
- задать значения параметров в соответствии с инструкциями, приведенными в следующих подразделах настоящего документа;
- для возврата в меню настроек необходимо коснуться точки в левом верхнем углу экрана. Настройки параметров будут сохранены.

Более подробное описание основных настроек МУ представлено в документе «Руководство пользователя»

1.3. Установка часового пояса, текущей даты и времени

Для установки часового пояса, текущей даты и времени необходимо выполнить следующие действия:

- в меню настроек системы коснуться пункта «Время и дата» . Отобразится страница настройки даты/времени (Рисунок 2);
- для автоматического обновления даты/времени коснуться переключателя «Автоматическое обновление». Значения полей часового пояса, даты и времени станут недоступными для редактирования. В дальнейшем обновление даты/времени будет происходить автоматически;

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

– для установки часового пояса вручную: коснуться поля «Часовой пояс» и на открывшейся странице выбрать необходимое значение (Рисунок 3). Для ускорения процесса выбора можно воспользоваться полем поиска;

При установке часового пояса вручную опция автоматического обновления времени должна быть выключена

– выбрать формат времени: коснуться переключателя «Использовать 24-часовой формат» 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»;

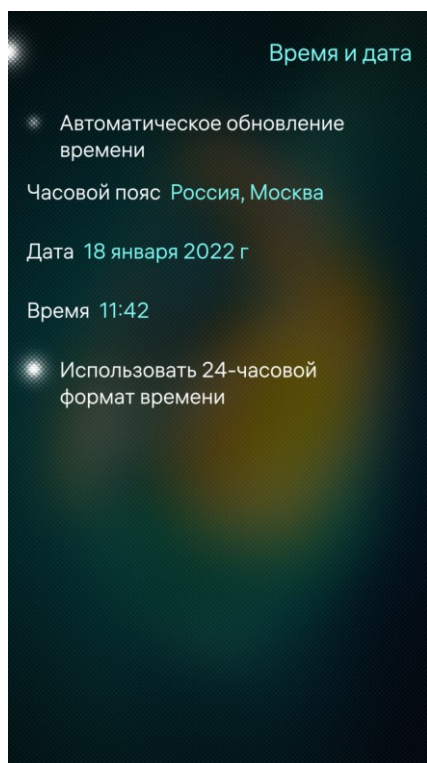


Рисунок 2

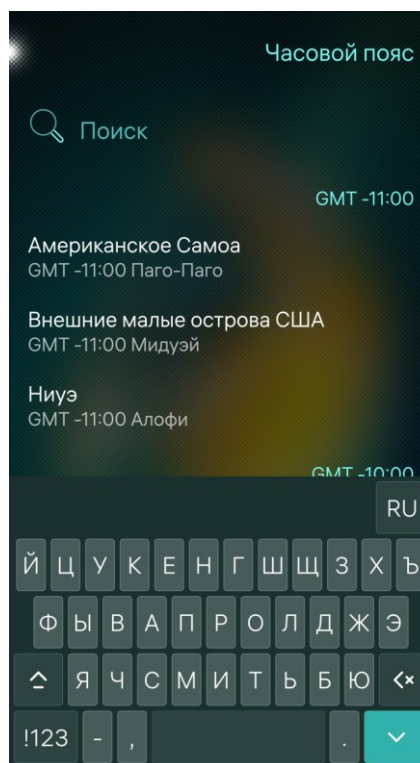


Рисунок 3

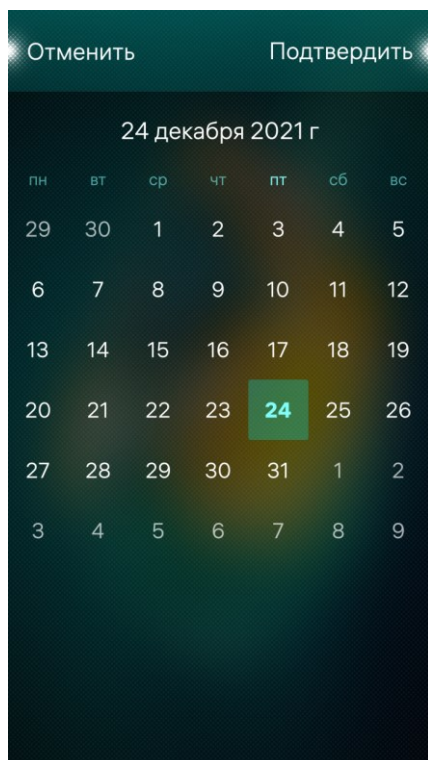


Рисунок 4

– для установки даты вручную: коснуться поля «Дата» (см. Рисунок 2), на открывшейся странице коснуться текущей даты, выбрать из списка текущий год, месяц и число (Рисунок 4);

– коснуться кнопки «Подтвердить» для сохранения даты либо кнопки «Отменить» для отмены операции. При выборе кнопки подтверждения выбранная дата отобразится на странице настройки даты/времени, при отмене дата останется прежней;

При установке даты вручную опция автоматического обновления должна быть выключена

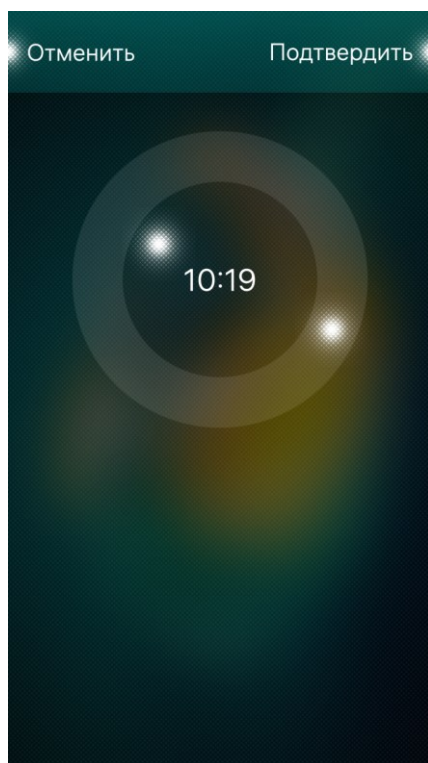


Рисунок 5

– для установки времени коснуться поля «Время» (см. Рисунок 2). Отобразится циферблат, метка во внутреннем круге которого играет роль часовой стрелки, во внешнем — минутной (Рисунок 5). 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.

При выборе кнопки подтверждения выбранная дата отобразится на странице настройки даты/времени, при отмене дата останется прежней.

1.4. Управление SIM-картами

В зависимости от конструктивных особенностей МУ в ОС Аврора допускается активировать до двух SIM-карт

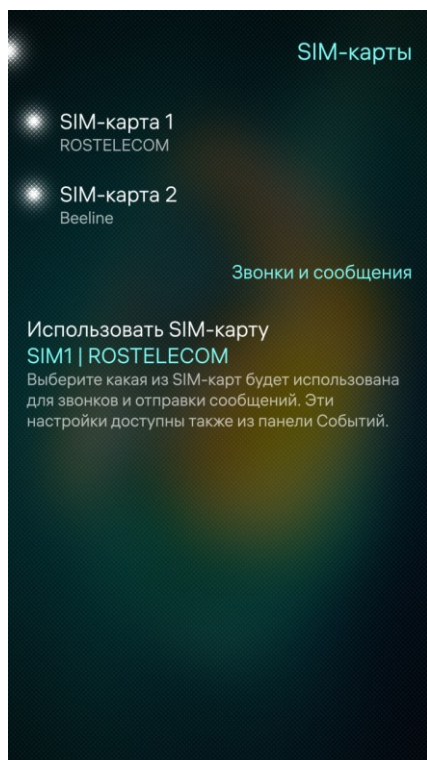



Рисунок 6


Для настройки SIM-карт, используемых в МУ, необходимо выполнить следующие действия (Рисунок 6):

- коснуться значка «SIM-карты»  в меню настроек сети;
- выбрать SIM-карты, которые будут использоваться в МУ, касанием соответствующих полей.

Информация об активных SIM-картах отразится в разделе «Звонки и сообщения».

1.5. Настройка режима разработчика

Для настройки режима разработчика необходимо выполнить следующие действия:

- в меню системных настроек коснуться пункта «Средства разработчика» .
- Отобразится страница с инструментами разработчика;
- коснуться переключателя «Режим разработчика» для активации режима разработчика (Рисунок 7);
 - подтвердить действие вводом текущего кода безопасности;
 - для включения обновлений разработчика коснуться переключателя «Включить обновления разработчика» в подразделе «SSU»;

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

- на открывшейся странице заполнить поля: «Имя пользователя», «Пароль», «Домен SSU» (Рисунок 8);
- коснуться кнопки «Вход» для сохранения введенных данных либо коснуться кнопки «Отменить» для отмены операции;

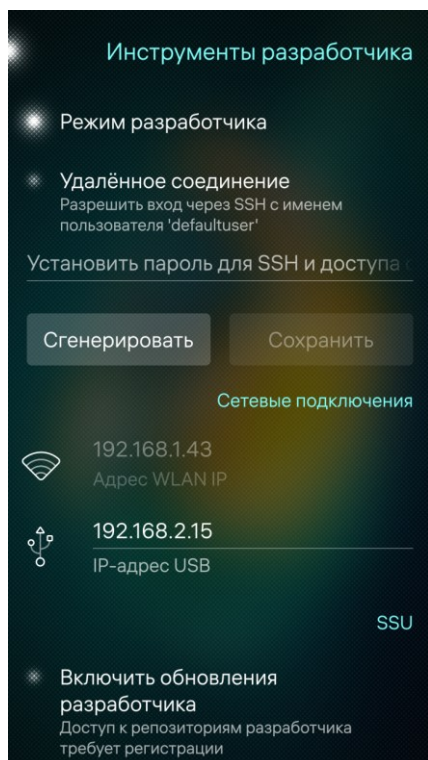


Рисунок 7

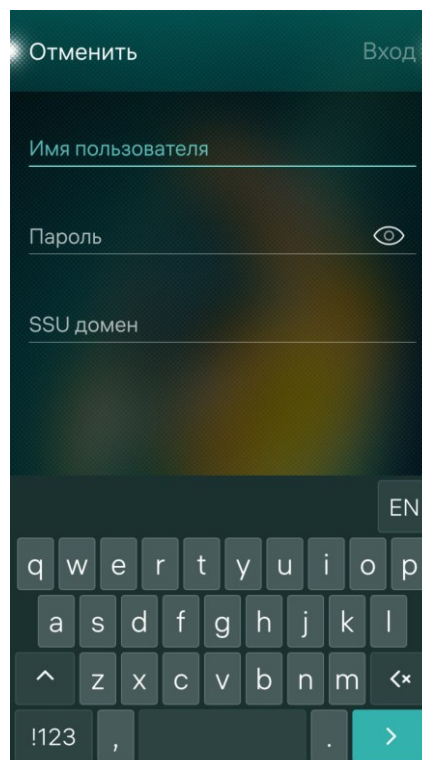


Рисунок 8

– для диагностики отображения частоты кадров запущенных МП в подразделе «Инструменты» открыть контекстное меню поля «Изображение частоты кадров» и выбрать пункт «Простое» или «Подробное» либо коснуться поля «Отключено» для отключения диагностики (Рисунок 9). В верхней части отображается частота кадров текущего МП, в нижней - состояние в целом;

– коснуться переключателя «Отображать кнопку перезагрузки в верхнем меню» (Рисунок 10) для отображения кнопки перезагрузки в верхнем меню;

– коснуться переключателя «Разрешить диагностический режим USB» для разрешения диагностического режима USB;

– коснуться переключателя «Разрешить действия с загрузчиком». для разрешения перепрошивки МУ;

– коснуться пункта «Сохранять отладочные символы в домашний каталог» для сохранения отладочных символов в домашнем каталоге.

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

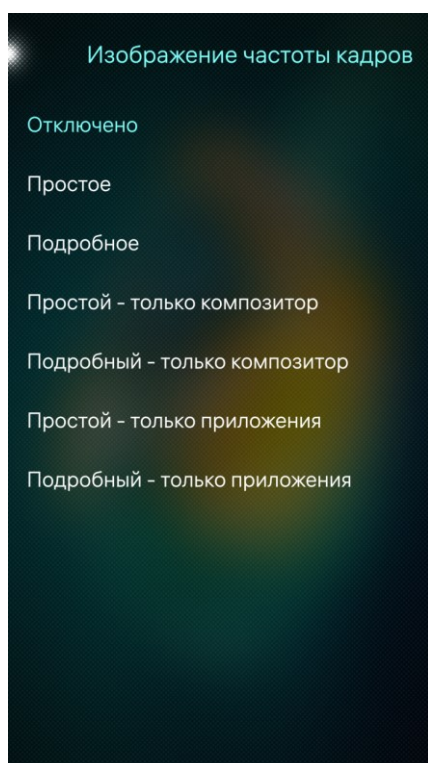


Рисунок 9

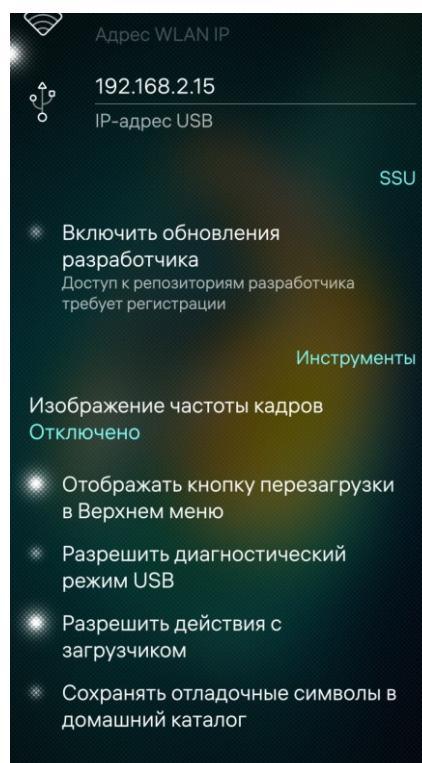




Рисунок 10

1.6. Обновление ОС Аврора

Для обновления версии ОС Аврора необходимо выполнить следующие действия:

– в меню системных настроек коснуться пункта «Обновления Аврора ОС»  . Отобразится страница с настройками обновления;

– коснуться значка  для проверки доступных обновлений. В результате отобразится список доступных обновлений либо сообщение: «Не требуют обновления» (Рисунок 11);

- коснуться кнопки «Скачать» для загрузки обновления. При необходимости загрузку обновления можно отменить касанием кнопки «Отмена»;
- коснуться кнопки «Установить»;

После касания кнопки «Установить» МУ будет перезагружено

- коснуться поля «Проверить наличие обновлений» в подразделе «Настройки» для задания частоты проверки наличия обновлений и в контекстном меню выбрать необходимый вариант: «Вручную», «Только WLAN» или «Всегда» (Рисунок 12).

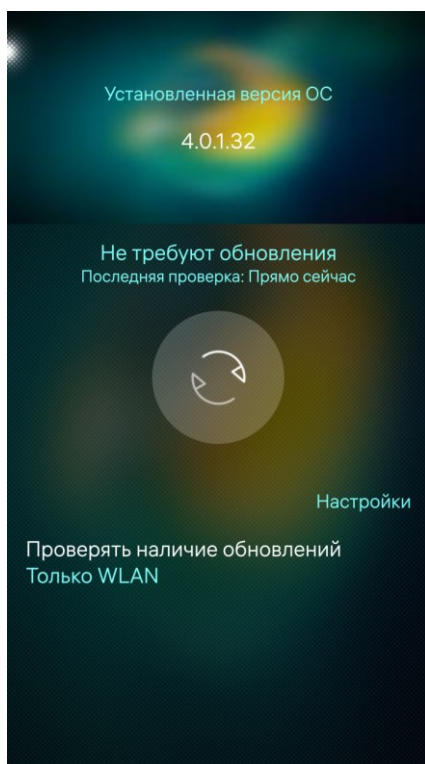


Рисунок 11

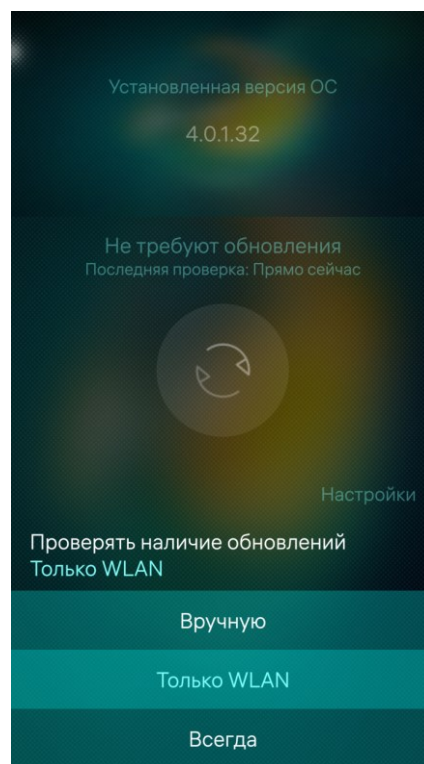


Рисунок 12

2. ВЫПОЛНЕНИЕ ПРОГРАММЫ

Управление ролями выполняется администратором системы в системных настройках. Пользователь с ролью Администратор (defaultuser) не является пользователем «root» (UID != 0)

2.1. Управление ролями

Роль – это совокупность прав доступа, на основе которых проверяется возможность выполнения пользователем того или иного действия в ОС. В зависимости от выбранной роли функциональные возможности МУ с установленной ОС Аврора могут отличаться.

В ОС Аврора предусмотрена возможность создания до 7 ролей:

1. Администратор – роль с расширенными правами, которая имеет доступ к данным других пользователей и не может быть удалена из системы. Данная роль обладает следующими функциональными возможностями:

- создание и удаление Пользователя;
- переименование Пользователя;
- управление ограничениями Пользователей (осуществление вызовов, отправка SMS, использование сотовых данных и т.д.);
- управление учетной записью Пользователя (срок жизни, время входа);
- управление настройками обновления ОС Аврора;
- установка ПО (без использования Прикладного программного обеспечения «Аврора Центр» (далее – ППО);
- управление настройками МУ;
- сброс МУ к заводским настройкам;
- управление парольными политиками (предназначено для настройки уровня сложности пароля);

2. Пользователь – роль, созданная Администратором, которая имеет возможность добавлять и изменять настройки своей роли, а также других пользователей в части их функционала, а именно:

- изменять период спящего режима экрана;
- изменять допустимое количество попыток неверного кода разблокировки;
- изменять время автоматической блокировки экрана.

В системе предусмотрено создание до 6 ролей Пользователя

При этом Администратор и Пользователь имеют следующие общие функциональные характеристики:

- индивидуальные идентификаторы (UID);
- домашние директории.


2.1.1. Получение привилегий Администратора

Лицо, осуществляющее первичный запуск после установки и настройку ОС Аврора, является Администратором системы.

В режиме администратора предоставляется возможность выполнять любые действия по настройке и/или администрированию системы, включая модификацию настроек функций безопасности (подраздел 2.3).

После выполнения установки и первоначальной настройки ОС Аврора (либо если МУ с установленной ОС Аврора поступило от предприятия-изготовителя) МУ автоматически загружается в режиме администратора

Для получения повышенных привилегий системного администратора необходимо в МП «Terminal» выполнить следующие действия:

- провести по экрану снизу вверх и на Экране приложений коснуться значка ;

Для отображения МП «Terminal» на Экране приложений необходимо активировать режим разработчика (подраздел 1.5)

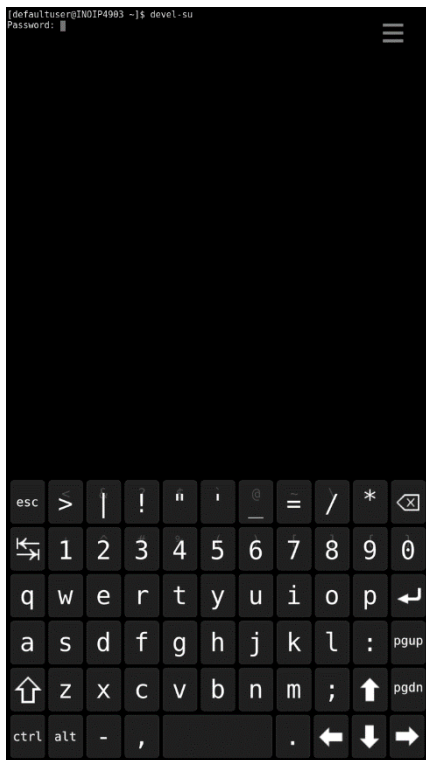


Рисунок 13

– на открывшейся странице «Terminal» выполнить команду:



```
devel-su
```

– указать пароль, заданный ранее, для перехода в режим администратора (Рисунок 13).

2.1.2. Создание и удаление Пользователя

Пользователи создаются администратором системы

Для создания Пользователя необходимо выполнить следующие действия:

- открыть меню настроек касанием значка  на Экране приложений;
- перейти к подразделу «Система»;
- выбрать пункт меню «Пользователи» . Отобразится страница «Пользователи» с представленным списком пользователей, созданных на МУ;

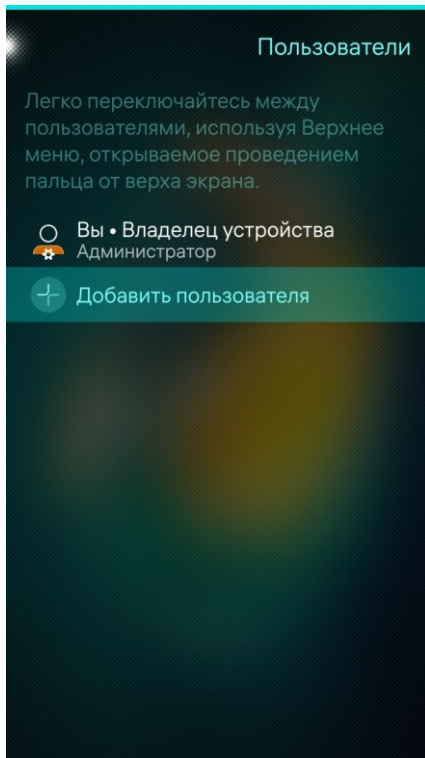


Рисунок 14

– коснуться пункта «Добавить пользователя» (Рисунок 14);

– подтвердить действие вводом текущего кода безопасности Администратора.

– ввести новое имя пользователя (Рисунок 15);

– на странице «Пользователи» отобразится строка с созданным Пользователем (Рисунок 16).

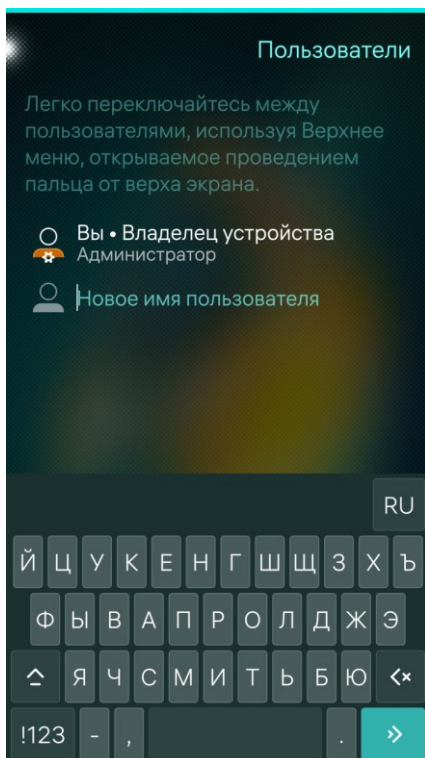


Рисунок 15

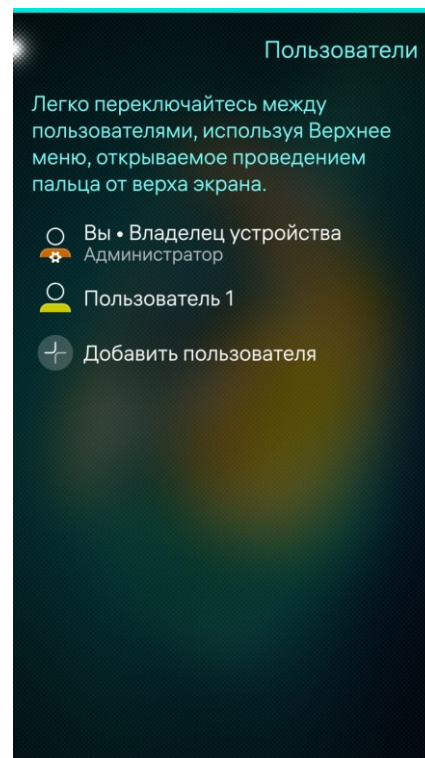



Рисунок 16

При первой загрузке ОС Аврора в режиме пользователя отобразится экран для введения кода безопасности, в котором необходимо ввести новый код безопасности и коснуться значка .

Подробная информация о включении/выключении МУ и задании кода безопасности представлена в документе «Руководство пользователя»

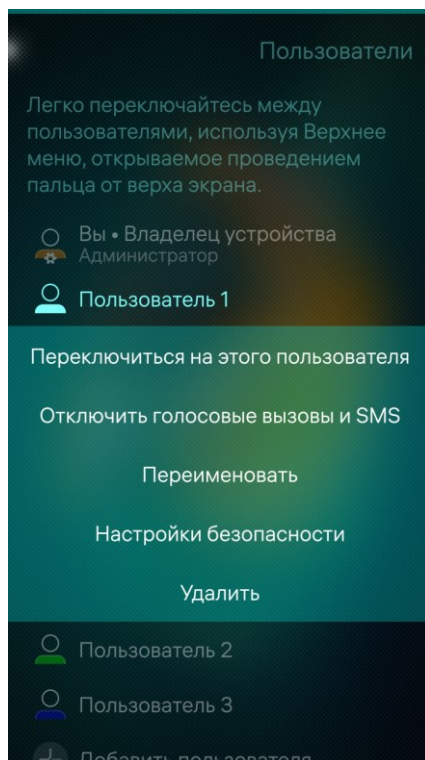


Рисунок 17

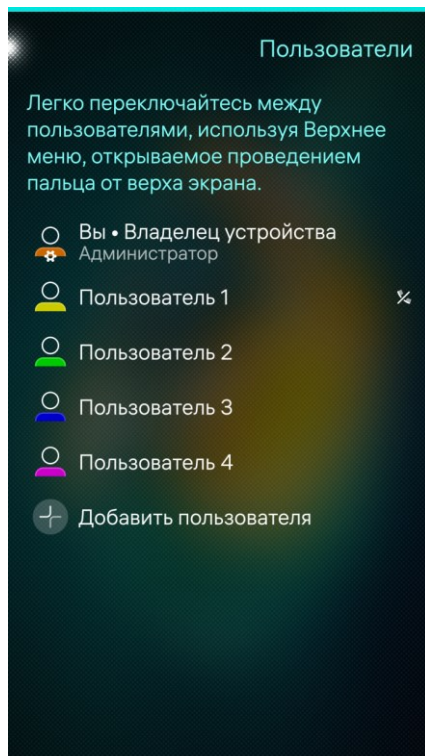



Рисунок 18


При вызове контекстного меню Администратору доступны следующие возможности (Рисунок 17):

- переключение на Пользователя;
- отключение голосовых вызовов и SMS;
- переименование Пользователя;
- настройки безопасности;
- удаление текущего Пользователя.

Для отключения голосовых вызовов и SMS Администратору необходимо в контекстном меню выбрать пункт «Отключить голосовые вызовы и SMS»

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

Для переименования Пользователя необходимо выполнить следующие действия:

- в контекстном меню выбрать пункт «Переименовать»;
- ввести новое имя (Рисунок 19);
- коснуться значка  для подтверждения действия.

Для удаления Пользователя из списка пользователей необходимо выполнить следующие действия:

- в контекстном меню выбрать пункт «Удалить» (Рисунок 20);
- подтвердить действие вводом текущего кода безопасности

Администратора.

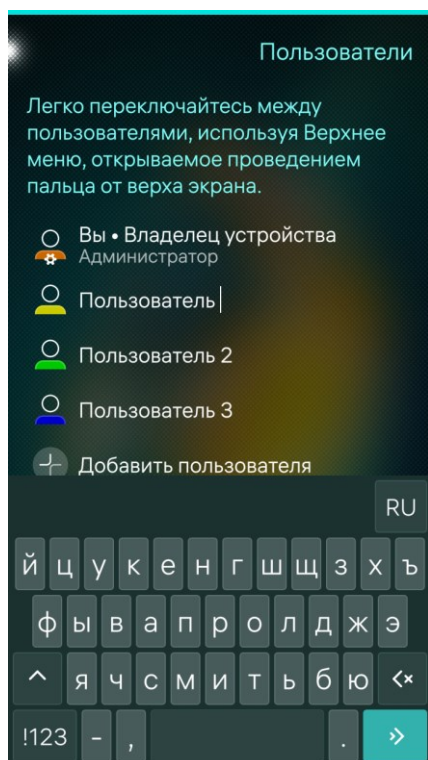


Рисунок 19

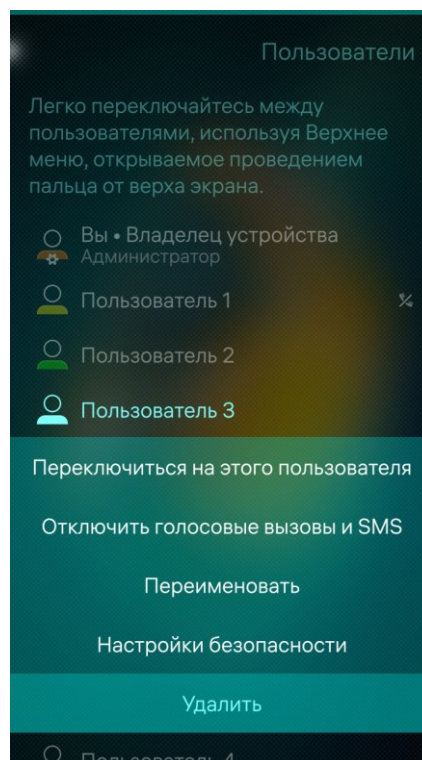


Рисунок 20

2.1.3. Переключение между режимами (ролями)

Для того, чтобы проверить, какая роль в настоящий момент активна необходимо выполнить следующие действия:

- коснуться пункта меню «Пользователи»  в меню системных настроек;

– отобразится страница со списком пользователей, созданных на МУ (Рисунок 21). Если текущая роль Администратор, то ОС Аврора находится в режиме администратора и на экране МУ отобразится: «Вы Владелец устройства» (Рисунок 21).

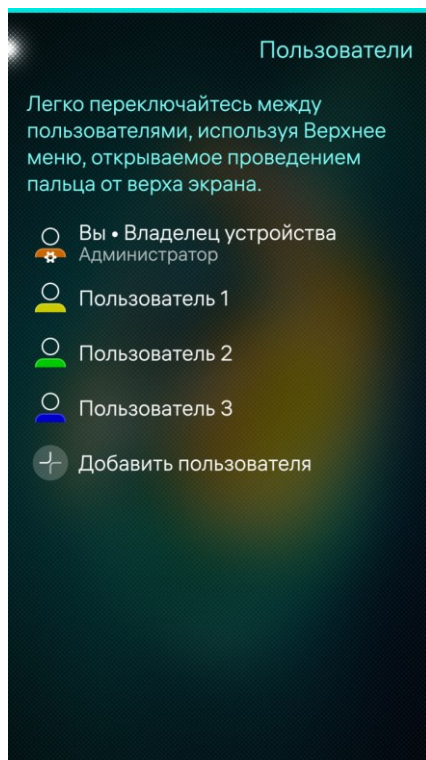


Рисунок 21

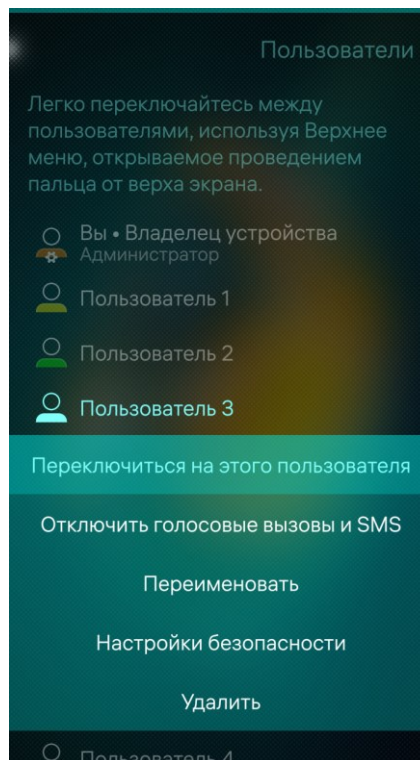


Рисунок 22

Для перехода в режим Пользователя необходимо выполнить следующие действия:

- выбрать одного из созданных пользователей;


В системе предусмотрено создание до 6 ролей Пользователя

– в контекстном меню коснуться пункта «Переключится на этого пользователя» (Рисунок 22);

– дождаться перезагрузки ОС Аврора и убедиться, что текущая роль Администратор сменилась на роль Пользователь.

Если текущая роль Пользователь, то ОС Аврора находится в режиме пользователя, и на экране МУ рядом с одним из Пользователей отобразится: «Вы [Имя пользователя]».

Для перехода в режим администратора необходимо выполнить следующие действия:

– в меню настроек системы коснуться пункта «Пользователи» . Отобразится страница «Пользователи» с представленным списком пользователей, созданных на МУ (см. Рисунок 21);

– из перечня пользователей коснуться строки с пометкой «Владелец устройства»;

– в контекстном меню коснуться пункта «Переключится на этого пользователя» (Рисунок 23);

– процесс переключения займет несколько секунд (Рисунок 24).

По окончании процесса переключения необходимо ввести код безопасности.

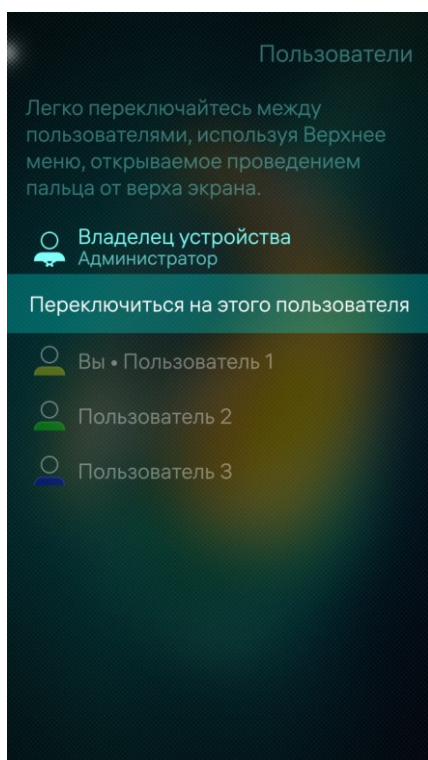


Рисунок 23

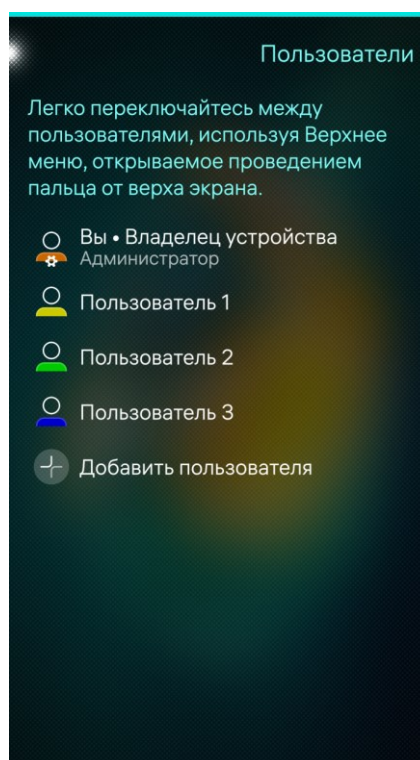


Рисунок 24

2.2. Настройки парольных политик

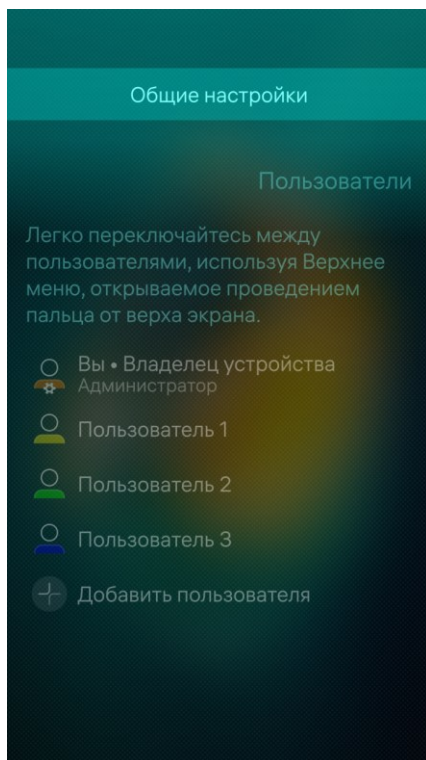



Рисунок 25

Для настройки парольных политик необходимо выполнить следующие действия:

- в меню настроек системы коснуться пункта «Пользователи» . Отобразится страница «Пользователи» с представленным списком пользователей, созданных на МУ;
- открыть меню действий;
- выбрать пункт «Общие настройки» (Рисунок 25). Отобразится страница «Парольная политика»;
- коснуться поля «Настройка» (Рисунок 26);

– на открывшейся странице «Настройки парольной политики» настроить необходимые параметры (Рисунок 27):

- уровень сложности пароля («Простой» или «Сложный»);
- длина пароля (от пяти до двенадцати символов);
- срок действия пароля («Неограничен» или от тридцати до ста восьмидесяти дней);
- отправка уведомления о количестве дней, по истечении которых необходимо сменить пароль («Никогда» или от одного до 10 дней).

При смене Администратором парольной политики, ее настройки будут применены ко всем пользователям МУ

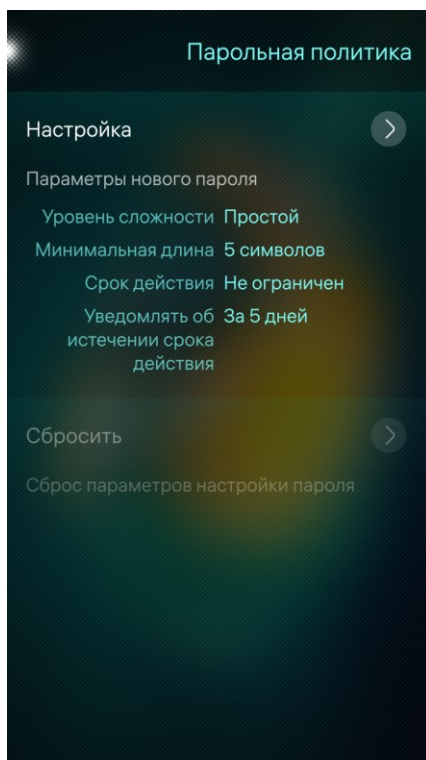


Рисунок 26

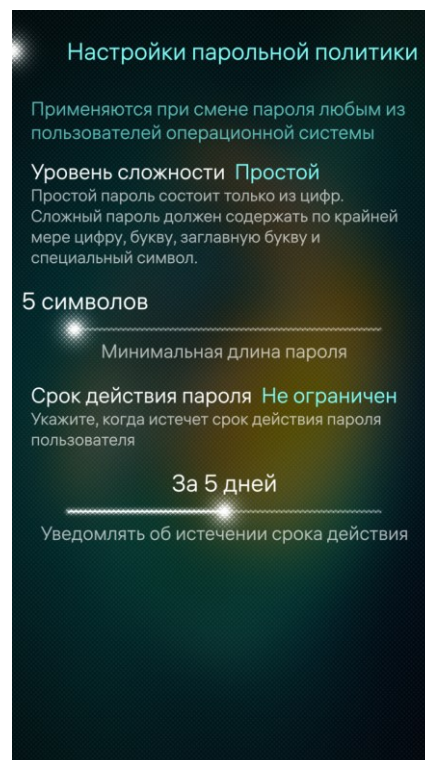


Рисунок 27

2.3. Настройки безопасности

Настройки безопасности применяются отдельно к каждому Пользователю

2.3.1. Политики безопасности

В ОС Аврора ролевое разграничение называется «Политики безопасности».

Описание управляемых политик безопасности приведено в Приложении 1


Ролевая политика разграничения доступа RBAC в ОС Аврора предназначена для разрешения или запрета доступа для тех или иных функций системы.


Настройка ролевой политики разграничения прав доступа доступна только Администратору

Политики безопасности применяется для всех ранее заведенных на МУ пользователей.

Администратор имеет возможность изменить настройку RBAC, при том, что Пользователь такой возможности не имеет

Для перехода к политикам безопасности необходимо выполнить следующие действия:


- открыть меню настроек безопасности касанием значка  на Экране приложений;


- в подразделе «Безопасность» коснуться пункта «Политики безопасности»  (Рисунок 28). Отобразится страница «Политики безопасности» (Рисунок 29);

- на открывшейся странице задать список функций МУ, которыми будет разрешено пользоваться при работе. Для включения политик безопасности необходимо коснуться переключателей справа, соответствующих требуемым политикам безопасности.

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

Для доступа к настройкам RBAC необходимо перейти к настройкам политики безопасности, выполнив следующие действия:



- открыть меню настроек безопасности касанием значка  на Экране приложений;

- в подразделе «Безопасность» коснуться пункта меню «Политики безопасности»  (Рисунок 28).

Для быстрого поиска политики безопасности требуется ввести первые буквы ее названия в поле «Поиск» (Рисунок 29).

Для блокирования/разблокировки той или иной политики безопасности необходимо коснуться соответствующих значков (Таблица 1) слева от выбранной политики.

Таблица 1

Значок	Описание
	Политика доступна (разблокирована)
	Политика недоступна (заблокирована)

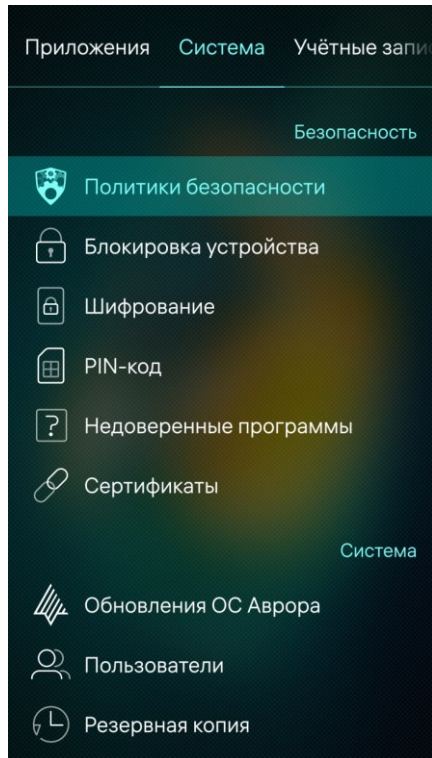


Рисунок 28

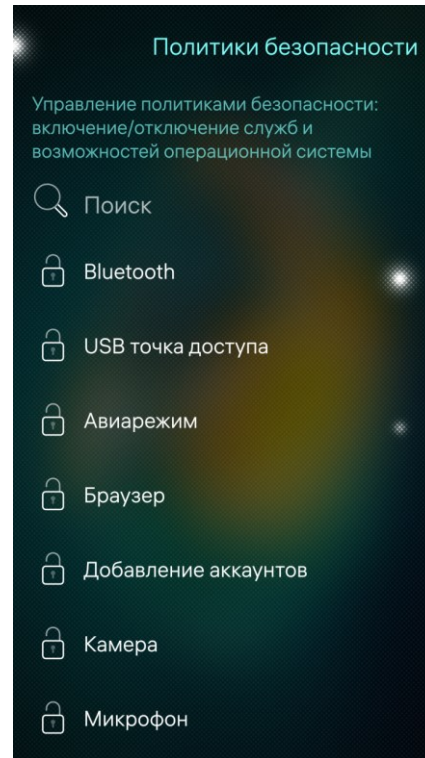


Рисунок 29

2.3.2. Аудит

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

Для сохранения всех событий в постоянную память МУ необходимо получить привилегии Администратора (п. 2.1.1), а после выполнить следующие действия:

– выполнить команду:

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

– установить параметры в следующие значения:

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

– затем необходимо перезагрузить МУ чтобы изменения вступили в силу.

Для выгрузки файла журнала необходимо выполнить команду:

```
journalctl -a > j.log
```

при этом необходимо создать файл лога, в котором будут находиться все события (–a = all), и который будет иметь название: j.log (при необходимости название файла можно изменить).

Для доступа и просмотра сообщений аудита администратору ОС Аврора доступны следующие инструменты:

- программа `journalctl`, имеющая интерфейс командной строки;
- программа `dmesg`, имеющая интерфейс командной строки;
- конфигурационный файл `/etc/omp/sdjd.conf`;
- МП «Журнал» (`/usr/bin/log-viewer`), имеющий графический

пользовательский интерфейс, где 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.

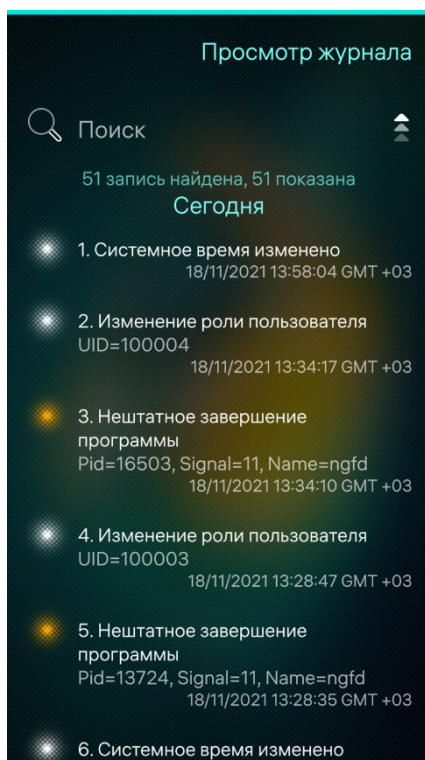



Рисунок 30

Подробное описание работы МП «Журнал» приведено в документе «Руководство пользователя»

Для просмотра отчетов необходимо запустить МП «Журнал», коснувшись значка  на Экране приложений.

Примеры сообщений, отображаемых в МП «Журнал», представлены на рисунке (Рисунок 30).

2.3.3. Шифрование

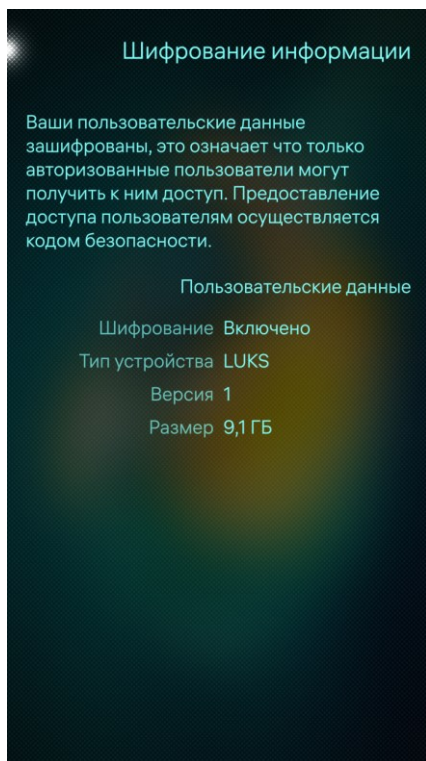



Рисунок 31

Для просмотра зашифрованных пользовательских данных (Рисунок 31) необходимо выполнить следующие действия:

- коснуться значка  на Экране приложений.

Отобразится меню настроек системы;

- в подразделе «Безопасность» коснуться пункта меню «Шифрование» . Отобразится страница «Шифрование информации» с пользовательскими данными.

2.3.4. Недоверенные программы

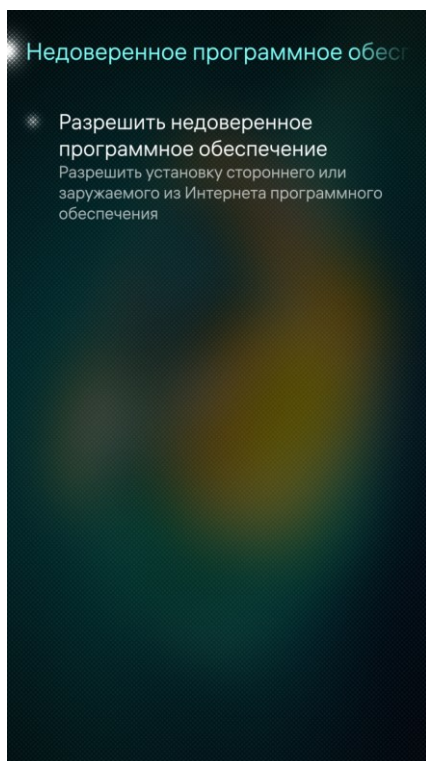




Рисунок 32

Для того, чтобы разрешить установку стороннего ПО, необходимо выполнить следующие действия:

- коснуться значка  на Экране приложений. Отобразится меню настроек системы;

- в подразделе «Безопасность» коснуться пункта меню «Недоверенные программы» . Отобразится страница «Недоверенное программное обеспечение» (Рисунок 32);

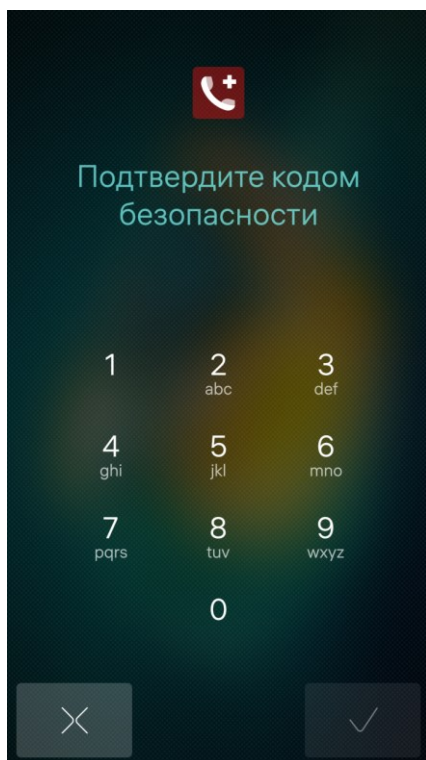


Рисунок 33

Для отключения заданной настройки необходимо на странице «Недоверенное программное обеспечение» деактивировать переключатель и подтвердить данное действие кодом безопасности (см. Рисунок 33).

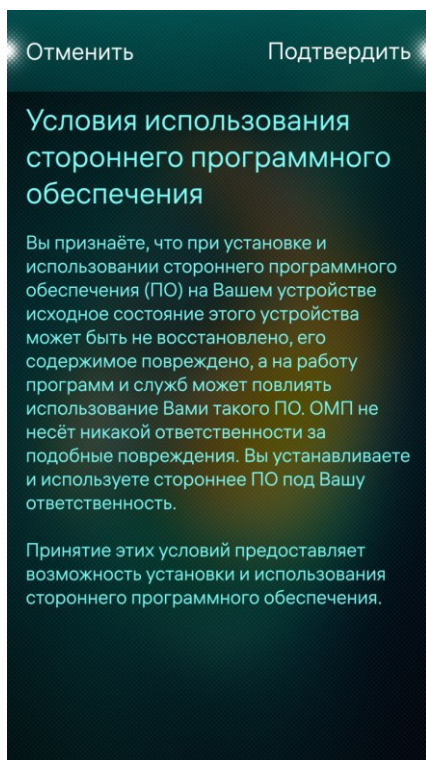


Рисунок 34

– коснуться переключателя «Разрешить недоверенное программное обеспечение» для разрешения установки недоверенного ПО;

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

– подтвердить действие вводом текущего кода безопасности (Рисунок 33);

– для подтверждения принятия условий использования стороннего ПО коснуться кнопки «Подтвердить» (Рисунок 34).

Для запрета установки недоверенного ПО необходимо выполнить аналогичные действия.

2.4. Управление мобильными приложениями

Предустановленные МП встроенные в установленную на МУ ОС Аврора являются базовыми МП. Однако, Пользователь имеет возможность дополнительно устанавливать на МУ иные МП и управлять ими.

Подробнее описание работы предустановленных МП приведено в документе «Руководство пользователя»

Управление МП может осуществляться администратором либо локально вручную, либо удаленно с использованием ППО.

Для получения информации по управлению МП посредством ППО следует обратиться к соответствующей документации на ППО, расположенной на ресурсе: <https://auroraos.ru/documentation/>

Для управления МП локально вручную необходимо получить привилегии Администратора (п. 2.1.1). Управление МП осуществляется в МП «Terminal» с помощью пакетного менеджера RPM, посредством выполнения следующих команд:

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

– для установки скачанного RPM-пакета:

```
#rpm -ihv имя_пакета
```

– для удаления МП:

```
#rpm -e имя_пакета
```

– для просмотра перечня установленных пакетов:

```
#rpm -qa
```

Подробнее с возможностями пакетного менеджера RPM можно ознакомиться, выполнив команду:

```
#rpm -help
```

Для получения информации о возникающих ошибках и нестандартных ситуациях в процессе управления МП необходимо настроить журналирование (п. 2.3.2) и ознакомиться с информацией, представленной в МП «Журнал»

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

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

Таблица 2

Термин/ Сокращение	Расшифровка
Администратор	Пользователь, уполномоченный выполнять некоторые действия по администрированию (имеющий административные полномочия) в соответствии с установленной ролью и требуемыми привилегиями на выполнение этих действий
Атмосфера (тема МУ)	Совокупность визуального оформления всех экранов и цветовое оформление интерфейса. Служит для придания индивидуальности и стиля МУ
МП	Мобильное приложение
МУ	Мобильное устройство
ОС	Операционная система
Пользователь	Лицо или организация, которое использует действующую систему для выполнения конкретной функции
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение «Аврора Центр»
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

Термин/ Сокращение	Расшифровка
MTP	Media Transfer Protocol – основанный на PTP аппаратно-независимый протокол, разработанный компанией Microsoft для подключения цифровых плееров к компьютеру
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
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
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

ПРИЛОЖЕНИЕ 1

Наименование и описание управляемых политик безопасности

Наименование и описание управляемых политик безопасности указано в таблице (Таблица 1.1).

Таблица 1.1

№	Название политики	Описание политики	Ключ	Политики, включенные по умолчанию	Примечание
1.	Камера	Возможность использования камеры	CameraEnabled	+	Может быть настроена с помощью GUI
2.	Bluetooth	Возможность использования интерфейса Bluetooth®	BluetoothEnabled	-	Может быть настроена с помощью GUI
3.	Настройки геолокации	Возможность использования служб местоположения	LocationSettingsEnabled	+	Может быть настроена с помощью GUI
4.	Настройки WLAN	Возможность использования сети WLAN	WlanToggleEnabled	+	Может быть настроена с помощью GUI
5.	Сброс к заводским настройкам	Возможность выполнения сброса ОС Аврора к заводским настройкам	DeviceResetEnabled	+	Может быть настроена с помощью GUI
6.	Снимок экрана	Возможность создавать снимки экрана	ScreenshotEnabled	+	Может быть настроена с помощью GUI

№	Название политики	Описание политики	Ключ	Политики, включенные по умолчанию	Примечание
7.	USB точка доступа	Возможность получения выбора действий при подключении к ЭВМ	UsbConnectionSharingEnabled	+	Может быть настроена с помощью GUI
8.	Передача файлов на ЭВМ (MTP)	Возможность передачи файлов на ЭВМ при USB-соединении с ним по протоколу MTP	UsbMtpEnabled	-	Может быть настроена с помощью GUI
9.		Возможность использования Android Debug Bridge	UsbAdbEnabled	+	Может быть настроена только с помощью policy.conf
10.		Возможность настройки пользователем мобильных точек доступа	MobileDataAccessPointSettingsEnabled	+	Может быть настроена только с помощью policy.conf
11.	Настройка даты и времени	Возможность использования (изменять) настроек времени и даты	DateTimeSettingsEnabled	+	Может быть настроена с помощью GUI
12.	Микрофон	Возможность использования микрофона	MicrophoneEnabled	+	Может быть настроена с помощью GUI
13.	Авиарежим	Возможность использования режима полета	FlightModeToggleEnabled	+	Может с помощью настроен через GUI
14.	Настройки прокси	Возможность изменения конфигурации прокси для каждого сетевого сервиса пользователем.	NetworkProxySettingsEnabled	-	Может быть настроена с помощью GUI

№	Название политики	Описание политики	Ключ	Политики, включенные по умолчанию	Примечание
15.	Настройки точки доступа Wi-Fi	Возможность использования МУ в качестве беспроводной точки доступа	InternetSharingEnabled	+	Может быть настроена с помощью GUI
16.	Настройки мобильной сети	Возможность настройки SIM-карт в меню настроек «Мобильная сеть»	MobileNetworkSettingsEnabled	+	Может быть настроена с помощью GUI
17.	Браузер		BrowserEnabled	+	Может быть настроена с помощью GUI
18.	Добавление аккаунтов		AccountCreationEnabled	+	Может быть настроена с помощью GUI
19.	Настройка VPN		VpnConnectionSettingsEnabled	+	Может быть настроена с помощью GUI
20.	Настройка VPN-соединения		VpnConfigurationSettingsEnabled	+	Может быть настроена с помощью GUI
21.	-	Возможность работы пользователя с обновлением ОС	OsUpdatesEnabled	+	Может быть настроена только с помощью policy.conf
22.	-	Возможность пользователя принимать решения о загрузке сторонних пакетов	SideLoadingSettingsEnabled	-	Может быть настроена только с помощью policy.conf
23.	-	Возможность выбора пользователем режима разработчика	DeveloperModeSettingsEnabled	+	Может быть настроена только с помощью policy.conf

№	Название политики	Описание политики	Ключ	Политики, включенные по умолчанию	Примечание
24.	-	Возможность установки пользователем приложений	ApplicationInstallationEnabled	-	Может быть настроена только с помощью policy.conf
25.	-	Возможность использования режима USB Mass Storage	UsbMassStorageEnabled	+	Может быть настроена только с помощью policy.conf
26.	-	Возможность работы пользователя со статистикой интернет данных	NetworkDataCounterSettingsEnabled	+	Может быть настроена только с помощью policy.conf
27.	-	Возможность работы пользователя со статистикой звонков	CallStatisticsSettingsEnabled	+	Может быть настроена только с помощью policy.conf
28.	-	Возможность изменения типа технологии мобильной передачи данных пользователем	CellularTechnologySettingsEnabled	+	Может быть настроена только с помощью policy.conf

